Infosec & Quality [ENG] - Sep. 2023

20 Sept 2023

Monte Ortigara (“Don’t forget”). August 2023. Photo by me.

Index

****

01- VERA 7.1

I try to improve the "back to work" after summer holidays issuing VERA 7.1 ("Very easy risk assessment", my Excel spreadsheet for information security risk assessment) in Italian and English on my website: https://www.cesaregallotti.it/Pubblicazioni.html.

VERA 7.1 reports the controls of ISO/IEC 27001:2013 and ISO/IEC 27001:2022 and can help in the transition.

****

02- NIS2 interpretation of the European Commission

On September 18, I participated to the conference on "NIS 2 and other stuff - Practical aspects and experiences". On that occasion, Pierluigi Perri cited the "Commission Guidelines on the application of Article 4 (1) and (2) of Directive (EU) 2022/2555 (NIS 2 Directive)", published on the 14th of September.

Thanks to a post on LinkedIn by Stefano Mele, I found them on the web: https://digital-strategy.ec.europa.eu/en/library/commission-guidelines-application-article-4-1-and-2-directive-eu-20222555-nis-2-directive.

I haven't read them yet, but they're certainly interesting.

****

03- Audit of algorithms (for DSA Regulation)

There is a draft of Delegated regulation (https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13626-Digital-Services-Act-conducting-independent-audits_en) about audits for the DSA Regulation.

The interesting parts are the ones about the audit approaches and the risk of audit. The described approaches are rarely used in information security (e.g. the Delegated regulation describes inherent, control and detection risks). Nevertheless it is good to know them.

****

04- NIST Cybersecurity Framework 2.0 in draft

NIST published the draft CSF 2.0 in early August: https://www.nist.go/cyberframework/updating-nist-cybersecurity-framework-journey-csf-20.

Comments can be sent by November 4th.

****

05- Pharma reference for risk management

Michaël Hooreman, via LinkedIn, pointed me to the document "ICH Q9 Quality risk management - Scientific guideline" of the European Medicines Agency: https://www.ema.europa.eu/en/ich-q9-quality-risk-management-scientific-guideline.

The document presents risk assessment approaches that can be used in the field of quality. In my opinion not only, because they could very well be applied, with some adjustments, also to information security and perhaps to other fields. In all cases, since these are valid and widespread approaches, information security practitioners should know them.

For quality management, this document can help in the identification of the areas of application of risk assessment. In my opinion, ISO 9001, with the latest edition based on HLS, is not very clear on the scope of risk management (problem found on all management system standards). The standard requires to perform only risk management for the effectiveness of the management system (i.e. to have a management risk assessment), but many apply it for operational risks and this is not necessarily a bad thing. This document allows us to improve our understanding on these aspects.

****

06- Recognizing deepfake threats

The NSA, FBI and CISA have published a short (18-page) report entitled "Contextualizing Deepfake Threats to Organizations": https://www.cisa.gov/news-events/alerts/2023/09/12/nsa-fbi-and-cisa-release-cybersecurity-information-sheet-deepfake-threats.

Well written and concise, it explains what these threats are.

One chapter explains why deepfake threats can impact organizations (attacking the image of people connected to the organization, the ability to impersonate someone and then attack someone or gain access to data or systems).

Countermeasures are related to the ability of each person to analyse the potentially altered material.

****

07- Healthcare: IT attacks and patient safety

Sandro Sanna recommended my the Sentinel Event Alert 67 "Preserving patient safety after a cyberattack": https://www.jointcommission.org/resources/sentinel-event/sentinel-event-alert-newsletters/sentinel-event-alert-67-preserving-patient-safety-after-a-cyberattack/.

It is interesting the analysis of the scenarios.

****

08- "Clean" installation of Windows

I recommend an article entitled "Windows 11 has made the "clean Windows install" an oxymoron": https://arstechnica.com/gadgets/2023/08/windows-11-has-made-the-clean-windows-install-an-oxymoron/.

Unfortunately, even before Windows 11, Windows is not "clean" and installs numerous useless (or, better, malicious) software.

****

09- EDPB clarifications on GDPR certifications

European Data Protection Board issued some clarifications about the GDPR certification: https://edpb.europa.eu/our-work-tools/our-documents/letters/edpb-letter-accredia_en.

Text is very technical and more important for certification bodies than for organizations. Here my highlights:

- EDPB repeats that its duty is to evaluate certification criteria, not the accreditation activities because this is the duty of national supervisory authorities;
- the "scheme owner" can be a certification body (for Europrivacy, the scheme owner is Europrivacy itself).

Finally, it seems to me that the accreditation is required for each state (and by each relevant Supervisory authority or national accreditation body) where the certification body works; this can be difficult, considering that EU states are 27 and maybe in the future a mechanism will be implemented for ease this duty. Giovanni Francescutti of DNV does not agrees with me (we had an interesting discussion on LinkedIn). I confess my confusion.

I thank the newsletter Project:IN Lawyers for having given the news.

****

10- Men can do everything (September 2023)

I thought I could not check my twelve-year-old son's WhatsApp chats (the ten-year-old doesn't have a cell phone yet).

Unfortunately, I discovered that some friends send hundreds of gifs and among them I saw blasphemies and a beheading (perhaps from a Daesh video). Then some subscribe others, without asking permission, in other groups of hundreds of people.

Some things are certainly a matter of good manners (avoid sending too much stuff in chats, avoid inserting people in chats without their permissions), others represent risks (spreading the phone number of others, especially if very young), others still concern stuff that require protection by parents.

The only weapon was to contact the parents of some of my son's friends. Luckily, good people who immediately understood the meaning of communication.

****

EONL