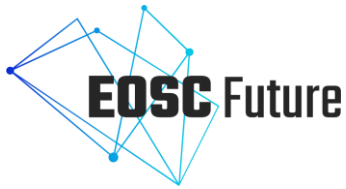
Authentication and Authorisation for Research and Collaboration



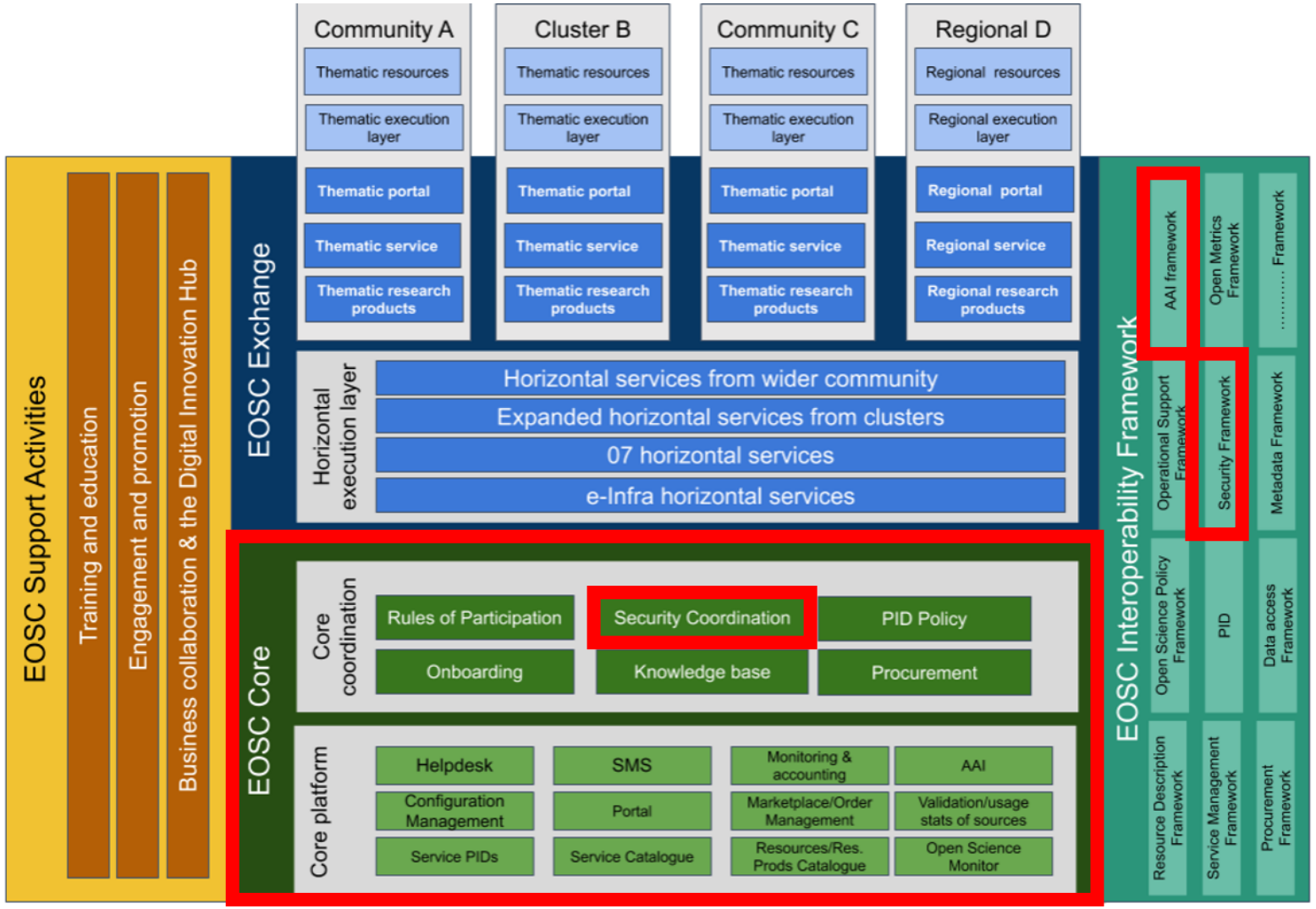
The Security Baseline for EOSC and beyond

‘for loosely connected services and infrastructure’

David Groep
EOSC Security Operations and Policy lead, AARC Policy Area coordinator
Nikhef Physics Data Processing (PDP) programme

WISE Community Autumn 2021 meeting
2021.10.26

EOSC structure – security coordination and the AAI

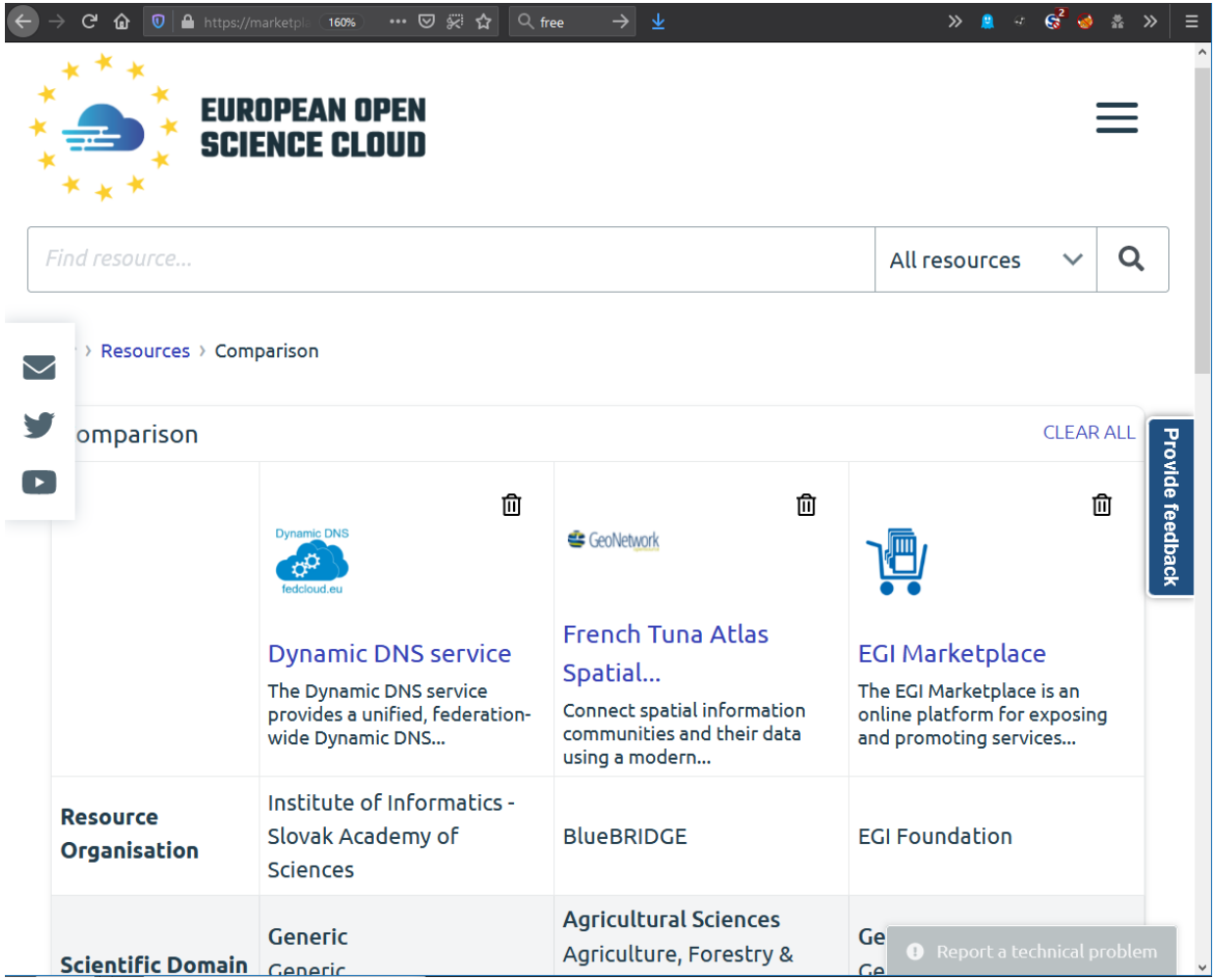


The diverse ecosystem compared

- **EOSC Core**
  set of internal services which allow EOSC to operate

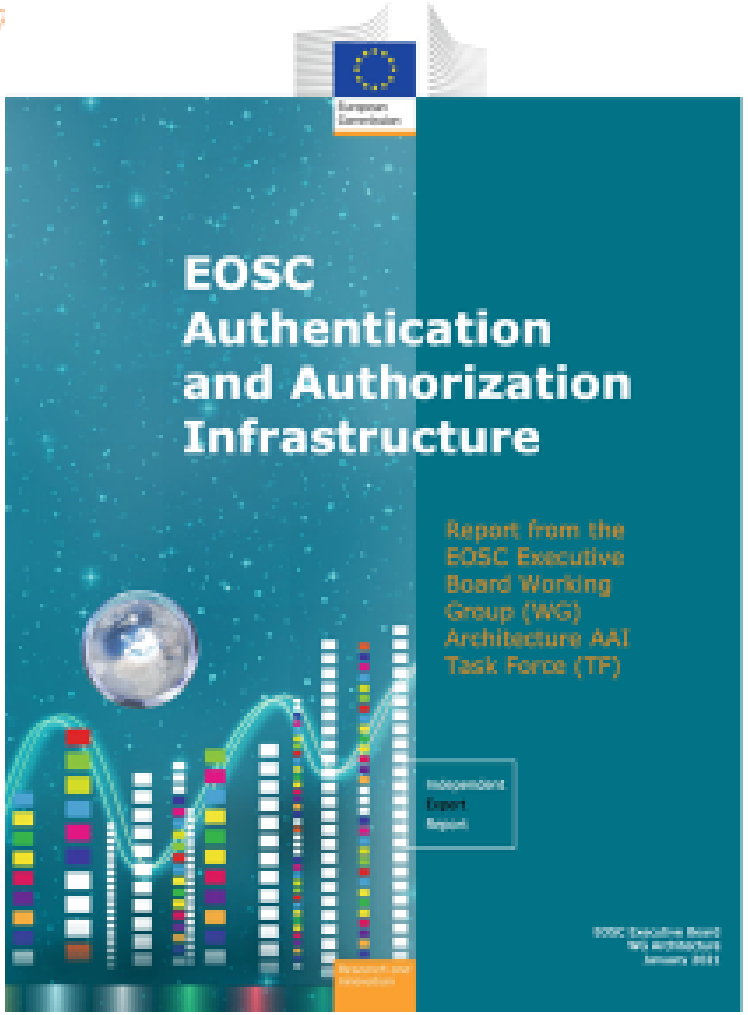
- **EOSC Exchange**
  set of federation services, resources registered into the EOSC
  to serve needs of research communities and widening to public and private sector

- **EOSC Interoperability Framework**
  standards and guidelines to support the interoperability and composability of resources

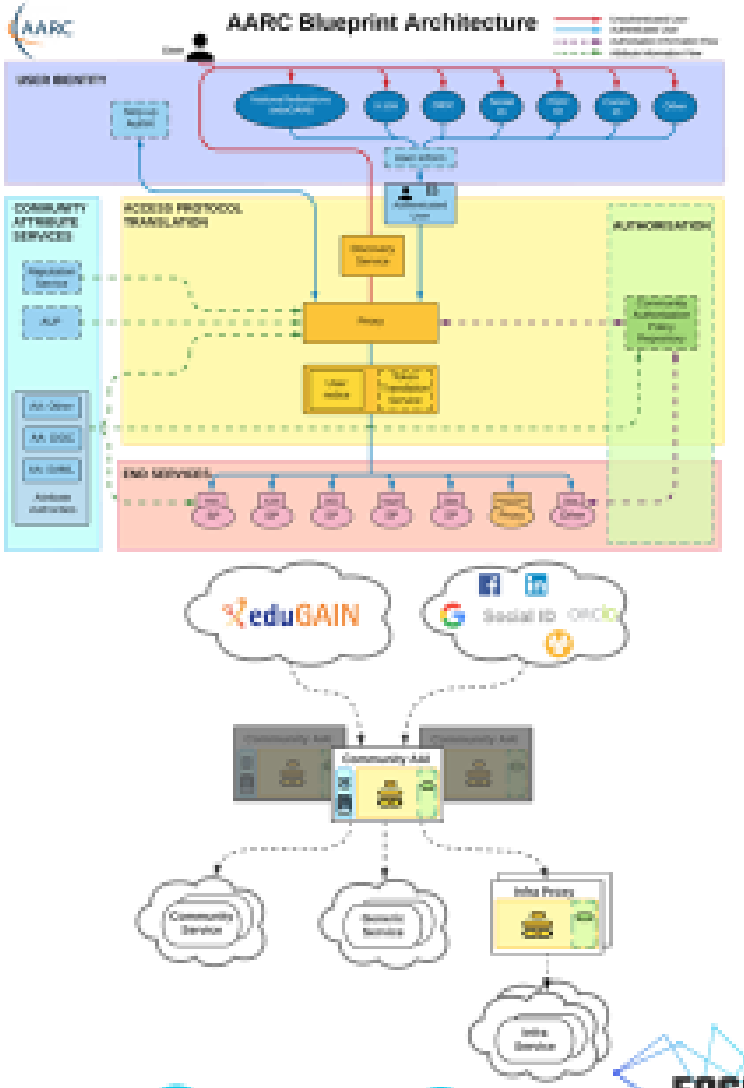


comparing services in the Exchange on the EOSC Portal – from https://eosc-portal.eu/

EOSC Authentication and Authorization Infrastructure



https://op.europa.eu/s/sWqj



slide: Christos Kanellopoulos, GEANT, for EOSC Future WP7.3

The EOSC Ecosystem – a loosely coupled federation of users and services

EOSC Core services

- drives the portal
- strongly coordinated
- ITSM processes in place
- underpin other services
- key to on-boarding, AAI, monitoring, accounting …

EOSC AAI federation

- services from the wider community
- horizontal and thematic
- many providers
- composed with other services
- use the EOSC AAI model for authentication, authorization, and federated identity

Exchange Listed services

- services from the wider community
- have no need for a technical AAI connection to the EOSC federation
- still are highly valuable services to the EOSC
- composed with other services
- merit security coverage

Security guidance & control points that apply to each category are - and should be - different

AARC Policy Development Kit – service (infrastructure)-centric policies

Document	Who should complete the template?	Audience	Description	Link
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	Google Doc
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.	Google Doc
Membership Management Policy	Infrastructure Management	Research Community (abides by)	This policy template defines how Research Communities should manage their members, including registration and expiration.	Goo Doc
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.	Goo Doc
isk	Infrastructure ement, Services & Contact	Infrastructure Management (completes)	This table can be used as a starting point for identifying whether a full Data Protection Impact Assessment is required.	Goo Doc
	ructure gement & Data ction Contact	Research Community, Services (abide by)	This document defines the obligations on Infrastructure Participants when processing personal data.	Goo Doc
	rastructure anagement (for general olicy) & Services (for ervice 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.	Goo Doc
Service Operations Security Policy	Infrastructure Management	Services (abide by)	This policy defines requirements for running a service within the Infrastructure.	Goo Doc
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.	Google Doc

Showing 1 to 9 of 9 entries Previous Next

		Management	Infrastructure Security Contact	User Community Management	Service Management	User
Top Level	Infrastructure Policy	Defines & Abides by	Abides by	Abides by	Abides by	Abides by
Data Protection	Privacy Statement	Defines			Defines	Views
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	

Guidance for Infrastructure Management and Service Contacts

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
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.
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.
Service Operations Security Policy	Infrastructure Management	Services (abide by)	This policy defines requirements for running a service within the Infrastructure.
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.

From an infrastructure to an ecosystem view

AARC ‘rev 1’ PDK version of “Service Operations” is purposefully specific

- includes ‘service-internal’ operations and software
- embedded in the PDK document suite:
  does not work well as a ‘stand-alone’ document
- has built-in assumption of coherent and coordinated single infrastructure

c. You shall use logged information, including personal data, only for administrative, operational, accounting, monitoring and security purposes. You shall apply due diligence in maintaining the confidentiality of logged information.

6. Provisioning of Services is at your own risk. Any software provided by the Infrastructure is provided <on an as-is basis | in accordance with service level agreements>, and subject to its own license conditions. There is no guarantee that any procedure applied by the Infrastructure is correct or sufficient for any particular purpose. The Infrastructure and other Participants acting as service hosting providers are not liable for any loss or damage in connection with your participation in the IT Infrastructure.
7. You may control access to your Service for administrative, operational and security purposes and shall inform the affected users where appropriate
8. Your Service’s connection to the Infrastructure may be controlled for administrative, operational and security purposes if you fail to comply with these conditions

Upon retirement of a service, the obligations specified in clauses 1, 2, 5 and 6 shall not lapse for

“Service Operations” developments

Evolved by UK-IRIS addressing many of these concerns

- can stand alone as policy guidance
- better implementable by adding references and notes (‘best practice’, or an ‘FAQ’)

Each Service Provider must

By running a Service, you agree to the conditions laid down in this document and other referenced documents, which may be subject to revision.

~~1. You shall comply with all relevant Infrastructure Policies [R1]~~

1. collaborate with others in the reporting and resolution of security events
incidents arising from their Service’s participation in the Infrastructure and thos
affecting the Infrastructure as a whole [R3][R4].

2. You shall provide and maintain accurate contact information, including at least one Security Contact who shall support Sirtfi [R2] on behalf of the service.

2. ensure that their Service operates in a manner which is not detrimental to t
Infrastructure nor to any of its Participants.

3. ~~You are held responsible for the safe and secure operation of the Service. Any information you provide regarding the suitability and properties of the Service should be accurate and maintained.~~ The Service shall not be detrimental to the Infrastructure nor to any of its Participants.

References and Notes

R1. Many of the requirements in this document derive from the WISE Community “Security for Collaborating Infrastructures Trust Framework” document, available here - https://wise community.org/sci/.

R2. IRIS Security Policies - https://www.iris.ac.uk/security/.

R3. Service Providers should support REFEDS SIRTFI - Security Incident Response Trust Framework for Federated Identity - https://refeds.org/sirtfi, which includes the requirement to maintain contact information for a security response capability (Normative Assertions on Incident Response - SIRTFI v1.0 Section 2.3).

R4. Alongside following site-local mandated policy and procedure requirements, efficient, collaborative incident response relies on participants agreeing on an incident response procedure before it is needed. Example procedure here - https://www.iris.ac.uk/security/, based on information from EGI (https://csirt.egi.eu/activities/).

R5. TrustedCI, The NSF Cybersecurity Centre of Excellence, provides a wide variety of security related resource material applicable to research environments - https://www.trustedci.org/resources, as well as more targeted information in the Resources section, such as “Security Best Practices for Academic Cloud Service Providers” - https://www.trustedci.org/cloud-service-provider-security-best-practices

thanks to Ian Neilson, David Crooks, Dave Kelsey, et al.

“Service Operations” developments

In the EOSC ecosystem, more of the original assumptions no longer hold

- services provided are less coherent, and much more autonomous then every before
- need to accommodate providers with varying maturity levels - and different intentions!

thanks to Ian Neilson, David Crooks, Dave Kelsey, et al.

Towards a Baseline instead of a single policy

Not all services are created equal

- EOSC primarily about user experience & research success: security there to support this goal
- Services are composable – and thus interdependent
- Premise: *do no harm*!

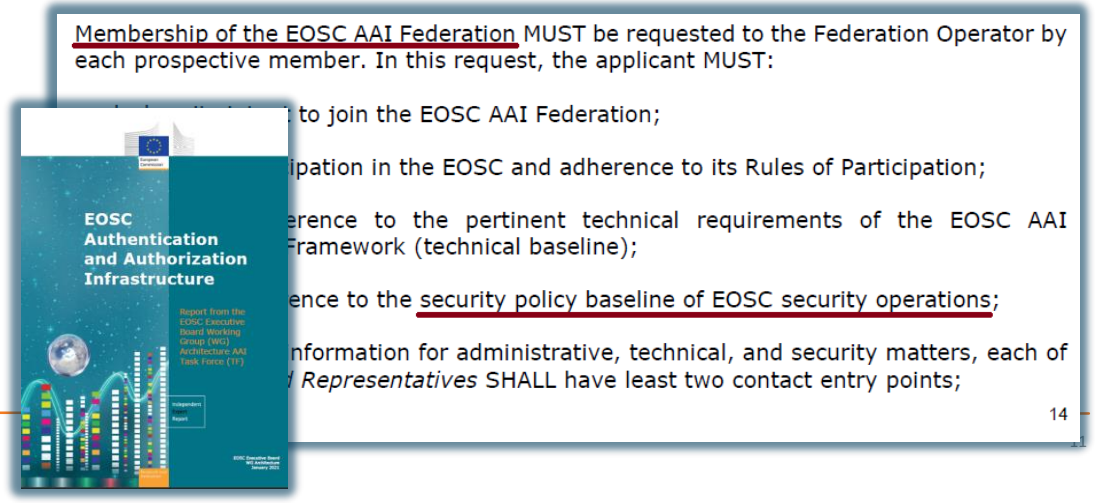
Security *Baseline*

- prerequisite for connecting to the Core Infra Proxy
- connection requirement for the EOSC AAI
- may evolve over time

Additional elements can be added to augment trust

- through service level agreements
- by maturity grading ('WISE SCI' peer assessments)

Group name	**EOSC AAI Implementation**
Chairs	Christos Kanellopoulos, GEANT
Short description	The purpose of this working group is to align the AAI related activities across work packages and to discuss, capture and analyse use cases and requirements for the EOSC AAI from the EOSC Core Services and the Research Infrastructures, including the security policy baselines and guidelines used.



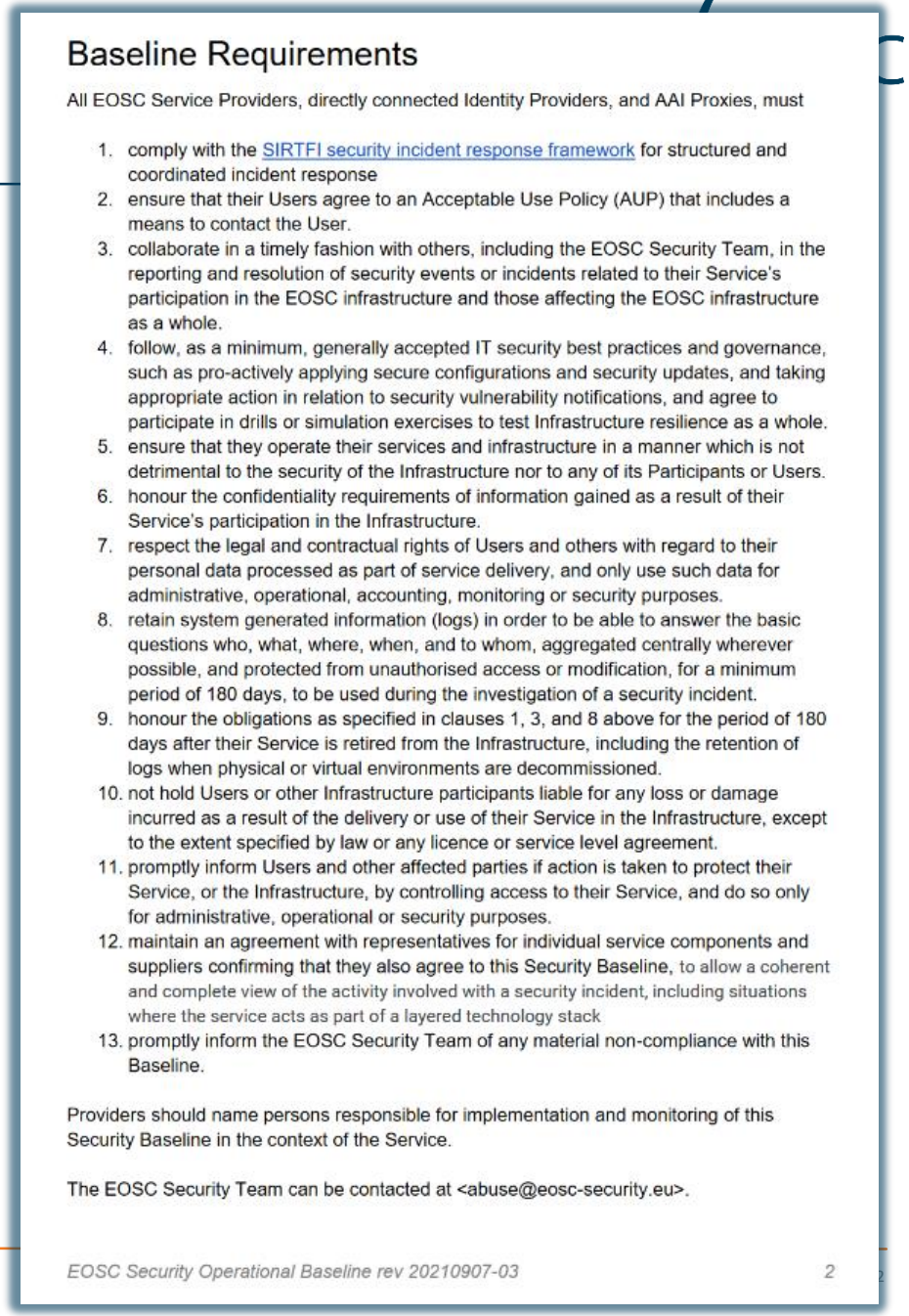
Baseline Process

Co-development of EOSC Future & AARC Policy Community

- version based on UK-IRIS evolution of the AARC PDK
- specifically geared towards the looser EOSC ecosystem
- mindful of urgent need for collective coherent response

AARC Policy team consultation – 1st round just finished

- 13 itemised points - https://edu.nl/avfv4
- complemented by an 'FAQ' with guidance and refs (no new standards, there is enough good stuff out there)
- leverages *Sirtfi* framework
- connects to the Core Security Team



Baseline Requirements

All EOSC Service Providers, directly connected Identity Providers, and AAI Proxies, must

1. comply with the SIRTFI security incident response framework for structured and coordinated incident response
2. ensure that their Users agree to an Acceptable Use Policy (AUP) that includes a means to contact the User.
3. collaborate in a timely fashion with others, including the EOSC Security Team, in the reporting and resolution of security events or incidents related to their Service's participation in the EOSC infrastructure and those affecting the EOSC infrastructure as a whole.
4. follow, as a minimum, generally accepted IT security best practices and governance, such as pro-actively applying secure configurations and security updates, and taking appropriate action in relation to security vulnerability notifications, and agree to participate in drills or simulation exercises to test Infrastructure resilience as a whole.
5. ensure that they operate their services and infrastructure in a manner which is not detrimental to the security of the Infrastructure nor to any of its Participants or Users.
6. honour the confidentiality requirements of information gained as a result of their Service's participation in the Infrastructure.
7. respect the legal and contractual rights of Users and others with regard to their personal data processed as part of service delivery, and only use such data for administrative, operational, accounting, monitoring or security purposes.
8. retain system generated information (logs) in order to be able to answer the basic questions who, what, where, when, and to whom, aggregated centrally wherever possible, and protected from unauthorised access or modification, for a minimum period of 180 days, to be used during the investigation of a security incident.
9. honour the obligations as specified in clauses 1, 3, and 8 above for the period of 180 days after their Service is retired from the Infrastructure, including the retention of logs when physical or virtual environments are decommissioned.
10. not hold Users or other Infrastructure participants liable for any loss or damage incurred as a result of the delivery or use of their Service in the Infrastructure, except to the extent specified by law or any licence or service level agreement.
11. promptly inform Users and other affected parties if action is taken to protect their Service, or the Infrastructure, by controlling access to their Service, and do so only for administrative, operational or security purposes.
12. maintain an agreement with representatives for individual service components and suppliers confirming that they also agree to this Security Baseline, to allow a coherent and complete view of the activity involved with a security incident, including situations where the service acts as part of a layered technology stack
13. promptly inform the EOSC Security Team of any material non-compliance with this Baseline.

Providers should name persons responsible for implementation and monitoring of this Security Baseline in the context of the Service.

The EOSC Security Team can be contacted at <abuse@eosc-security.eu>.

EOSC Security Operational Baseline rev 20210907-03 2

https://wiki.eoscfuture.eu/x/Q4sb

Most current version

All EOSC Service Providers, directly connected Identity Providers, and AAI Proxies, must

1. comply with the SIRTFI security incident response framework for structured and coordinated incident response
2. ensure that their Users agree to an Acceptable Use Policy (AUP) [or Terms of Use] and that there is a means to contact each User.
3. collaborate in a timely fashion with others, including the EOSC Security Team, in the reporting and resolution of security events or incidents related to their Service's participation in the EOSC infrastructure and those affecting the EOSC infrastructure as a whole.
4. follow, as a minimum, generally accepted IT security best practices and governance, such as pro-actively applying secure configurations and security updates, and taking appropriate action in relation to security vulnerability notifications, and agree to participate in drills or simulation exercises to test Infrastructure resilience as a whole.
5. ensure that they operate their services and infrastructure in a manner which is not detrimental to the security of the Infrastructure nor to any of its Participants or Users.
6. honour the confidentiality requirements of information gained as a result of their Service's participation in the Infrastructure.
7. respect the legal and contractual rights of Users and others with regard to their personal data processed, and only use such data for administrative, operational, accounting, monitoring or security purposes.

Most current version

8. retain system generated information (logs) in order to be able to answer the basic questions who, what, where, when, and to whom, [aggregated centrally wherever possible, and protected from unauthorised access or modification], for a minimum period of 180 days, [to be used during the investigation of a security incident].
9. honour the obligations as specified in clauses 1, 3, and 8 above for the period of 180 days after their Service is retired from the Infrastructure, including the retention of logs when physical or virtual environments are decommissioned.
10. not hold Users or other Infrastructure participants liable for any loss or damage incurred as a result of the delivery or use of their Service in the Infrastructure, except to the extent specified by law or any license or service level agreement.
11. promptly inform Users and other affected parties if action is taken to protect their Service, or the Infrastructure, by controlling access to their Service, and do so only for administrative, operational or security purposes.
12. maintain an agreement with representatives for individual service components and suppliers confirming that they also agree to this Security Baseline, to allow a coherent and complete view of the activity involved with a security incident, including situations where the service acts as part of a layered technology stack
13. promptly inform the EOSC Security Team of any material non-compliance with this Baseline.

Providers should name persons responsible for implementation and monitoring …

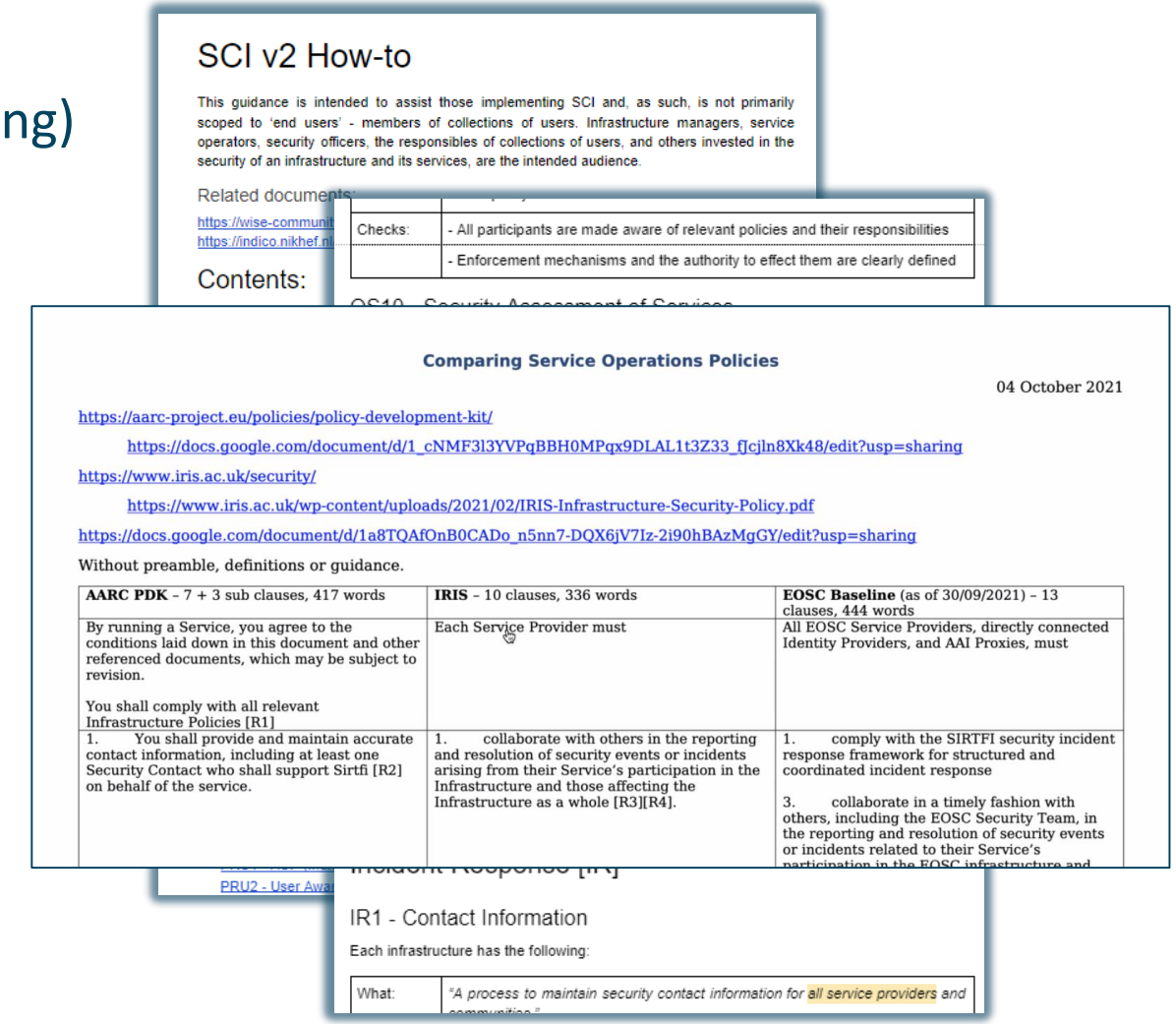
But also the Security Baseline lives in an ecosystem with Complementing elements

- the FAQ ‘Annotated Baseline’
  (which is actually essential to its understanding)

- an EOSC Core Security Team
  and response processes and guidance

And the WISE context

- SCI maturity assessment model
- WISE Risk Assessment Templates
- …



EOSC Security Operational Baseline (rev 20210908-03)

- lastest version (after initial AARC Policy consultation) at https://edu.nl/avfv4
- FAQ for now at https://wiki.eoscfuture.eu/display/EOSCF/EOSC+Security+Operational+Annotated+Baseline
- very much linked to work in the WISE SCIv2 WG

Thank you

Any Questions?

davidg@nikhef.nl

https://aarc-community.org

The work leading to these results has received funding from the European Union's Horizon 2020 research and innovation programme and other sources.

this work is co-supported by the EOSC-Future project, the GN4-3 project, UK-IRIS, and SURF