Security Summary

EOSCF WP7 F2F, May 2022

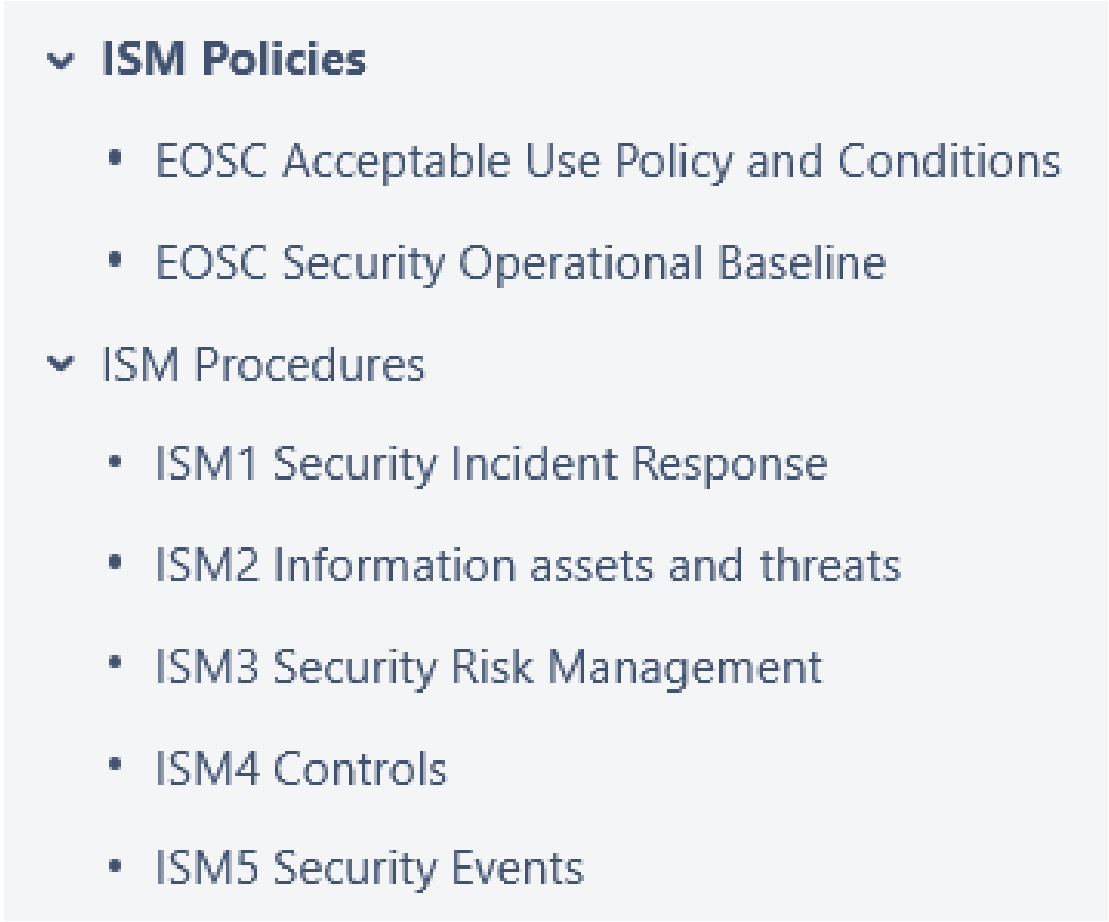
Nikhef
Maastricht University

David Groep – WP7.5 Security Operations and Policy lead
Nikhef Physics Data Processing programme
UM Faculty of Science and Engineering, DKE

ISM SMS revision

- Entirely de-Hubbed now
- Down to 2 policies
- and 5 procedures, but subtly different ones
- added the ‘comms challenge’ as a KPI we can track (2x per year)

- To align with FITSM, security ‘events’ (rather than incidents) are also explicitly triaged
  fixing of the formalities in the procedure will be done later



Incident processing and a common entry point

- *There will (also) be a Zammad security support entry point*
- *Zammad should add at the top of submission UI a warning **not to enter confidential data**, but point to abuse@*
- *The abuse@ email remains in place*
- *On transfer of a ticket to a private system (RTIR or similar), record the transfer and cleanse the confidential data afterwards.*
  (needs testing with Zammad UI, masking titles and content of tickets)
- *Subject to resources in (and beyond) EOSCF, the CSIRT will look at scoped tools (RTIR, hosted at CESNET)*
- *Additional people look at the Zammad queue:*
  DavidG, Baptiste, Alf, DaveK, Ralph (for tracking) + the abuse@ team
- *Will use security-team@eosc-security.eu - to get guaranteed response times*
- *Define the (internal) procedures on the use of Zammad processing.*

Communications challenges (2x per year)

- *Will be mail with the simple question "help" for contact data fixes*
- *Response by email*
- *From address (comms-challenge@eosc-security.eu)*
  (with reply-to set to comms-challenge-response@eosc-security.eu)
  addresses now exists, forwards to pinja, davidc, daniel, and alf
- *No longer than 20+ϵ words.*
- *Defer question "volunteer for tabletop" to the next mail - slowest responders get designated as volunteers.*

Risk management

Need to find a balance between simplicity and unstructured responses, structured responses to simple questions in a (larger) tool, and what could be useful for in-depth risk assessment (as a bonus for those Core services that want that)

Tools, like e.g. MONARC shown by Sven, can do both “ISO27k” as well as other frameworks. But that would need to be configured in such a tool (not all is just ‘CIA’, but one would need to define the risks associated with the ‘assets’, i.e. the Services in EOSC

The risk management team (Urpo, Linda, et al.) will need to discuss this further – but it needs real care and attention now. Baptiste and DavidC, for instance :)

Data protection

“We welcome the identification of data protection
as an effort separate from IT security”

but of course there are close links. But the DPMS does answer lots of question sfor the (relatively simple) EOSC case of ‘everyone is a controller’, and ‘limited number’ of interactions.
Questions such as those from the Observatory, or the Recommender System, can really benefit from the DPMS … if they find it.

Discussion on the pretty-binding-not-quite-corporate rules approach from WISE to data protection guidance will be continued (with input also from EnCo) next week.

Security Frameworks

There are many of these out there – in a free-format discussion we reviewed the NIST Cyberframework (*https://www.nist.gov/cyberframework*), and its mapping to ISO27k2, NIST SP800-53, and others.

But ISO27k10 (multi-domain messaging and information exchange) build very strongly on 27k2, so that might not be the 'light weight' options we were looking for. Still very interesting, though!

And we have the framework based on SCIv2 and can recommend that for EOSC!

Thanks to the EOSC Future WP7.5 collaborators: Alf Moens, Daniel Kouřil, Baptise Grenier, David Crooks, David Groep, David Kelsey, Ian Neilson, Linda Cornwall, Matt Viljoen, Pinja Koskinen, Ralph Niederberger, Romain Wartel, Sven Gabriel, and Urpo Kaila.

EOSC Future

… and now just read the notes in the Agenda

eoscfuture.eu

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

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