Authentication and Authorisation for Research and Collaboration

AARC G084 – Security Baseline

evolving operations security in EOSC and the PDK

David Groep
AARC Policy Area
Nikhef & Maastricht University

EUGridPMA+ 64 AARC, IGTF, and EnCo joint meeting
October 2025, Karlsruhe

AARC TREE - Operational Trust for Community and (Infrastructure) Proxies

"Baselining trust and security has proven an effective way to align multi-domain infrastructures. Both in the R&E identity provider space […] as well as for service providers in the EOSC Interoperability Framework and for the EOSC Nodes […], this has enabled secure interworking of providers across organisational, jurisdiction, and sectoral domains.

However, for the research infrastructure proxy services in the AARC BPA (the membership management services in attribute authorities, and in the central proxy components), operational trust and security guidance is lacking.

*And even for the EOSC Federation, **generalized** guidance for a Security Operational Baseline was missing*

- what was available comes either from projects that could not be considered, or
- from specific infrastructures, rather than being cross-sectoral and organization-agnostic

An open ecosystem of providers, across many layers

Founded on subsidiarity, this translates to

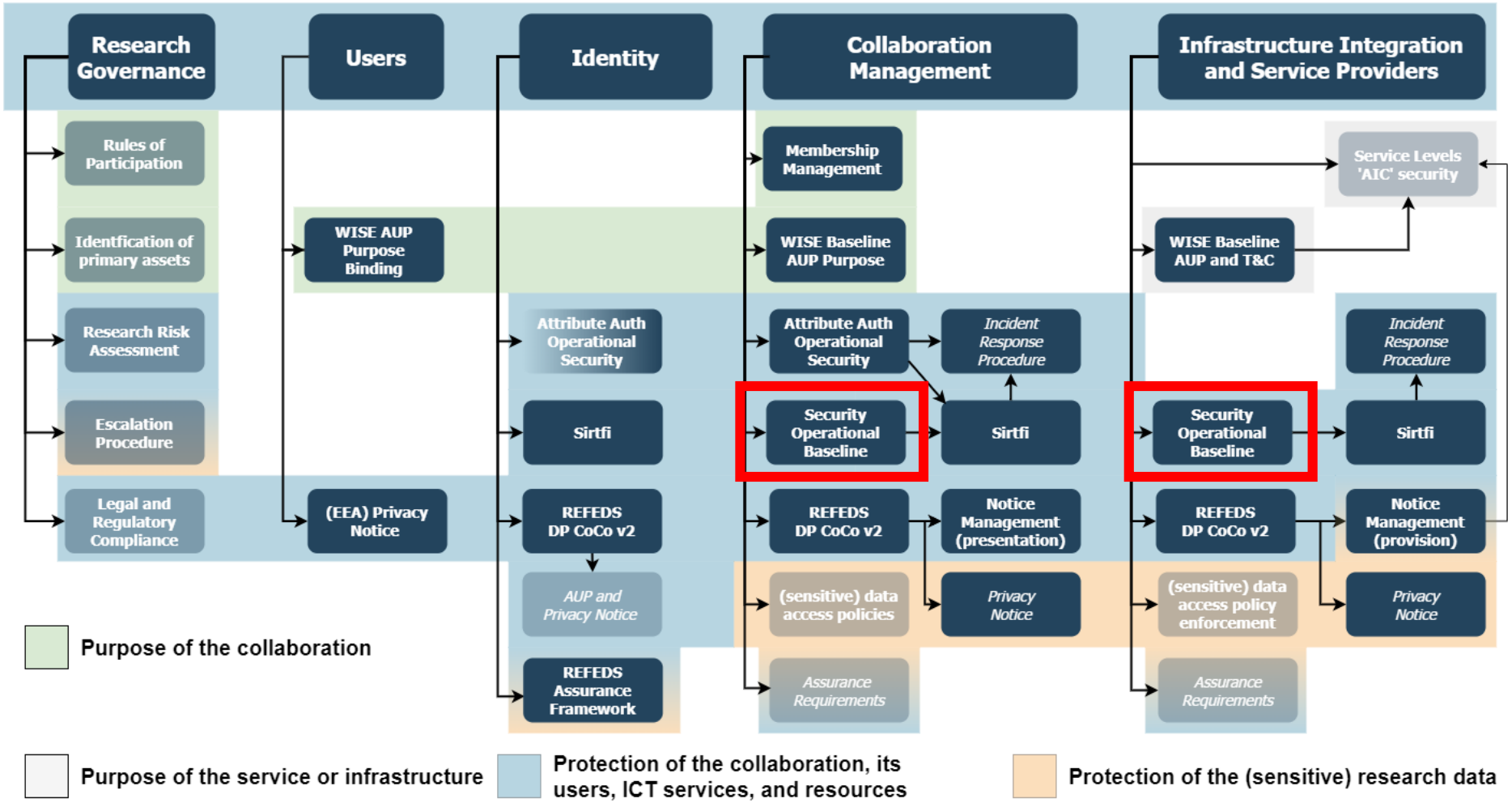
- *primum non nocere*: do no harm to interests & assets of others, including users
- not expose other service providers in the EOSC ecosystem to enlarged risk *as a result of their participation in EOSC*
- be transparent about infosec maturity and risk to its customers and suppliers

Expected concrete result

A set of (one or more) guidelines that represent

- a widely agreed and jointly-developed operational trust baseline for infrastructure membership management and proxy components. This is
- supplemented by policy model guidance on how to connect sectoral federations that have more specific policies to this baseline. These guidelines are
- based on the dialogue between AARC policy experts, the current (EOSC and sectoral) provider federations, and the research infrastructure community,
- through FIM4R and WISE

Making a Security Operational Baseline part of the AARC PDK will address this outcome


Research Governance
Users
Identity
Collaboration Management
Infrastructure Integration and Service Providers
Rules of Participation
Identfication of primary assets
Research Risk Assessment
Escalation Procedure
Legal and Regulatory Compliance
WISE AUP Purpose Binding
(EEA) Privacy Notice
Attribute Auth Operational Security
Sirtfi
REFEDS DP CoCo v2
AUP and Privacy Notice
REFEDS Assurance Framework
Membership Management
WISE Baseline AUP Purpose
Attribute Auth Operational Security
Incident Response Procedure
Security Operational Baseline
Sirtfi
REFEDS DP CoCo v2
Notice Management (presentation)
(sensitive) data access policies
Privacy Notice
Assurance Requirements
Service Levels 'AIC' security
WISE Baseline AUP and T&C
Incident Response Procedure
Security Operational Baseline
Sirtfi
REFEDS DP CoCo v2
Notice Management (provision)
(sensitive) data access policy enforcement
Privacy Notice
Assurance Requirements
Purpose of the collaboration
Purpose of the service or infrastructure
Protection of the collaboration, its users, ICT services, and resources
Protection of the (sensitive) research data

A good starting point …

- evolved from the Site Operations, UK-IRIS, EOSC Security Ops Baseline, now generalised

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 Ser
   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 administrati
   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 incide
7. follow, as a minimum, generally accepted IT security best practices and governance, such as pro-actively applying secure configurations and secu
   updates, and taking appropriate action in relation to security vulnerability notifications, and agree to participate in drills or simulation exercises t
   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 it
   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 relate
   their Service's participation in the EOSC infrastructure and those affecting the EOSC infrastructure as a whole.
10. honour the obligations security collaboration and log retention (clauses 1, 6, and 9 above) for the period of 180 days after their Service is retired
    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
    result in violation of this Security Baseline.

Providers should name persons responsible for the implementation of, and the monitoring of compliance to, this Security Baseline in the context of the
Service. They shall promptly inform the EOSC Security Team of any material non-compliance with this Baseline should such occur.

The EOSC Security Team can be contacted at <abuse@eosc-security.eu>.

The EOSC Incident response team can be contacted via abuse AT eosc

What are 'IT security best practices' in item 7?

On a global scale there are myriad different documents and sources d
well known recommendations that fit your needs. This can depend on
requirements derived from for example certifications like ISO 27000 o
It is important that you take these into consideration, as well as add th
you, especially if there are no written security policies or recommenda

Generic information security

1. ISO standardisation, for example ISO 27000 which covers inform
   processes. Closed standard.
2. National standards, offered by for example national public offic
   covering various security aspects. These can also address local l
   individuals.
3. NIST (https://www.nist.gov/cybersecurity) and CISA (https://ww
   example CISA's Cyber Essentials Starter Kit and NIST's cyber sec
4. CIS (https://www.cisecurity.org/cybersecurity-best-practices/), s
5. SANS (https://www.sans.org) provides guidelines and trainings

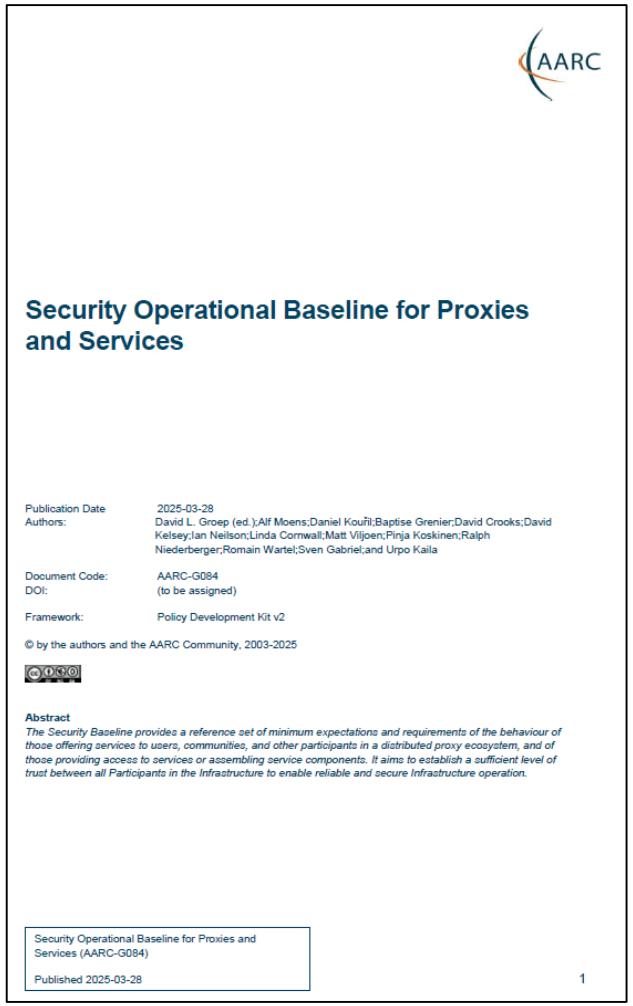
Cloud platforms

1. Cloud security alliance (https://cloudsecurityalliance.org/) provi
2. BSI C5, Cloud Computing Compliance Controls Catalogue (https
   Cloud_Computing-C5.pdf)
3. Several nations provide their standards, which may be targeted

Software development

1. OWASP (https://owasp.org/) provides extensive documentation
   ensure that your software has capabilities to defend against cor
2. Microsoft SDLC (https://www.microsoft.com/en-us/securityengi

AARC G084



Security Operational Baseline for Proxies and Services

Publication Date 2025-03-28
Authors: David L. Groep (ed.);Alf Moens;Daniel Kouřil;Baptise Grenier;David Crooks;David Kelsey;Ian Neilson;Linda Cornwall;Matt Viljoen;Pinja Koskinen;Ralph Niederberger;Romain Wartel;Sven Gabriel;and Urpo Kaila

Document Code: AARC-G084
DOI: (to be assigned)

Framework: Policy Development Kit v2

Abstract
The Security Baseline provides a reference set of minimum expectations and requirements of the behaviour of those offering services to users, communities, and other participants in a distributed proxy ecosystem, and of those providing access to services or assembling service components. It aims to establish a sufficient level of trust between all Participants in the Infrastructure to enable reliable and secure Infrastructure operation.

Security Operational Baseline for Proxies and Services (AARC-G084)

Published 2025-03-28

1

The Security Baseline provides a reference set of minimum expectations and requirements of the behaviour of those offering services to users, communities, and other participants in a distributed proxy ecosystem, and of those providing access to services or assembling service components.

It aims to establish a sufficient level of trust between all Participants in the Infrastructure to enable reliable and secure Infrastructure operation

“Adherence to the Security Operational Baseline implies that *you*, as a service provider, proxy operator, identity provider must: …”

The 12 points

- 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. operate 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, specifically those with which there is a direct AAI trust relationship, in the reporting and resolution of security events or incidents related to their participation in the infrastructure and those affecting the infrastructure as a whole.
- 10. honour the obligations security collaboration and log retention (clauses 1, 6, and 9 above) for the period of 180 days after their Service is retired 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 the 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.

Concluding remarks

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 all security teams of infrastructures with which they have an AAI trust relationship of any material non-compliance with this Baseline should such occur.

Security teams of infrastructures that act as aggregators and incident response coordination centres must publish one of more contact addresses and inform partners about those.

What to do with the background guidance – AARC Wiki?

- The guidance we have is (was?) on the EOSCF Wiki, which is both inaccessible for updates and not ‘AARC-blessed-and-branded’
- Migrate to AARC Wiki?
- How to integrate with the Compendium?

Thank you

Any Questions?

https://aarc-community.org

The work leading to these results has received funding from the European Union and other sources.

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union. Neither the European Union nor the granting authority can be held responsible for them. Grant Agreement No. 101131237 (AARC TREE).