Science and Technology Facilities Council

IRIS Security

IRIS TWG, 21st April

David Crooks UKRI-STFC
david.crooks@stfc.ac.uk

WISE COMMUNITY

IRIS Trust Framework status

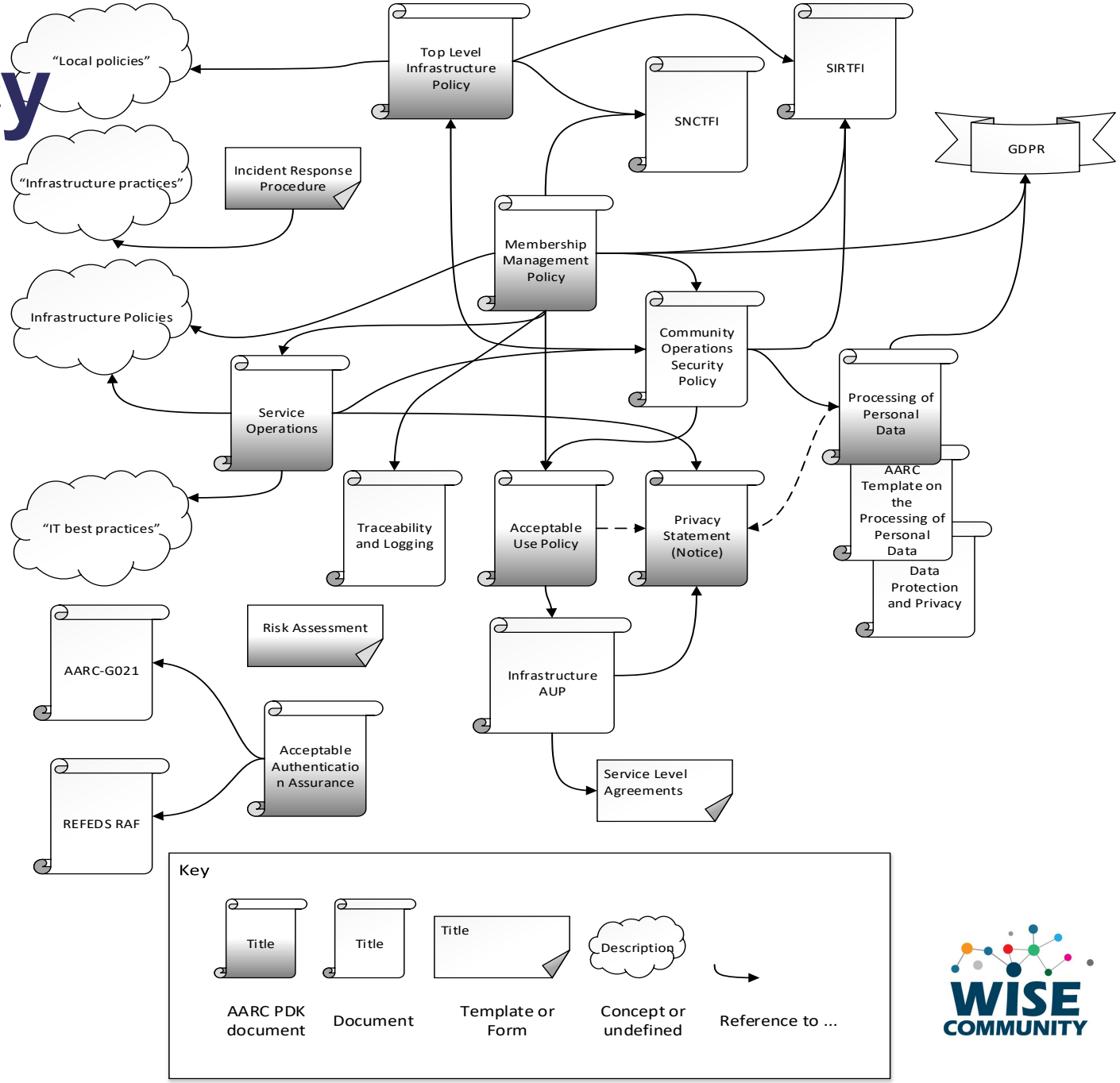
- Draft AUP, Privacy Policy have been discussed at TWG
  - Interim versions in use by IRIS-IAM
- Top Level policy discussed at DB
  - Form small “Policy Group” to give further feedback and report back
- Incident Response procedure in draft
- First meetings of expanded Security Team have taken place
  - Jon Wakelin at Leicester on behalf of DiRAC

AARC Policy Development Kit

Document	Who should complete the template?	Audience	Description
Top Level Infrastructure Policy	Infrastructure Management	All Infrastructure Participants (abides by)	This policy template defines the roles of actors in the Research Infrastructure and binds the policy set together
Incident Response Procedure	Infrastructure Management & Security Contact	Infrastructure Security Contact, Services (abides by)	This template procedure provides a step-by-step breakdown of actions to take following a security incident.
Membership Management Policy	Infrastructure Management	Research Community (abides by)	This policy template defines how Research Communities should manage their members, including registration and expiration.
Acceptable Authentication Assurance	Infrastructure Management	Research Community, Services (abide by)	This is a placeholder for the Infrastructure to determine rules for the acceptable assurance profiles of user credentials.
Risk Assessment	Infrastructure Management, Services & Security Contact	Infrastructure Management (completes)	This table can be used as a starting point for identifying whether a full Data Protection Impact Assessment is required.
Policy on the Processing of Personal Data	Infrastructure Management & Data Protection Contact	Research Community, Services (abide by)	This document defines the obligations on Infrastructure Participants when processing personal data.
Privacy Policy	Infrastructure Management (for general policy) & Services (for service specific policies)	Users (view)	This can be used to document the data collected and processed by the Infrastructure and its participants. Each service in the infrastructure, as well as the infrastructure itself, should complete the template.
Service Operations Security Policy	Infrastructure Management	Services (abide by)	This policy defines requirements for running a service within the Infrastructure.
Acceptable Use Policy	Infrastructure Management (for baseline) & Research Communities (for community specific restrictions)	Users (abide by)	This is a template for the acceptable use policy that users must accept to use the Research Infrastructure. It should be augmented by the Research Community.

IRIS Security: Policy

- Policy map derived from AARC PDK and others in first year of IRIS Trust Framework
- Shows there are many policies, groups, procedures, ‘standards’, notices, agreements, regulations and fuzzy objects in this space.
- Shows relationships between different policy items
- Can be used to inform most useful next steps



Science and Technology Facilities Council

WISE COMMUNITY

IRIS Security: Policy

- Both from considering this policy map and from IRIS-IAM developments, identify two key next steps

- Membership Management
- Service Operations Security Policy

IRIS Security: Policy

- (Community) Membership Management is a vital area, particularly following the continued deployment of IRIS-IAM
  - This has also been identified as a particular area where work for IRIS can benefit the wider development of these policies
  - Work will continue as part of the WISE (WISE Information Security for Collaborating eInfrastructures) community
  - IRIS feedback really important to this!
- Coupled to this is a Service Operations Security Policy
  - Security baseline for IRIS resource providers
  - As always, acting in concert with existing local policy

Science and Technology Facilities Council

WISE COMMUNITY

IRIS Security

- From a general security standpoint, following from enhancement of Security Team and drafting of Incident Response Procedure, identify two key additional areas:

- Communications Challenge
- Security Training Materials

IRIS Security: Communications Challenge

- Shortly begin gathering/ensuring security contacts for IRIS resource providers where we don't already have them

- Following this, run a brief Communications Challenge to make sure that we can contact sites rapidly in case of an incident

- Follow up accordingly

Science and Technology Facilities Council

WISE COMMUNITY

IRIS Security: Security Training Materials

- Part of a wider look at security training materials for system administrators
  - Share best practice for IRIS resource providers
  - Help the Security Team in understanding the IRIS security environment

- Alongside the digital asset, arrange a training event later in the year
  - Follow previous events for GridPP admins but extend to IRIS
  - Currently considering how best to do this via Zoom

Science and Technology Facilities Council

Questions?

Facebook: Science and Technology Facilities Council

Twitter:@STFC_matters

YouTube: Science and Technology Facilities Council

WISE COMMUNITY