Science and
Technology
Facilities Council

IRIS Trust Framework

WISE virtual meeting, April 2020

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

WISE
COMMUNITY

IRIS Background

- e**I**nfrastructure for **R**esearch and **I**nnovation for **S**TFC

- Collaboration of **Science Activities** and **Provider Entities**
  - Driven by the physics communities supported by UKRI-STFC

- Does not run infrastructure **directly**
  - Commissions deployment of resources available to all of its science activities

IRIS Background

Science Activities

- ALMA
- ATLAS
- CCFE
- CLF
- CMS
- CTA
- DLS
- DUNE
- eMERLIN
- EUCLID
- GAIA
- ISIS
- LHCb
- LIGO
- LSST
- Lux-Zeplin
- SKA

Provider Entities

- The Ada Lovelace Centre (ALC)
- DiRAC [HPC]
- GridPP [HTC]
- The Hartree Centre
- STFC Scientific Computing Department
- The DLS Computing Department
- CCFE computing

Requirements for trust framework

- IRIS contains a range of resource providers with existing policy frameworks
  - Some providers are already part of wider federated world (GridPP/EGI/WLCG)

- However: it does represent a new community in its own right
  - Exists within a distributed, federated infrastructure landscape

- Need policies to allow interoperation between resource providers, services and user groups
  - Coexisting with existing local policy

IRIS Trust Framework

- The IRIS Trust Framework is intended to build the security policy required by IRIS
  - Start with foundational and user-facing policies

- Address Incident Response for IRIS

- Parallel to development of Identity and Access Management for IRIS through IRIS-IAM
  - Deployment of INDIGO IAM Identity Proxy
  - In operation, part of UK AMF
  - Follows AARC Blueprint Architecture

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.

AARC Policy Development Kit

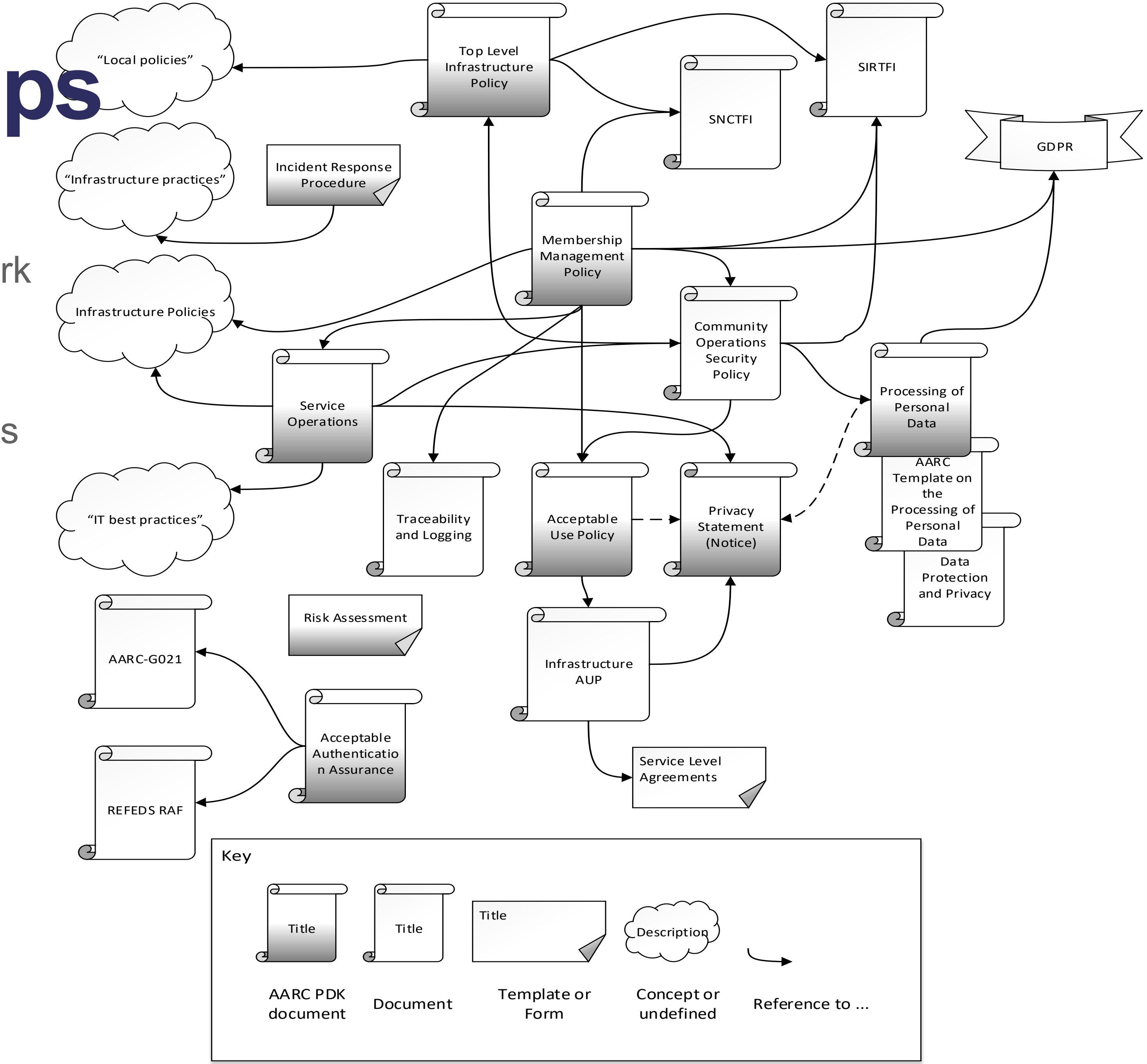
Document	Who should complete the template?	Audience	Description
Top Level Infrastructure Policy	**Infrastructure Management**	**All Infrastructure Participants (abides by)**	**This policy template defines the roles of actors in the Research Infrastructure and binds the policy set together**
Incident 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.**

Current status

- Draft AUP, Privacy Policy and Top Level policy out for comment by IRIS
- Feedback suggested a rebalancing of the Top Level policy to make roles and responsibilities clear in one document
- We are feeding back our experiences of using the AARC PDK for a new Infrastructure and hope this will be useful to the SCI-WG
- Process has been very useful in exploring and clarifying the structures within IRIS, as well as establishing the workflow for future policies
- Incident Response underway through expansion of GridPP Security Team

Policy Relationships

- 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



“Local policies”

Top Level Infrastructure Policy

SNCTFI

SIRTFI

GDPR

“Infrastructure practices”

Incident Response Procedure

Membership Management Policy

Infrastructure Policies

Community Operations Security Policy

Service Operations

Processing of Personal Data

AARC Template on the Processing of Personal Data

Data Protection and Privacy

“IT best practices”

Traceability and Logging

Acceptable Use Policy

Privacy Statement (Notice)

AARC-G021

Risk Assessment

Infrastructure AUP

Acceptable Authenticatio n Assurance

REFEDS RAF

Service Level Agreements

Key

Title — AARC PDK document

Title — Document

Title — Template or Form

Description — Concept or undefined

Reference to ...

Science and
Technology
Facilities Council

Thank you

Facebook: Science and Technology Facilities Council

Twitter:@STFC_matters

YouTube: Science and Technology Facilities Council