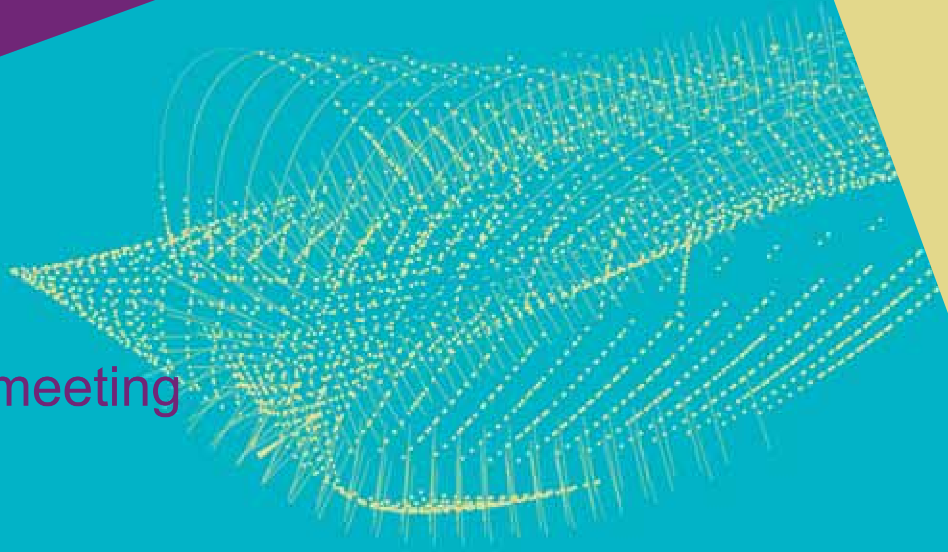
Nikhef



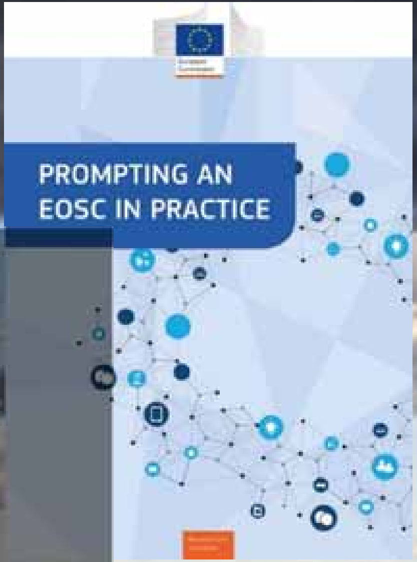
WISE Community May 2021 meeting

Trust and Security in the EOSC era

David Groep (Nikhef) et al.
2021-05-25

The "European Open Science Cloud"

- a 'commons' for research data aiming to combine all disciplines across all (European) countries
- not quite a 'cloud', but with evolving means and methods
- its nature subject to evolution
  'lean' or 'comprehensive', 'infrastructure' or its 'data twin'
- co-guided by an association with diverse composition


PROMPTING AN EOSC IN PRACTICE

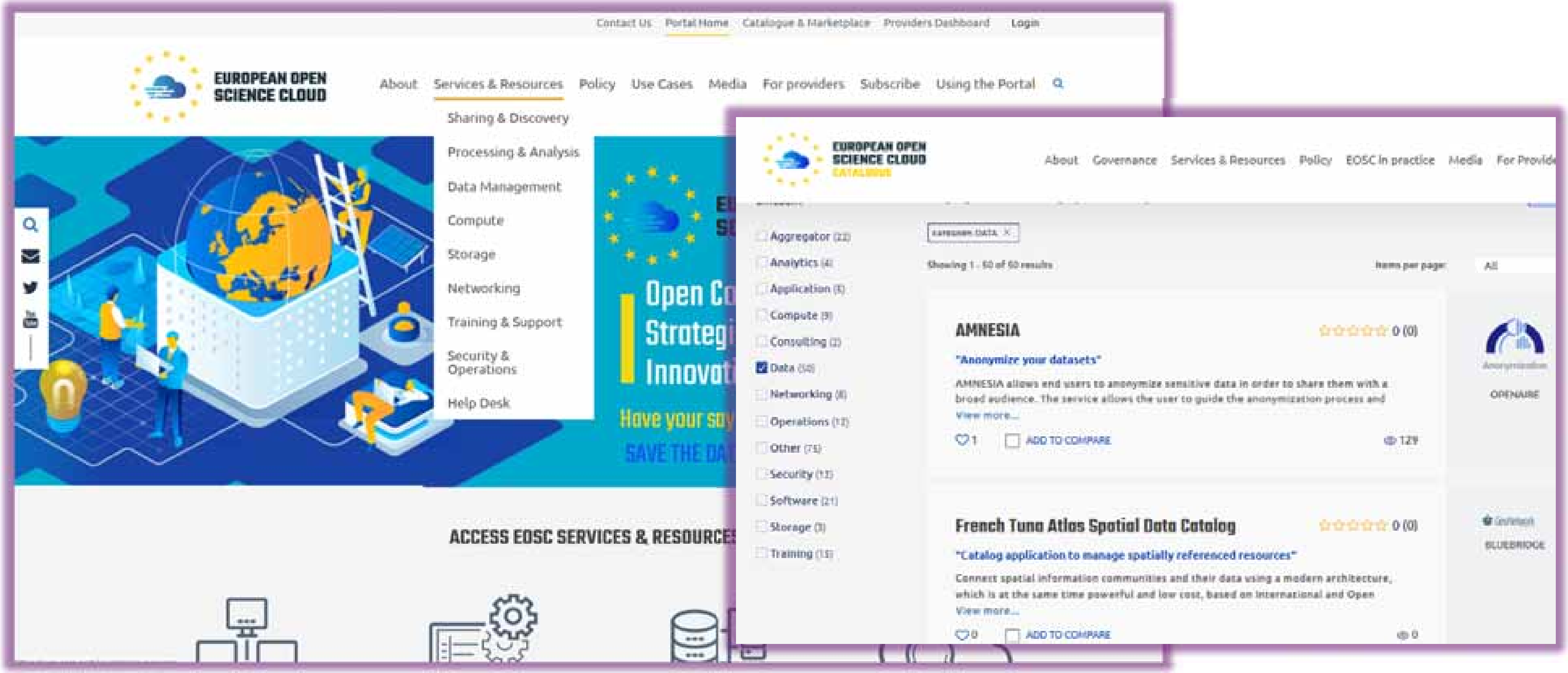
ENVRI
panosc
ESCAPE
SSHOC
EOSC PORTAL
SERVICE CATALOGUE

whatever it is, it will be structuring data-driven research in Europe in the 2020s

Photo by Pop & Zebra on Unsplash

graphic sources: https://www.eoscsecretariat.eu/eosc-symposium-programme

An ecosystem more than an infrastructure



Contact Us Portal Home Catalogue & Marketplace Providers Dashboard Login

EUROPEAN OPEN SCIENCE CLOUD

About Services & Resources Policy Use Cases Media For providers Subscribe Using the Portal

- Sharing & Discovery
- Processing & Analysis
- Data Management
- Compute
- Storage
- Networking
- Training & Support
- Security & Operations
- Help Desk

ACCESS EOSC SERVICES & RESOURCES

EUROPEAN OPEN SCIENCE CLOUD CATALOGUE

About Governance Services & Resources Policy EOSC in practice Media For Provide

- □ Aggregator (22)
- □ Analytics (4)
- □ Application (5)
- □ Compute (9)
- □ Consulting (2)
- ☑ Data (50)
- □ Networking (8)
- □ Operations (13)
- □ Other (75)
- □ Security (13)
- □ Software (21)
- □ Storage (3)
- □ Training (15)

category: Data ×

Showing 1 - 50 of 50 results

Items per page: All

AMNESIA ☆☆☆☆☆ 0 (0)

"Anonymize your datasets"

AMNESIA allows end users to anonymize sensitive data in order to share them with a broad audience. The service allows the user to guide the anonymization process and

View more...

♡1 □ ADD TO COMPARE 129

French Tuna Atlas Spatial Data Catalog ☆☆☆☆☆ 0 (0)

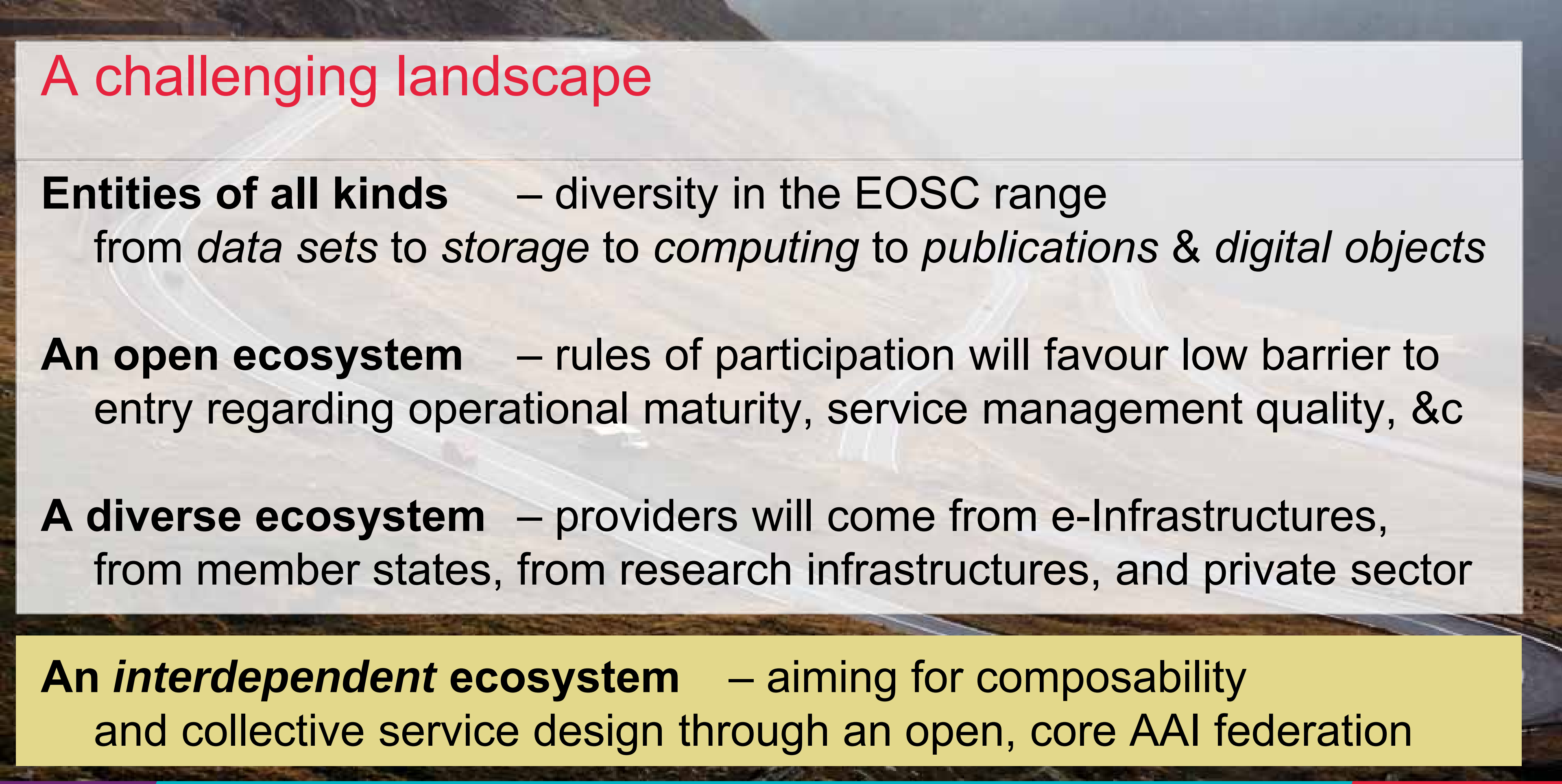
"Catalog application to manage spatially referenced resources"

Connect spatial information communities and their data using a modern architecture, which is at the same time powerful and low cost, based on International and Open

View more...

♡0 □ ADD TO COMPARE 0

EOSC Portal (https://www.eosc-portal.eu/) – as built by EOSChub



A challenging landscape

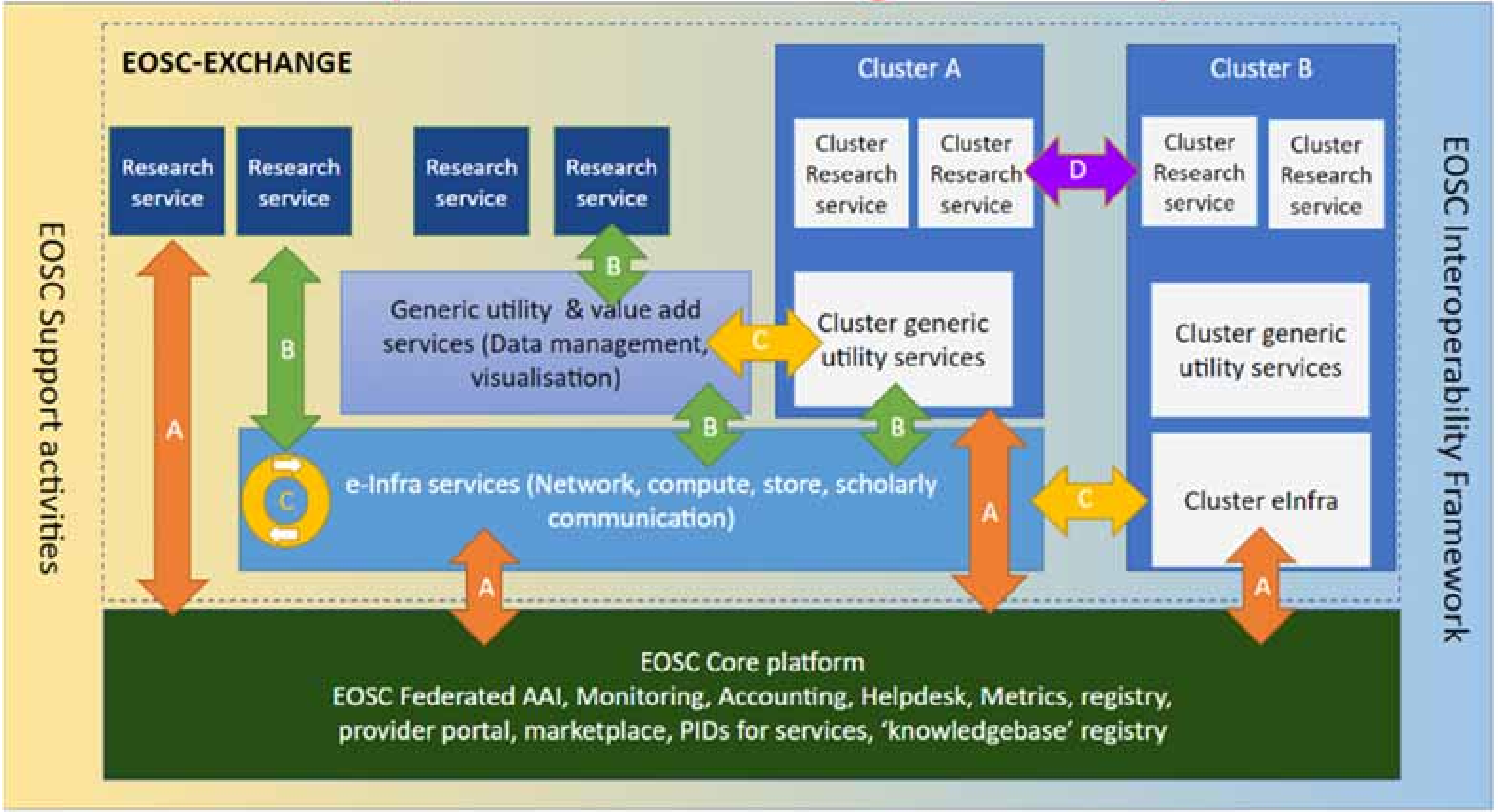
Entities of all kinds – diversity in the EOSC range
from *data sets* to *storage* to *computing* to *publications* & *digital objects*

An open ecosystem – rules of participation will favour low barrier to entry regarding operational maturity, service management quality, &c

A diverse ecosystem – providers will come from e-Infrastructures, from member states, from research infrastructures, and private sector

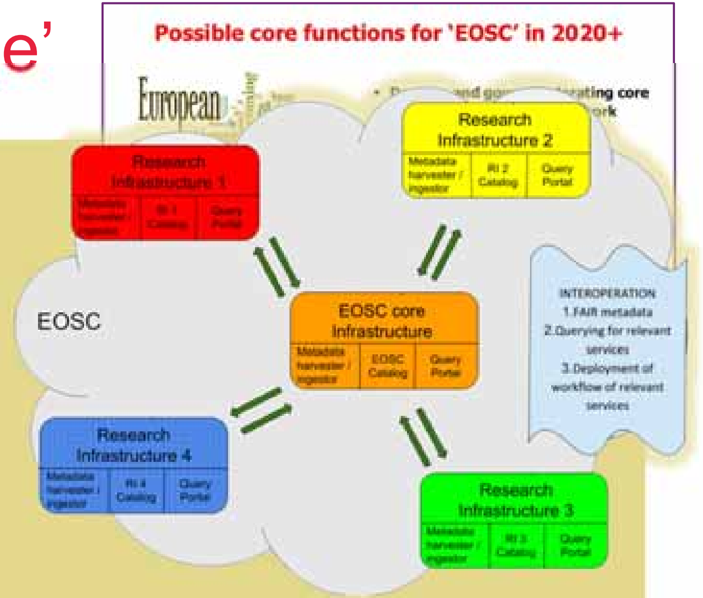
An *interdependent* ecosystem – aiming for composability and collective service design through an open, core AAI federation

EOSC: an ‘interoperable exchange’ built upon a core


EOSC Support activities
EOSC-EXCHANGE
Research service
Research service
Research service
Research service
Cluster A
Cluster Research service
Cluster Research service
D
Cluster B
Cluster Research service
Cluster Research service
EOSC Interoperability Framework
B
Generic utility & value add services (Data management, visualisation)
C
Cluster generic utility services
Cluster generic utility services
A
B
B
B
e-Infra services (Network, compute, store, scholarly communication)
C
A
C
Cluster eInfra
A
A
EOSC Core platform
EOSC Federated AAI, Monitoring, Accounting, Helpdesk, Metrics, registry, provider portal, marketplace, PIDs for services, ‘knowledgebase’ registry

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**


Possible core functions for ‘EOSC’ in 2020+
European
ting core
ork
Research Infrastructure 1
Metadata harvester / ingestor
RI 1 Catalog
Query Portal
Research Infrastructure 2
Metadata harvester / ingestor
RI 2 Catalog
Query Portal
EOSC
EOSC core Infrastructure
Metadata harvester / ingestor
EOSC Catalog
Query Portal
INTEROPERATION
1.FAIR metadata
2.Querying for relevant services
3.Deployment of workflow of relevant services
Research Infrastructure 4
Metadata harvester / ingestor
RI 4 Catalog
Query Portal
Research Infrastructure 3
Metadata harvester / ingestor
RI 3 Catalog
Query Portal

Sustainability and Architecture WGs set criteria for inclusion of additional services
Architecture WG and its taskforces set interoperability standards

and for the ‘BPA’ AARC Blueprint Architecture? See https://aarc-community.org/architecture/

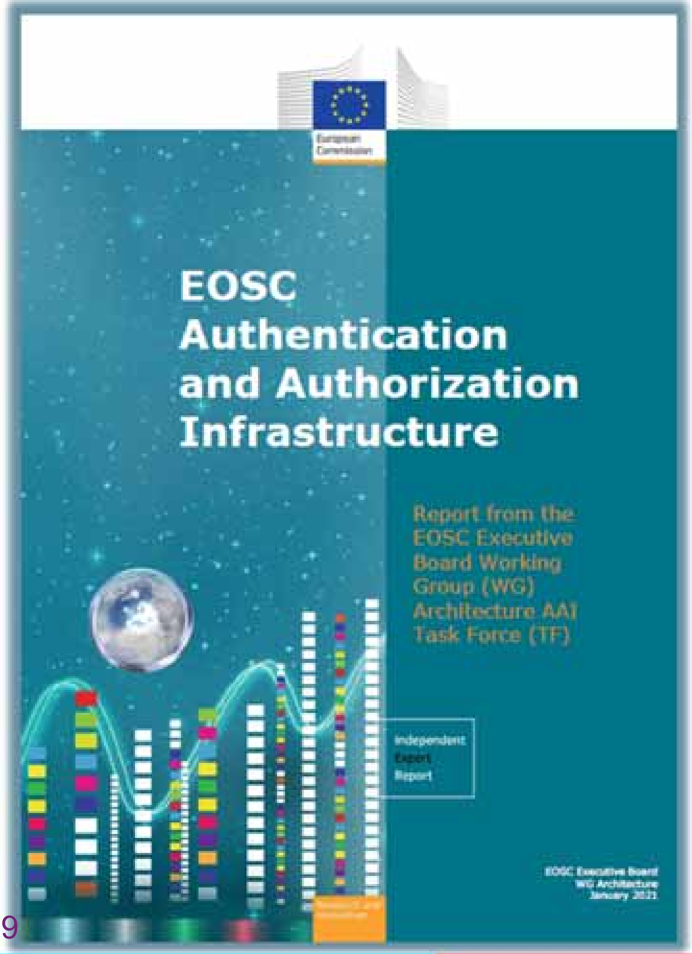
image sources: EOSC Secretariat, Karel Luyben, EOSC-Future drafts, v14

The EOSC AAI and federation

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]



European Commission

EOSC Authentication and Authorization Infrastructure

Report from the EOSC Executive Board Working Group (WG) Architecture AAI Task Force (TF)

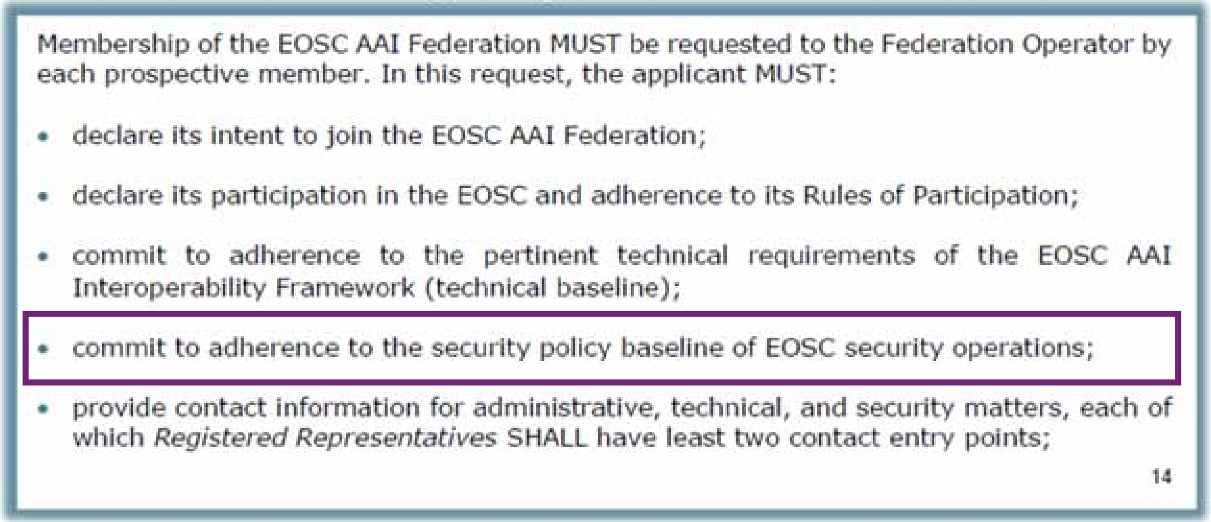
Independent Expert Report

EOSC Executive Board
WG Architecture
January 2021

DOI:10.2777/8702 – ISBN 978-92-76-28113-9

EOSC federation and the operational security baseline

… the new ‘EOSC’ federation gets policies and baseline at ‘onboarding’ time



Membership of the EOSC AAI Federation MUST be requested to the Federation Operator by each prospective member. In this request, the applicant MUST:

- declare its intent to join the EOSC AAI Federation;
- declare its participation in the EOSC and adherence to its Rules of Participation;
- commit to adherence to the pertinent technical requirements of the EOSC AAI Interoperability Framework (technical baseline);
- commit to adherence to the security policy baseline of EOSC security operations;
- provide contact information for administrative, technical, and security matters, each of which *Registered Representatives* SHALL have least two contact entry points;

14

leveraging existing trust frameworks: SCI, AARC Policy Development Kit, …
implementing a baseline at the start, learning from previous experiences

Back to Basics: the few tenets for the EOSC ecosystem security

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

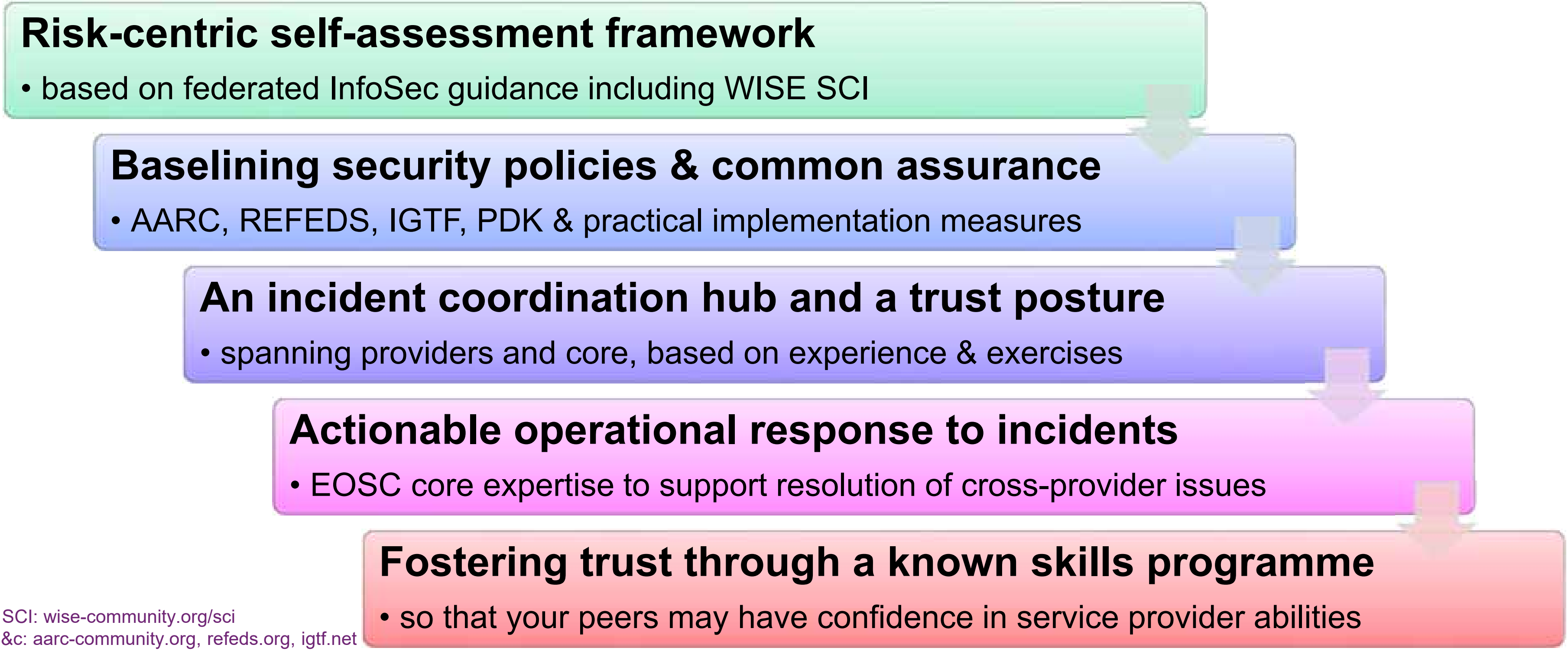
A service provider should

- **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

this will mean *some minimum requirements* in the Rules of Participation

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

Making the EOSC a trusted place



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

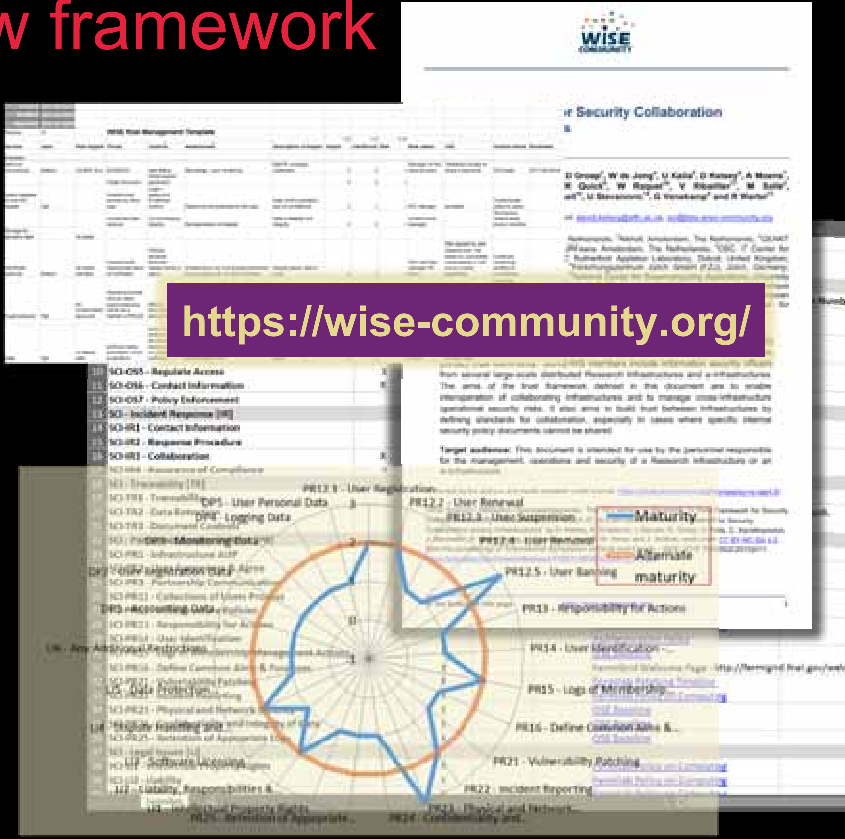
WISE SCI: wise-community.org/sci
AARC&c: aarc-community.org, refeds.org, igtf.net
PDK: aarc-community.org/policies/policy-development-kit

Assessing risk … in a peer-review framework

InfoSec **risk assessment framework** for EOSC services based on a federated evolution of WISE SCI and a multi-tier maturity model, also addressing data security and protection

- risks ‘play out’ differently in different infrastructures
- more than storage or compute, but also risks for (open) data and for reputation

Many risks are generic, some need context and expertise to assess. Or are under regulated regime


WISE COMMUNITY
Security Collaboration
WISE Risk Management Template
SCI-OS5 - Regulate Access
SCI-OS6 - Contact Information
SCI-OS7 - Policy Enforcement
SCI - Incident Response [IR]
SCI-IR1 - Contact Information
SCI-IR2 - Response Procedure
SCI-IR3 - Collaboration
PR12.1 - User Registration
PR12.2 - User Renewal
PR12.3 - User Suspension
PR12.4 - User Removal
PR12.5 - User Banning
PR13 - Responsibility for Actions
PR14 - User Identification
PR15 - Logs of Membership
PR16 - Define Common Aims &...
PR21 - Vulnerability Patching
PR22 - Incident Reporting
PR23 - Physical and Network...
PR24 - Confidentiality and...
PR25 - Retention of Appropriate...
DP5 - User Personal Data
DP6 - Logging Data
DP8 - Monitoring Data
DP3 - Accounting Data
LI5 - Data Protection
LI7 - Software Licensing
LI3 - Liability, Responsibilities &...
LI4 - Intellectual Property Rights
Maturity
Alternate maturity

https://wise-community.org/

this spider diagram is fictional – idea by Urpo Kaila, CSC

Shared understanding of a baseline?

Closely coordinated infrastructures – e.g. WLCG, EGI – started with a single common policy set and assurance level

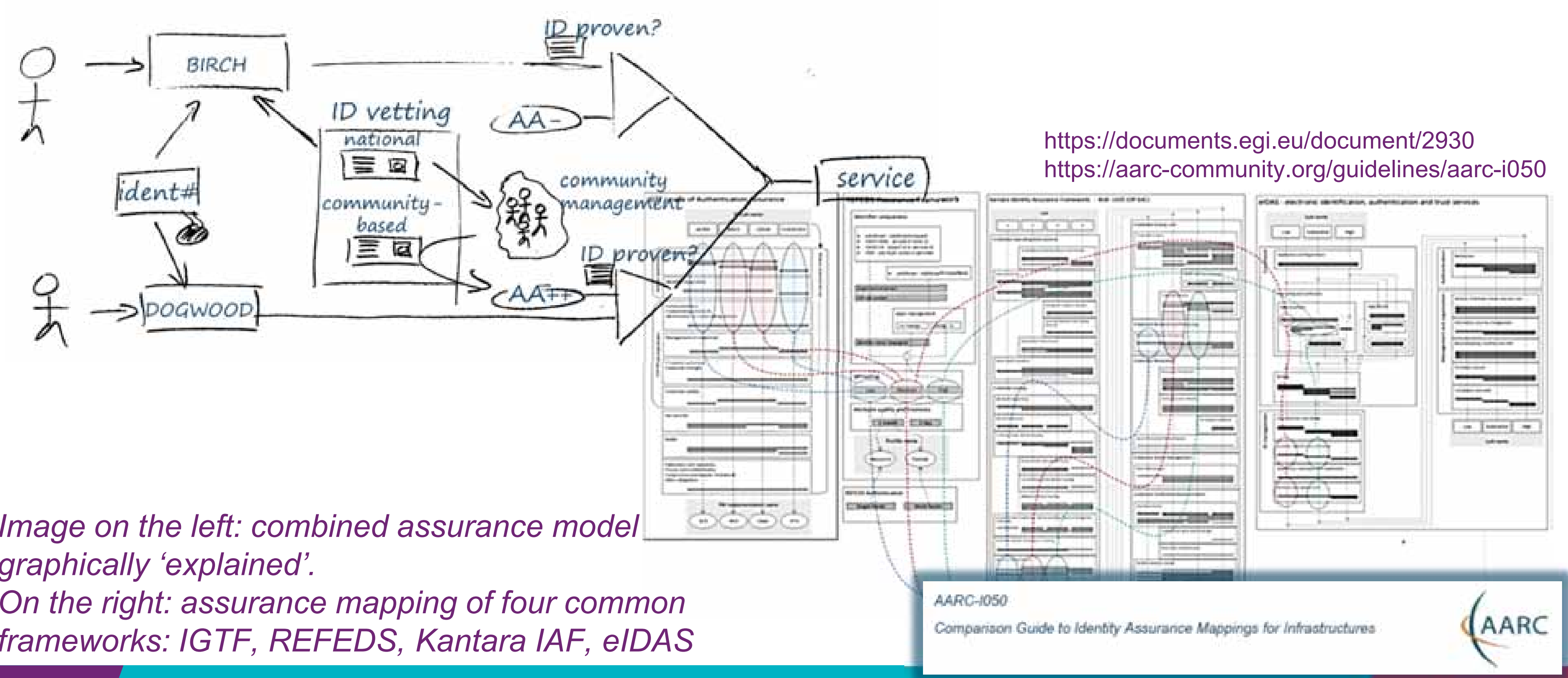
- service providers and users ‘understand’ its meaning and compliance - and the understanding is shared

Move towards differentiated models adds flexibility, but also complexity!

- different means to achieve same goal
- varying means to achieve different goals with diverse risk

Image credit: ZULTAX, https://www.youtube.com/watch?v=NRznoYCJOHg

Diversification is complex



https://documents.egi.eu/document/2930
https://aarc-community.org/guidelines/aarc-i050

Image on the left: combined assurance model graphically 'explained'.
On the right: assurance mapping of four common frameworks: IGTF, REFEDS, Kantara IAF, eIDAS

Start with baselining

baselining has been very effective
with Sirtfi, for R&S, and for InCommon …

Trust marks or seals
for specific service levels, access classes, types of data, regulatory domains, &c

SCI-based policy mapping
common templates like WISE baseline Acceptable Use Policy, risk assessment comparisons …

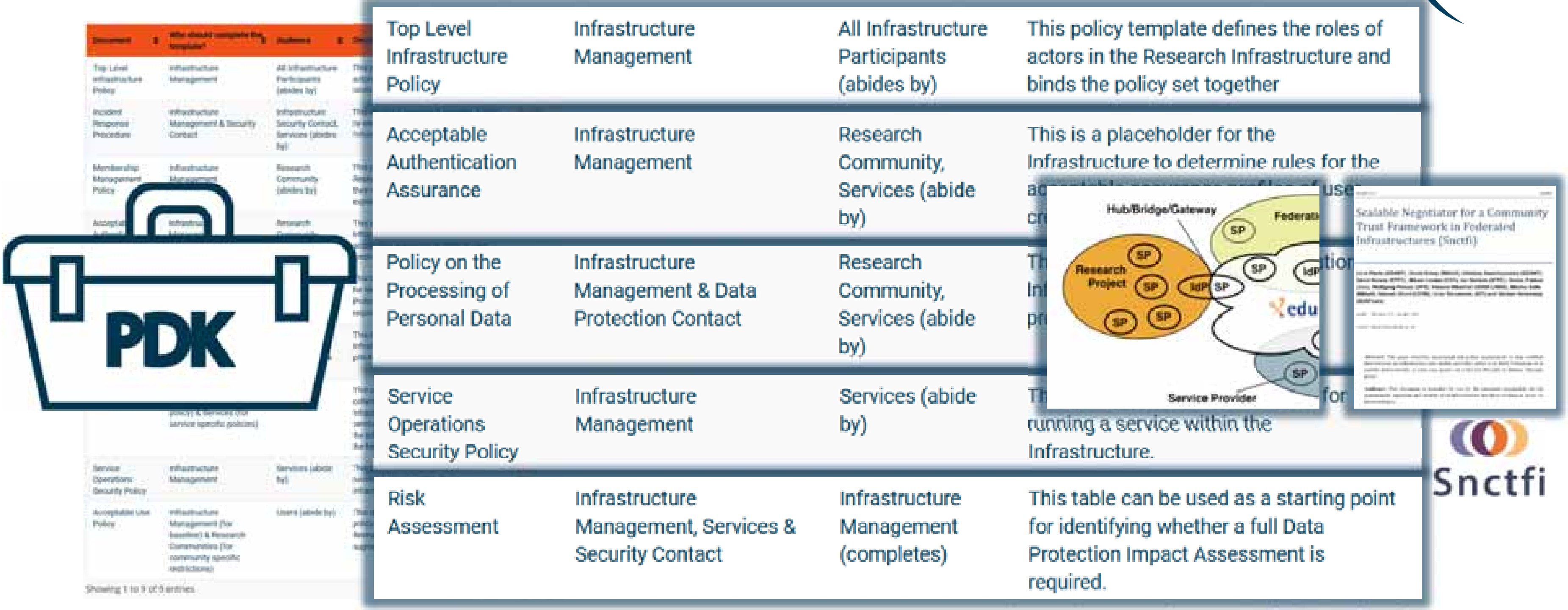
Good Practice
and implementation guidance

small number of assurance profiles (e.g. REFEDS, IGTF, eIDAS), AARC/AEGIS recommendations, CSIRT capability

Technical guidance
e.g. assurance expression,
service operations policy & service security

Rules of Participation
minimal set of capabilities – initially maybe just contact information, responsiveness, confidentiality

THE POLICY DEVELOPMENT KIT



Document	Who should complete the template?	Audience
Top Level Infrastructure Policy	Infrastructure Management	All Infrastructure Participants (abides by)
Incident Response Procedure	Infrastructure Management & Security Contact	Infrastructure Security Contact, Services (abides by)
Membership Management Policy	Infrastructure Management	Research Community (abides by)
Acceptabl	Infrastru	Research
	policy) & Services (for service specific policies)	
Service Operations Security Policy	Infrastructure Management	Services (abide by)
Acceptable Use Policy	Infrastructure Management (for baseline) & Research Communities (for community specific restrictions)	Users (abide by)

Showing 1 to 9 of 9 entries

Top Level Infrastructure Policy	Infrastructure Management	All Infrastructure Participants (abides by)	This policy template defines the roles of actors in the Research Infrastructure and binds the policy set together
Acceptable Authentication Assurance	Infrastructure Management	Research Community, Services (abide by)	This is a placeholder for the Infrastructure to determine rules for the ac use cr
Policy on the Processing of Personal Data	Infrastructure Management & Data Protection Contact	Research Community, Services (abide by)	Th tion Inf pr
Service Operations Security Policy	Infrastructure Management	Services (abide by)	Th for running a service within the Infrastructure.
Risk Assessment	Infrastructure Management, Services & Security Contact	Infrastructure Management (completes)	This table can be used as a starting point for identifying whether a full Data Protection Impact Assessment is required.

Scalable Negotiator for a Community Trust Framework in Federated Infrastructures (Snctfi)

Snctfi

https://aarc-project.eu/policies/policy-development-kit/
https://aarc-community.org/policies/snctfi/

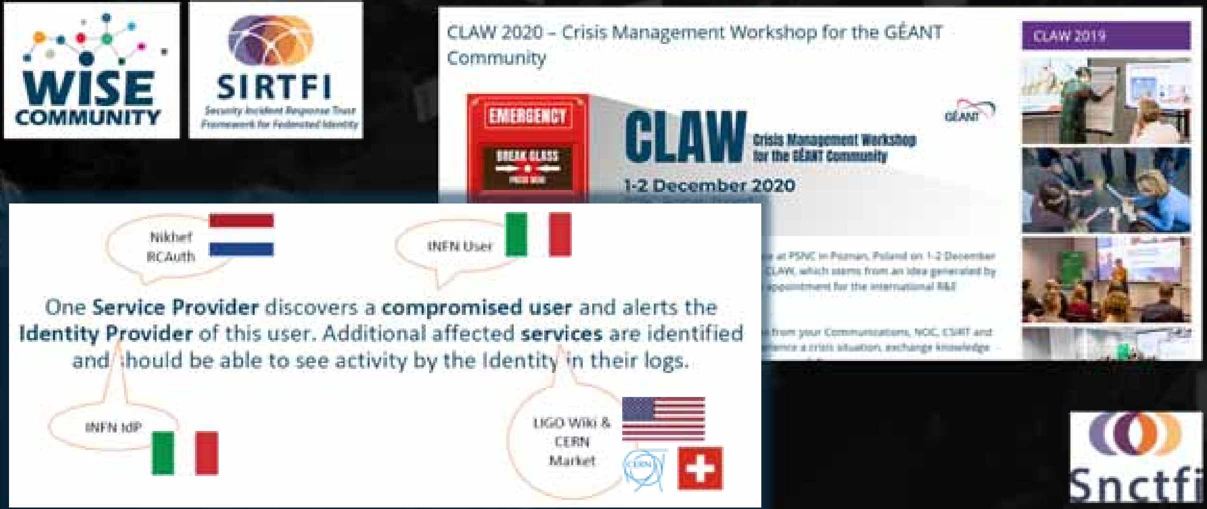
graphic IdP-SP bridge: Lukas Hammerle and Ann Harding, SWITCH

Establishing the trust basis for response

Collaboration frameworks, processes, exercises – the basis of trust
since not everything can be done on personal trust and 'blind faith'

WISE COMMUNITY

SIRTFI
Security Incident Response Trust Framework for Federated Identity



CLAW 2020 – Crisis Management Workshop for the GÉANT Community

CLAW 2019

CLAW Crisis Management Workshop for the GÉANT Community

1-2 December 2020

…e at PSNC in Poznan, Poland on 1-2 December
…CLAW, which stems from an idea generated by
…appointment for the international R&E

…from your Communications, NOC, CSIRT and
…ence a crisis situation, exchange knowledge –

One **Service Provider** discovers a **compromised user** and alerts the **Identity Provider** of this user. Additional affected **services** are identified and should be able to see activity by the Identity in their logs.

TF-CSIRT Trusted Introducer

FIRST

APCERT
Asia Pacific Computer Emergency Response Team

EGI CSIRT

lacnic warp
Warning Advice and Reporting Point

REN-ISAC

AfricaCERT
United in promoting cyber security in Africa

Snctfi

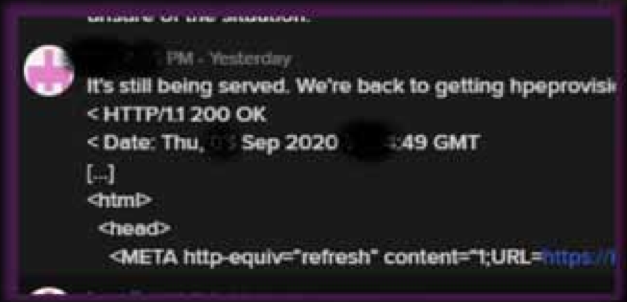
sources: GEANT CLAW
Sirtfi: Hannah Short et al. https://wiki.geant.org/pages/viewpage.action?pageId=123766092

Actionable Response – coordination involving the Core

We *know* we cannot address all needs, but we can make progress

> **‘in the end, the same people do the same work, together, and regardless of the project of funding label’**

- EOSC core will itself be a significant hub
- tightly-knit team of experts
  looking after the security of the core
- who can work collaboratively
  with peer infrastructures and groups



unaware of the situation.

[redacted] PM - Yesterday

It's still being served. We're back to getting hpeprovisi

```
< HTTP/1.1 200 OK
< Date: Thu, [redacted] Sep 2020 [redacted]:49 GMT
[...]
<html>
 <head>
  <META http-equiv="refresh" content="1;URL=https://
```

this team is essential to glue together the information during incidents – leveraging the trust built up before through engagement

Do I know that you know what to know about what?

Training - and ability to exercise - intelligence sharing framework and best practices, but *also* collective technical and forensic expertise!

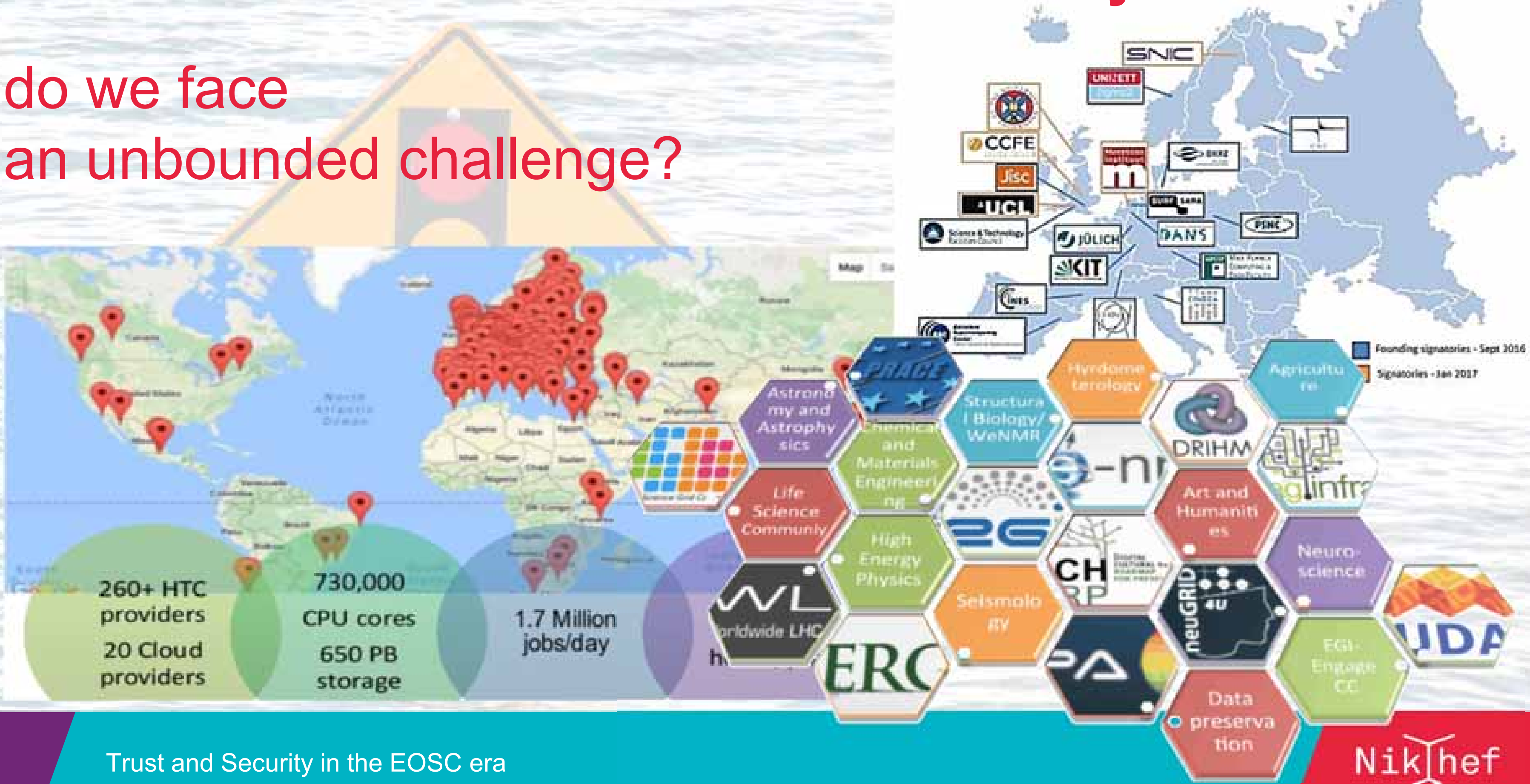
- build up expertise to desired maturity – esp. across EOSC portal providers and research communities
- desirable, but not yet likely, to have training a requirement for participation
  that is hard for an EOSC
  that does not wish barriers to entry ☹

Participation is critical to making this work
You need OpSec people to 'get around', and work globally

image credits: TRANSITS-I

Must EOSC-level mechanisms solve everyone’s issue?

do we face
an unbounded challenge?



What we expect in the infrastructures and services

Service providers should be at, or grow towards, a mature security stance

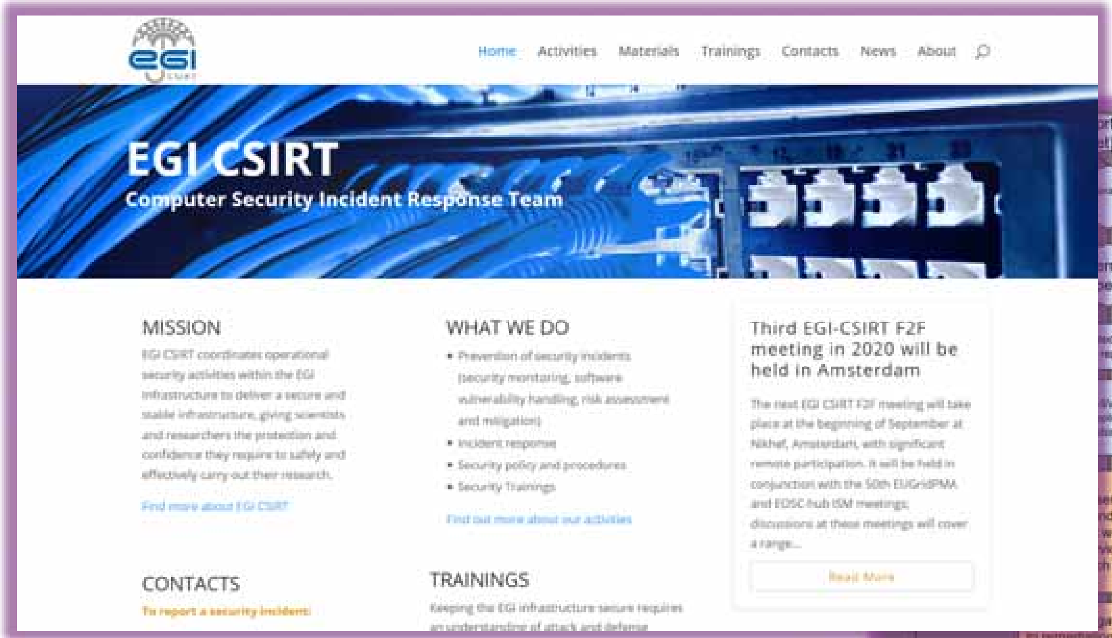
and an **infrastructure** provides coordination amongst 'similar' things

- providers in an infrastructure can **benefit from their commonalities** *in response and security verification, and vulnerability management*
- a mature EOSC security capability can be structured with infrastructure in **a scalable way** across many service providers

While 'services' generally are very broad, including data, publications, &c

Infrastructures: profiting from shared services and understanding

common vulnerabilities,
or common risk environment



EGI CSIRT
Computer Security Incident Response Team

MISSION

EGI CSIRT coordinates operational security activities within the EGI infrastructure to deliver a secure and stable infrastructure, giving scientists and researchers the protection and confidence they require to safely and effectively carry out their research.

Find more about EGI CSIRT

WHAT WE DO

- Prevention of security incidents (security monitoring, software vulnerability handling, risk assessment and mitigation)
- Incident response
- Security policy and procedures
- Security Trainings

Find out more about our activities

Third EGI-CSIRT F2F meeting in 2020 will be held in Amsterdam

The next EGI CSIRT F2F meeting will take place at the beginning of September at Nikhef, Amsterdam, with significant remote participation. It will be held in conjunction with the 50th EUGridPMA and EOSC-hub ISM meetings; discussions at these meetings will cover a range...

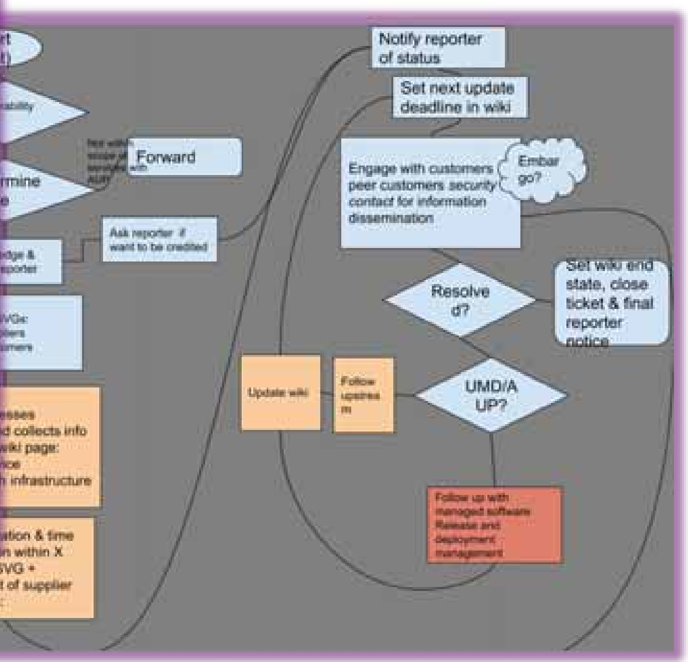
Read More

CONTACTS

To report a security incident:

TRAININGS

Keeping the EGI infrastructure secure requires an understanding of attack and defense


Notify reporter of status
Set next update deadline in wiki
Forward
Engage with customers peer customers security contact for information dissemination
Embar go?
Ask reporter if want to be credited
Resolve d?
Set wiki end state, close ticket & final reporter notice
Update wiki
Follow upstrea m
UMD/A UP?
Follow up with managed software Release and deployment management
...rmine ...e
...ledge & reporter
...SVGs: ...pliers ...stomers
...esses ...nd collects info ...wiki page: ...vice ...h infrastructure
...gation & time to remediation within X hours: Sub-SVG + Management of supplier -> Wiki page

commonality in user base
and access patterns – and testing

image sources: csirt.egi.eu and EGI SVG

Thus even generic capabilities will be widely distributed

EOSC core and ecosystem

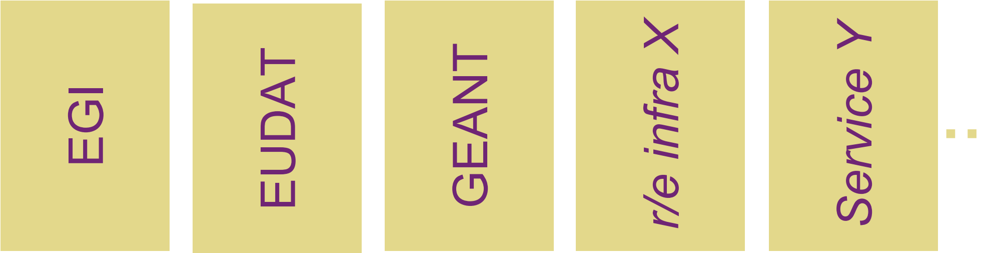
security for a loosely coupled ecosystem

- risk management for collective services
- security baselining and trust marking
- coherence of response, community readiness/collaboration, and information sharing
- resolution, forensics, resolution and remediation for core and stakeholders
- training and capability enhancement

Core in EOSC-Future

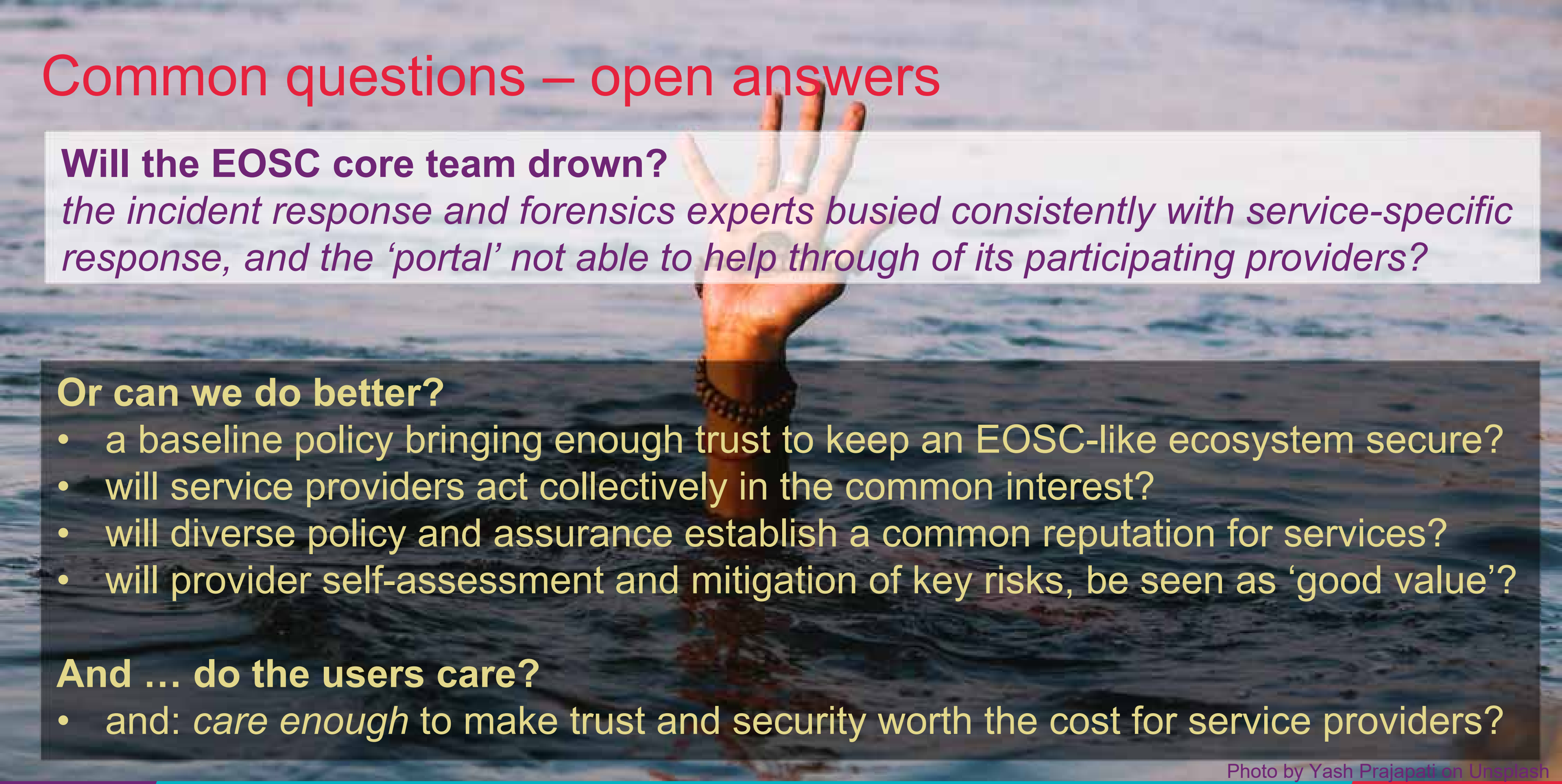
(e-)Infrastructures, services, content

- service security & integrity, responsiveness, compliance monitoring
- vulnerability management and pro-active security management
- incident response and resolution within the infrastructure or service



See also *Trust Coordination for Research Collaboration in the EOSC era,* February 2020, https://g.nikhef.nl/eosc-sec-wp; https://doi.org/10.5281/zenodo.3674676

Common questions – open answers



Will the EOSC core team drown?
the incident response and forensics experts busied consistently with service-specific response, and the 'portal' not able to help through of its participating providers?

Or can we do better?

- a baseline policy bringing enough trust to keep an EOSC-like ecosystem secure?
- will service providers act collectively in the common interest?
- will diverse policy and assurance establish a common reputation for services?
- will provider self-assessment and mitigation of key risks, be seen as 'good value'?

And … do the users care?

- and: *care enough* to make trust and security worth the cost for service providers?

Photo by Yash Prajapati on Unsplash

long read: *Trust Coordination for Research Collaboration in the EOSC era* http://doi.org/10.5281/zenodo.3674677

So, do we stand a chance?

partially based on the white paper co-authored with Jens Jensen, Dave Kelsey, Daniel Kouřil, Maarten Kremers, and Hannah Short and on discussions in the EOSC Future Security Operations & Policy collaboration

David Groep
davidg@nikhef.nl
https://www.nikhef.nl/~davidg/presentations/
https://orcid.org/0000-0003-1026-6606

Nikhef

Parts of this work are based on results that received support from projects co-funded from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 856726 (GN4-3), grant agreement No. 777536 (EOSC-hub), and under Grant Agreement No. 730941 (AARC2).