Information Security Management

EOSCF WP7 SMS Updates, August 2022

David Groep – WP7.5 Security Operations and Policy lead
Nikhef Physics Data Processing programme
UM Faculty of Science and Engineering, DKE

The EOSC ISM Policies and Processes

- EOSC ISM policies and processes
- ISM in the Core vs. the Exchange
- Security Baseline for the EOSC
- Doing incident response
- Readiness table-top exercises
- Doing risk assessment
- Evolution: what is brewing?

Goal of Information Security Management (ISM)

“ensure confidentiality, integrity and availability”

“protecting sensitive data from threats and vulnerabilities”

In our heterogeneous EOSC at large, founded on subsidiarity, this translates to

- *primum non nocere*: do no harm to interests & assets of users
- not expose other service providers in the EOSC ecosystem to enlarged risk *as a result of their participation in EOSC*
- be transparent about infosec maturity and risk to its customers and suppliers

The ISM policies and processes

EOSC ISM differentiates between Core and Exchange

- both are in scope for all security policies
- Core: mandatory adherence (and pro-active support from the security team)
- Exchange: based on Interoperability Framework (& ‘RFC2119-RECOMMENDED’)

Participants are autonomous

- but subscribe to shared commitment of maintaining trustworthy & secure EOSC

With everyone expected to participate in incident response and ‘drills’

- for the Core services, expert forensics support is provided for if desired
- in the Exchange, coordination and liaison are the primary tasks of the CSIRT

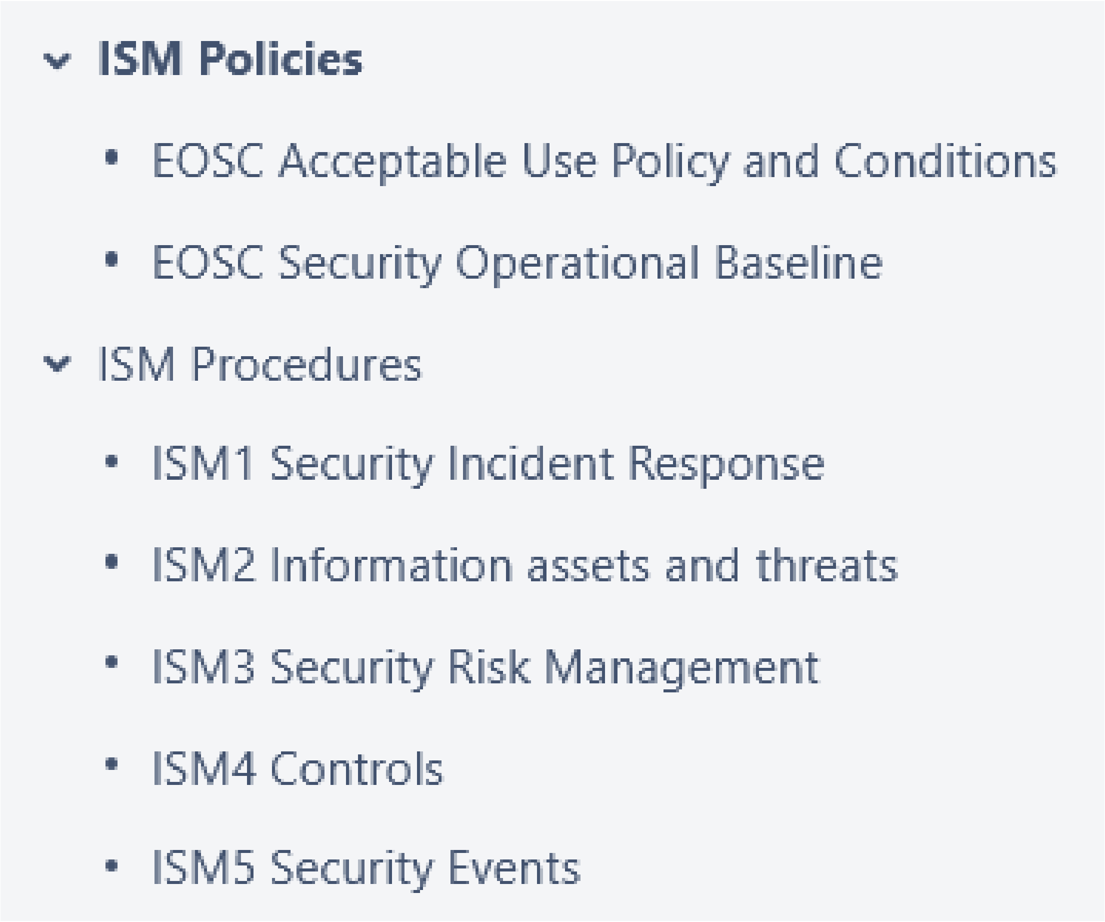
ISM SMS structure

- **start with just 2 policies**

- **and 5 procedures**

Supported by

- a ‘comms challenge’ as a KPI that we can track (~2x per year)
- standing CSIRT response team
- security ‘events’ monitoring & triage (to align with FitSM)



ISM Policies

- EOSC Acceptable Use Policy and Conditions
- EOSC Security Operational Baseline

ISM Procedures

- ISM1 Security Incident Response
- ISM2 Information assets and threats
- ISM3 Security Risk Management
- ISM4 Controls
- ISM5 Security Events

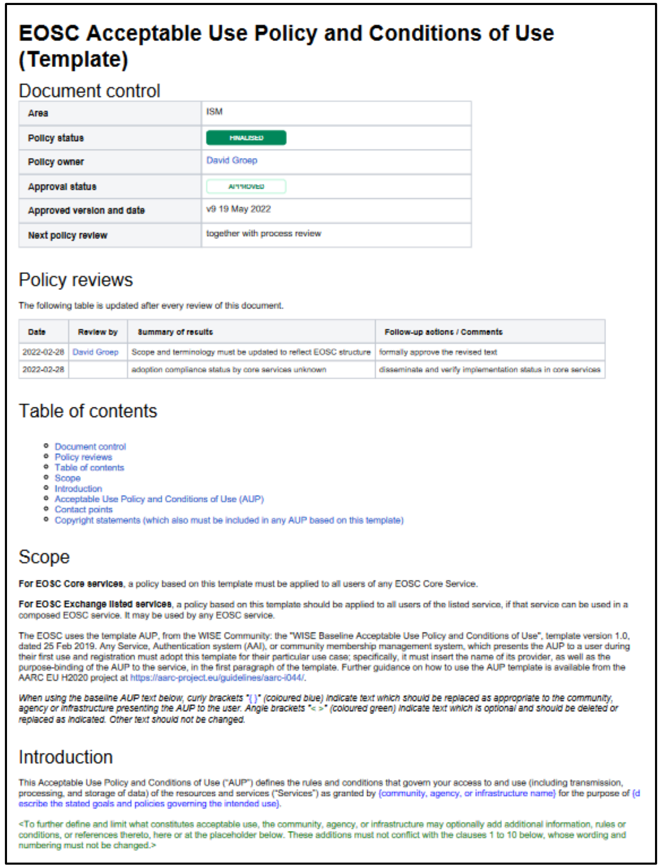
Important roles

The key role is the CSIRT at abuse@eosc-security.eu

Of course there are real people, but for long-term stability and tracking only generic addresses should be used for communication

- CSIRT central team: Pinja, Daniel, DavidC
- ISM processes and (public) procedures: Alf, DaveK, SvenG, DavidG
- ISM Policies: DavidG, DaveK, Ralph, Alf, IanN,
- ISM Risk Assessment process: Urpo, Linda, DaveK, IanN, JoukeR

Policy – a baselining approach



EOSC Acceptable Use Policy and Conditions of Use (Template)

Document control

Area	ISM
Policy status	FINALISED
Policy owner	David Groep
Approval status	APPROVED
Approved version and date	v9 19 May 2022
Next policy review	together with process review

Policy reviews

The following table is updated after every review of this document.

Date	Review by	Summary of results	Follow-up actions / Comments
2022-02-28	David Groep	Scope and terminology must be updated to reflect EOSC structure	formally approve the revised text
2022-02-28		adoption compliance status by core services unknown	disseminate and verify implementation status in core services

Table of contents

Scope

For EOSC Core services, a policy based on this template must be applied to all users of any EOSC Core Service.

For EOSC Exchange listed services, a policy based on this template should be applied to all users of the listed service, if that service can be used in a composed EOSC service. It may be used by any EOSC service.

The EOSC uses the template AUP, from the WISE Community: the "WISE Baseline Acceptable Use Policy and Conditions of Use", template version 1.0, dated 25 Feb 2019. Any Service, Authentication system (AAI), or community membership management system, which presents the AUP to a user during their first use and registration must adopt this template for their particular use case; specifically, it must insert the name of its provider, as well as the purpose-binding of the AUP to the service, in the first paragraph of the template. Further guidance on how to use the AUP template is available from the AARC EU H2020 project at https://aarc-project.eu/guidelines/aarc-i044/.

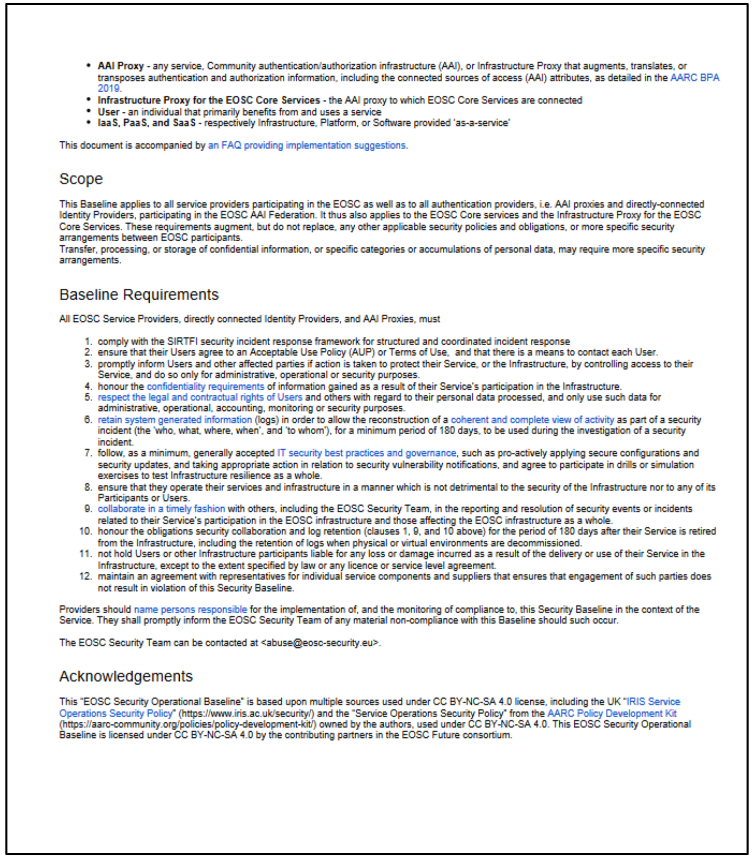
When using the baseline AUP text below, curly brackets "{ }" (coloured blue) indicate text which should be replaced as appropriate to the community, agency or infrastructure presenting the AUP to the user. Angle brackets "< >" (coloured green) indicate text which is optional and should be deleted or replaced as indicated. Other text should not be changed.

Introduction

This Acceptable Use Policy and Conditions of Use ("AUP") defines the rules and conditions that govern your access to and use (including transmission, processing, and storage of data) of the resources and services ("Services") as granted by {community, agency, or infrastructure name} for the purpose of {d escribe the stated goals and policies governing the intended use}.

<To further define and limit what constitutes acceptable use, the community, agency, or infrastructure may optionally add additional information, rules or conditions, or references thereto, here or at the placeholder below. These additions must not conflict with the clauses 1 to 10 below, whose wording and numbering must not be changed.>

Common AUP (based on WISE AUP) – required for core services to ensure consistency, strongly recommended for all services and for community AAI proxies



- **AAI Proxy** - any service, Community authentication/authorization infrastructure (AAI), or Infrastructure Proxy that augments, translates, or transposes authentication and authorization information, including the connected sources of access (AAI) attributes, as detailed in the AARC BPA 2019.
- **Infrastructure Proxy for the EOSC Core Services** - the AAI proxy to which EOSC Core Services are connected
- **User** - an individual that primarily benefits from and uses a service
- **IaaS, PaaS, and SaaS** - respectively Infrastructure, Platform, or Software provided 'as-a-service'

This document is accompanied by an FAQ providing implementation suggestions.

Scope

This Baseline applies to all service providers participating in the EOSC as well as to all authentication providers, i.e. AAI proxies and directly-connected Identity Providers, participating in the EOSC AAI Federation. It thus also applies to the EOSC Core services and the Infrastructure Proxy for the EOSC Core Services. These requirements augment, but do not replace, any other applicable security policies and obligations, or more specific security arrangements between EOSC participants.
Transfer, processing, or storage of confidential information, or specific categories or accumulations of personal data, may require more specific security arrangements.

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) or Terms of Use, and that there is a means to contact each User.
3. 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.
4. honour the confidentiality requirements of information gained as a result of their Service's participation in the Infrastructure.
5. 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.
6. retain system generated information (logs) in order to allow the reconstruction of a coherent and complete view of activity as part of a security incident (the 'who, what, where, when', and 'to whom'), for a minimum period of 180 days, to be used during the investigation of a security incident.
7. 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.
8. 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.
9. 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.
10. honour the obligations security collaboration and log retention (clauses 1, 9, and 10 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.
11. 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.
12. maintain an agreement with representatives for individual service components and suppliers that ensures that engagement of such parties does not result in violation of this Security Baseline.

Providers should name persons responsible for the implementation of, and the monitoring of compliance to, this Security Baseline in the context of the Service. They shall promptly inform the EOSC Security Team of any material non-compliance with this Baseline should such occur.

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

Acknowledgements

This "EOSC Security Operational Baseline" is based upon multiple sources used under CC BY-NC-SA 4.0 license, including the UK "IRIS Service Operations Security Policy" (https://www.iris.ac.uk/security/) and the "Service Operations Security Policy" from the AARC Policy Development Kit (https://aarc-community.org/policies/policy-development-kit/) owned by the authors, used under CC BY-NC-SA 4.0. This EOSC Security Operational Baseline is licensed under CC BY-NC-SA 4.0 by the contributing partners in the EOSC Future consortium.

EOSC Security Operational Baseline
a mere 12 points that make you a trustworthy provider organisation towards your peers and the EOSC

EOSC Security Operational Baseline

Co-development of EOSC Future & AARC Policy Community

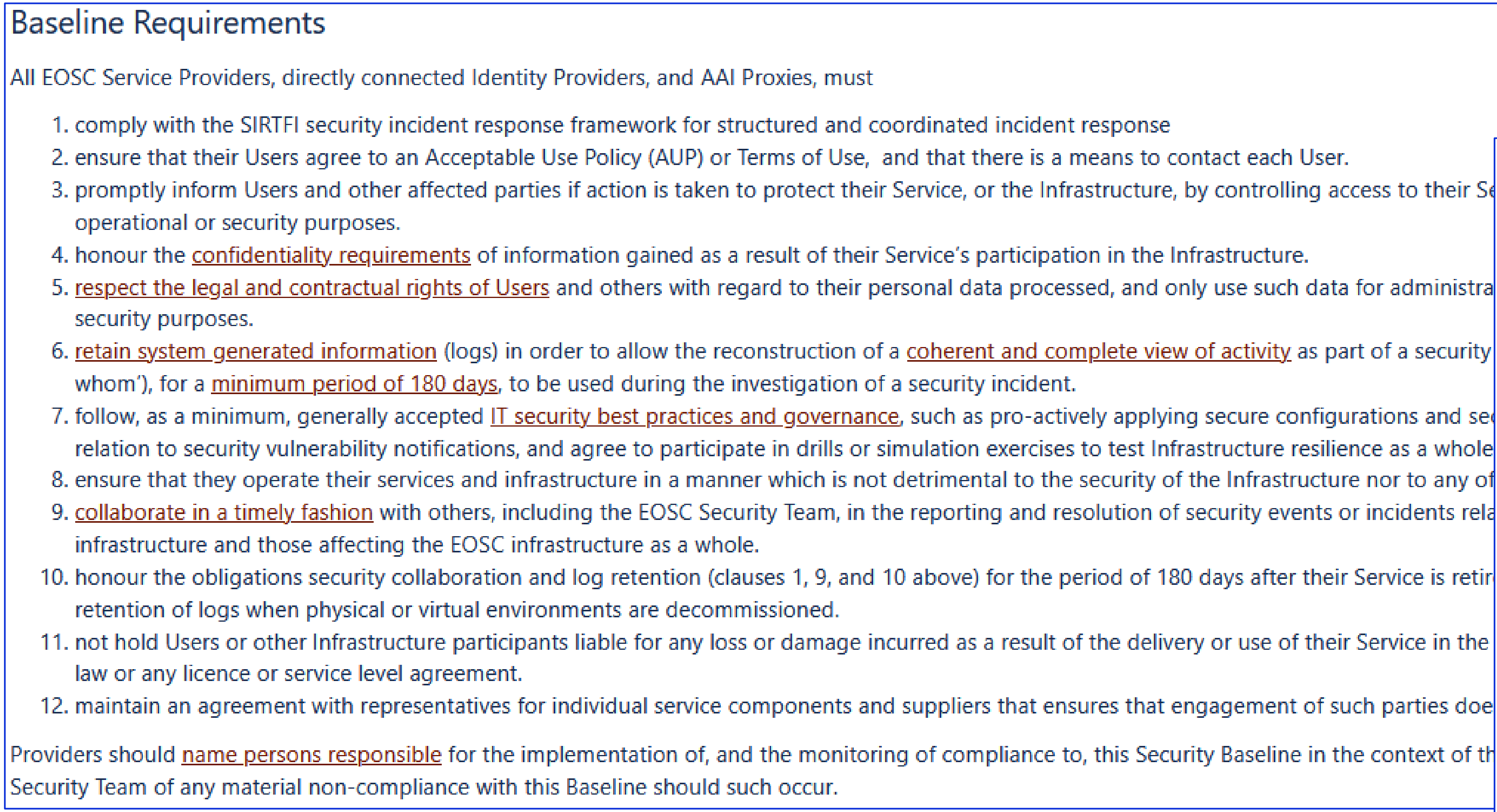
- version based on UK-IRIS evolution of the AARC PDK
- specifically geared towards the looser EOSC ecosystem
- mindful of urgent need for collective coherent response

EOSC consultation together with AEGIS, AARC, and GEANT EnCo

- complemented by an ‘FAQ’ with guidance and references, but no new standards: ‘there is enough good stuff out there’
- leverages Sirtfi framework
- connects to the Core Security Team
- part of the EOSC SMS and Core Participation Agreement

Joint input to the new WISE AARC Service Operational Policy work in SCI

EOSCSMS – EOSC Security Operational Baseline & FAQ

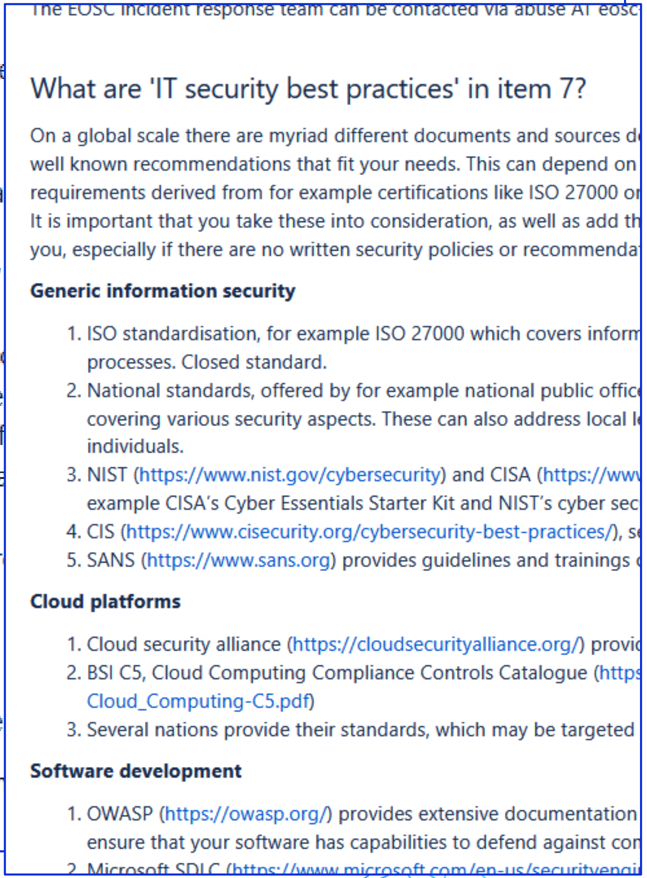


Baseline Requirements

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) or Terms of Use, and that there is a means to contact each User.
3. promptly inform Users and other affected parties if action is taken to protect their Service, or the Infrastructure, by controlling access to their Se operational or security purposes.
4. honour the confidentiality requirements of information gained as a result of their Service's participation in the Infrastructure.
5. respect the legal and contractual rights of Users and others with regard to their personal data processed, and only use such data for administra security purposes.
6. retain system generated information (logs) in order to allow the reconstruction of a coherent and complete view of activity as part of a security whom'), for a minimum period of 180 days, to be used during the investigation of a security incident.
7. follow, as a minimum, generally accepted IT security best practices and governance, such as pro-actively applying secure configurations and se relation to security vulnerability notifications, and agree to participate in drills or simulation exercises to test Infrastructure resilience as a whole
8. 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
9. collaborate in a timely fashion with others, including the EOSC Security Team, in the reporting and resolution of security events or incidents rela infrastructure and those affecting the EOSC infrastructure as a whole.
10. honour the obligations security collaboration and log retention (clauses 1, 9, and 10 above) for the period of 180 days after their Service is retir retention of logs when physical or virtual environments are decommissioned.
11. 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 law or any licence or service level agreement.
12. maintain an agreement with representatives for individual service components and suppliers that ensures that engagement of such parties doe

Providers should name persons responsible for the implementation of, and the monitoring of compliance to, this Security Baseline in the context of th Security Team of any material non-compliance with this Baseline should such occur.



The EOSC incident response team can be contacted via abuse AT eosc

What are 'IT security best practices' in item 7?

On a global scale there are myriad different documents and sources d well known recommendations that fit your needs. This can depend on requirements derived from for example certifications like ISO 27000 or It is important that you take these into consideration, as well as add th you, especially if there are no written security policies or recommenda

Generic information security

1. ISO standardisation, for example ISO 27000 which covers inform processes. Closed standard.
2. National standards, offered by for example national public offic covering various security aspects. These can also address local l individuals.
3. NIST (https://www.nist.gov/cybersecurity) and CISA (https://ww example CISA's Cyber Essentials Starter Kit and NIST's cyber sec
4. CIS (https://www.cisecurity.org/cybersecurity-best-practices/), s
5. SANS (https://www.sans.org) provides guidelines and trainings

Cloud platforms

1. Cloud security alliance (https://cloudsecurityalliance.org/) provi
2. BSI C5, Cloud Computing Compliance Controls Catalogue (https Cloud_Computing-C5.pdf)
3. Several nations provide their standards, which may be targeted

Software development

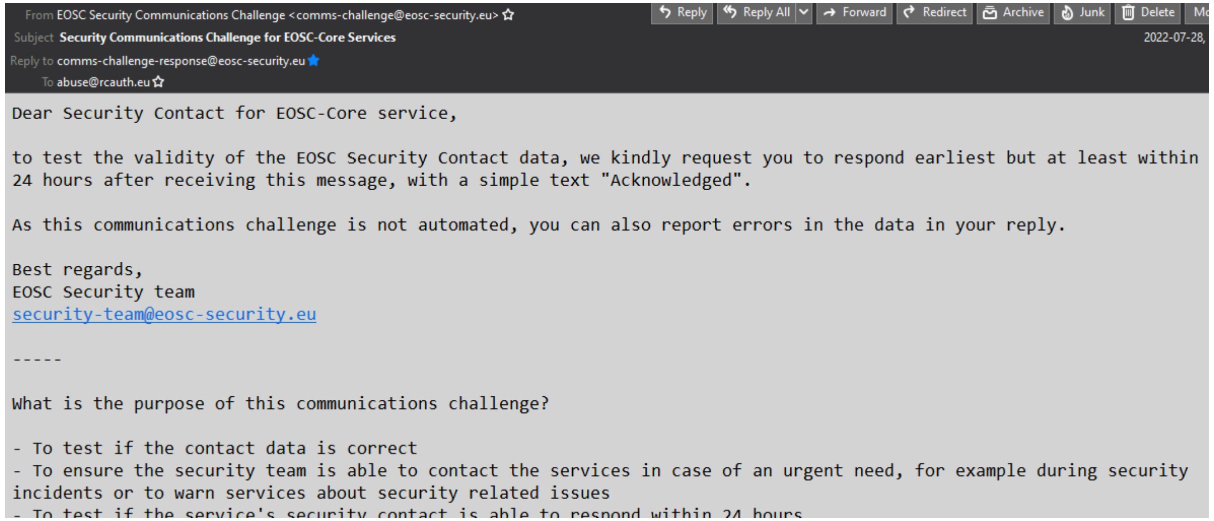
1. OWASP (https://owasp.org/) provides extensive documentation ensure that your software has capabilities to defend against co
2. Microsoft SDLC (https://www.microsoft.com/en-us/securityengi

https://wiki.eoscfuture.eu/display/EOSCSMS/EOSC+Security+Operational+Baseline

Communications challenges (~ 2x per year)

You already got the mail with the simple question for contact data fixes

- response can be done by email
- verifies the security contacts (and proved useful already)



From EOSC Security Communications Challenge <comms-challenge@eosc-security.eu>
Subject **Security Communications Challenge for EOSC-Core Services**
2022-07-28,
Reply to comms-challenge-response@eosc-security.eu
To abuse@rcauth.eu

```
Dear Security Contact for EOSC-Core service,

to test the validity of the EOSC Security Contact data, we kindly request you to respond earliest but at least within
24 hours after receiving this message, with a simple text "Acknowledged".

As this communications challenge is not automated, you can also report errors in the data in your reply.

Best regards,
EOSC Security team
security-team@eosc-security.eu

-----

What is the purpose of this communications challenge?

- To test if the contact data is correct
- To ensure the security team is able to contact the services in case of an urgent need, for example during security
incidents or to warn services about security related issues
- To test if the service's security contact is able to respond within 24 hours
```

The request to join as a “volunteer for tabletop exercises ” will come
– a great way to get prepared for the future multiplayer RPGs

Participation in drills or simulation exercises to test Infrastructure resilience as a whole is necessary (and part of the Baseline …)

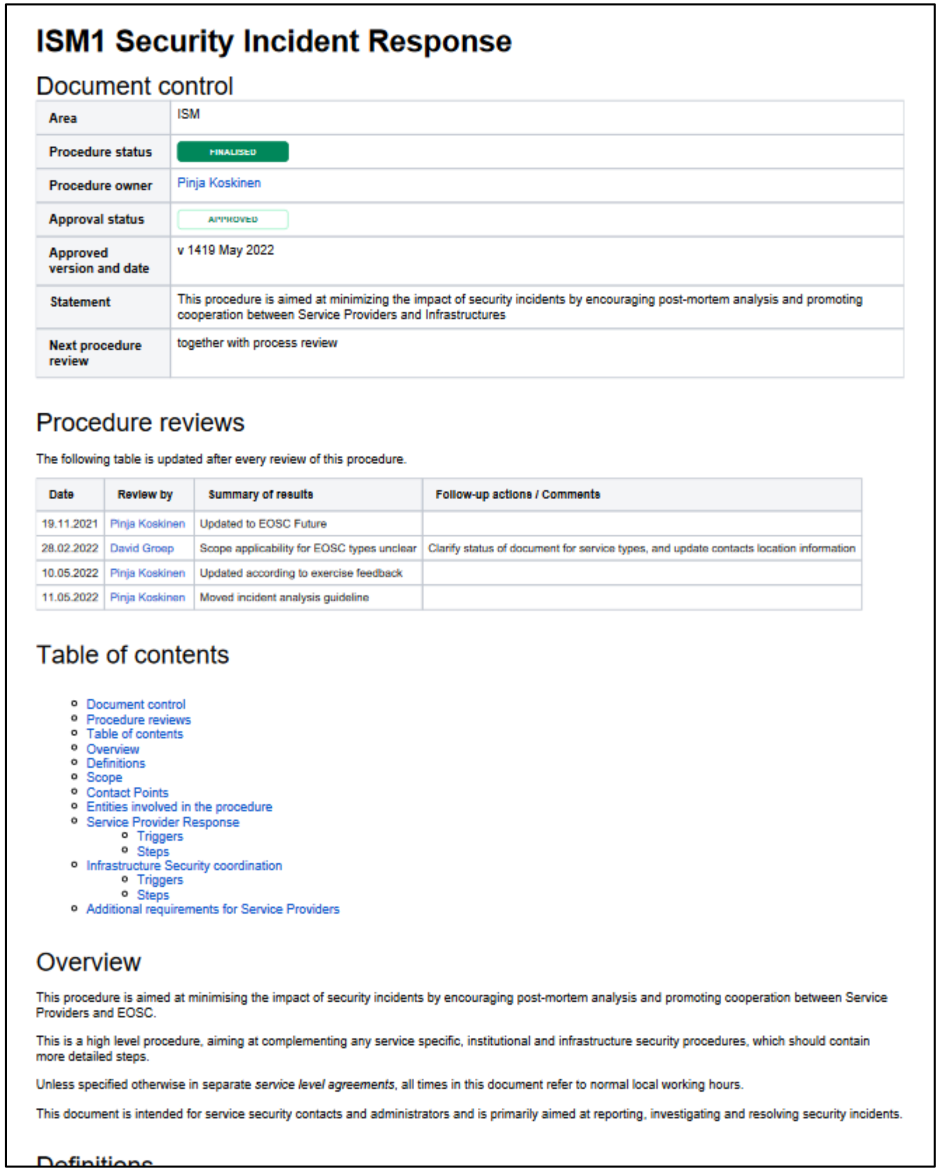
Procedures for incident response

Two parts to the incident process

- This (public) ISM1 response procedure
- Focussing on interaction between central CSIRT and the provider organisation
- Ingress from Zammad and by mail

There is a 2nd element …

an internal detailed technical note, focussing on the team interaction within the CSIRT (how to use RT, mail templates)
The internal note is private, as it contains quite a lot of confidential address information



ISM1 Security Incident Response

Document control

Area	ISM
Procedure status	FINALISED
Procedure owner	Pinja Koskinen
Approval status	APPROVED
Approved version and date	v 1419 May 2022
Statement	This procedure is aimed at minimizing the impact of security incidents by encouraging post-mortem analysis and promoting cooperation between Service Providers and Infrastructures
Next procedure review	together with process review

Procedure reviews

The following table is updated after every review of this procedure.

Date	Review by	Summary of results	Follow-up actions / Comments
19.11.2021	Pinja Koskinen	Updated to EOSC Future	
28.02.2022	David Groep	Scope applicability for EOSC types unclear	Clarify status of document for service types, and update contacts location information
10.05.2022	Pinja Koskinen	Updated according to exercise feedback	
11.05.2022	Pinja Koskinen	Moved incident analysis guideline	

Table of contents

Overview

This procedure is aimed at minimising the impact of security incidents by encouraging post-mortem analysis and promoting cooperation between Service Providers and EOSC.

This is a high level procedure, aiming at complementing any service specific, institutional and infrastructure security procedures, which should contain more detailed steps.

Unless specified otherwise in separate *service level agreements*, all times in this document refer to normal local working hours.

This document is intended for service security contacts and administrators and is primarily aimed at reporting, investigating and resolving security incidents.

Definitions

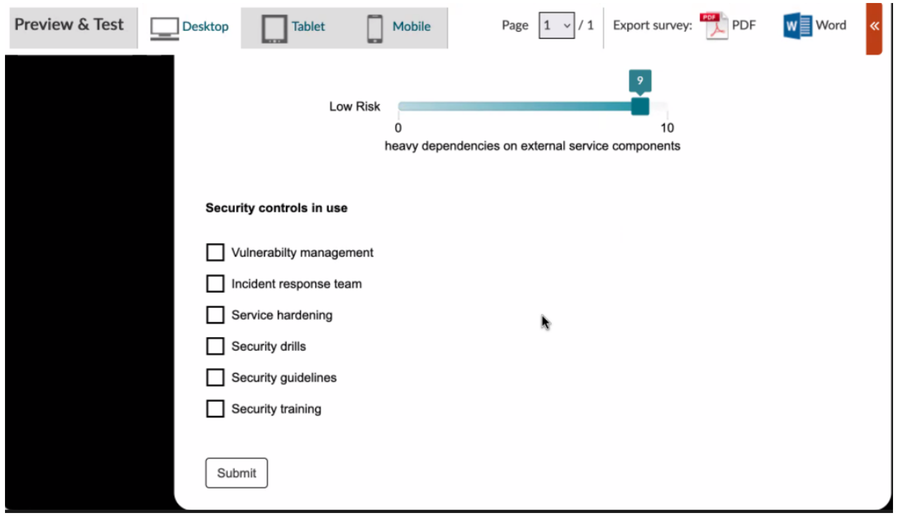
Security Frameworks

There are many of these out there:
NIST Cyberframework (*https://www.nist.gov/cyberframework*),
mapping to ISO27k2, NIST SP800-53, and others

ISO27k10 (multi-domain messaging and information exchange)
builds strongly on 27k2, so is not quite the 'light weight' option we look for

Risk Management Framework

We *do have* the framework based on SCIv2 and the Risk Assessment WG
Simple risk assessment questionnaire almost complete (on webropol), and core service providers will be requested to answer (and discuss) the questions



Low Risk

heavy dependencies on external service components

Security controls in use

- □ Vulnerabilty management
- □ Incident response team
- □ Service hardening
- □ Security drills
- □ Security guidelines
- □ Security training

Submit

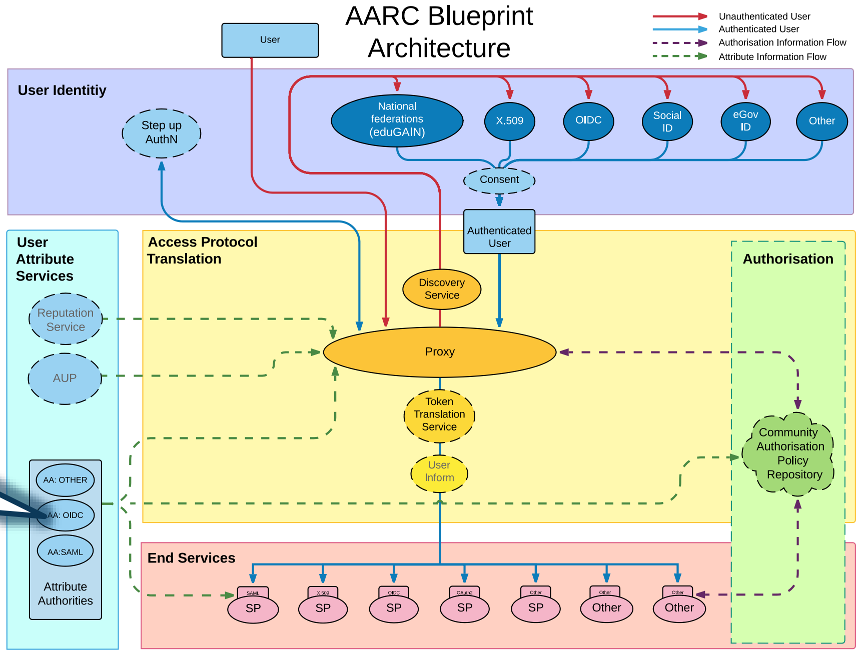
We will use a reference community to evaluate the risk-assessment approach for the EOSC Exchange (using SKA as a 'fresh' example community)

Evolving Security and Trust for attribute sources & proxies

Beyond the baseline:
supporting interoperable trust for the EOSC Federation

Community membership management directories and attribute authorities

- integrity of membership
- identification, naming and traceability
- site and service security
- protection on the network
- assertion integrity



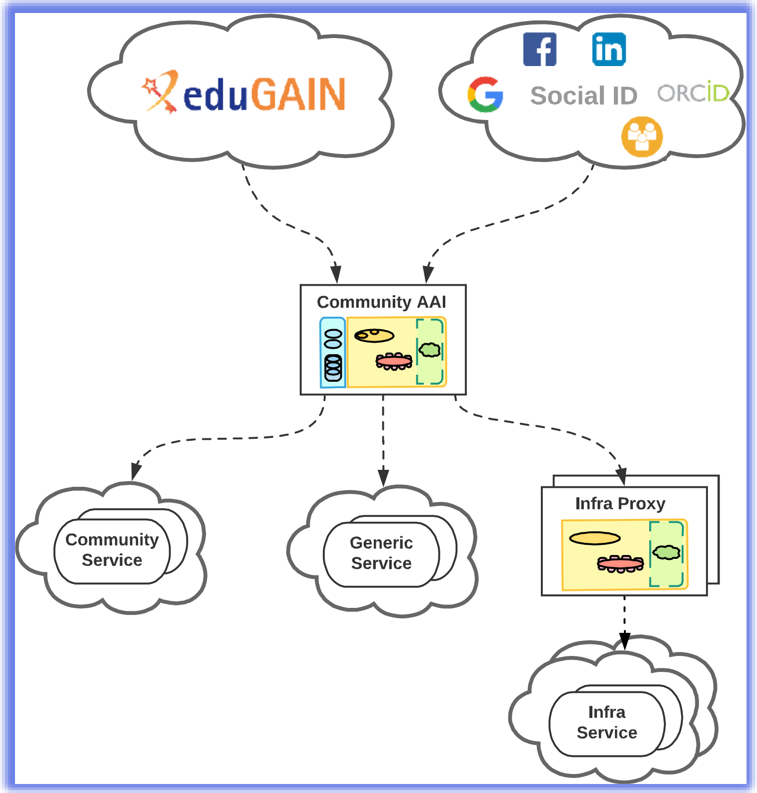
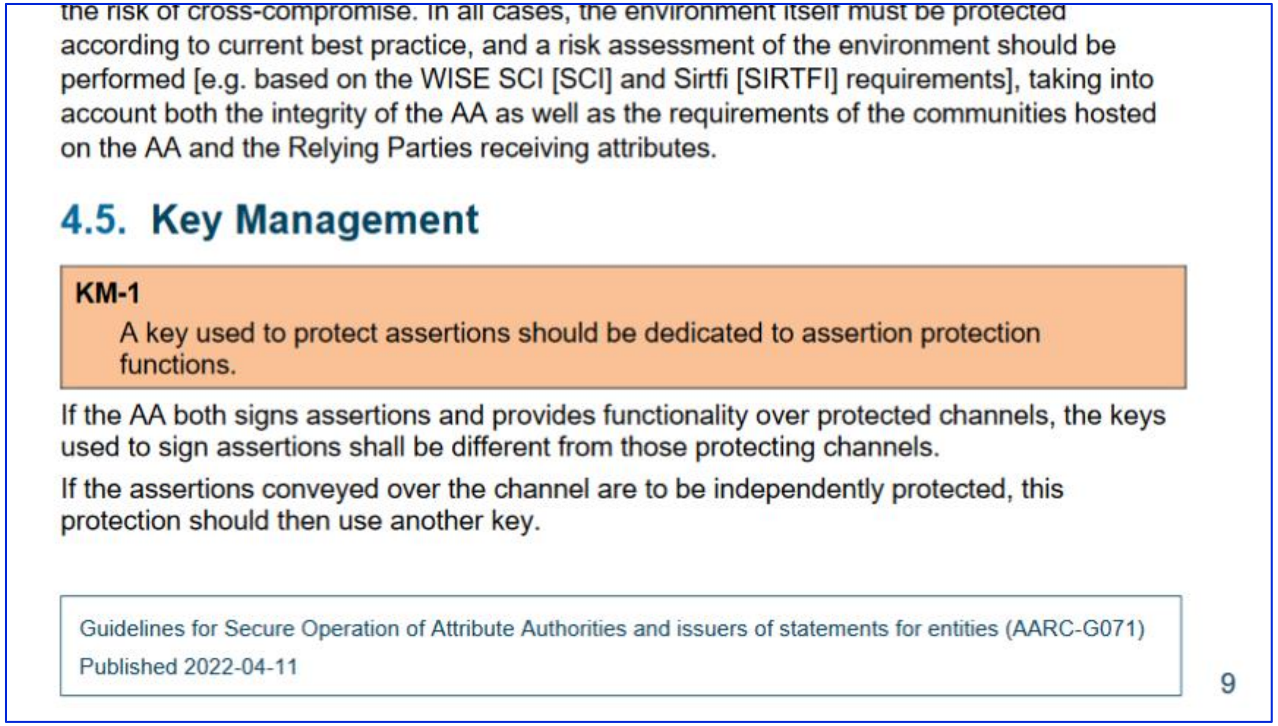


Image source: AARC Community
https://aarc-community.org/architecture/

Specific guidance and implementation recommendations

Following the IGTF “Annotated Requirements” model, each statement is accompanied by implementation guidance.

Technology neutral, i.e. both push and pull* models are in scope



the risk of cross-compromise. In all cases, the environment itself must be protected according to current best practice, and a risk assessment of the environment should be performed [e.g. based on the WISE SCI [SCI] and Sirtfi [SIRTFI] requirements], taking into account both the integrity of the AA as well as the requirements of the communities hosted on the AA and the Relying Parties receiving attributes.

4.5. Key Management

KM-1

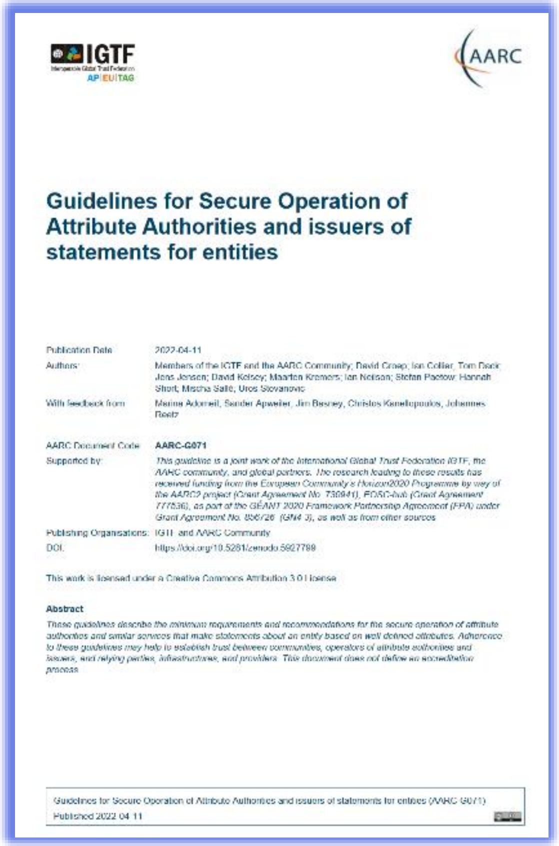
A key used to protect assertions should be dedicated to assertion protection functions.

If the AA both signs assertions and provides functionality over protected channels, the keys used to sign assertions shall be different from those protecting channels.

If the assertions conveyed over the channel are to be independently protected, this protection should then use another key.

Guidelines for Secure Operation of Attribute Authorities and issuers of statements for entities (AARC-G071)
Published 2022-04-11

9



Guidelines for Secure Operation of Attribute Authorities and issuers of statements for entities

Publication Date	2022-04-11
Authors:	Members of the IGTF and the AARC Community; David Groep; Ian Collier; Tom Dack; Jens Jensen; David Kelsey; Maarten Kremers; Ian Neilson; Stefan Paetow; Hannah Short; Mischa Sallé; Uros Stevanovic
With feedback from	Marina Adomeit, Sander Apweiler, Jim Basney, Christos Kanellopoulos, Johannes Reetz
AARC Document Code	**AARC-G071**
Supported by:	*This guideline is a joint work of the International Global Trust Federation IGTF, the AARC community, and global partners. The research leading to these results has received funding from the European Community's Horizon2020 Programme by way of the AARC2 project (Grant Agreement No. 730941), EOSC-hub (Grant Agreement 777536), as part of the GÉANT 2020 Framework Partnership Agreement (FPA) under Grant Agreement No. 856726 (GN4-3), as well as from other sources*
Publishing Organisations:	IGTF and AARC Community
DOI:	https://doi.org/10.5281/zenodo.5927799

This work is licensed under a Creative Commons Attribution 3.0 License

Abstract

These guidelines describe the minimum requirements and recommendations for the secure operation of attribute authorities and similar services that make statements about an entity based on well defined attributes. Adherence to these guidelines may help to establish trust between communities, operators of attribute authorities and issuers, and relying parties, infrastructures, and providers. This document does not define an accreditation process.

Guidelines for Secure Operation of Attribute Authorities and issuers of statements for entities (AARC-G071)
Published 2022-04-11

aarc-community.org/guidelines/aarc-g071
https://doi.org/10.5281/zenodo.5927799
** see RFC2904 for the model descriptions*

Thanks to the EOSC Future WP7.5 collaborators: Alf Moens, Daniel Kouřil, Baptise Grenier, David Crooks, David Groep, David Kelsey, Ian Neilson, Linda Cornwall, Matt Viljoen, Pinja Koskinen, Ralph Niederberger, Romain Wartel, Sven Gabriel, and Urpo Kaila.

EOSC Future

Discussion time!

eoscfuture.eu

Nikhef Maastricht University

David Groep

https://www.nikhef.nl/~davidg/presentations/

https://orcid.org/0000-0003-1026-6606

The EOSC Future project is co-funded by the
European Union Horizon Programme call
INFRAEOSC-03-2020, Grant Agreement number 101017536