Science and Technology Facilities Council

Developing a Trust and Security Framework for IRIS

EGI Conference 2020

David Crooks UKRI-STFC

iris

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 4x4 is a capital project coordinated by IRIS
  - £4 million per year for 4 years
  - No money for operations
  - Can issue grants for equipment and grants to make things
    - Such as the trust framework

UKRI Science and Technology Facilities Council

iris

WISE COMMUNITY

IRIS Partners

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

UKRI Science and Technology Facilities Council

iris

WISE COMMUNITY

IRIS Background

- Need some common elements to support these communities working together:
  - Policy and Trust Framework
  - Identity Management
  - Resource Accounting
  - Monitoring

Science and Technology Facilities Council

iris

WISE COMMUNITY

IRIS Background

- Need some common elements to support these communities working together:
  - **Policy and Trust Framework**
  - Identity Management
  - Resource Accounting
  - Monitoring

Science and Technology Facilities Council

iris

WISE COMMUNITY

Context and requirements

- IRIS contains a range of resource providers with existing policy frameworks
  - Need to develop a framework that sits alongside these and enables secure distributed operations
- Some providers are already connected within the wider federated world
  - Particularly GridPP/WLCG
- However: it does represent a new community in its own right
  - And exists within a distributed, federated infrastructure landscape
- Establish the necessary policies to allow interoperation between resource providers, services and user groups
  - And relationships to existing policy

Challenges

- IRIS is a relatively new collaboration but with well established participants
  - What implications does this have?
- Well established policies in place at individual institutions
  - New operational workflows being developed
- Bootstrap security policy set
  - Challenge of deciding best order of work while governance structures being established
  - Need to show end users AUP/Privacy Notice so these are a priority

IRIS Trust and Security Framework

- The IRIS Trust Framework is intended to build the security policy required by IRIS
  - Start with foundational and user-facing policies
  - Roadmap for the future
- Security Incident Response
  - Clear roles and basic policy framework

Process

- Build on extensive existing experience developing policy within existing communities
  - GridPP/WLCG, UK Access Management Federation, EGI, …
  - Extend to new resource providers and user communities
- Identify key stakeholders and develop trust relationships
- Parallel work in the operation of an IRIS-IAM Identity Proxy for IRIS
  - See talk tomorrow

Roadmap

- AARC Policy Development Kit
  - Authentication and Authorisation for Research Collaboration
  - Recently completed EU projects
- 9 documents aimed at best practice bootstrap for infrastructures & communities deploying the AARC Blueprint Architecture
  - Federated IDPs with services/resources ‘behind’ an AAI Proxy
- Policies intended to co-exist with local policies where applicable

WISE

- Wise Information Security for Collaborating e-Infrastructures
  - https://wise-community.org/about-wise/
- Global collaborative community of security experts
- IRIS policy work takes place under aegis of WISE
  - Benefit to IRIS of considerable experience
  - Benefit to WISE and wider community of new requirements and context

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.**

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.**

Draft IRIS AUP

- Use of a common, baseline AUP
  - Based on the WISE Baseline AUP template
    - Promotes trust in users' behaviour across infrastructures
    - Reduce need to agree to multiple different AUPs
  - Allows for consistent presentation of necessary Privacy Notices
  - Allows for augmentation with additional local / community requirements
    - 10 immutable clauses + scope to add specific additional ones
  - Easier bootstrapping – don't reinvent the wheel

Draft IRIS Privacy Notice

- Presented to user at time of registration alongside AUP
- Assumes GDPR legal basis of “legitimate interest” for processing
  - i.e. not consent – due to imbalance of power (employer – employee)
- To be taken from (final) deployment context
  - Personal data gathered / processed
  - Data retention period

Draft IRIS Infrastructure Security Policy

- Provides high-level framework for other subordinate policies
  - Approved/adopted by infrastructure management body to give
  - **"…authority for actions which may be carried out by designated individuals and organisations and places responsibilities on all participants."**
  - Roles and Responsibilities of Management
  - Roles and Responsibilities of Security Contact
  - Physical and Network Security
    - Delegated to local/service policies, but scoped.
  - Exceptions to Compliance and Sanctions

Policy lifecycle

- Process has lead to some interesting questions?
- What policies do we need to start with?
  - Defining policies when the infrastructure topology/governance is being established
- What does it mean to be an “IRIS User”?
  - Mixed authentication workflows

Status and future plans

- Use Infrastructure Policy as foundation
  - Proceeding through approval process now
- Obvious outcome: most progress made when you get feedback
  - Newly expressed concerns are good
  - When these can then be addressed and acted upon
- Senior infrastructure management backing is essential
  - In addition to user communities expressing a need for rules of engagement, supporting the policy development effort.
- Establishing policy can lead to introspection of the infrastructure organisation

Status and future plans

- Working AUP and Privacy Notice in place for IRIS-IAM Identity Proxy
  - See talk tomorrow
- IRIS work contributes directly back to development of the PDK
- Leading participant in ongoing development of PDK under WISE for
  - Infrastructure Policy
  - Service Operations Policy
  - Community Policy

Science and Technology Facilities Council

Thank you

Facebook: Science and Technology Facilities Council

Twitter:@STFC_matters

YouTube: Science and Technology Facilities Council