Information Security Management in EOSC's Future

May 2023

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)

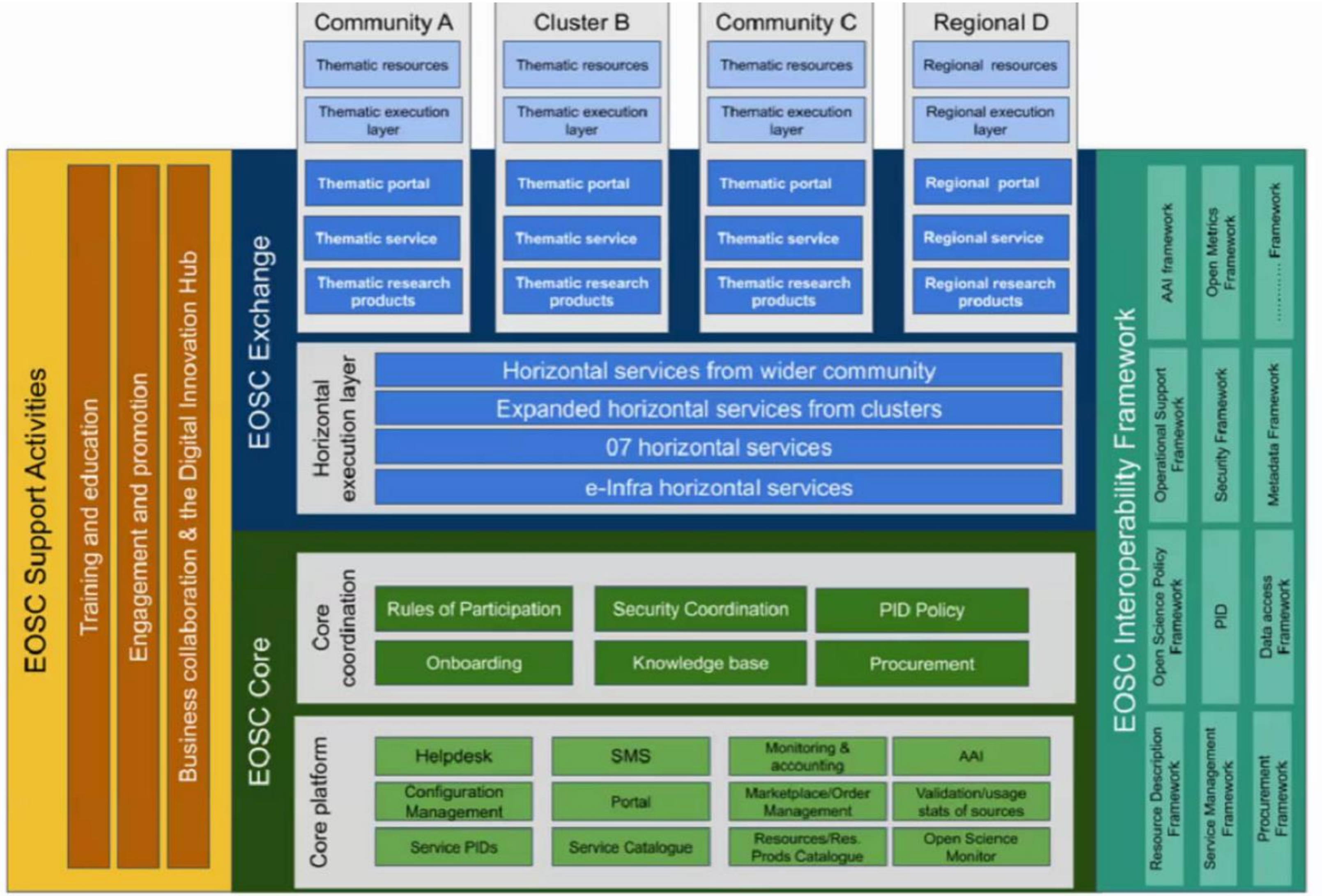
"ensure confidentiality, integrity and availability"

"protecting sensitive data from threats and vulnerabilities"

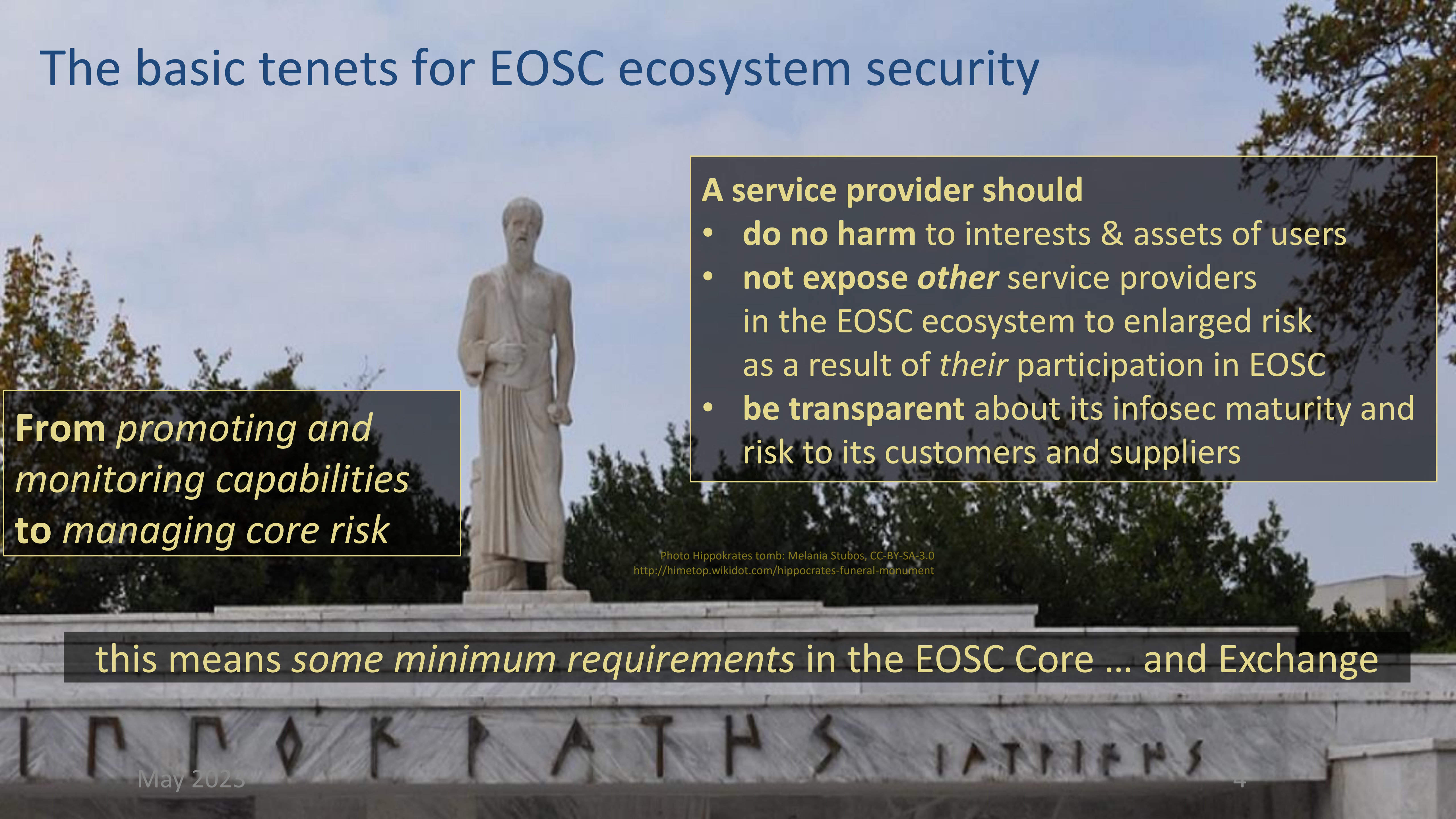
In our heterogeneous EOSC at large, founded on subsidiarity, this translates to

- *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 European Open Science Cloud



The basic tenets for EOSC ecosystem security



A service provider should

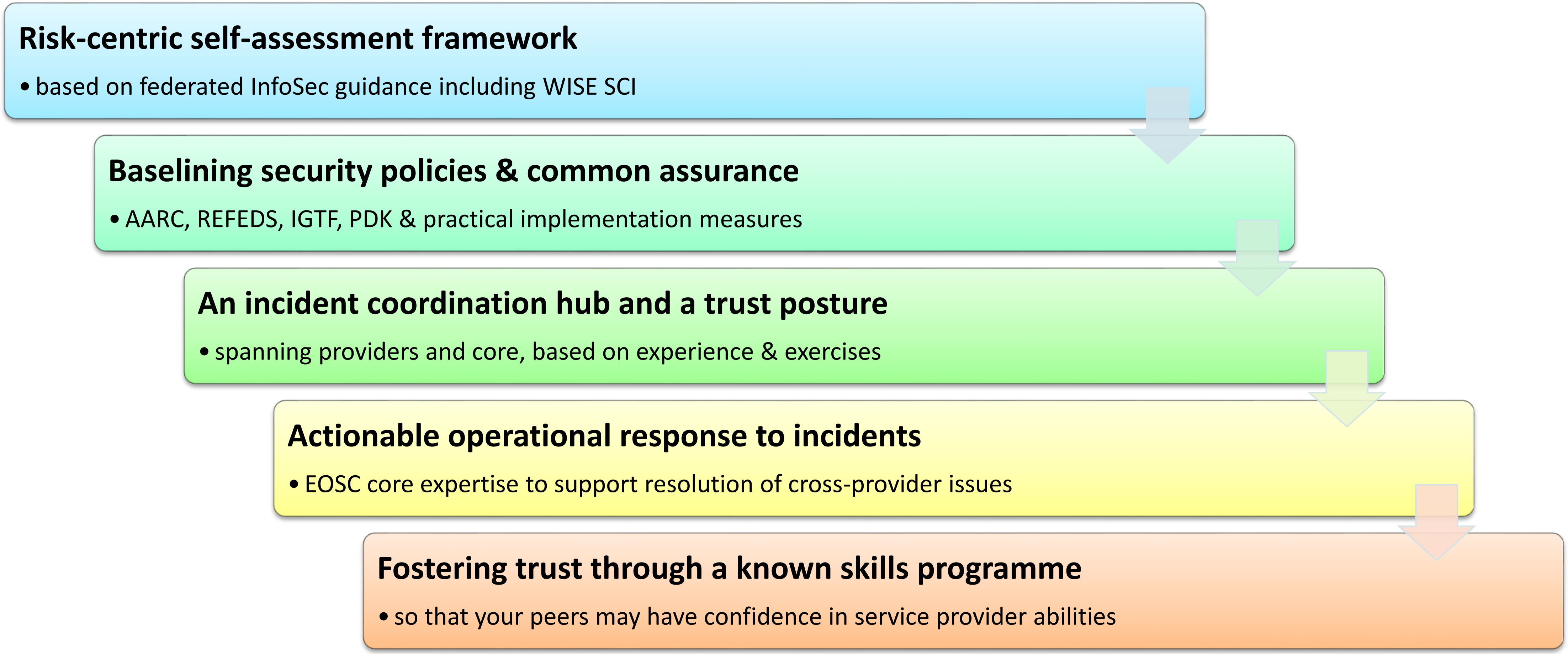
- **do no harm** to interests & assets of users
- **not expose *other*** service providers in the EOSC ecosystem to enlarged risk as a result of *their* participation in EOSC
- **be transparent** about its infosec maturity and risk to its customers and suppliers

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

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

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

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

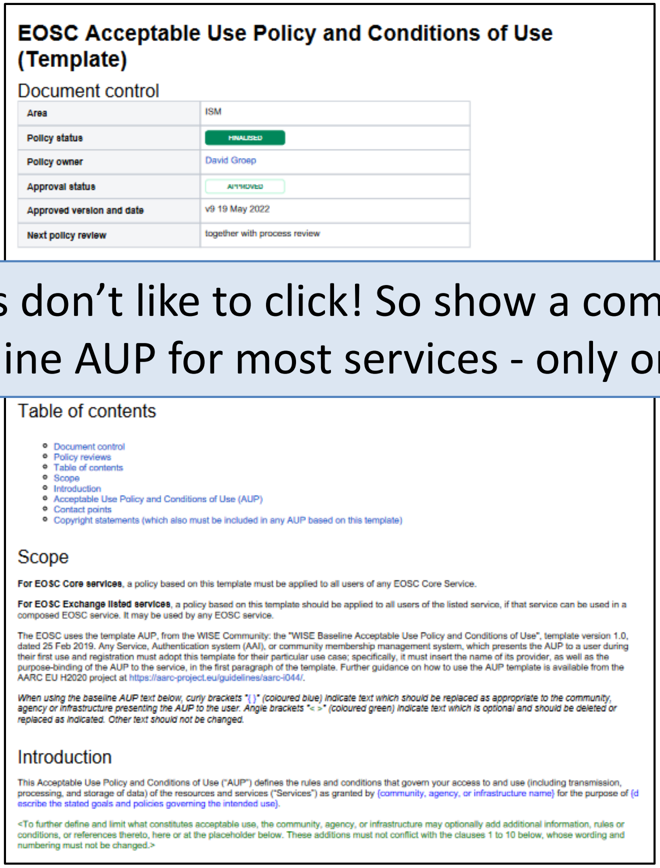
- core service providers are subject to the EOSC Core Agreement, but the operating entities are the primary responsible for their own services
- exchange service providers bring their own (existing) services, and join based on the EOSC *Rules of Participation,* the *On-boarding Agreement,* and the *AAI*

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

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



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/.

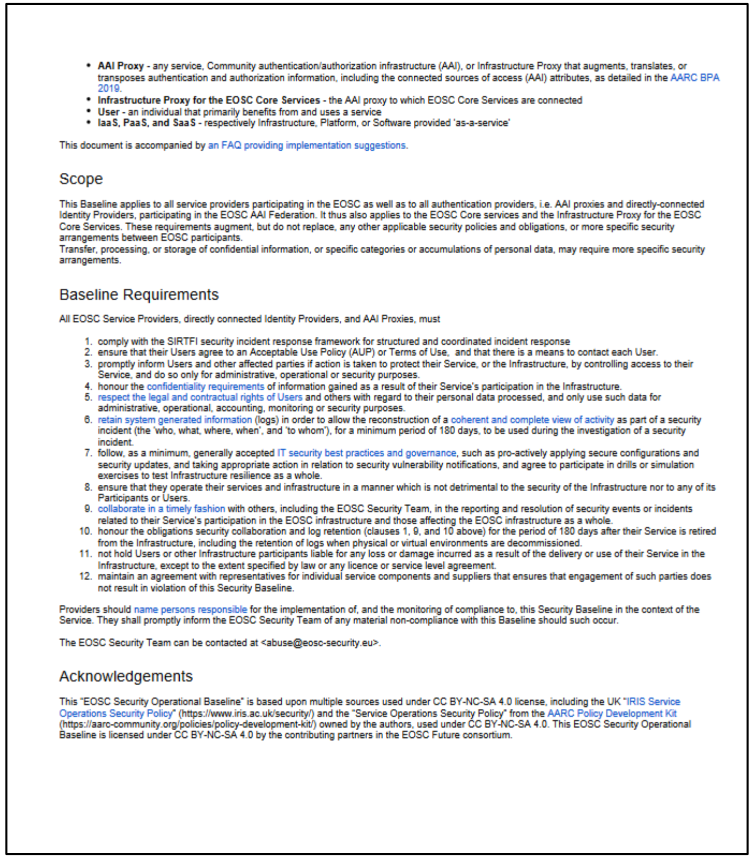
When using the baseline AUP text below, curly brackets "{ }" (coloured blue) indicate text which should be replaced as appropriate to the community, agency or infrastructure presenting the AUP to the user. Angle brackets "< >" (coloured green) indicate text which is optional and should be deleted or 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 {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

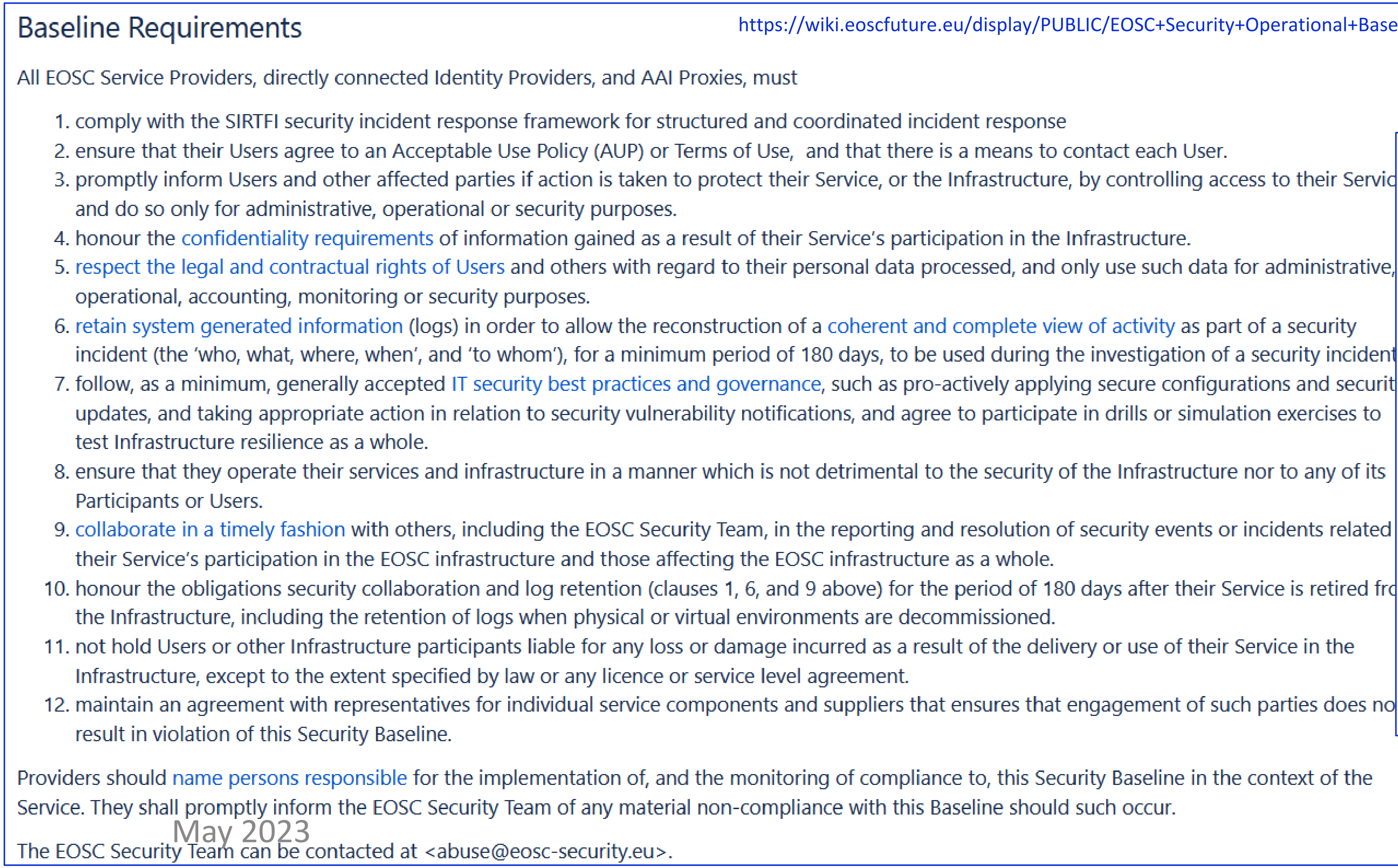
- version based on UK-IRIS evolution of the AARC PDK
- specifically geared towards the looser EOSC ecosystem
- mindful of urgent need for collective coherent response

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
- 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

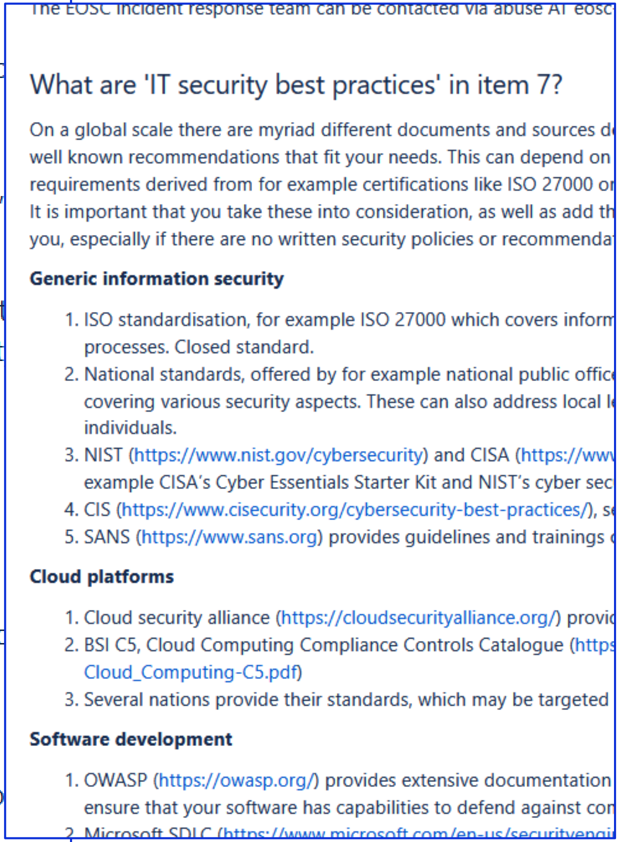
https://wiki.eoscfuture.eu/display/PUBLIC/EOSC+Security+Operational+Baseline

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

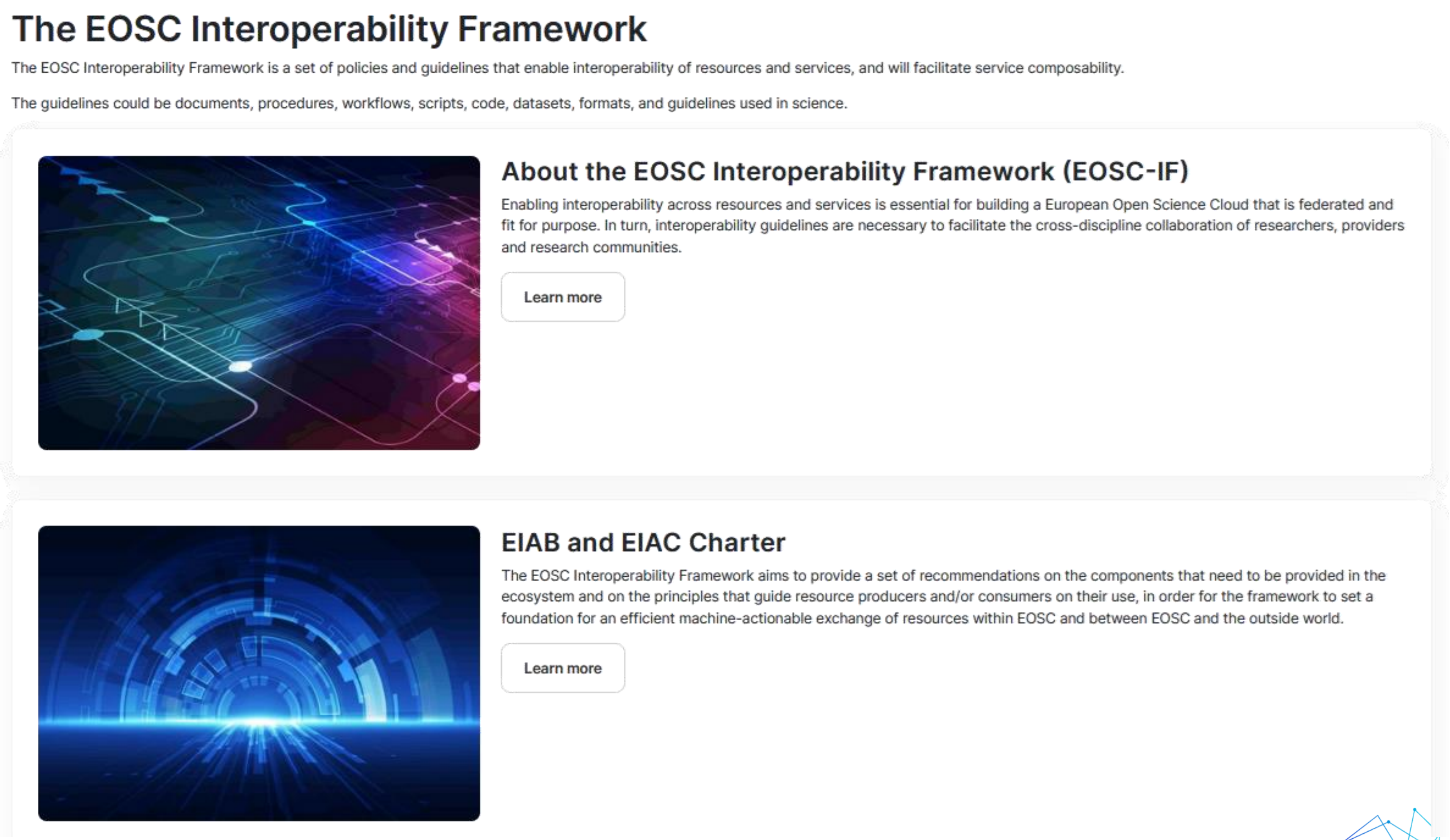
1. ISO standardisation, for example ISO 27000 which covers inform processes. Closed standard.
2. National standards, offered by for example national public office covering various security aspects. These can also address local l individuals.
3. NIST (https://www.nist.gov/cybersecurity) and CISA (https://www 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/) provid
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 con
2. Microsoft SDLC (https://www.microsoft.com/en-us/securityengi



The EOSC Interoperability Framework

The EOSC Interoperability Framework is a set of policies and guidelines that enable interoperability of resources and services, and will facilitate service composability.

The guidelines could be documents, procedures, workflows, scripts, code, datasets, formats, and guidelines used in science.

About the EOSC Interoperability Framework (EOSC-IF)

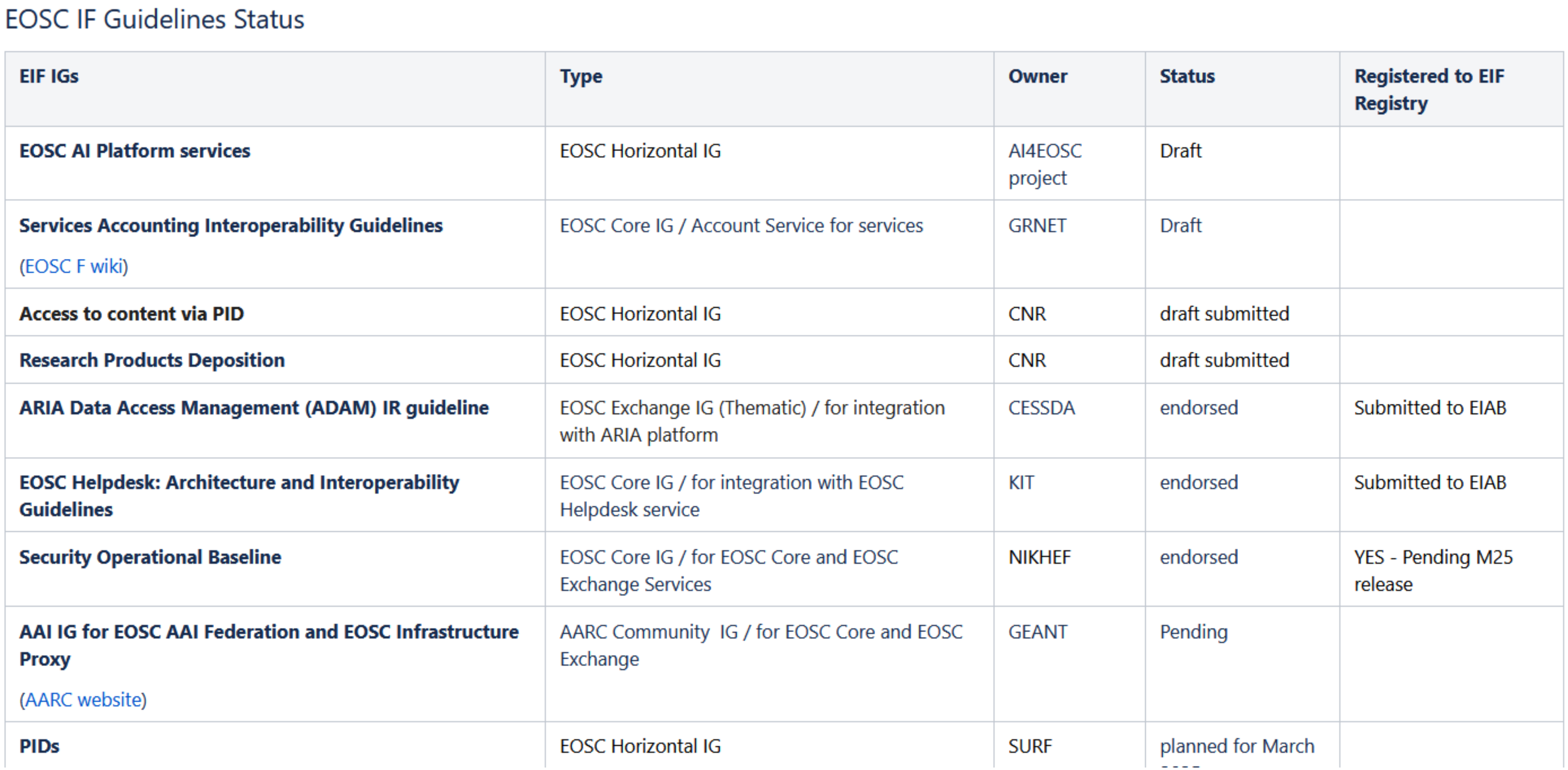
Enabling interoperability across resources and services is essential for building a European Open Science Cloud that is federated and fit for purpose. In turn, interoperability guidelines are necessary to facilitate the cross-discipline collaboration of researchers, providers and research communities.

EIAB and EIAC Charter

The EOSC Interoperability Framework aims to provide a set of recommendations on the components that need to be provided in the ecosystem and on the principles that guide resource producers and/or consumers on their use, in order for the framework to set a foundation for an efficient machine-actionable exchange of resources within EOSC and between EOSC and the outside world.

EOSC Interoperability Framework (processing queue)

This table describes the standards and interfaces already recognised as a starting point for the EOSC Future project and will be built upon to form the EOSC Interoperability Registry.



EOSC IF Guidelines Status

EIF IGs	Type	Owner	Status	Registered to EIF Registry
EOSC AI Platform services	EOSC Horizontal IG	AI4EOSC project	Draft	
Services Accounting Interoperability Guidelines (EOSC F wiki)	EOSC Core IG / Account Service for services	GRNET	Draft	
Access to content via PID	EOSC Horizontal IG	CNR	draft submitted	
Research Products Deposition	EOSC Horizontal IG	CNR	draft submitted	
ARIA Data Access Management (ADAM) IR guideline	EOSC Exchange IG (Thematic) / for integration with ARIA platform	CESSDA	endorsed	Submitted to EIAB
EOSC Helpdesk: Architecture and Interoperability Guidelines	EOSC Core IG / for integration with EOSC Helpdesk service	KIT	endorsed	Submitted to EIAB
Security Operational Baseline	EOSC Core IG / for EOSC Core and EOSC Exchange Services	NIKHEF	endorsed	YES - Pending M25 release
AAI IG for EOSC AAI Federation and EOSC Infrastructure Proxy (AARC website)	AARC Community IG / for EOSC Core and EOSC Exchange	GEANT	Pending	
PIDs	EOSC Horizontal IG	SURF	planned for March	

https://wiki.eoscfuture.eu/display/PUBLIC/EOSC+IF+Guidelines+overview

Planning the rest of EOSCF

For D7.5b in M27 (June 2023)

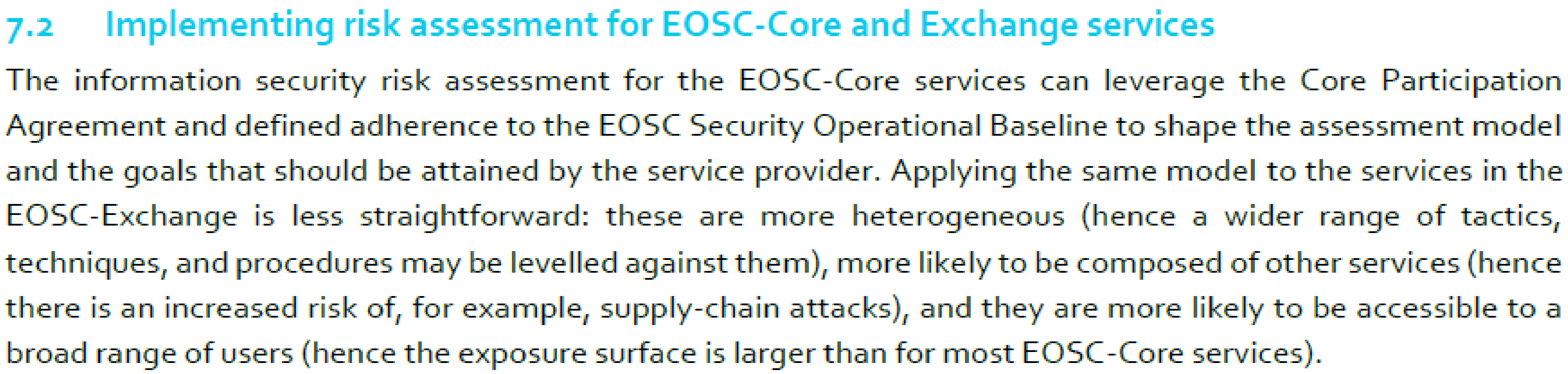
7.1 Policy recommendations: WISE recommendations and the Attribute Authority Secure Operations Guidelines

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.

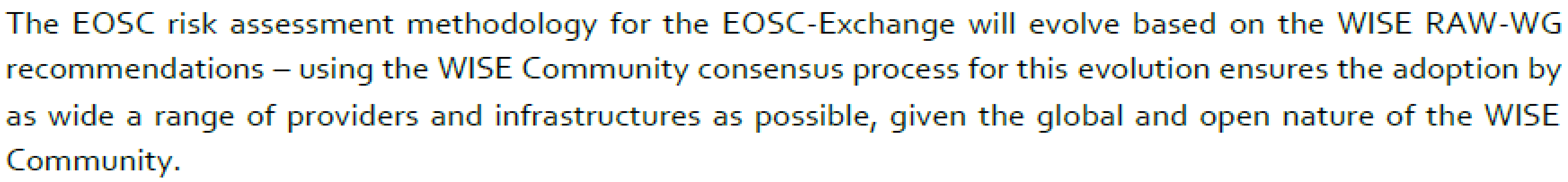
For the AAI Proxy operations, updated technology-agnostic guidance has recently been released by the AARC Engagement Group for e-Infrastructures (AEGIS) on how to best structure operational security and attribute authority integrity for both the proxies themselves as well as for their associated attribute 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 …



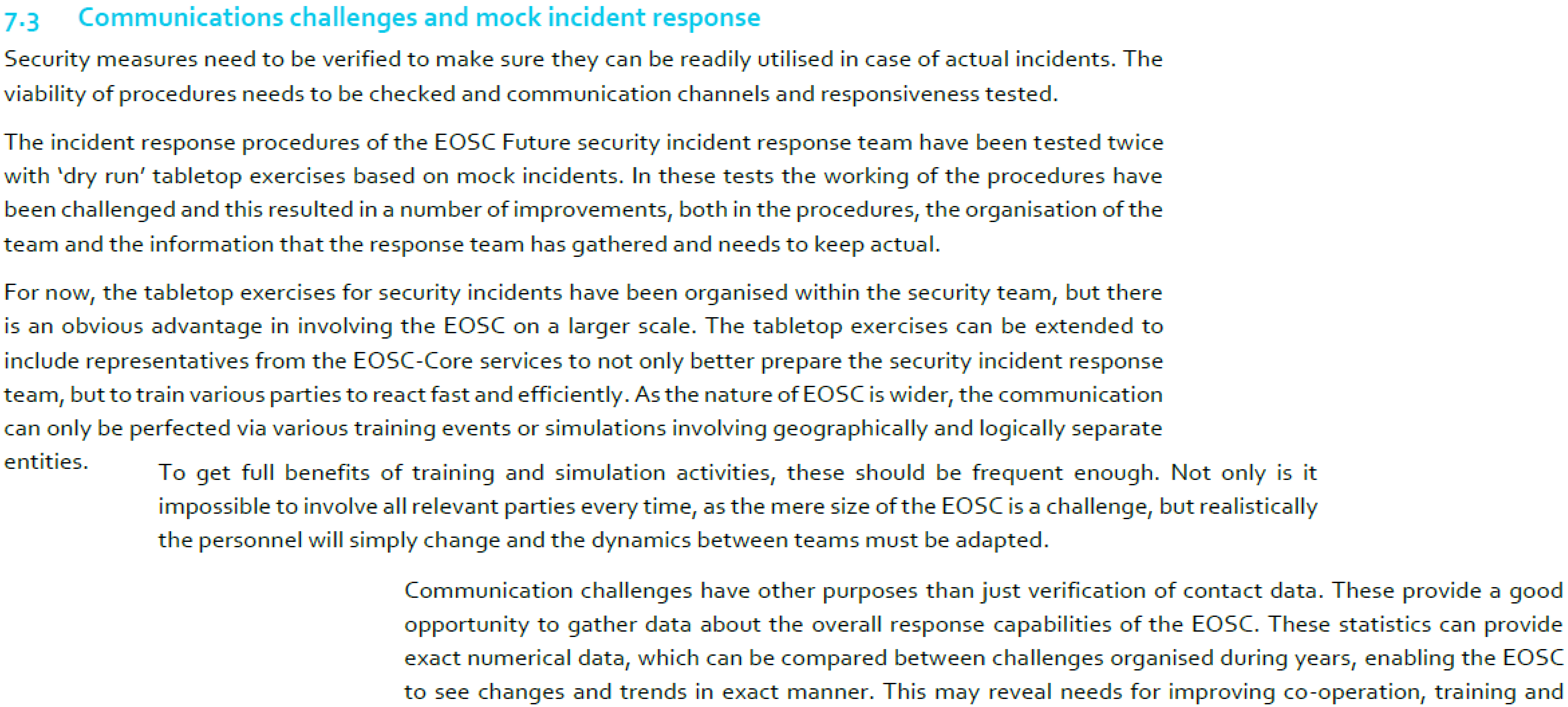
7.2 Implementing risk assessment for EOSC-Core and Exchange services

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.

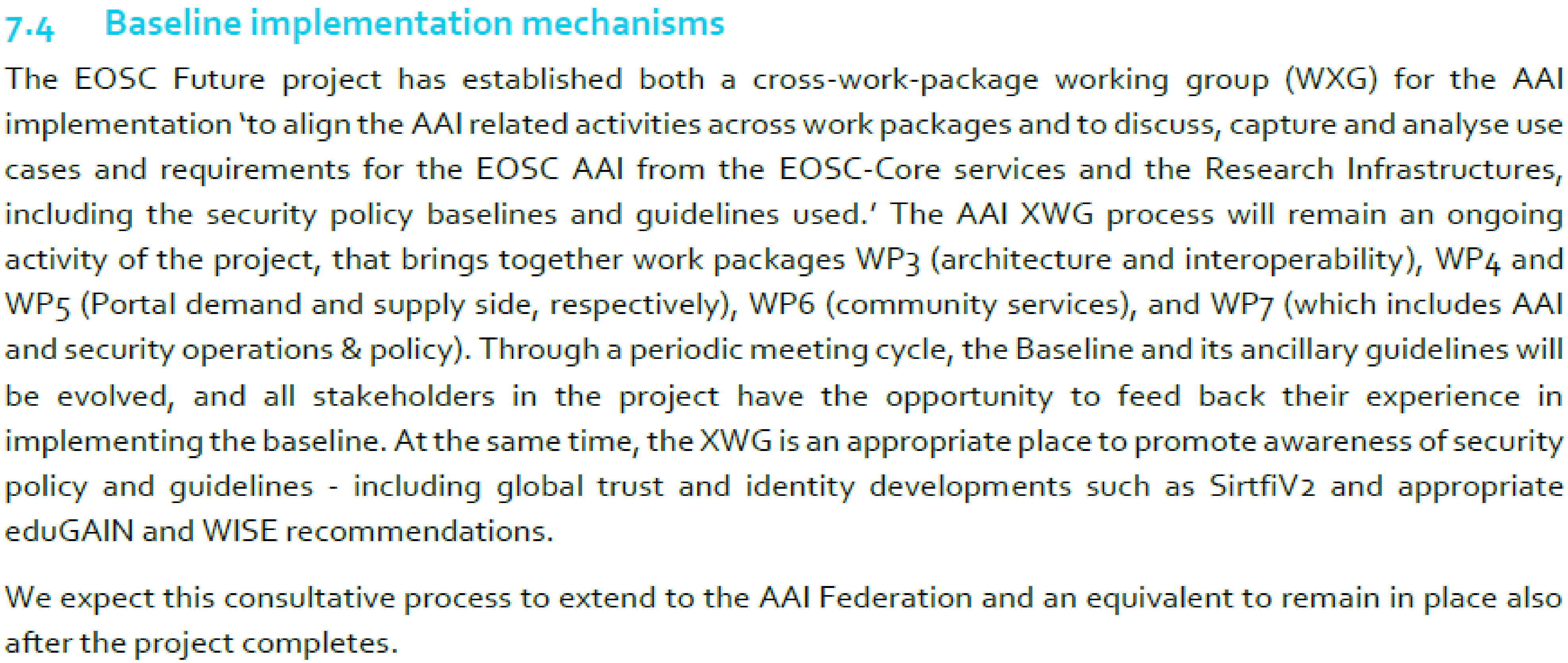
The incident response procedures of the EOSC Future security incident response team have been tested twice with 'dry run' tabletop exercises based on mock incidents. In these tests the working of the procedures have been challenged and this resulted in a number of improvements, both in the procedures,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

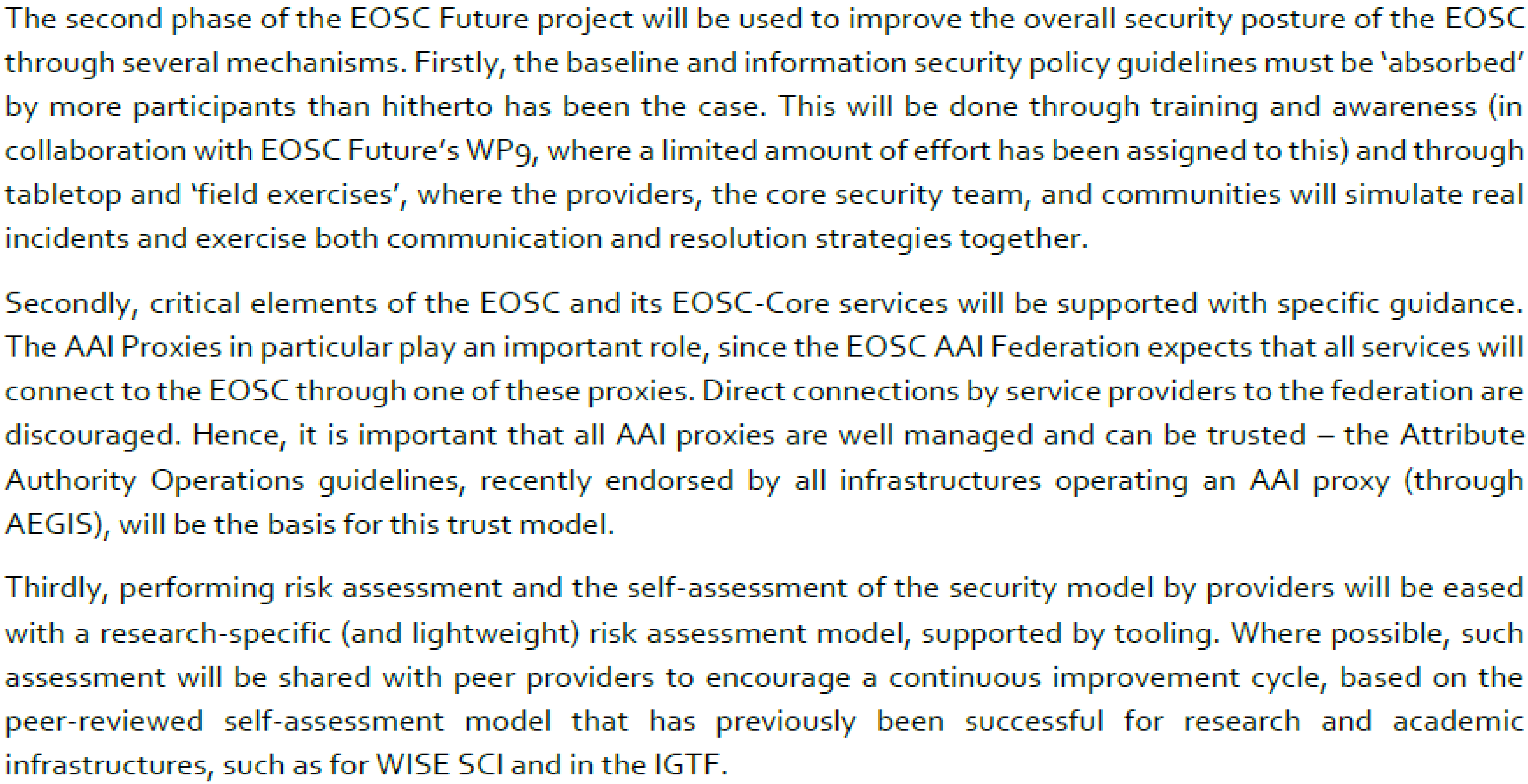
A key part of the development of incident response, mitigation and resolution is ensuring that the entire EOSC constituency that is in scope for the EOSC Security Team is aware of the team's existence, and familiar with the relevant procedures and processes. This can be approached through arranging ongoing 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

Current status

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