EOSC Future

Information Security Management in the EOSC Future SMS evolution

January 2023

Nikhef
Maastricht University

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

Goal of Information Security Management (ISM)

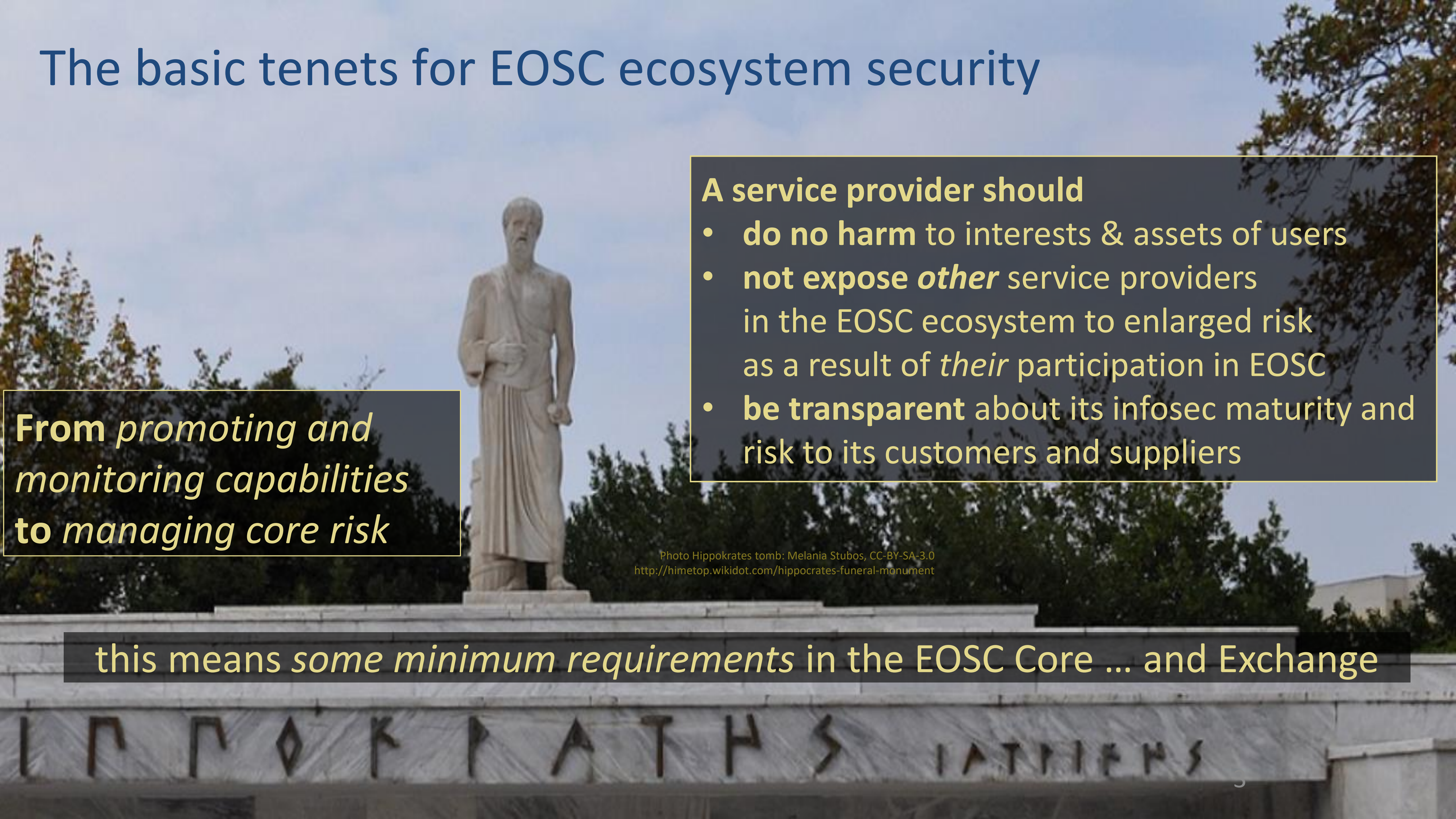
“ensure confidentiality, integrity and availability”

“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 basic tenets for EOSC ecosystem security



A service provider should

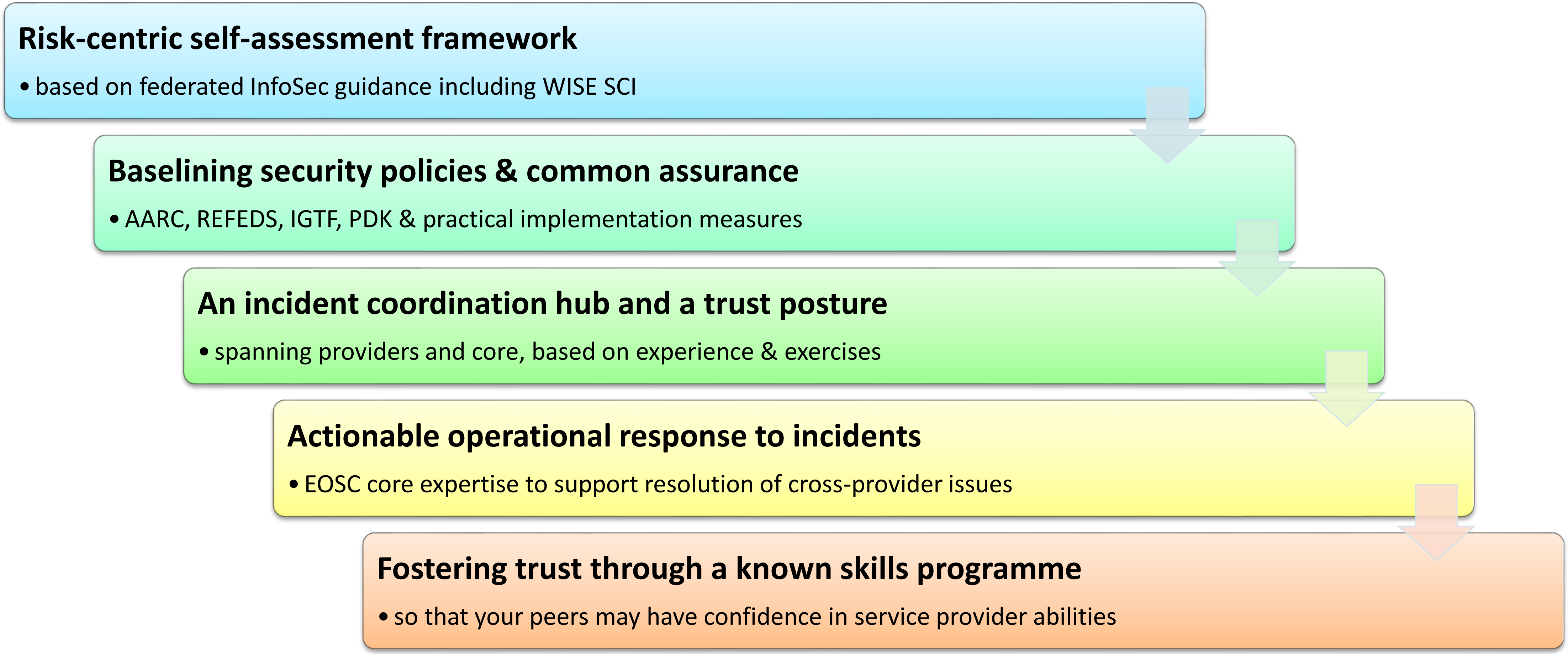
- **do no harm** to interests & assets of users
- **not expose *other*** service providers in the EOSC ecosystem to enlarged risk as a result of *their* participation in EOSC
- **be transparent** about its infosec maturity and risk to its customers and suppliers

From *promoting and monitoring capabilities* **to** *managing core risk*

this means *some minimum requirements* in the EOSC Core … and Exchange

Photo Hippokrates tomb: Melania Stubos, CC-BY-SA-3.0
http://himetop.wikidot.com/hippocrates-funeral-monument

How the security coodination team supports a trusted EOSC



Risk-centric self-assessment framework

- based on federated InfoSec guidance including WISE SCI

Baselining security policies & common assurance

- AARC, REFEDS, IGTF, PDK & practical implementation measures

An incident coordination hub and a trust posture

- spanning providers and core, based on experience & exercises

Actionable operational response to incidents

- EOSC core expertise to support resolution of cross-provider issues

Fostering trust through a known skills programme

- so that your peers may have confidence in service provider abilities

WISE SCI: wise-community.org/sci
AARC&c: aarc-community.org, refeds.org, igtf.net
PDK: aarc-community.org/policies/policy-development-kit

How the Information Security Process helps

EOSC ISM differentiates between Core and Exchange

- **Core**: mandatory adherence (and pro-active support from the security team) since the security of the Core services underpins the whole EOSC ecosystem
- **Exchange**: based on Interoperability Framework (& ‘RFC2119 RECOMMENDED’)

Participants are autonomous

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

We need everyone’s help in incident response and ‘drills’ (that also a lot of fun!)

- 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 *but the EOSC CSIRT will of course help where it can!*

Structuring security for the EOSC

1. Information security **risk assessment framework** based on SCI and a maturity model – targeting connected services as well as data, and correlated risks
2. Coordinate security policies for a **baseline** aligned with the Rules of Participation of the EOSC, and the EOSC AAI federation – ensuring transparency for the ‘risk appetite’ of the participants
3. Mechanisms for **coordination** and resolution of incidents through Information Security Management (ISM) **processes** – leveraging WISE community and Sirtfi, and enabling the (tested) framework for information sharing
4. Security **operations and incident response capabilities** related to or affecting the EOSC Core (in relatively broad sense) - with content and service providers

Information Assets in the EOSC

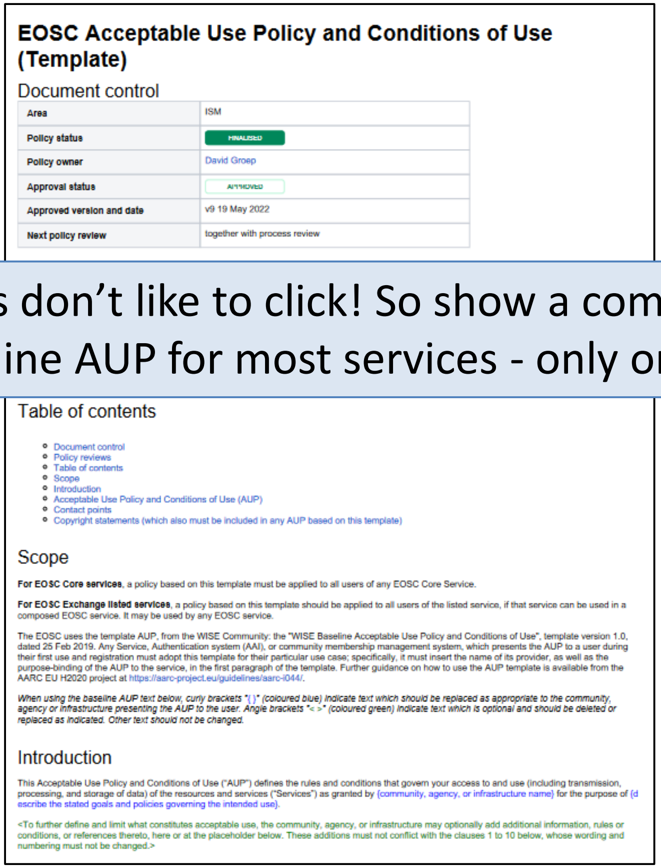
Subsidiarity

- core service providers are subject to the EOSC Core Agreement, but the operating entities are the primary responsible for their own services
- exchange service providers bring their own (existing) services, and join based on the EOSC *Rules of Participation,* the *On-boarding Agreement,* and the *AAI*

Hence the *assets* that the EOSC Security sees are *services,*
including the data and digital objects they manage, but
not their hardware, service components, middleware, or people

this provides the touchstone for the ISM policies, following the *EOSChub* model

Policy – a baselining approach for AUP and Operations



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

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.

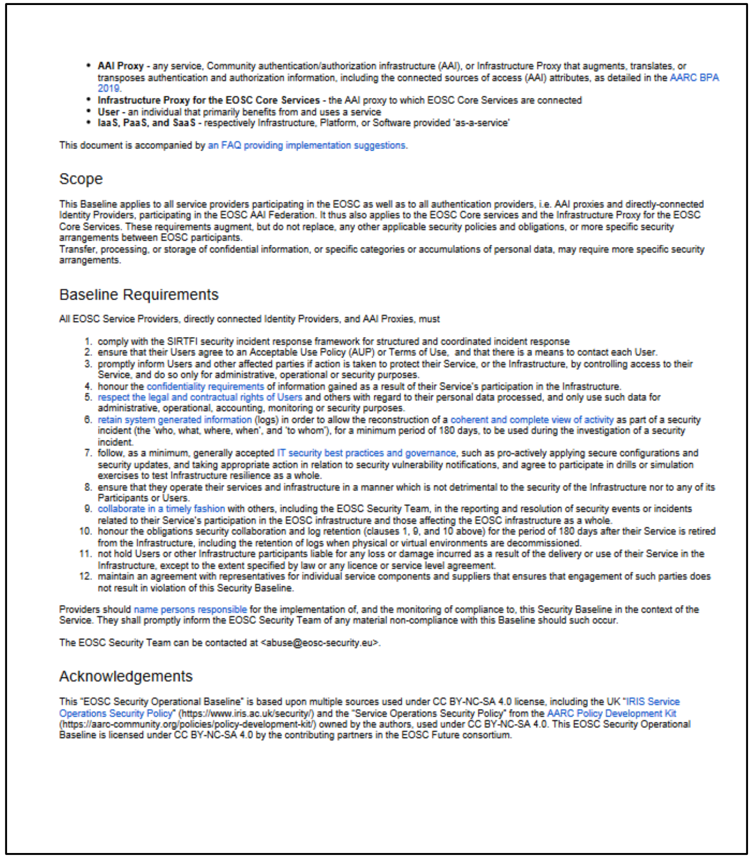
Introduction

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 {describe 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.>

Users don’t like to click! So show a common baseline AUP for most services - only once

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

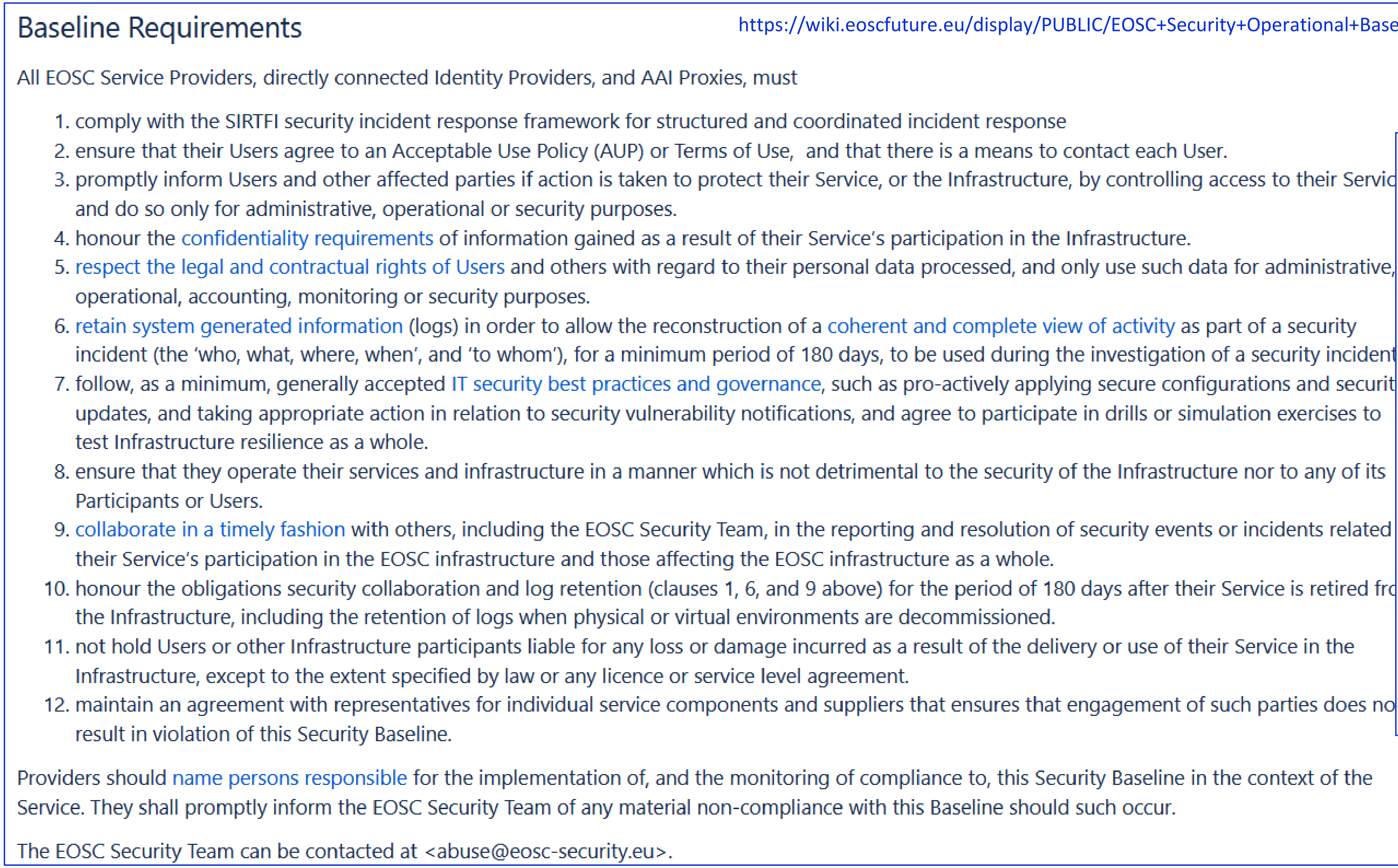
- version based on UK-IRIS evolution of the AARC PDK
- specifically geared towards the looser EOSC ecosystem
- mindful of urgent need for collective coherent response

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
- part of the EOSC SMS, endorsed by TCB, in Core Participation Agreement
- submitted as part of the EOSC I/F

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

EOSCSMS – EOSC Security Operational Baseline & FAQ



Baseline Requirements

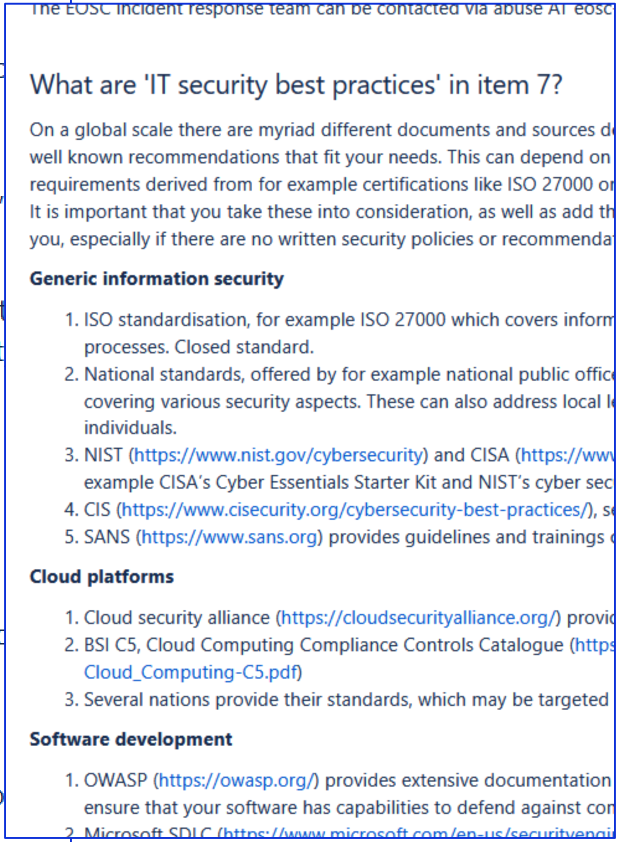
https://wiki.eoscfuture.eu/display/PUBLIC/EOSC+Security+Operational+Baseline

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 Servic 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 securit 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 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, 6, and 9 above) for the period of 180 days after their Service is retired fro 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 no 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>.



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 office covering various security aspects. These can also address local l individuals.
3. NIST (https://www.nist.gov/cybersecurity) and CISA (https://www example CISA's Cyber Essentials Starter Kit and NIST's cyber sec
4. CIS (https://www.cisecurity.org/cybersecurity-best-practices/), se
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

FitSM SMS ISM Audit

December 19th, 2022

FitSM ISM - identified 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: Pau, 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

FitSM ISM Requirements

PR6.1: two information security policies defined, following initial suitability assessment

PR6.2: security controls defined at asset level through the Security Operational Baseline, as included in the Core Service provider agreement, the EOSC AAI federation requirements, and (to be) the EOSC I/F

PR6.3: annual review foreseen together with process review

PR6.4: both general security events (ISM.6) and emergency incidents (under ISM.1) are treated with appropriate priority.

PR6.5: consistency is delegated to the (core) service providers, subject to the EOSC AAI and the risk assessment. Risk assessment methodology defined but procedures not implemented yet.

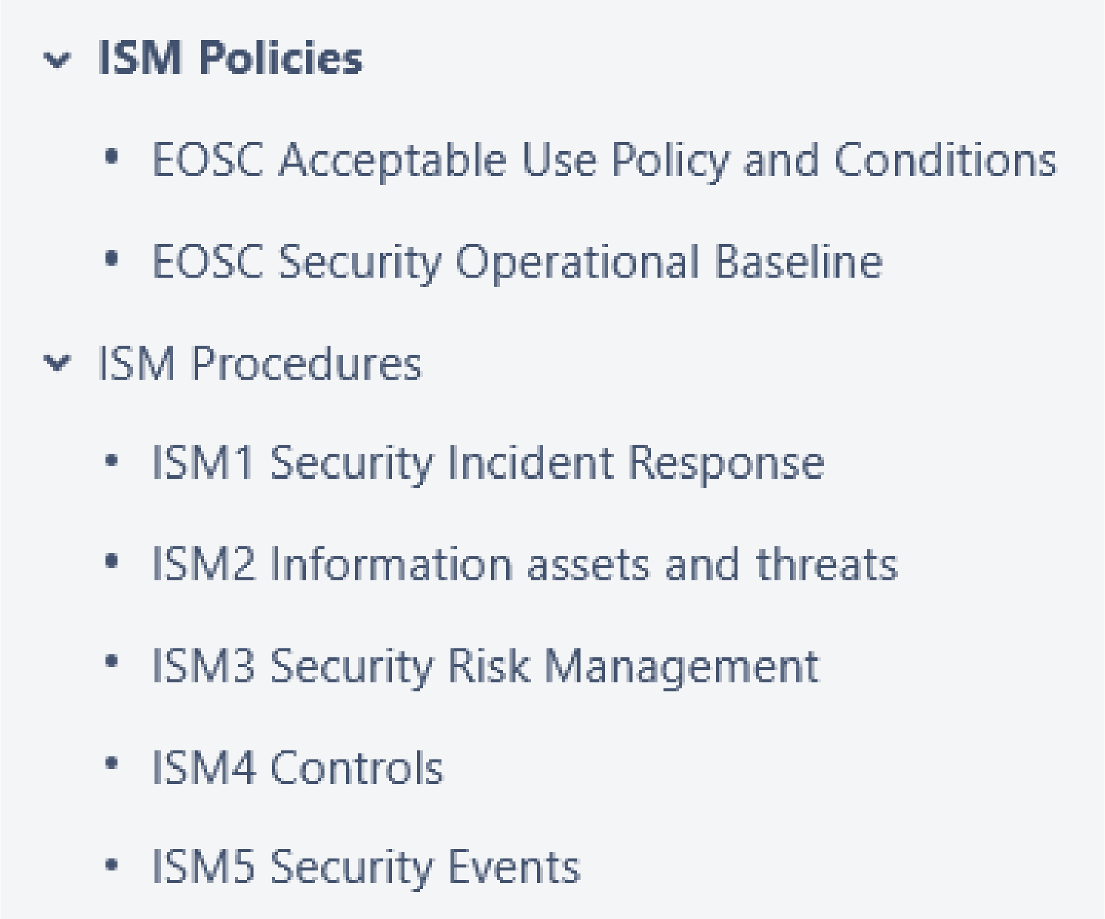
ISM SMS structure

- **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)



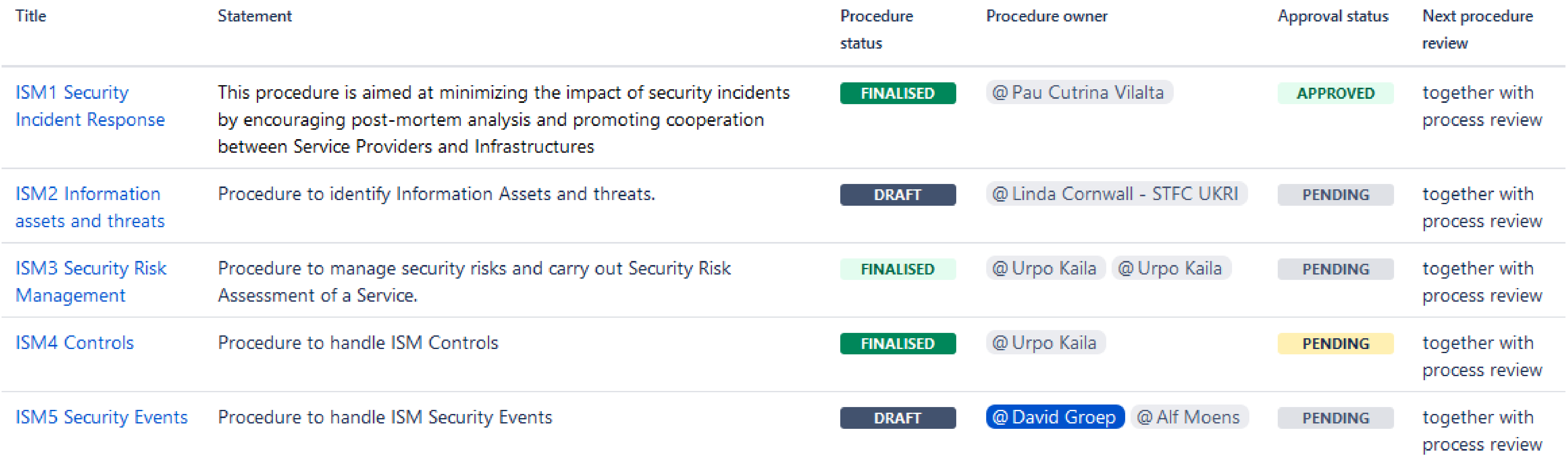
ISM Policies

- 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

ISM Procedures – at various stages of maturity



Title	Statement	Procedure status	Procedure owner	Approval status	Next procedure review
ISM1 Security Incident Response	This procedure is aimed at minimizing the impact of security incidents by encouraging post-mortem analysis and promoting cooperation between Service Providers and Infrastructures	FINALISED	@ Pau Cutrina Vilalta	APPROVED	together with process review
ISM2 Information assets and threats	Procedure to identify Information Assets and threats.	DRAFT	@ Linda Cornwall - STFC UKRI	PENDING	together with process review
ISM3 Security Risk Management	Procedure to manage security risks and carry out Security Risk Assessment of a Service.	FINALISED	@ Urpo Kaila @ Urpo Kaila	PENDING	together with process review
ISM4 Controls	Procedure to handle ISM Controls	FINALISED	@ Urpo Kaila	PENDING	together with process review
ISM5 Security Events	Procedure to handle ISM Security Events	DRAFT	@ David Groep @ Alf Moens	PENDING	together with process review

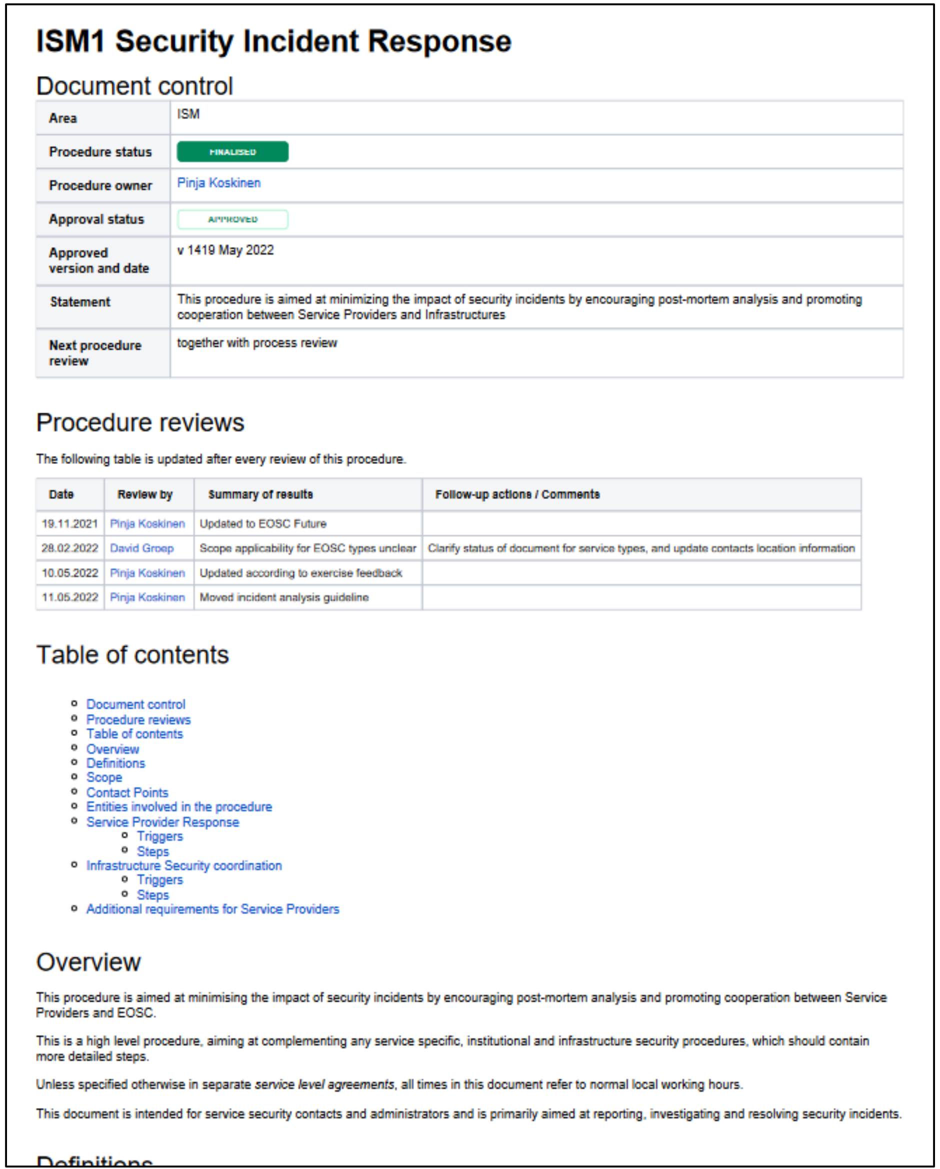
Procedures for incident response

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.

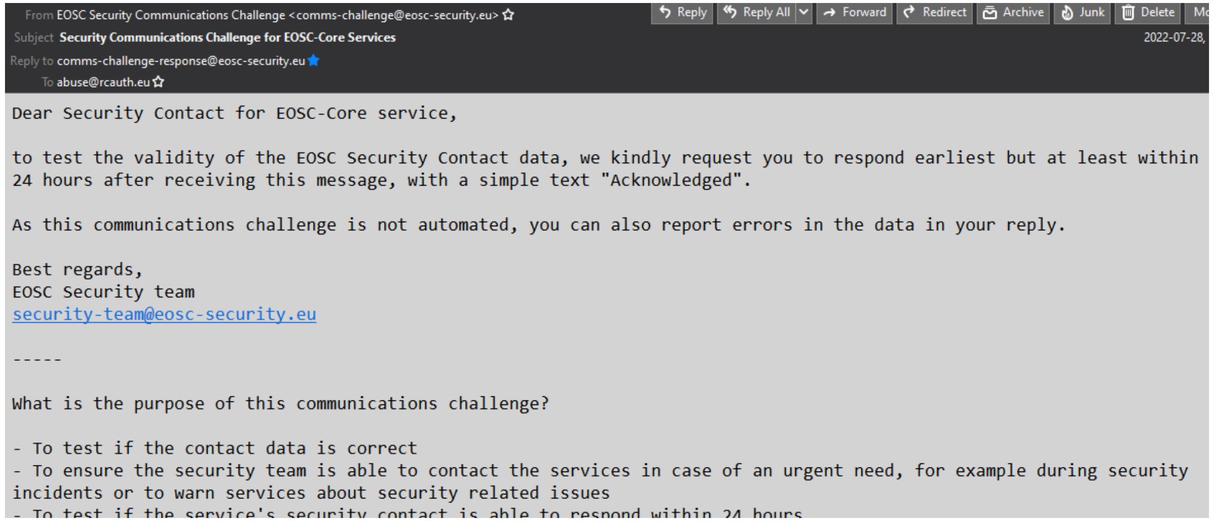
This document is intended for service security contacts and administrators and is primarily aimed at reporting, investigating and resolving security incidents.

Definitions

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 …)

KPIs

ISM.1	•Average number of actions, per incident, taken during incident handling not following procedures (exceptional actions):Actions not covered by any procedure •Procedure covering actions incorrect	By the debriefing at quarterly F2F meeting, which reviews all the records registered in our ticket tracker: - Number of actions is counted during the debriefing on each incident	Incidents are reviewed at each F2F meeting of the Security Operations Team (3 or 4 times per year).	NA	January 2023	greater than 3
ISM.2	•Time, accumulated over sites, between EOSC Security Team being notified and affected service providers taking actionMeasures delay introduced by EOSC Security Team procedures •Measures clarity of messages sent (broadcast or targetted) to sites	By the debriefing at quarterly F2F meeting, which reviews all the records registered in our ticket tracker: - Time is the difference between each update from user and following response from us (unless it was pending information from someone else) and between when we get information and we create other tickets	Incidents are reviewed at each F2F meeting of the Security Operations Team (3 or 4 times per year).	NA	January 2023	not applicable
ISM.3	Number of communications challenges run against the EOSC-Core providers	Counting runs	2 per year	2	October 2023	less than 1

Maturity & actions – now @level 2: partially complete

Action	Person responsible	Due date	Status
Rename file with process abbreviation and review date (e.g. CSI-2022-09-07.docx) and attach to SMS Process Reviews page	[Process Manager]	2022-12-20	Done, 2022-12-13
Review by process owner	[Process Owner]	2022-12-19	Done, 2022-12-14
Risk management procedure will be revised and registry established based on the self-assessment/questionnaire model following WISE RAW-WG methodology Includes tracking assets (i.e. services) through the registry.	@Urpo Kaila	2023-08-31	Ongoing
Security Event procedure (ISM.5) will be validated and exercised	[Security Incident Coordinator], @Alf Moens	2023-02-01	Ongoing
Security Controls review – following risk assessment	@Urpo Kaila, [Security Incident Coordinator]	2023-08-31	Ongoing
Security Incident Response weekly coordination meetings will resume once staff returns	[Security Incident Coordinator]	2023-01-01	Ongoing

Known action items

- Complete procedures 2 .. 5!
- Risk assessment for the ticketing system itself
  Risk assessment for the security ticketing system has identified relevant risks, but these have not yet been rated (or mitigations been assessed)
- Coordination meetings had been suspended
  Weekly update meetings have been suspended from August 2022 until January 2023 until new staff commences. Operational activity continued as scheduled.

SMS Report at https://wiki.eoscfuture.eu/display/EOSCSMS/ISM+Reports

Audit process itself

4.8. Information Security Management
(FitSM-1, PR6)
Audit evidence:
(EV) SIRTIFI framework
(EV) EOSC Security Operational Baseline (Confluence)
(EV) ISM3 Security Risk Management (Confluence)
(EV) WISE Risk Assessment framework
(EV) IR maptable exercise
(EV) ISM1 Security Incident Response (Confluence)
(EV) ISM5 Security Events (Confluence)
(EV) ISM KPI (Confluence)

Audit findings

Classification	Finding
(SR)	The development of a risk management approach (and tooling) to be applied as part of the information security management process is still work in progress and should be further promoted.
(H)	It could be considered to add another KPI, based on KPI ISM.3, to report on the results of the communication challenges (e.g. number of challenges where the security contact did not respond within the required period of time).
(H)	It could be reviewed, to which extent additional Information security aspects and requirements can or should be added to the EOSC interoperability framework and the provider / service onboarding process.

Risk Assessment Methodology

Audit Finding ISM#3

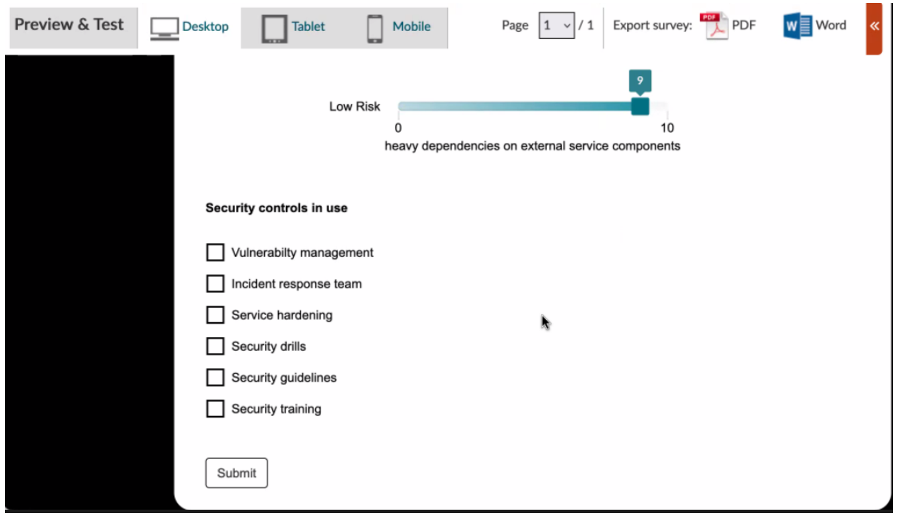
Security Frameworks

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)

Planning the rest of EOSCF

For D7.5b in M27 (June 2023)

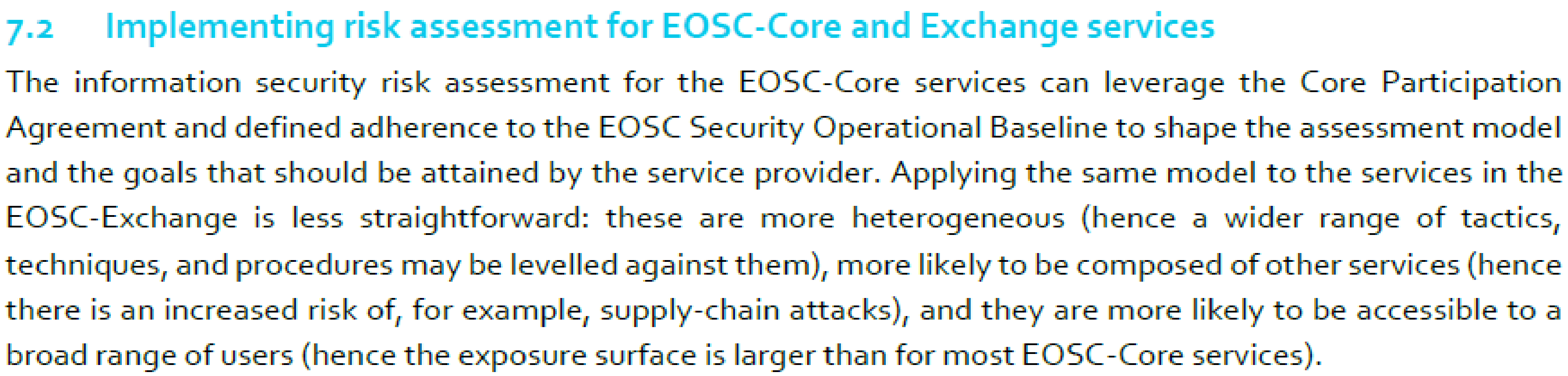
7.1 Policy recommendations: WISE recommendations and the Attribute Authority Secure Operations Guidelines

The EOSC Security Operational Baseline and the WISE Baseline AUP cater for different aspects of security interoperability for the EOSC. The EOSC Security Operational Baseline supports integrity, availability, and confidentiality for (composite) services. The use of the WISE Baseline AUP by all EOSC-Core services supports ease of use of all EOSC services by users and communities (by virtue of it being common, those services that need no additional conditions can presume the AUP has been shown and met by all users coming through the EOSC Portal).

Early implementation practice of EOSC-Core services has indicated that supplementary guidance is welcome and appropriate. This in particular holds for the requisite privacy notices for services. Regulation within the European Union requires that data processing information is explicitly shown to the users, and the EOSC on-boarding process thus includes a check on the presence of such notices in the appropriate locations. The WISE Baseline AUP also includes placeholders for references to privacy notices, and the AARC-I044 'Implementers Guide to the WISE Baseline Acceptable Use Policy'[9] provides the mechanisms that can be used for doing so. In practice, the variance in correctness of the privacy notices for EOSC services is significant – requiring significant rewrites even for EOSC-Core services and delaying the on-boarding process at the AAI stage. Joint guidance on privacy notices, especially for global services, has been identified by the WISE Community as a valuable addition. EOSC Future will contribute to this development and promote the dissemination of existing privacy notice guidance amongst the EOSC participants.

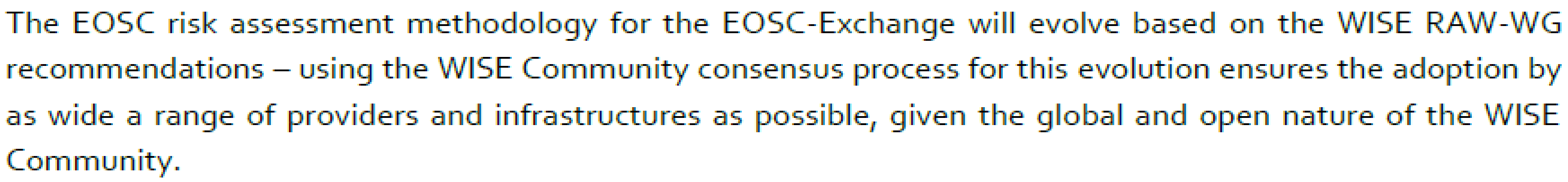
For the AAI Proxy operations, updated technology-agnostic guidance has recently been released by the AARC Engagement Group for e-Infrastructures (AEGIS) on how to best structure operational security and attribute authority integrity for both the proxies themselves as well as for their associated attribute stores. These 'Guidelines for Secure Operation of Attribute Authorities and other issuers of access statements' (AARC-G071) will be used also in the EOSC Federation to express security maturity for the AAI Proxies and foster the trust relationship between community and e-Infrastructure proxies. The operators of AAI Proxies in AEGIS have, through the endorsement of this guideline, committed to its implementation. It is expected that the guideline will evolve based on their feedback and implementation experience.

Risk …



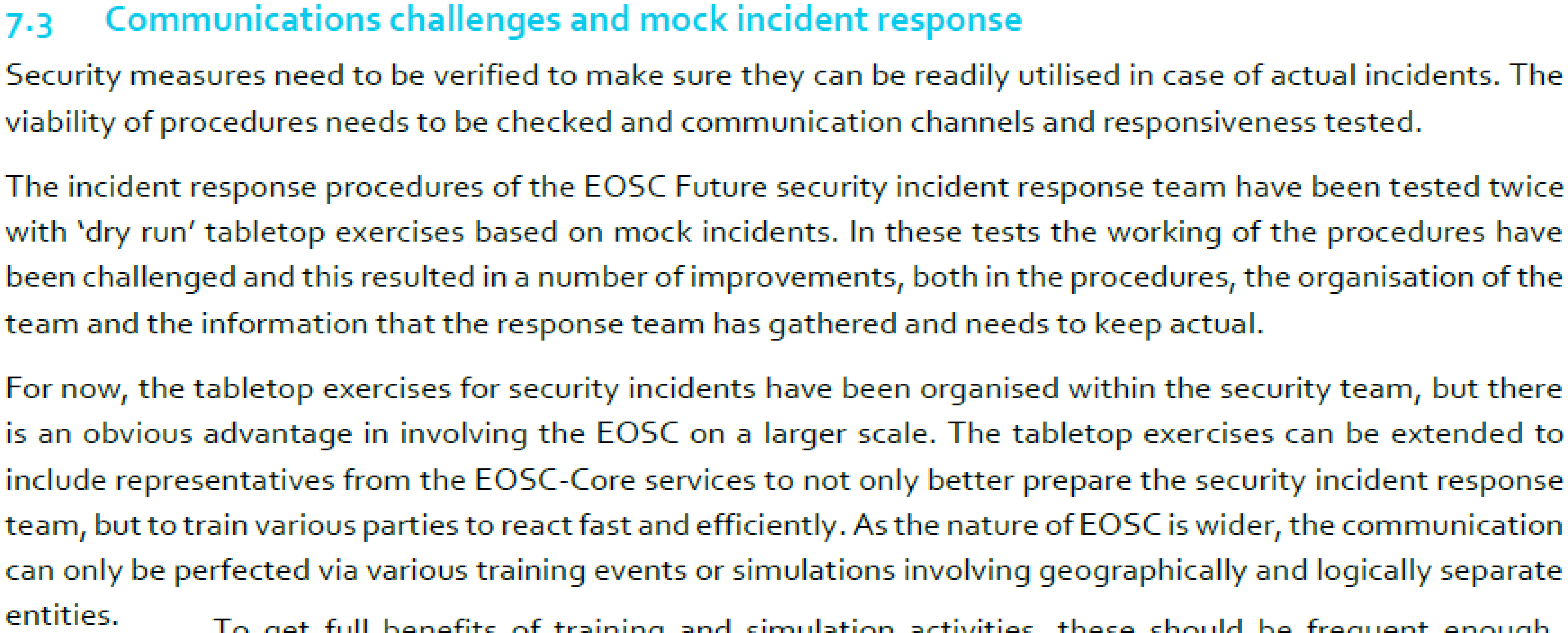
7.2 Implementing risk assessment for EOSC-Core and Exchange services

The information security risk assessment for the EOSC-Core services can leverage the Core Participation Agreement and defined adherence to the EOSC Security Operational Baseline to shape the assessment model and the goals that should be attained by the service provider. Applying the same model to the services in the EOSC-Exchange is less straightforward: these are more heterogeneous (hence a wider range of tactics, techniques, and procedures may be levelled against them), more likely to be composed of other services (hence there is an increased risk of, for example, supply-chain attacks), and they are more likely to be accessible to a broad range of users (hence the exposure surface is larger than for most EOSC-Core services).



The EOSC risk assessment methodology for the EOSC-Exchange will evolve based on the WISE RAW-WG recommendations – using the WISE Community consensus process for this evolution ensures the adoption by as wide a range of providers and infrastructures as possible, given the global and open nature of the WISE Community.

Processes and exercises

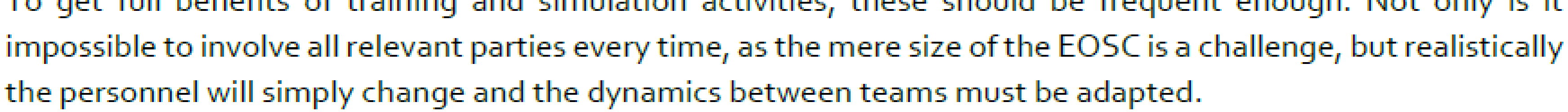


7.3 Communications challenges and mock incident response

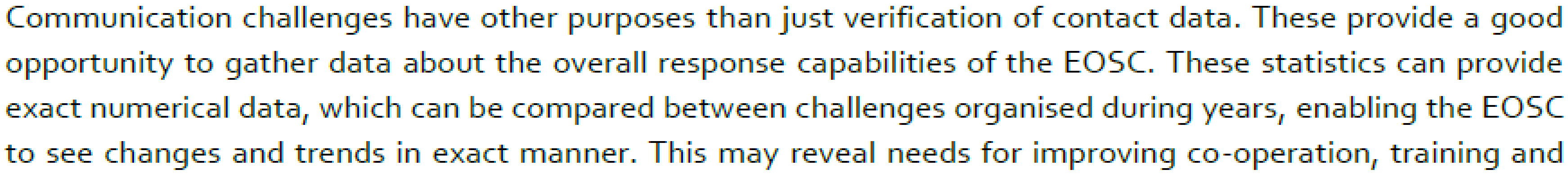
Security measures need to be verified to make sure they can be readily utilised in case of actual incidents. The viability of procedures needs to be checked and communication channels and responsiveness tested.

The incident response procedures of the EOSC Future security incident response team have been tested twice with 'dry run' tabletop exercises based on mock incidents. In these tests the working of the procedures have been challenged and this resulted in a number of improvements, both in the procedures, the organisation of the team and the information that the response team has gathered and needs to keep actual.

For now, the tabletop exercises for security incidents have been organised within the security team, but there is an obvious advantage in involving the EOSC on a larger scale. The tabletop exercises can be extended to include representatives from the EOSC-Core services to not only better prepare the security incident response team, but to train various parties to react fast and efficiently. As the nature of EOSC is wider, the communication can only be perfected via various training events or simulations involving geographically and logically separate entities.

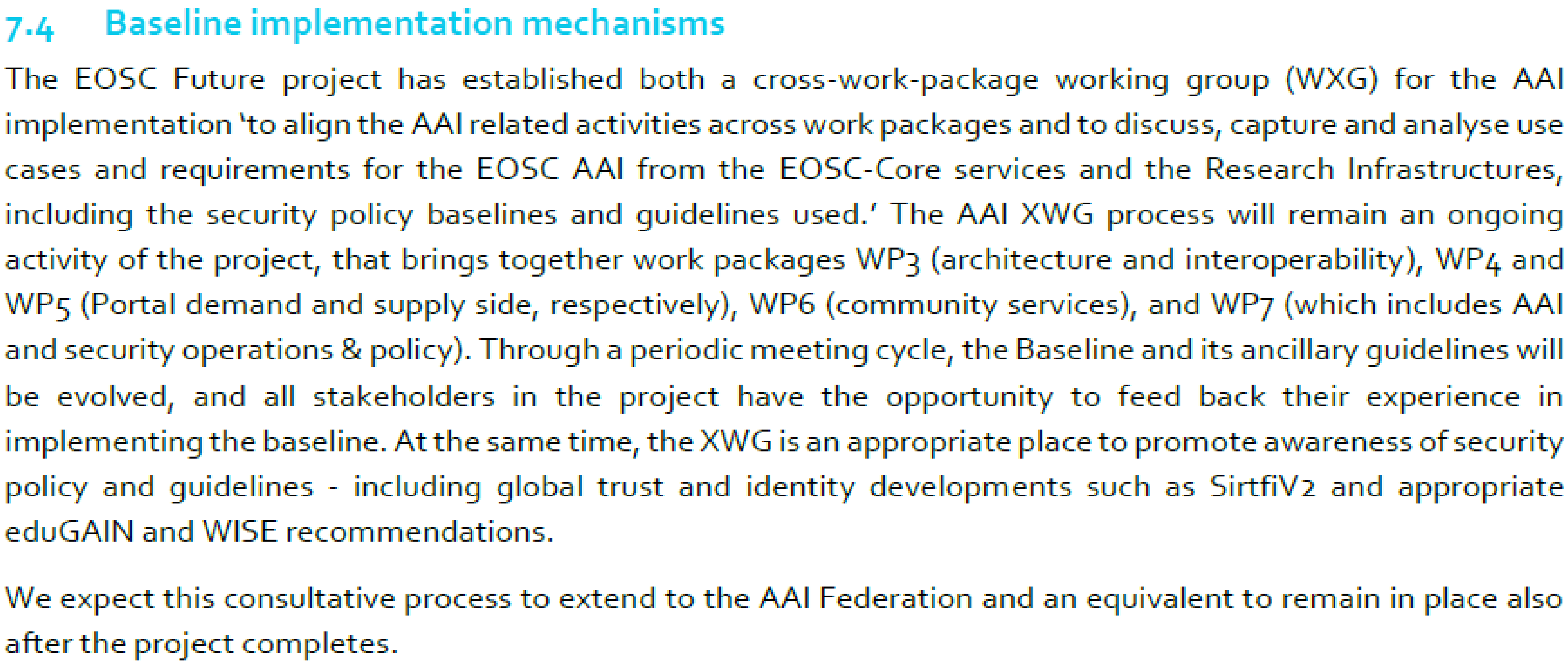


To get full benefits of training and simulation activities, these should be frequent enough. Not only is it impossible to involve all relevant parties every time, as the mere size of the EOSC is a challenge, but realistically the personnel will simply change and the dynamics between teams must be adapted.



Communication challenges have other purposes than just verification of contact data. These provide a good opportunity to gather data about the overall response capabilities of the EOSC. These statistics can provide exact numerical data, which can be compared between challenges organised during years, enabling the EOSC to see changes and trends in exact manner. This may reveal needs for improving co-operation, training and

Baselines



7.4 Baseline implementation mechanisms

The EOSC Future project has established both a cross-work-package working group (WXG) for the AAI implementation '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.' The AAI XWG process will remain an ongoing activity of the project, that brings together work packages WP3 (architecture and interoperability), WP4 and WP5 (Portal demand and supply side, respectively), WP6 (community services), and WP7 (which includes AAI and security operations & policy). Through a periodic meeting cycle, the Baseline and its ancillary guidelines will be evolved, and all stakeholders in the project have the opportunity to feed back their experience in implementing the baseline. At the same time, the XWG is an appropriate place to promote awareness of security policy and guidelines - including global trust and identity developments such as SirtfiV2 and appropriate eduGAIN and WISE recommendations.

We expect this consultative process to extend to the AAI Federation and an equivalent to remain in place also after the project completes.

7.5 Incident mitigation and resolution

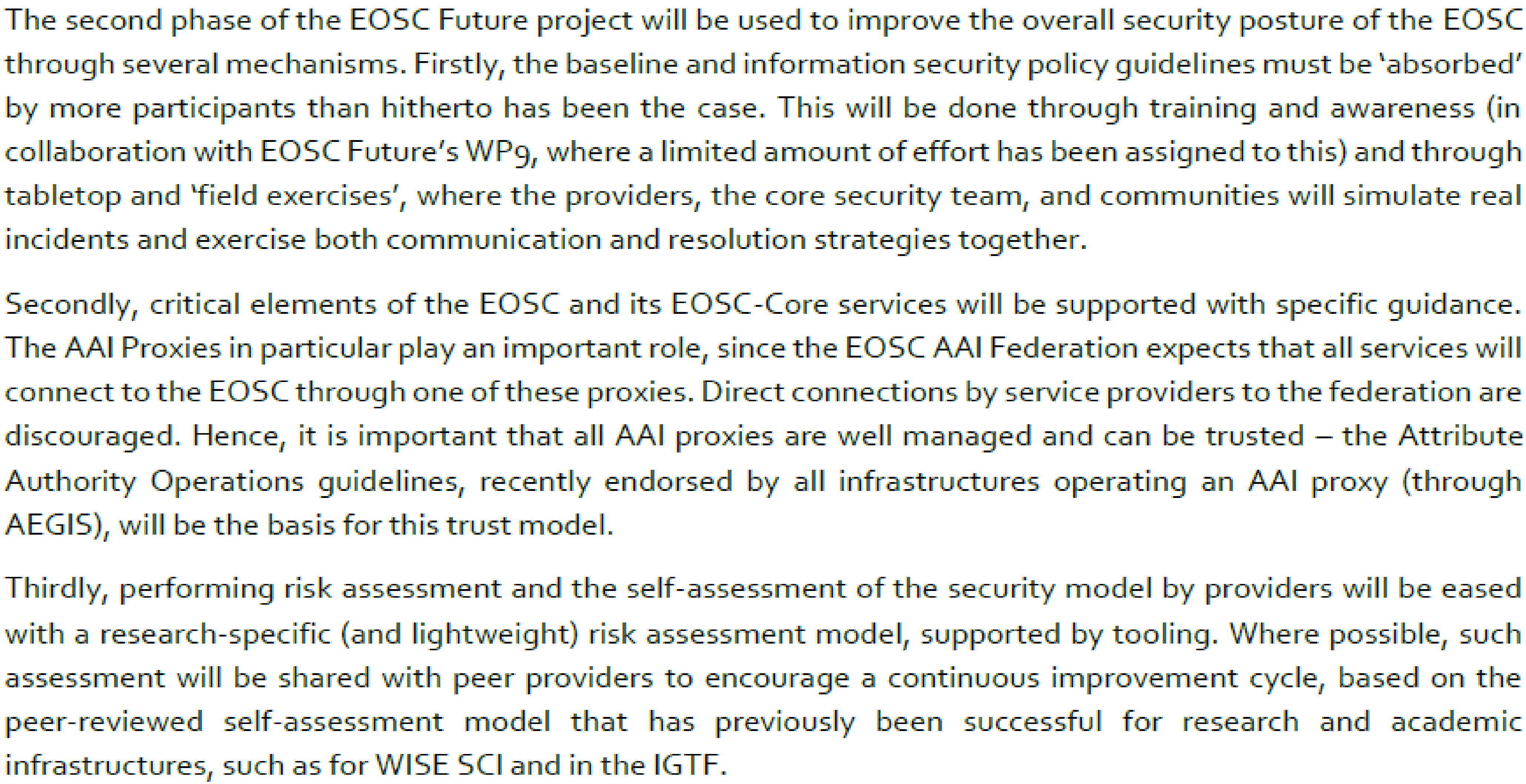
A key part of the development of incident response, mitigation and resolution is ensuring that the entire EOSC constituency that is in scope for the EOSC Security Team is aware of the team's existence, and familiar with the relevant procedures and processes. This can be approached through arranging ongoing discussions between the security team and the EOSC-Core service providers along with regular communication challenges and tabletop exercises as outlined above.

Once the incident procedure for EOSC-Core services is adopted, it will then be appropriate to develop appropriate metrics - learning from experience and reviewing those developed for EOSC-hub - for EOSC security. These should focus on maximising the opportunities for applying lessons learned for the community and empowering EOSC-Core Services and the EOSC Security Team to work most effectively. The EOSC Security Team currently benefits from personal overlap and acquaintance with the security teams from all horizontal e-Infrastructures. These links will be strengthened based on joint incident resolution work as and when such incidents affect the EOSC (the incidence thereof naturally depends on the incidents that occur, and to which extent EOSC resources are involved). Standard operating procedures, guiding the internal operation of the team, will be developed based on both real and mock incidents, and the feedback based on the metrics defined.

Collaborative incident response and resolution is essential in the current security landscape; it is vital that the EOSC Security Team be in a position to work with other distributed security teams to make most use of community threat intelligence and fine-grained security monitoring through the use of facility-based and distributed Security Operations Centres.

During months to come, the aim will be in gathering and ingesting the data about services. In addition to obvious use cases mentioned in section 6.3, this data is vital for assessing status and needs of the services, when preparedness is concerned. It is likely that this data would provide further insight into requirements on the development of security related services, so that they are optimised for EOSC's needs.

What we anticipated in D7.5a



The second phase of the EOSC Future project will be used to improve the overall security posture of the EOSC through several mechanisms. Firstly, the baseline and information security policy guidelines must be 'absorbed' by more participants than hitherto has been the case. This will be done through training and awareness (in collaboration with EOSC Future's WP9, where a limited amount of effort has been assigned to this) and through tabletop and 'field exercises', where the providers, the core security team, and communities will simulate real incidents and exercise both communication and resolution strategies together.

Secondly, critical elements of the EOSC and its EOSC-Core services will be supported with specific guidance. The AAI Proxies in particular play an important role, since the EOSC AAI Federation expects that all services will connect to the EOSC through one of these proxies. Direct connections by service providers to the federation are discouraged. Hence, it is important that all AAI proxies are well managed and can be trusted – the Attribute Authority Operations guidelines, recently endorsed by all infrastructures operating an AAI proxy (through AEGIS), will be the basis for this trust model.

Thirdly, performing risk assessment and the self-assessment of the security model by providers will be eased with a research-specific (and lightweight) risk assessment model, supported by tooling. Where possible, such assessment will be shared with peer providers to encourage a continuous improvement cycle, based on the peer-reviewed self-assessment model that has previously been successful for research and academic infrastructures, such as for WISE SCI and in the IGTF.

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, Pau Cutrina Vilalta, 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

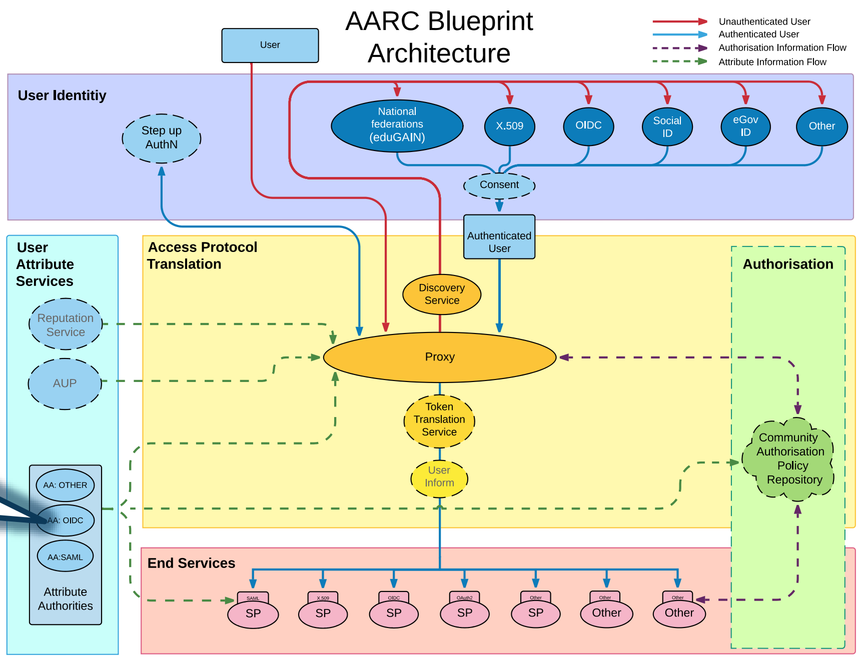
The EOSC Future project is co-funded by the
European Union Horizon Programme call
INFRAEOSC-03-2020, Grant Agreement number 101017536

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



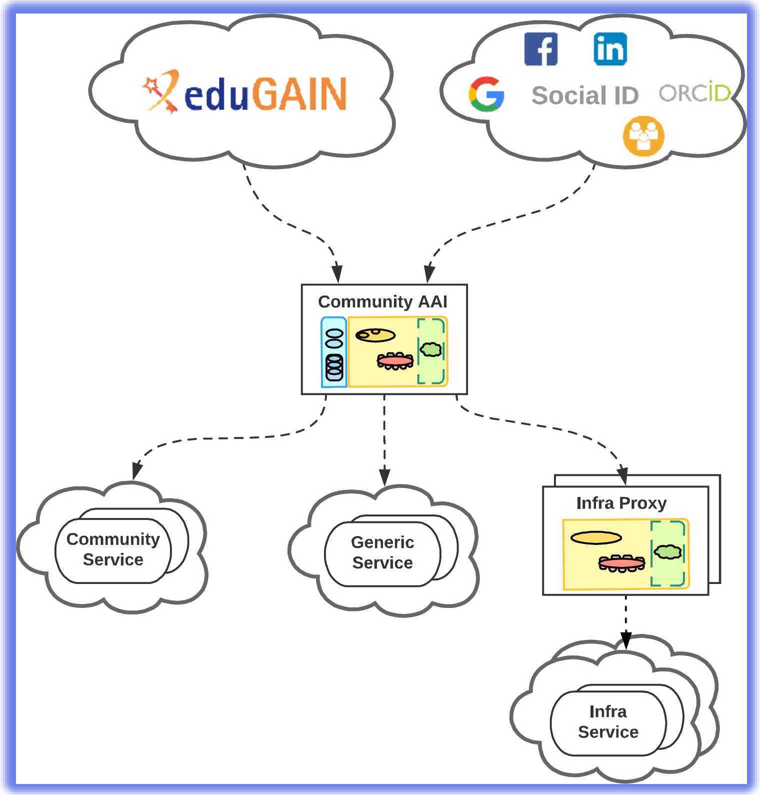
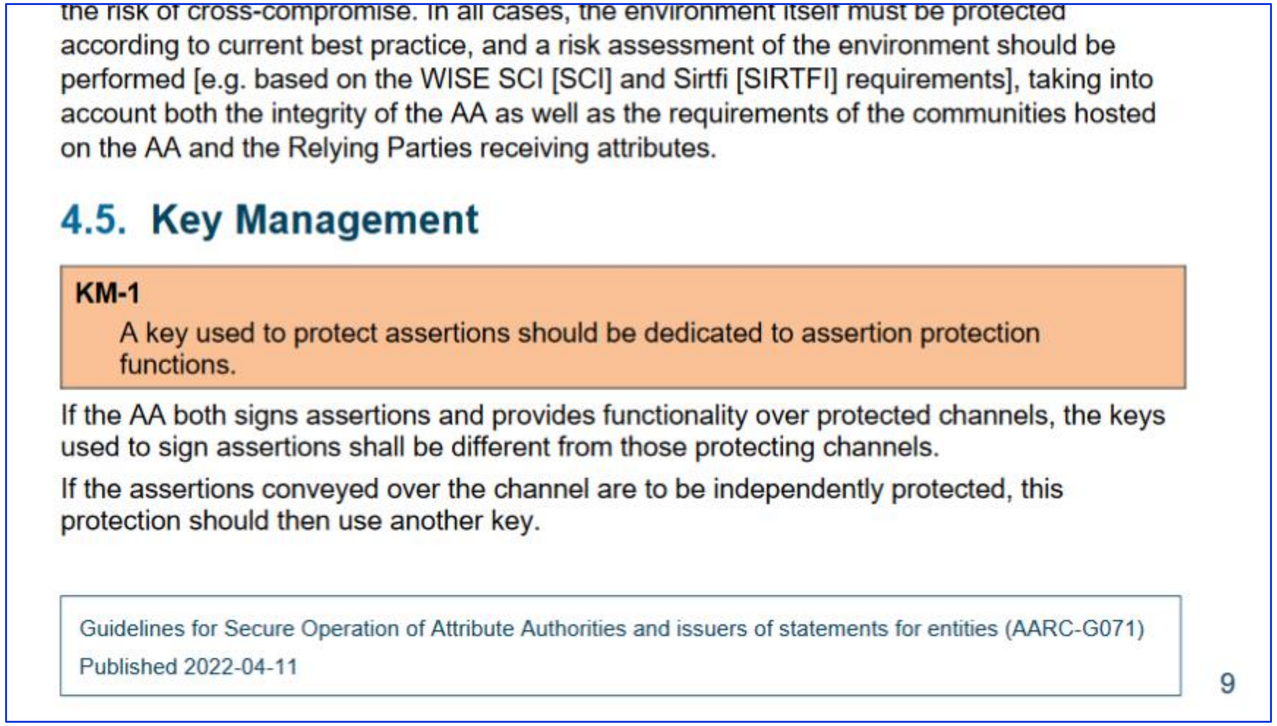


Image source: AARC Community
https://aarc-community.org/architecture/

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

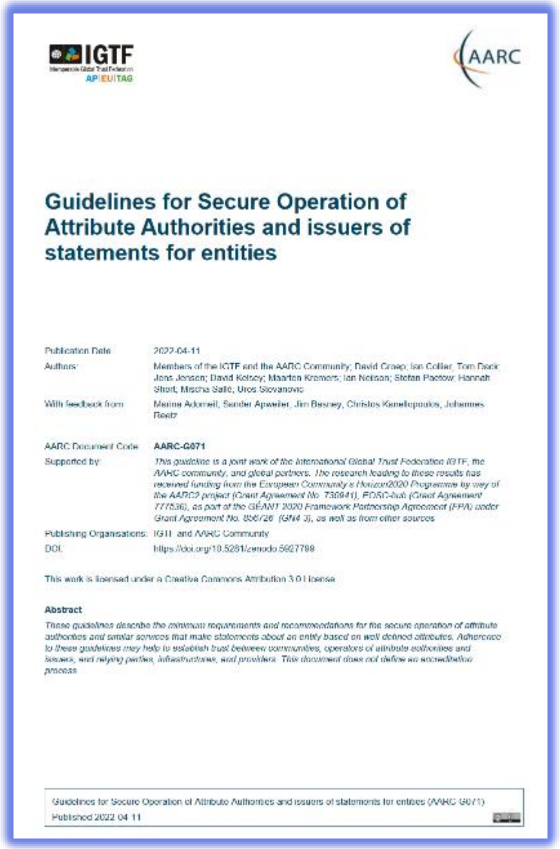
A key used to protect assertions should be dedicated to assertion protection functions.

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



IGTF

AARC

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

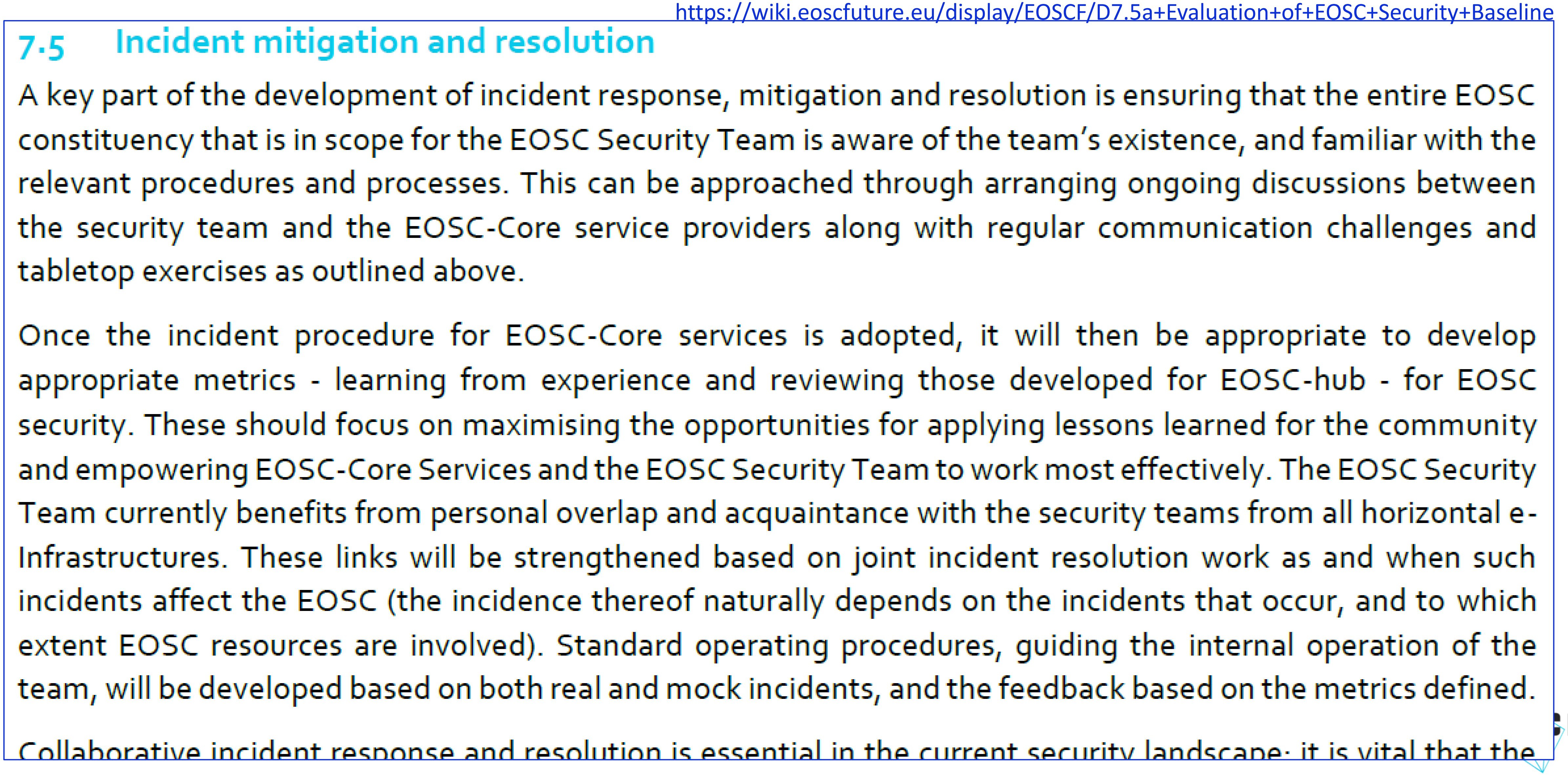
These guidelines describe the minimum requirements and recommendations for the secure operation of attribute authorities and similar services that make statements about an entity based on well defined attributes. Adherence to these guidelines may help to establish trust between communities, operators 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*

For incident response

https://wiki.eoscfuture.eu/display/EOSCF/D7.5a+Evaluation+of+EOSC+Security+Baseline



7.5 Incident mitigation and resolution

A key part of the development of incident response, mitigation and resolution is ensuring that the entire EOSC constituency that is in scope for the EOSC Security Team is aware of the team's existence, and familiar with the relevant procedures and processes. This can be approached through arranging ongoing discussions between the security team and the EOSC-Core service providers along with regular communication challenges and tabletop exercises as outlined above.

Once the incident procedure for EOSC-Core services is adopted, it will then be appropriate to develop appropriate metrics - learning from experience and reviewing those developed for EOSC-hub - for EOSC security. These should focus on maximising the opportunities for applying lessons learned for the community and empowering EOSC-Core Services and the EOSC Security Team to work most effectively. The EOSC Security Team currently benefits from personal overlap and acquaintance with the security teams from all horizontal e-Infrastructures. These links will be strengthened based on joint incident resolution work as and when such incidents affect the EOSC (the incidence thereof naturally depends on the incidents that occur, and to which extent EOSC resources are involved). Standard operating procedures, guiding the internal operation of the team, will be developed based on both real and mock incidents, and the feedback based on the metrics defined.

Collaborative incident response and resolution is essential in the current security landscape; it is vital that the