EOSC Future

D7.5a

Evaluation of EOSC Security Baseline and Operational Security Experience, and Recommendations for Security Evolution

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

Version 1.0
May 2022

D7.5a / Evaluation of EOSC Security Baseline and Operational Security Experience, and Recommendations for Security Evolution

Lead by **Nikhef (NWO-I) by way of EGI.eu**

Authored by David L. Groep (Nikhef NWO-I), Linda Cornwall (STFC RAL), David Crooks (STFC RAL), Baptiste Grenier (EGI.eu), Urpo Kaila (CSC), David Kelsey (STFC RAL), Pinja Koskinen (CERN), Daniel Kouřil (CESNET), Alf Moens (GÉANT), Ralph Niederberger (FZJülich)

Reviewed by Paul Gondim van Dongen (SURF) & Athanasia Spiliotopoulou (JNP)

Dissemination Level of the Document

Public

Abstract

The development of trust, operational security policy and incident response of the EOSC-Core and EOSC-Exchange services are discussed, and how their constituent elements – information security management, baseline security policies and guidelines, risk assessment models, and incident response and resolution – have been defined. The information security model for the EOSC is based around subsidiarity of security maturity, monitoring, and incident response, but with a core incident response coordination team, which provides actionable support for the core services. The same team ensures a coordinated response for incidents in compose and distributed EOSC services and is linked to the global academic and research security community.

The evolution of operational security during the EOSC Future project is laid out by identifying the three primary challenges: increasing awareness and maturity of security posture within the providers connecting to the EOSC, specific topic guidance for critical elements for composite services (including attribute authority and AAI proxy operations) and supporting IT risk self-assessment and definition of controls by means of risk-management tooling.

The EOSC Security Incident Coordination, also supporting the incident response for the EOSC-Core services, remains a central part of the operational security activities.

Version History

Version	Date	Authors/Contributors	Description
V0.1	10/03/2022	David L. Groep (Nikhef NWO-I)	Structure and foundational text
V0.7	02/05/2022	David L. Groep (Nikhef NWO-I), Linda Cornwall (STFC RAL), David Crooks (STFC RAL), Baptiste Grenier (EGI.eu), Urpo Kaila (CSC), David Kelsey (STFC RAL), Pinja Koskinen (CERN), Daniel Kouřil (CESNET), Alf Moens (GÉANT), Ralph Niederberger (FZJülich),	Version submitted for EOSCF internal QA
V0.8	20/05/2022	David L. Groep (Nikhef NWO-I), Linda Cornwall (STFC RAL), David Crooks (STFC RAL), Baptiste Grenier (EGI.eu), Urpo Kaila (CSC), David Kelsey (STFC RAL), Pinja Koskinen (CERN), Daniel Kouřil (CESNET), Alf Moens (GÉANT), Ralph Niederberger (FZJülich)	Revised version incorporating comments provided by the reviewers
V0.9	23/05/2022	David L. Groep (Nikhef NWO-I), Linda Cornwall (STFC RAL), David Crooks (STFC RAL), Baptiste Grenier (EGI.eu), Urpo Kaila (CSC), David Kelsey (STFC RAL), Pinja Koskinen (CERN), Daniel Kouřil (CESNET), Alf Moens (GÉANT), Ralph Niederberger (FZJülich), Athanasia Spiliotopoulou (JNP)	Version for circulation to the consortium for information and possible feedback
V1.0	27/05/2022	David L. Groep (Nikhef NWO-I), Linda Cornwall (STFC RAL), David Crooks (STFC RAL), Baptiste Grenier (EGI.eu), Urpo Kaila (CSC), David Kelsey (STFC RAL), Pinja Koskinen (CERN), Daniel Kouřil (CESNET), Alf Moens (GÉANT), Ralph Niederberger (FZJülich), Athanasia Spiliotopoulou (JNP) Ron Dekker (TGB), Mike Chatzopoulos (ATHENA)	Final Version submitted to EC

Copyright Notice

Table of Contents

Glossary 3
List of Abbreviations 3
1 Executive Summary 4
2 Introduction 5
3 Information Security Model and the Security Assets 6
4 EOSC Security Operational Baseline 8
4.1 EOSC Security Operational Baseline consultation process 9
4.2 Implementation of the baseline 9
4.3 EOSC WISE Baseline AUP 10
5 Risk assessment for EOSC service or resource providers 12
6 Security Incident Response 13
6.1 What is a security incident for the EOSC 13
6.2 Incident Response process and the core security team 14
6.3 Gathering critical infrastructure information and ensuring freshness 14
7 Evolving the information security for EOSC 15
7.1 Policy recommendations: WISE recommendations and the Attribute Authority Secure Operations Guidelines 15
7.2 Implementing risk assessment for EOSC-Core and Exchange services 15
7.3 Communications challenges and mock incident response 16
7.4 Baseline implementation mechanisms 17
7.5 Incident mitigation and resolution 17
8 Conclusions 18
Appendix A – The EOSC Security Operational Baseline 19
References 21

Glossary

EOSC Future project Glossary is incorporated by reference: https://wiki.eoscfuture.eu/x/JQCK

List of Abbreviations

Acronym	Definition
AAI	Authentication and Authorisation Infrastructure
AARC	Authentication and Authorisation for Research Collaboration
AEGIS	AARC Engagement Group for e-InfrastructureS
AUP	Acceptable Use Policy
CSIRT	Computer Security Incident Response Team (also known as a 'CERT', i.e., a Computer Emergency Response Team)
eduGAIN	EDUcation Global Authentication INfrastructure (R&E interfederation service)
IdP	Identity Provider (source of authentication and attributes in an AAI interaction)
IGTF	Interoperable Global Trust Federation
ISM	Information Security Management
NREN	National Research and Education Network organisation
OP	OpenID Provider (source of authentication and claims in an AAI interaction)
OSCRP	Open Science Cyber Risk Profile
PDK	Policy Development Kit
R&E	Research and Education
RAW-WG	Risk Assessment WISE Working Group (see also: WISE)
RP	Relying Party
SCI	Security for Collaborating Infrastructures (WISE working group)
Security Baseline	Set of minimum security controls defined for an information system that has been established through information security strategic planning activities (herein also 'baseline', see e.g. https://csrc.nist.gov/glossary)
SIG-ISM	Special Interest Group on Information Security Management (GÉANT)
SQAaaS	Software Quality Assurance as-a-Service
SMS	Service Management System
SP	Service Provider (relying party in an AAI interaction)
TCB	Technical Coordination Board
WISE	WISE Information Security for E-infrastructures community
XWP WG	Cross-Work-Package Working Group

1 Executive Summary

The operational security of the EOSC ecosystem and the information security management process of its core services are centred on a risk-assessment methodology and an incremental mechanism of defining a baseline: the initially established set of minimum security controls. These can be either mandatory for EOSC-Core services, or as community good practice guidelines for the services listed in the EOSC-Exchange, complemented by an incident response and coordination scheme comprised of operational security and forensics analysis experts. In the EOSC 'system-of-systems' scheme, with composite services and dynamic dependencies between the services, a conventional approach to information security management (defining the list of assets, performing a risk assessment for each of these, and then implementing specific controls) is not a scalable mechanism. Hence, the EOSC security model emphasises risk assessment at the service edge, loosely based on the 'do no harm' principle: EOSC participants, services, and datasets should not intentionally alter the risk profile of other services in the EOSC without prior agreement.

For the EOSC security model, services (including the digital objects contained therein), are considered the 'assets' in need of protection, and the central security team considers services to be autonomous and in principle capable of managing their own security. Yet, participation in the EOSC brings challenges in collective service provisioning, and in case of an incident, only a coordinated response of all affected services will be effective in mitigating the impact and resolving the security breach. Hence, the EOSC security team provides central coordination, a communication model, and practical support across all EOSC participants. For the EOSC-Core services, whose confidentiality, integrity, and availability are foundational for EOSC service provisioning, the central security team in addition provides analysis, forensics, and intervention support – based on the policies and procedures of the information security management system [10] for the EOSC-Core services.

While the asset definitions, the EOSC Security Baseline, and the incident response process (being the most urgent in case of detected incidents), as well as a simplified risk assessment model, have been defined in the first phase of the project, having the documents in place obviously does not guarantee a secure system. Collecting security-relevant information from both EOSC-Core and EOSC-Exchange services has identified variations in information security maturity level that need to be addressed.

The evolution of the security activities will address the gaps identified in the ecosystem: practical support for risk assessment by EOSC services through dialogues and a set of closed-question targeted interviews using the example risk assessments as a reference. For services in the EOSC-Exchange, where the EOSC Security Baseline is to be seen as the community best practice, documented alignment of the existing service and infrastructure security practices with the EOSC Security Operational Baseline will be pursued. The widely endorsed 'WISE Community SCI (Security for Collaborating Infrastructures)' framework will be used as the basis for that common trust.

Monitoring of the security of the EOSC-Core services, and responding to security incidents and emergent threats, will remain a key element of the EOSC security activities. The readiness-posture activities, in the form of 'communications challenges' and response to mock incidents, will continue to ensure all EOSC participants are ready to respond.

2 Introduction

The trope 'security is only so strong as its weakest link' has been so frequently repeated that its urgency and relevance is nowadays often lost. Yet for the EOSC, with its aims to link together research portals, resources and services in a web of data and services, security and trust does not stop at the boundary of services, but necessarily extends between the services in the EOSC-Core, and between EOSC-Core and EOSC-Exchange, as well as involving research community services from which the trust in users ultimately flows.

The diverse multi-stakeholder landscape of the EOSC has been a driving factor in the design of the information security management (ISM) framework that the project has set up for both EOSC-Core and EOSC-Exchange services. This leads to a set of guiding principles driving the operational security activities and the security baseline:

- The Hippocratic principle of 'primum non nocere' – those participating in the EOSC should pose no intentional risk to any other participant by their participation and must not change the risk to which other participants in the EOSC are exposed without mutual consent.
- Differentiate between 'EOSC-Core' service and 'EOSC-Exchange' services (those listed in the portal and contributed by the research clusters).
- Participants are autonomous, but subscribe to the shared commitment of maintaining a trustworthy and secure EOSC, and thus agree to collaborate to reduce the adverse effects of security incidents and mitigate their detrimental effect on the EOSC and its participants.
- EOSC-Core services, which have a pivotal and exclusive role in the operation of the EOSC, are bound more tightly to security controls, for which they are supported directly by the central operational security team in case of incidents.

These principles are reflected in the structure of the operational security activities in EOSC Future (and likewise in the structure of this document). It also provides the rationale for supporting different information security maturity levels between the various parties in the EOSC. While for EOSC-Core services adherence to the EOSC Security Baseline is thus a mandatory pre-condition for, e.g. connecting to the EOSC-Core AAI Proxy, it is positioned as a 'community best practice' guideline for services in the EOSC-Exchange. Yet also there, its implementation may be mandated by the research communities and e-Infrastructures themselves so as to strengthen their own security posture – and for that, the EOSC Security Operational Baseline has been co-developed in close coordination with the global WISE community and with inputs from many of these infrastructures.

In addition to services, datasets also have specific security requirements, and face a variety of threats. However, datasets and their associated meta-data do not exist *in vacuo*, but are resident in repositories, storage systems, and processing environments. Thus, while the risk assessment for datasets is determined by the confidentiality, integrity, and availability requirements of the data itself, the controls that are used to mitigate risks are applied to the services that host and process such data. Hence, the operational security baseline, and the controls and response mechanisms implemented in the project, target the services and their controls.

With the diversity of data accessible through the EOSC, the risk assessment of datasets is also most appropriately conducted by the managers of the datasets and domain experts. The risk assessment methodology is to a large extent common to both services and data, and threats to services are also a threat to the data contained within them, but in the first phase of the project, the risk assessment methodology primarily targets services. In this, the methodology follows the community best practice model developed by the WISE Information Security for e-Infrastructures community (through the WISE RAW-WG), tailored to the EOSC environment and emphasising its cross-service risks. Application of the framework – potentially evolved from this first version to cater also for more abstract data security – to specific data classes will intentionally remain the remit of the research infrastructures and data managers, who are the only ones qualified to assess the value and security requirements of such datasets.

3 Information Security Model and the Security Assets

The EOSC Information Security model follows the subsidiarity principle. For the EOSC-Core services in EOSC Future, this means that although all EOSC-Core services collectively provide the requisite EOSC functionality, each of the services is provided by a service provider governed by an understanding of what such 'Core Participation' entails. Each provider is responsible for operating and maintaining their service in a secure manner and is the primary responsible entity in case of (suspected) security incidents. The EOSC-Core security team and the Security Incident Coordinator can and will provide contact, response, mitigation, and (forensic) analysis for such incidents, but will do this in alignment with the service provider's organisation and its computer security staff.

For the services in the EOSC-Exchange, subsidiarity is even stronger: their attachment to the EOSC is controlled by the Rules of Participation and – when they need to connect to the AAI federation – by the EOSC AAI Federation Participation Policy[2] . To the EOSC Operational Security Team they appear as self-managed entities, with defined information security characteristics (an AUP, a security contact endpoint, potentially with security standards certification and quality seals, or a privacy notice). Although services will likely be connected through an infrastructure or community (in terms of the AAI, they connect to an AAI proxy operated by or on behalf of a community or infrastructure), and some may be addressed collectively through their infrastructure federation, generally they appear as single entities.

Based on the EOSC structure, it is appropriate to identify the service as the basic unit of asset management in the EOSC Information Security Management system. This follows the model established for EOSC-hub, where this concept has first been explored for the services governed by the Service Management System (SMS).

The EOSC Information Security Management (ISM) system has been based on EOSC-hub and subsequently evolved for application to the EOSC-Core Services. The initial version from EOSC-hub[3] comprised three ISM policies (a service operations policy putting security requirements on participating providers; a policy requiring informing the user of the acceptable use and conditions of use; and a 'top-level' policy outlining the basic security requirements for providers, and giving authority for specific actions to the security incident response team). There were also six specific procedures defined, detailing the response process, intra-service software vulnerability management, asset risk management and controls definition and the approval process for policies. The evolution to the EOSC SMS included a critical re-appraisal of the policy and procedures. From the three ISM policies in effect in EOSC-hub:

- The EOSC Security Operational Baseline replaces the service operations policy. This indicates a change from setting specific requirements on the implementation and operation of the services involved to an approach of governing the functional requirements on the services. Services (including the EOSC-Core services) are appreciated as (semi-)opaque entities. These have to meet or exceed specific requirements on integrity, response time, having documented procedures and contact points that can be probed from the outside. For services in the EOSC-Exchange, the EOSC Security Operational Baseline acts as a community best practice guideline rather than a mandatory requirement.
- The policy on 'Acceptable Use Policy and Conditions of Use' was already well established based on the WISE Baseline AUP[4] . Besides minor textual changes this ISM policy has been incorporated as-is.
- The 'top-level' policy, as written for EOSC-hub, was based on the assumption that there is a limited number of infrastructures that are responsible for all services, and that the project (in that case EOSC-hub) is responsible for all of these. This assumption does not hold in the EOSC in general, and hence this policy has been withdrawn for the time being. The key element of this policy was to give authority to the CSIRT at a central level to take immediate mitigating technical measures in case of a security incident, and have such measures take effect within the individual services. In the EOSC subsidiarity model, for the EOSC-Core service such authority is to be exercised only in coordination with the EOSC-Core service providers and is most appropriately granted in the Core Participation Agreement. For services in the EOSC-Exchange, the application of controls will be at the portal (and where possible) at the EOSC AAI federation level but will not be exercised within the services. A further evolution of the EOSC SMS may withdraw this policy entirely, but it is retained for the moment since the text does contain useful definitions and context for service providers.

The ISM Procedures in EOSC-hub targeted both target-oriented policies (such as incident response, vulnerability management) as well as project-internal procedures (such as the procedure to adopt new ISM policies in EOSC-hub). All of these procedures are being re-evaluated for the EOSC SMS, emphasising those procedures with direct target-oriented effects:

- The EOSC-hub 'Software Vulnerability Handling procedure' has been withdrawn. In the EOSC subsidiarity model, the handling of software vulnerabilities (rather than service vulnerability) is a responsibility of the service provider, since only they know the software and platform that is being employed to offer a service. While handling software vulnerabilities is an extremely important aspect of security, and many of the operational security incidents can be traced to the continued deployment of vulnerable software and exposing unpatched systems to the internet, the procedures to handle software vulnerabilities are service specific. The EOSC Security Operational Baseline therefore specifically highlights the need for 'pro-actively applying secure configurations and security updates, and taking appropriate action in relation to security vulnerability notifications' (item 7 therein). The service providers and infrastructures offering services should implement and monitor software vulnerability handling through their own service management system. However, since the constituent assets of the EOSC are services, not software, a software vulnerability handling procedure is not applicable. Rather, follow-up and assessment of service vulnerability is a component of the security risk management process.
- The Security Incident Response Procedure was evolved (from the EOSC-hub version) to match the new EOSC Security Operational Baseline policy for EOSC-Core services. The incident response process implemented is extensively described in section 6 ('Security Incident Response') and the resulting procedures are included in the ISM system as the ISM1 Procedure[5] . The procedure was validated through tabletop exercises.

The five other procedures that have been defined in the EOSC-hub SMS ('information assets and threats', 'approval and adoption', 'risk management', 'controls', and 'security event handling') are all currently subject to revision and will be re-evaluated during the remainder of the EOSC Future project. The adoption of ISM policies and procedures at this point has been implemented through a consultation mechanism involving the XWP-WG on AAI and security, the core services consultation group, and with adoption by the project's Technical Coordination Board (TCB).

4 EOSC Security Operational Baseline

The EOSC brings together communities and services from a wide range of stakeholders, and they will have to establish mutual operational trust in order to interoperate. Interaction between them needs to preserve the risk appetite of the participants involved, so trust should be transparent, comparably formulated and address existing and emergent usage patterns driven by the user communities. Given that much of the risk is ultimately absorbed by service providers (either directly, or because data security ultimately relies on the security of the service hosting the data), shared policies and best-practice implementation patterns will help providing collective services – since if many providers and infrastructures share common practices, research communities can move and compose services without much friction.

However, because the EOSC-Core services are in themselves distributed and – based on their scope and operational requirements – have different operational trust models, enforcing a single common policy for even those services would either unduly constrain the services in offering the most effective and functional solution, or else result in a policy agreement process that would be overly cumbersome. Experience in the research and education federation domain, as well as in the global e-Infrastructures (IGTF) and in general Internet governance, has confirmed that rather than enforcing a single common policy, a *security baseline* that defines a minimum agreed level which services must 'meet or exceed' is an effective way to establish a 'foundational trust level'. The assurance 'profiles' of for instance the Interoperable Global Trust Federation (IGTF) have enabled global recognition of identity credentials without the need for a single policy or practice statement. The REFEDS specifications and guidelines, such as *Sirtfi* (the Security incident response trust framework for federated identity)[11] and the REFEDS Assurance Framework (RAF)[12] are similar 'baseline' definitions – allowing adherence to the specification without forcing providers to change their own processes, as long as they remain compatible with the stated minimum specifications.

The EOSC Security Operational Baseline was conceived to follow the same model. Since the smallest 'asset entity' in the EOSC for the purposes of information security management is defined to be the *service* (in a broad sense of the work, including entities connected to the EOSC AAI that are identity and proxies), the baseline 'minimum requirements' are addressed primarily to these service providers.

Respectful of the scope of the EOSC SMS with regard to research (user) data, and keeping in mind the subsidiarity principle in the diverse EOSC ecosystem, the EOSC Security Operational Baseline is operational in nature: its scope deals with the security of the service as it interacts with the other EOSC participants, and deals with data security at the infrastructure layer (so for example the protection of data collected as a result of access to the infrastructure, not the protection of the data that is processed by the infrastructure).

The expectation of compliance with the EOSC Security Operational Baseline also differs for 'EOSC-Core' services, and for the other services and resources in the EOSC-Exchange that are listed in the portal. For EOSC-Core services, full adherence to the EOSC Security Operational Baseline is expected, and the 'Core Participation Agreement' specifically states that 'the Service/Service Component supplier shall abide by the EOSC Security Operational Baseline'.

For services in the EOSC-Exchange, their primary requirement is risk-based, in that they shall not wittingly expose other participants in the EOSC to additional risks without their consent, and that they shall be transparent about their information security maturity and policies. The adherence to the EOSC Security Baseline, although of great value to the integrity and trust of the EOSC, can only flow from the Rules of Participation to which the providers in the EOSC-Exchange have to adhere.

The EOSC Security Operational Baseline is derived from the AARC Policy Development Kit (PDK) 'Service Operations Policy'. However, since the AARC PDK is targeted at coordinated infrastructures and communities (i.e. infrastructures that collectively provide federated services), the Service Operations Policy is not directly applicable to the more diverse EOSC ecosystem. Hence, also based on contemporary evolution of the PDK for the UK-based 'IRIS' research e-Infrastructure, we evolved the AARC reference policy into a new EOSC Baseline, following a similar bulleted structure but leveraging to a greater extent the intra-service security capabilities. The EOSC Security Operational Baseline emphases the security interactions of a service with its surroundings, rather than being normative on the internal operation of an individual service.

As an example of such a change, the requirement to 'You shall respond appropriately, and within the specified time period, on receipt of security notices from the Infrastructure or any of its Participants.', which is appropriate in coordinated federated infrastructures but less applicable to the more diverse EOSC ecosystem, is replaced by 'follow, as a minimum, generally accepted IT security best practices and governance, [... and take] appropriate action in relation to security vulnerability notifications'. While the accompanying FAQ provides specific measures and controls that can help an EOSC (Core) service provider to meet or exceed this baseline, such measures are no longer normative.

The full text of the EOSC Security Operational Baseline, comprising 12 single-statement items, is provided for reference in Appendix A. However, in its overarching aim to be compact and simple to part and 'check off' the requisite compliance, for service providers whose primary interest does not lie with information security management the practical implementation of the baseline, may seem to be exceedingly complex. The EOSC security teams therefore provided an implementation guide (an FAQ or 'annotated baseline') that accompanies the 12-item checklist in the baseline. This FAQ, maintained on the EOSC Future Wiki[1] , provides up-to-date suggestions on how the baseline can be best implemented, what constitutes 'IT security best practice and governance', and what to do in case of suspected incidents or vulnerabilities.

4.1 EOSC Security Operational Baseline consultation process

The baseline consultation process for EOSC Future followed a staged approach. The initial development has been driven through the AARC Policy Community open multi-stakeholder forum, in which both the European research and e-Infrastructures participate, but that also includes national infrastructure providers and global stakeholders. Through this process, the initial AARC PDK service operations and the UK-IRIS service policies have evolved to match the structure of EOSC. The draft baseline was subsequently presented to the AEGIS (AARC Engagement Group for Infrastructures), where each of the research and generic infrastructures that operate an AAI (community) proxy is represented, and where these infrastructures can formally express commitment to adoption of the guidelines. Their feedback was incorporated into the EOSC Security Operational Baseline before it was discussed in the EOSC Future Cross-Work-Package Working Group (XWG) established under the TCB on EOSC AAI Implementation – whose remit '[includes] the security policy baselines and guidelines used'[1].

The practical impact of the baseline, such as the need to collect security contact information for service providers and the assessment of operational readiness of service providers to participate in incident response, were discussed in joint services with the EOSC-Core service providers and the 'EOSC helpdesk process' to obtain their feedback.

On both the guideline itself, as well as on the immediate practical impact on the EOSC-Core services, 'rough consensus' (in the sense customarily assumed in Internet governance) was obtained. This consensus, rather than any formal ratification at this stage, was especially important to ensure that the 'reality on the ground' matches the expectations, rather than create a mere bureaucratic process.

4.2 Implementation of the baseline

The baseline is implemented through three different mechanisms, depending on the target stakeholder segment:

- For all EOSC-Core services supported by the project, it is incorporated (by reference) as a requirement in the EOSC Core Participation Agreement. Through its section 'Information security and data protection', the Agreement states 'The Service/Service Component supplier shall abide by the EOSC Security Operational Baseline'. This is a binding requirement for the provider, but at the same time gives the provider additional advanced security support from the EOSC Security Incident Coordinator.
- For services connected to the EOSC AAI's Core Infrastructure Proxy, the 'EOSC-Core Infrastructure Proxy - Integration guide for SPs'[2] specifies adherence to the baseline as part of its technical and policy requirements for services

[1] https://wiki.eoscfuture.eu/display/EOSCF/EOSC+AAI+Implementation+XWG
[2] https://wiki.eoscfuture.eu/display/EOSCF/EOSC+Core+Infrastructure+Proxy+-+Integration+guide+for+SPs

- For services listed in the EOSC-Exchange, or connected through the EOSC AAI Federation, the baseline currently retains the status of a 'community good practice' guideline. The 'EOSC AAI Federation Participation Policy draft', as given in the 'EOSC Authentication and Authorization Infrastructure Report'[3] , from the EOSC Executive Board Working Group (WG) Architecture AAI Task Force (TF), provides (in section 5.2 on membership eligibility and ownership) in all applications for membership to require from the applicant that it must 'commit to adherence to the security policy baseline of EOSC security operations'.

Given the potentially large variance in maturity levels with respect to operational security for EOSC services listed in the EOSC-Exchange, and in order to encourage material adoption of good security practices rather than generate discrepancy between documentation and reality, a phased implementation approach to the baseline adherence for listed services seems called for. Such an implementation process should be supported with both training and periodic 'field exercises' – and in the service on-boarding process the EOSC Security Operational Baseline is called out specifically to emphasise that willing participation in such exercises is envisioned also from the EOSC-Exchange-listed services. Alignment with the EOSC Security Operational Baseline is expected to mature over time as services participate in the EOSC. For those services that are part of most of the clustered research and e-Infrastructures, the security maturity level and baseline compatibility is already well established.

4.3 EOSC WISE Baseline AUP

Presenting purpose, acceptable use, and access conditions for services is a common requirement, and such terms and conditions have to be presented, as soon as is feasible, to the (prospective) users. There are both legal and regulatory requirements involved (for instance, in many jurisdictions having an explicit 'click-through' acceptable use policy or terms and conditions facilitates reporting of cybercrime, since it is then obvious that access by miscreants was manifestly unwanted), but it is also the most appropriate place to clarify to users the intent and any limitations in the service. A single notice usually serves both roles: the 'acceptable use policy' (AUP) states the permitted use and intended purpose, the 'terms and conditions' clarify what the user may expect from the service, and what its limitations (if any) are.

In an ecosystem like the EOSC, we expect users to be interacting with multiple services at the same time. This interaction can be direct (user-to-service), but there are also brokered services (where a service will contact other services on behalf of the user, also when the user is not present), and composite services (where a service collates resources provided by others). In such scenarios, the end-user is not and cannot be made aware of all services that will be used – and similarly such 'indirect' services have no way of interacting with the user directly at the point of use. Yet these 'indirect' services will also need assurance that usage follows their AUP. But it is neither scalable nor desirable to ask the user ex-ante to click through the AUPs of all potential services involved in a workflow.

The WISE community, with support from the AARC project and others, developed a scalable solution for this issue by establishing an AUP baseline. This 'WISE Baseline AUP' defined acceptable use only (so does not describe service specifics) and is modelled on the 'Taipei Accord' acceptable use policy that was adopted for several global research infrastructures in 2005 to ease their interoperation. The WISE Baseline AUP consists of a single-sentence purpose binding (required to identify permitted use), 10 commandments, a placeholder for attaching (GDPR) privacy notices, and optional service-specific extensions. The AARC Guideline AARC-I044[9] provides the implementation mechanisms for the WISE Baseline AUP in research infrastructures and for horizontal e-Infrastructures and services. When a user-facing service adopts the Baseline AUP and ensures its presentation to and acceptance by the user, all contributing ('downstream') services that are subsequently accessed during the delivery to the user can automatically benefit from the initial acceptance by the user. In this way, an AUP needs only to be presented once, significantly easing the user's journey through to the EOSC ecosystem. For collaboration platforms (such as community AAI proxies in the AARC BPA), the implementation model can be extended to include composite privacy notices, thus addressing the Article 13 and 14 privacy notice requirements of GDPR in a more scalable way.

We have adopted the WISE Baseline AUP for EOSC-Core services because of the unique place these services (especially the EOSC Portal) hold in the ecosystem. When the WISE Baseline AUP is presented by all core services (especially the Portal) and accepted at that point, all services for which the WISE Baseline AUP is

sufficient do not need to request user acceptance again. In practice, we have observed that many generic infrastructures and those research infrastructures that do not need to handle sensitive data consider the Baseline AUP to be sufficient.

We have therefore included the enforcement of the WISE Baseline AUP in the Core Participation Agreement information security and data protection clauses.

5 Risk assessment for EOSC service or resource providers

Risk management requires the engagement of all stakeholders, and it should include 'different kinds of users and roles to ensure that every aspect of risk is addressed, including hardware, software, employee awareness, users and business processes. Risk management is one of the key activities in information security management.' This comprehensive approach identified in the GÉANT SIG-ISM Whitepaper[7] is a well-recognised element in the risk management standards, and in the same vein, appropriate risk management as well as risk acceptance underpin the subsidiarity concept of security in the EOSC ecosystem. SIG-ISM is the GÉANT supported community for more than 100 security officers of NRENs and works exclusively on information security management subjects for Research and Education.

But although risk management is a fundamental and well-established part of information security in general within the industry and among IT service providers, the concept of risk assessments has been somewhat unfamiliar among providers and brokers at EOSC. Therefore, previous risk assessment methodologies have required substantial facilitation and extensive meetings with expert consultants to focus on risks, security controls, and risk ownership. This resource-intensive approach is ill suited to the diversity of the EOSC resource provider landscape.

We are now in the process of developing a more streamlined and focused framework to manage information security risks in the EOSC (both the EOSC-Core and the Exchange). This new approach introduces well-known standard information security risks, such as data breaches, system compromises, unattended vulnerabilities or weak configurations, and unscheduled service unavailability due to faults or denial of service attacks. Services can also add service-specific risks, such as heavy dependencies on EOSC-Core service components, or an external software library, and similar factors external to the service itself. Especially for Core services, tooling in the form of 'static analysis' during integration and deployment can check for the compliance and for implemented risk mitigations in the service, such as the presence of security contact information.

The motivation for the new approach is to make risk assessment more scalable and get most of the risk assessments implemented as self-assessments. We are also in the process of identifying suitable platforms for the risk assessment for flexible processing and analysis; using file-based sheets is neither a scalable nor an efficient method to perform risk assessments. These platforms have to be able to record the outcomes and, preferably, keep track of the associated controls and mitigations with the risks identified. At the same time, we aim to change the traditional risk management focus from merely host or software specific risk to a comprehensive view of the risks related to services, data, liabilities, and trust.

In addition to improving methods, tools, and guidelines for self-assessments of risk we will use the new tools in a facilitated mode for the most critical IT components of EOSC. Prior risk assessments of some of the key infrastructure AAI proxy components were performed based on the WISE RAW-WG 'spreadsheet-supported' method. This included both B2ACCESS (from EUDAT/DICE) and EGI Check-in (from EGI). The approach used then was resource-intensive and resulted in a detailed list of threats for which the associated likelihood and impact was estimated. This intra-service focus does not fit the more distributed model of responsibilities in EOSC. Using the experience from both prior assessments and from a preliminary assessment of the EOSC Portal, we have done an internal dry run based on the new approach. Pending the evaluation of this trial run, the updated assessment framework documentation will not be available until the second half of 2022.

The risk self-assessment trials will prioritise key EOSC-Core services, both re-assessing the two infrastructure proxies to establish a point of reference (also to establish whether appropriate controls are now in place), and then applying the method to the AAI Core Proxy and the EOSC Portal. We then plan to improve monitoring of the implementation of any specific controls we recommend putting in place.

For the majority of services in the EOSC catalogue, we plan to invite them to carry out a simplified self-assessment, based on a questionnaire. Some responses could be a simple 'yes' or 'no' answer; in other cases people will be asked to read a short description of what is expected, verify their understanding, and query whether they have such measures in place or request a description of what they do. We envisage on the order of 10-12 questions in this form. The aim is to keep it short to encourage as many services as possible to complete the (likely on-line) questionnaire.

6 Security Incident Response

Maintaining a security baseline and targeted risk assessments need to be complemented by reactive capabilities. A focused security team was established, which provides essential services for security incident response. The incident response capability in EOSC is centred on the EOSC Security Incident Coordinator, a CSIRT (Computer Security Incident Response Team) that has a dual role:

- for the EOSC-Core services, it provides operational security response and participatory support in incident mitigation, supporting the providers of the EOSC-Core services in their service specific response and adding in-depth forensic, coordination and remediation capabilities as needed;
- for the EOSC ecosystem, it provides a central point of reporting for security incidents, and can – in support of the EOSC and its connected service providers – act as the central incident response coordination point and liaison with peer security teams in the research and education sector (such as the NREN CSIRTS and the eduGAIN Security Team), with national cybersecurity centres, and global forums of response teams. Although we expect (through the Rules of Participation) all service providers in the EOSC to have a security contact and a response capability, the EOSC Security Incident Coordinator usually has additional avenues available for coordination, both through trust groups as well as through organisational structures.

This dual model reflects the variability in participation models that is inherent in the EOSC.

6.1 What is a security incident for the EOSC

Security incident response in the EOSC ecosystem has its unique features that determine the functions of the security team and its position in the whole EOSC ecosystem.

A crucial feature is the overall architecture of the EOSC environment, which is inherently very distributed and requires broad distribution of responsibilities. In addition to having an infrastructure provider that is EOSC-Core and end services built on top of it, the EOSC-Core itself is a multi-provider collection of services. This is an intriguing challenge the security incident response activities must take into account.

Another important factor is the potential impact of security incidents. While the notion of a security incident is the same in EOSC as in other environments, due to the interconnected nature of EOSC infrastructure their impacts may easily affect multiple services and technologies. This is especially true in the case of the EOSC-Core services that provide the fundamental infrastructure for the EOSC end user services. The infrastructure is indeed complex and unique, with many different services in EOSC-Core interconnected and often having dependencies to myriad outside sources, for example organisations and software. Incidents can quickly affect multiple targets. Therefore, handling incidents may require cooperation and involvement over several service providers.

Since the EOSC is interconnected to a wide academic and research world, incidents triggered in EOSC services may quickly affect services outside the EOSC boundaries and vice versa. Not only make these overlaps the incident handling harder, they can also amplify the impact, including potential damage to reputation. All incident response capabilities have to consider these aspects and be ready to handle multi-domain incidents as a normal course of business. It is also a unique opportunity to look at security incident response in a large-scale environment from a very different perspective.

As increasingly many providers join the EOSC infrastructure to provide additional end user services, it is expected that the attack surface will grow at the same pace, since there is no service with absolute security. In addition to malicious activities of adversaries, unintentional incidents will become more likely as a result of the increasing potential threat landscape. The importance of being able to react to new threats and incidents is ever increasing; this is further emphasised as the number of interconnected services is growing due to EOSC's expansion. In EOSC Future's context, this means targeting the core incident response capabilities to assets that ensure the existence of the EOSC.

6.2 Incident Response process and the core security team

During the first phase of EOSC Future, it has been set as a goal to create response readiness. It is not enough to just have the persons and skills, but to have procedures and communication channels have commonly known ways to operate and cooperate, not to forget the means to improve and adjust the activities. The EOSC security team has built various security incident response tools and processes.

To gain transparency and to clarify the operations, the incident response procedure in ISM1 has been constructed. This has been worked on with clear goals to make the procedure not just to contain generic industry practices, but also to make it easier to operate within the specific EOSC ecosystem. The process has included not only collaborative improvement of the written contents, but also practical testing of these deliverables.

To build viable response capabilities, the team decided to build up a shift rota for assigning lead responsibility working to have better tools of communication including a ticketing system. The team has also established internal communication channels to complement the public ones, and a process to share information on a regular basis.

For testing of developed processes, the security team started with tabletop exercises. This type of exercise is a cost effective yet very powerful tool. An exercise run circles about a simulated incident, which is handled by the team and representatives of affected services, following current procedures. It focuses mainly on communication, trying to verify the feasibility of the procedures and possibly identify areas that are not sufficiently covered. Technical aspects are mocked and suppressed to the bare minimum.

The first conducted exercise was focused on essential functions of the team and its ability to execute the plan. The key findings from the tabletop exercise included a need to update the procedure and some demands to improve the team's practices. For example, the order of actions and communication channels needed to be improved. On the other hand, several details specific to EOSC needed to be added, these include for example incident report source verification, taking into account the ever-increasing number of technologies involved in the deliverables, and communication between incident response team and various service providers.

The second exercise was yet more realistic, putting the team and its procedures under more pressure. The changes already made after the first exercise were tested and for the most proved to be successful. On the other hand, the increased demands revealed more fine-grained needs for improvement, which are currently being worked on. The biggest improvements will be about finally enhancing the internal processes and procedures, to have well-defined actions to be performed. This also ensures that the security incident response is more scalable, transferrable and the quality is even.

The updates and exercise efforts are planned to continue in the near future and the third tabletop exercise is already in an initial planning phase. In the future, the aim is to run even more realistic exercises to ensure sufficient capabilities and procedures tailor-made for the EOSC.

6.3 Gathering critical infrastructure information and ensuring freshness

Collecting data from infrastructure and information tied to them is crucial for security activities. This data is increasingly important for activities concerning security incidents, especially for their requirements to quickly gather information about dependencies and contact points for assessment and involvement purposes. As the EOSC Future project is evolving, the EOSC security has aimed at gathering current information about services and their status. Currently, the focus has been on EOSC-Core services, in the future this will be likely not enough.

To gather information the EOSC security team collaborated with EOSC-Core service providers to acquire contact data and held a small series of events. While these gather-ups increased awareness of security incident response activities, they proved to be too time consuming and heavy to organise. This took too much time and effort compared to the outcome, and as a result the team has now focused on building a questionnaire with relevant information inquiries to obtain the data. This approach also serves better the information gathering for services in the EOSC-Exchange. Nevertheless, this questionnaire must be aligned so that it works with other EOSC activities and cannot be published before the questionnaire for 'Services connected to EOSC-Core Infrastructure Proxy' is finished. This aforementioned questionnaire also provides data for security purposes.

7 Evolving the information security for EOSC

The EOSC ecosystem as a whole and the security activities evolve in tandem, and the updates to the EOSC Interoperability Framework, Rules of Participation, and the implementation of the EOSC-Core affects the way trust and operational security fits into that framework. At the same time, clearer security requirements (and the increasingly recognised need to secure critical infrastructure in society in general) also influence interoperability and co-determine the conditions under which service providers can connect to the EOSC. The incorporation of the baseline in both the Core Participation Agreement and in the AAI Federation rules are indicators of this interaction. The direction of the trust and security activities in EOSC Future point to a need for further practical and actionable guidance, now that the baselines have been established. The evolution hence focuses on operational security guidance for key AAI elements and EOSC-Core services, the risk assessment tooling and community good practice reference cases, communications challenges and mock security drills, baseline 'FAQ' guidance, and incident mitigation and resolution.

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.

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).

For the EOSC-Core services, selected risk mitigation measures such as vulnerability monitoring can be added as part of a continuous integration and deployment methodology. Systems such as the SQAaaS (software quality assurance as-a-service) can incorporate checks for the presence and compliance of specific security artefacts in the service, such as the AUP, privacy notice, and security contact details. Monitoring - either externally, or through agents - can identify the presence of vulnerabilities and trigger the corresponding remediation process by the service provider.

For services in the EOSC-Exchange, other risk assessment methods, monitoring, and controls, are more appropriate. The WISE Risk Assessment Working group (RAW-WG) adopted a 'top risks' method, inspired by the TrustedCI 'Open Science Cyber Risk Profile' (OSCRP)[9] , that data and service providers can employ to identify the key assets ('Public Data', 'Accounting Information', 'User Portals', etc.) and review their associated risks in terms of avenues of attack, concerns, and consequences. Based on this assessment, providers can select the appropriate controls to mitigate risk to an acceptable level. The realisation that a residual risk will remain, that such a risk has to be accepted, and thus that the provider should have both capacity and capability to absorb that risk, is essential. In the EOSC context, communicating this risk to other connected parties (underlying services, science communities, end-users) is required to ensure no inadvertent changes occur to their risk exposure and 'risk appetite'.

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.

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.

Another side-track is keeping the communication channels in good shape, for various security and even operational purposes. The EOSC ecosystem is constantly changing and the contact details data must be frequently updated and tested to ensure their correctness. For this, periodical communications challenges are a well-proven tool. When it comes to security incidents, these can easily be widely visible and have a detrimental effect on EOSC's reputation. Ensuring fast and functioning communication is crucial to reliably recover from any obscurities.

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 similar activities. In fact, the communication challenges themselves can provide to educate the services via material that can be embedded inside these campaigns. As such, these campaigns should be adapted to provide

for other needs, from which the most acute is raising the awareness of security resources available for the EOSC-Core services.

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.

8 Conclusions

The approach taken for EOSC operational security and security policy is based on subsidiarity of responsibilities between the central security team in EOSC Future and the providers of assets – the services and digital objects – that jointly make up the EOSC ecosystem. Following the model proposed in the whitepaper 'Trust Coordination for Research Collaboration in the EOSC era'[6] , the complementary elements of EOSC and its constituent elements are mutually reinforced by placing responsibility for service (and data-set) security with the providers, and define the interfaces between providers and EOSC-Core through risk-management modelling and a 'baselining' of information security maturity. This allows providers to connect with the EOSC despite their non-uniform state of information security.

There are clear risks associated with this model as well. In particular, since the EOSC envisions composite and layered services, taking service components from multiple providers, infrastructures, and research communities, the 'weakest link' is likely to determine the overall resilience of the system. For example, a compromise in an intermediate system that holds access tokens for end-users can result in re-use of the tokens to access underlying services; or insufficient investigation of an incident may fail to identify the root cause of a compromise in time, so that services built on top of such a service remain exposed to credentials stolen in the initial compromise, allowing an attacker to propagate and 'worm' through multiple EOSC services without an effective means to squash the incident.

The EOSC Security Operational Baseline as such will not address this issue; having the baseline defined and having both letter and intent of that baseline internalised by all providers, are quite different. The Security Incident Response Team, established in EOSC Future with the 'core security team', is put in place not only to coordinate between mature service providers, but also acts as a team empowered to take specific actions with respect to all service providers in the EOSC-Core, and can – within the limits of the resources allocated to it by the project – provide expert support as a fall-back for incidents that affect multiple EOSC participants. Its close integration, both at an organisational as well as personal level, with the security teams of the research and e-Infrastructure, and with the academic security community at large (eduGAIN and the NREN security teams), to a reasonable extent provides 'de-facto' emergency support. Most organisations with a mature security capability have long since recognised that collaboration is essential to prevent and mitigate incidents.

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.

As the EOSC Future project will transfer its security responsibilities, both EOSC-Core and EOSC-Exchange services will have a better understanding of their security posture, sufficient guidance to self-manage their risks for service composition, and be able to collaborate to resolve EOSC-wide threats and incidents.

Appendix A – The EOSC Security Operational Baseline

To fulfil its mission, it is necessary for the European Open Science Cloud (EOSC) to be protected from damage, disruption, and unauthorised use. This Security Baseline supports these goals by defining minimum expectations and requirements of the behaviour of those offering services to users and communities connected to the EOSC, and of those providing access to services or assembling service components through the EOSC. It thereby applies to all participants in the EOSC authentication and authorization infrastructure (EOSC AAI). It aims to establish a sufficient level of trust between all Participants in the Infrastructure to enable reliable and secure Infrastructure operation.

Definitions

Terminology in this document follows conventional IT service management vocabulary (such as ITIL and FitSM) and the RFC 2119 key words:

- Service Provider - an organisation (or part of an organisation) that manages and delivers a service or services to customers
- Identity Provider - a service that creates, maintains, and manages identity information for principals and provides authentication services to relying parties
- 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[2] .

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.

References

[1] EOSC Future Security Team, 'EOSC Security Operational Annotated Baseline', retrieved from https://wiki.eoscfuture.eu/display/EOSCF/EOSC+Security+Operational+Annotated+Baseline (April 2022)

[2] European Commission, Directorate-General for Research and Innovation, Wierenga K, Johansson L, Kanellopoulos C, Groep D, Vaghetti D, Liampotis N. 'EOSC Authentication and Authorization Infrastructure (AAI) : report from the EOSC Executive Board Working Group (WG) Architecture AAI Task Force (TF)', Publications Office; 2021. Available from: https://doi.org/10.2777/8702 (ISBN 978-92-76-28113-9)

[3] Viljoen, M. *et al.*, 'EOSChub deliverable D4.3 - Procedures and policies for the production infrastructure', https://documents.egi.eu/document/3500

[4] WISE Community SCI working group, 'The WISE Baseline Acceptable Use Policy and Conditions of Use Version 1', February 2019, retrieved from https://wise-community.org/wise-baseline-aup/ (April 2022)

[5] Koskinen, P. , *et al.* 'EOSC SMS Procedure: ISM1 Security Incident Response', retrieved from https://wiki.eoscfuture.eu/display/EOSCSMS/ISM1+Security+Incident+Response (April 2022)

[6] Groep, D.L. *et al.* 'Trust Coordination for Research Collaboration in the EOSC era' (whitepaper), https://doi.org/10.5281/zenodo.3674677

[7] Normann, Rolf Sture, *et al.* 'SIG-ISM Risk Management Whitepaper', retrieved from https://wiki.geant.org/display/SIGISM/SIG+ISM+white+paper+risk+management (April 2022)

[8] Trusted CI OSCRP working group, 'The Open Science Cyber Risk Profile (OSCRP)', Trusted CI, the NSF Cybersecurity Center of Excellence, retrieved from https://www.trustedci.org/oscrp (April 2022)

[9] Groep, David L., Neilson, Ian, WISE SCI WG members, 'Implementers Guide to the WISE Baseline Acceptable Use Policy', AARC-I044, retrieved from https://aarc-community.org/guidelines/aarc-i044/ (April 2022)

[10] EOSC Future WP7 team, 'EOSC Service Management System', retrieved from https://wiki.eoscfuture.eu/display/EOSCSMS (May 2022)

[11] T. Barton *et al.* (REFEDS), 'A Security Incident Response Trust Framework for Federated Identity (Sirtfi)', retrieved from https://refeds.org/sirtfi (May 2022)

[12] REFEDS Community, 'REFEDS Assurance Framework ver 1.0', retrieved from https://refeds.org/assurance (May 2022)