EOSC-hub/GN4-3/EGI/EUDAT/WLCG/IGTF/WISE/SCI Joint Security Policy Group Workshop

Monday afternoon

Do we disseminate ebough? EIRG? - what's the contact for that?

EGI has a monthly newsliter, also EOSC-hub - should we take part in that more?

DaveK presented work at EGI Conference to good response

Opportunities in UK through IRIS to share work (imminent)
If UK, top level, ministry, if they suggest names it's not us

EGI Annual report
Tiziana said it in final presentation

Do we need to spend more time promoting ourselves?

Staff time to spend on outreach.

ISM scope

High medium low integration has been superseded?
Discussion of services now under our scope

What is CMDB? Pavel is Service owner

Need guidance on what implications are for policy - which services would they apply to?
https://confluence.egi.eu/display/EOSC/ISM+scope

Discussion of CMDB - GOCDB+DPMT as implementations of FitSM definition (Configuraiton Management Database)

Where is out work targeted - is it the service catalogue?

Scope includes AAI/accounting “Hub service portfolio”

Where do compute/storage resource providers fit in? Both operationally and for vuln management.

Internal vs external: hub services vs … ?

Policies were developed with user services in mind.

Back office services also important, perhaps different security implications.

Good to have guidance from Matthew Viljoen on this

Combined assurance

Combining assurance from certificate chain and from membership management.
Example of LIGO asking for guidance.
Review of
https://www.eugridpma.org/meetings/2019-05/summary-eugridpma-2019-05-utrecht.txt
Re short term process for LIGO

“We” being IGTF? (IanN)
As relying party, EGI SPG should check?

Enabling communities activity

Define detailed agenda:

GDPR policies: DPK really wants to do today/tomorrow. Privacy notice.
Update of WLCG DP policy framework - today, do more tomorrow

LIGO Combined Assurance, description of vetting, comments and concerns?
Vetting policy, specific points - how to make progress in short term

Community Membership - written up for EGI, consulted on/approved, never formally taken on board

EUDAT comments to be shared

Some discussion - where are we with VM endorsement, haven't expanded to containers, VO portal policy, multi user pilot job, workload…

What do we see the risks are, what are the controls that are needed?

What monitoring is required?

Difficult discussion but should have some.

Vincent: Traceability/Isolation on one part of it. Should also apply to VM.

Who is "they" - scientists don't typically want to have to deal with VMs, communities do.

Risk based discussion we need to have. No point in having policies that are going to be ignored.

Vincent: Site reputation/funding that is at risk.

Commercial provider have set thing up that they can blame customer. For EGI FedCloud, eg, would be reputation of EGI.

VB: Commercial providers have significant security teams, we do not have that per site

With VO in the middle, we can delegate.

Jan: Need to rely on VOs - for large VOs who have their own security teams - for the others?

Vincent: Dirac

Jan: Requirements for sites - also requirements for VOs.

Jan: many of the new centres that have been announced will support containers.

Jan: Deploying software by container is a new issue from a security perspective.

VB: ATLAS wants users to have their own containers.

Jan: User upload container to common hub, or have something that can download from anywhere?

VB: Not sure they are at that stage.

Pilot containers?
VO Portal policy: security requirements follow type of work - canned work vs complete freedom.

Trust marque that says service meets some security policy… (DavidG)

Had resistance to VM endorsement

For today: GDPR/LIGO/AUP

For tomorrow: the rest.

GDPR

Under auspices of WLCG but hopefully useful to others

WLCG Privacy Notice

This is the privacy notice that will be available on the WLCG website, approved by the MB.

IanN: this was originally the overarching thing, which is what it says in the introduction

First para: have been through this
General principles: DK: Is this sufficient for the LHC VOMS instances?
IanN: I would have said so.
Types of data: registration and access.
Registration: Group and role: (for access which role you are you using at that very moment for that very record)

- Discussion of Groups and Roles language.

VO vs Experiment computing

Monday afternoon - got to “How your personal data is protected”

Check on dashes

Tuesday morning

Traceability/Isolation WG recommendations

Current policy on multi-user pilot jobs. Requires mapping of user. Also need to enforce local argus or glexec. None of the 4 VOs are using it (CMS stopped).

WG developing recommendation on how to move traceability forward. Officially split responsibility between site and VO.

https://docs.google.com/document/d/1BmLutIcZZbX0ZqYVWIPDJOUVPNZrssM0SgQF7R3A1B4/edit

Namespaces and cgroups, allow you to isolate users w/out static mapping.

High level recommendation + specific scenarios that match these

Note that this is not a policy, this is a set of recommendations that should go to the GDB next (July?)

What set of policies do we need - need container policy to match VM one
t
VM endorsement policy potentially has implementation guidance as well as policy

These recommendations don't cover direct submission (wherein sites *would* have all the information necessary to do full traceability).

Agreed that recommendations were important and should go to GDB and policy group had identified this as something to be done.

Privacy policy

Discussion of legitimate interest
Before coffee, addressed comments following TIIME
Should we use the WLCG privacy policy as a template?
Take forward to ask for comments at GDB

Baseline AUP questions

https://aarc-project.eu/guidelines/aarc-i044/

Wait for reply from Pavel

Privacy Notice

Security Policy Scope

Discussion around writing policies to be widely applicable by default

CAM discussion

Discussion of LIGO document with notes per section:

1. Overview

Who is Virgo?

2. Scope

3. Onboarding

If you are asking for different levels of assurance, are you asking for different things?

- Ligo Lab
- LSC
- Virgo

3.1 LIGO Lab

- what kind of identification? does this include both photo and national ID number? UK Passport has passport number but not identity number. Sven: we have country id which is separate from passport number. How vital is national number

- Mischa: (MICS or CLASSIC)

3.1.1 process

- an existing LIGO Lab [member]?

Mischa: email with URL. Hard to estimate risk, not something we'd do. Nikhef have to go to helpdesk first. Is this an issue? Procedure - you get an email link, which then in principal anyone can use? How do we know that the password is reset by the person and the person only?

DK: Easier if someone is physically at helpdesk

Linda: must be standard way of doing this.

Mischa: will affect assurance, will it have a major effect.

DK: Is there some other secret that is not in the same email? Ask for clarification?
Mischa: EMail collected during enrollment.

3.1.2 policy

Mischa: if this is same email, then this ensures that the user did get the email.
Vincent: *how* does the sponsor follow up?
DK: Perhaps the policy should come first
Mischa: Would be good to always follow up.
DK/IN: This should be out of band.

3.2 LSC

DK: "Assumed to"? Perhaps as part of MOU it should be required that this is the case? A concern

3.2.1 process

"Typically?" What if not?

IN: Unless we want to protect against them finding a spoof version?

Mischa: How do we know that the Group Manager knows the applicant? It hangs on this.

- How big are the research groups?
- Should be institutional email

3.2.2 policy

Misha: Would be good if this verification was mentioned in the process.

Not sure if this is OK with the IGTF assurance. DG is the one that should say things. Phone might not be sufficient. F2F or via VC with notarised photo ID. Don't allow phone calls or verified emails, this would be lower assurance.
IN: Remote vetting?

3.3 Virgo

3.3.1

No photo ID...

3.3.2 policy

4

5

ACTIONS

Haven't addressed exceptional accounts
Mischa: Does user have to renew, once a year say? If the expiry can be infinite?
DK: Require a maximum length of 13 months. Renewal, existing cred can happen for up to 5 years...
Mischea: MICS CA can't renew you need to prove with IdP.
DK: Potential whole, having got InCommon credential can renew...
DK: Worth documenting what they do.
Mischa: Know that DG has had long discussions with Jim Basney, seemed satisfied, don't know if he's seen the write up.
DK: He's seen it now, pity he's not here...
Mischa/VIncent: Doc number is messed up.

Question: who are we asking about, is this only LIGO Lab?
DK: Formal process, need spreadsheet and checklist