EOSC Future Security Operations and Policy

October 2021 WISE Workshop

David Groep
PDP group Nikhef, Amsterdam, NL
EOSC Future WP7.5 task lead
A challenging landscape ahead

**Entities of all kinds** – EOSC spans *data sets to storage to computing to publications & digital objects*

**An open ecosystem** – user driven favouring a low barrier to entry

**A diverse ecosystem** – e-Infrastructures, research services, private sector, ...

**EOSC Future**

is an EU-funded H2020 project that is implementing the European Open Science Cloud (EOSC). This EOSC will give European researchers access to a wide variety of research data and professionally provided services.

**An interdependent ecosystem** – aiming at composability, collective service design, and a federated approach to AAI
Operating core services and ‘exchange’

- IT service management for the (core) services
- Portal operation, with a demand and supply side
- **AAI federation** - authentication and authorization based on the ‘AARC BPA’ and federation concepts
- operational security capabilities, trust policy, and security risk structuring

**Sustainability and Architecture WGs**

**Architecture WG**

set criteria for inclusion of additional services
set interoperability standards

WISE Community Workshop Autumn 2021
In order to outline a globally viable, scalable and secure EOSC AAI, the group defined the following three core principles, on which to base their work:

- **User experience** is the only touchstone.
- All trust flows from **communities**.
- **There is no centre** in a distributed system.

“The human element was the starting point of our exploration. We believe that providing a good user experience and making use of the existing trust relations that users already have within their research communities are the key factors for delivering a successful EOSC AAI.” [Klaas Wieringa, EOSC AAI TF chair]
Why is the EOSC AAI important here?

... the new ‘EOSC’ federation gets policies and a base line at ‘onboarding’ time

- leveraging existing trust frameworks
- not repeat earlier mistakes: so implement a baseline at the start
Start with the basics for ‘EOSC at large’

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 provider specific capabilities to managing core risk this means *some minimum requirements* in the Rules of Participation and a *response capability* in the core that protects ecosystem integrity
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
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
Risk Assessment

- base on WISE Risk Assessment for WISE (RAW-WG) assessment template
- moves beyond single-domain framework
- specifically challenging if you cannot enumerate your assets?
- EOSC-specialised maturity model and (self-)assessments
- assessment of risk of combined and composite services
Security policy baseline and trust

- needs to preserve the risk appetite of the participants involved
- trust should be transparent, comparably formulated, and address existing and emergent usage patterns
- taking in EOSC Rules of Participation WG, governance activities, and WISE

1. security policy baseline to be incorporated into EOSC AAI Federation participation policy and incorporate secure service operations guidelines
2. evolving trust ‘mapping’ framework of WISE SCI by explicitly incorporating federative aspects
3. effective peer-reviewed self-assessment of information security maturity
Coordination framework and operational sharing process

- Incidents are not limited to just one participant, so their mitigation, containment, and ultimate resolution requires a collective response.
- Leverage, enhance mechanisms developed in WISE and REFEDS.
- Procedures for collaborating and sharing of the so-called ‘Indicators of Compromise’ (IoCs).
- Since incidents do not stop at the EOSC edge, needs engagement with whole constituency: EOSC Core, Exchange, providers, community.
- Concrete processes that enable collaboration during actual response.
- Periodically exercised!
Remediation of Core incidents and coordinated security response

- interdependency of services requires exchange of information and a coherent and simultaneous response to incidents both across services as well as inside each individual service
- coordinating response for incidents affecting the EOSC
- remediation of incidents in the Portal, Core Services, and key infrastructure elements

Effective remediation of incidents in the EOSC at large also depends on subsidiarity and participation of service providers and Infra’s
‘EOSC will shape the research area – and trust drives its resilience and security’