Infosec & Quality [ENG] - Oct. 2023

23 Oct 2023

Changdeokgung (Seoul). October 2023. Picture by myself.

Table of contents

****

01- Standardization: Status of standards ISO/IEC 270xx - ISMS

The semi-annual meeting of ISO/IEC JTC 1 SC 27 WG 1 (information security management systems or ISMS) and WG 5 (privacy) ended on October 20.

I report the activities of WG 1 that I consider the most significant ones.

For ISO/IEC 27000 (Overview of ISMS), ISO/IEC 27003 (guidelines for implementing an ISMS), ISO/IEC 27008 (guidelines for evaluating information security controls) and ISO/IEC 27109 on cybersecurity education and training, the works for the update or drafting have started.

For ISO/IEC 27017 (extension of ISO/IEC 27002 controls to cloud services), work is in progress for aligning the current version with ISO/IEC 27002:2022 controls. I imagine the new standard will be published in late 2024.

An update of ISO/IEC 27006-1 (standards for accreditation of certification bodies) will be published soon, and then work will start again to "clean" it of incorrect references to requirements and controls, remembering that controls are not requirements and controls don't need to be implemented, but only used as a reference for the Statement of Applicability.

ISO/IEC 27011 (extension of controls of ISO/IEC 27002 for the telecommunications sector) will be published soon. ISO/IEC 27013 (relationships between ISO/IEC 27001 and ISO/IEC 20000-1) and ISO/IEC 27019 (extension of controls of ISO/IEC 27002 for the energy sector) are at an earlier stage and will probably be published in mid-2024.

The next version of ISO/IEC 27001 will have to have climate change requirements because of changes made to the HLS (or Annex SL, i.e., the basic structure for all management systems standards). The question has been raised as to what climate change impacts can be considered for an information security management system.

****

02- Standardization: Status of standards ISO/IEC 270xx - Privacy

The semi-annual meeting of ISO/IEC JTC 1 SC 27 WG 1 (information security management systems or ISMS) and WG 5 (privacy) ended on October 20.

I report the activities of WG 5 that I consider the most significant ones.

About ISO/IEC 27701, for privacy information management systems (PIMS): an update, intended only to realigning controls with those in ISO/IEC 27002:2022, was scheduled to be published in mid-2024. Instead, the ISO Central Secretariat required to restructure the standard like others on management systems. All experts agreed on the need to restructure it completely and, therefore, delay publication to avoid inconsistencies and errors (some hope publication by early 2025, I think it will take longer).

A new version of ISO/IEC 27006-2 (for certification bodies) will be published by mid-2024, but work will have to start againg to draft a standard compatible with the future ISO/IEC 27701. The risk is that we will be quick in publishing certification criteria (the future

ISO/IEC 27701), but slower for accreditation criteria (the future ISO/IEC 27006-2, assuming it keeps this numbering); in other words, we may have a new version of ISO/IEC 27701, but no certification body that can carry on audits and issue certificates for lack of appropriate rules.

Work is continuing on ISO/IEC 27018 (extension of ISO/IEC 27002 controls for privacy in cloud services) to align the current version with ISO/IEC 27002:2022 controls. They plan to publish the update in mid-2024 (but that seems too optimistic and I predict late 2024).

ISO/IEC 29151 is being discussed (work on the update has just started). This standard is intended only for data controllers and takes the controls of ISO/IEC 27002, extends its implementation guidelines and adds others specific to privacy. It seems to me that it is completely ignored in Italy, while in other countries it is used as a reference by SMEs that do not intend to use ISO/IEC 27701 (although then, a quick online search tells me that Huawei Cloud, certainly not an SME, is "certified" against this standard, which, by the way, does not have a certification scheme). An update is expected to be published in late 2025.

****

03- CISA Guide on Identity and Access Management

In SANS NewsBites of October 6, 2023, I recommend the news "CISA and NSA: Identity and Access Management Guidance", which in turn refers to the publication "Identity and Access Management: Developer and Vendor Challenges".

This publication does not seem very interesting to me because it summarizes some critical issues, which are also known.

However, there is a reference to document dated March 2023 and entitled "Identity and Access Management: Recommended Best Practices for Administrators": https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/3336001/esf-partners-nsa-and-cisa-release-identity-and-access-management-recommended-be/.

This, although it does not say anything new, seems to me interesting for a review of the basic rules for access control and IAM. It should be noted that a large part of the document is dedicated to the MFA techniques.

****

04- Security-by-Design and Default Principles del CISA - Update

In April I recommended the excellent paper by CISA (U.S. Cybersecurity & infrastructure security agency) entitled "Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Security-by-Design and -Default." It has been updated with more detail to demonstrate compliance with the three principles: https://www.cisa.gov/resources-tools/resources/secure-by-design.

Actually, the previous version is no longer available, so I can't point to the exact changes. In April I had said that "in a few pages (15 in all, including table of contents and introductory

fuff) the principles of safe development and engineering are given and explained." Now there are 36 pages, but I think the extra details help and do not weigh down.

****

05- The most common IT network configuration errors (and mitigations)

From SANS NewsBites of October 6, 2023, I report the news "CISA and NSA: Most Common Network Misconfigurations", which in turn refers to the document "NSA and CISA Red and Blue Teams Share Top Ten Cybersecurity Misconfigurations": https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-278a.

The pdf can be found at the following link: https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/3549369/nsa-and-cisa-advise-on-top-ten-cybersecurity-misconfigurations/.

Nothing new, certainly, but always useful to review.

I would like to point out that from page 17 to page 27 you will find recommendations for users, from page 27 to page 31 you will find recommendations for software developers.

****

06- Is there a lack of information security (or cybersecurity) experts?

From Crypto-gram of October 2023 I recommend "On the Cybersecurity Jobs Shortage": https://www.schneier.com/blog/archives/2023/09/on-the-cybersecurity-jobs-shortage.html.

Many complain about the shortage of skilled people in the information security and cybersecurity fields. Bruce Schneier reports on a comment by Ben Rothke. He basically says that many required roles are specialized, not generalist. And it's true that there's a shortage of people with specialized skills, and it's even harder to find them if we think that to have specialized skills you also need to have experience.

I would add that, at least in Italy, there are difficulties in finding people to fill certain roles, even generalist ones.

****

07- European Cybersecurity Skills Framework (ECSF)

Franco Vincenzo Ferrari pointed me to the publication of ENISA's European Cybersecurity Skills Framework (ECSF): https://www.enisa.europa.eu/topics/education/european-cybersecurity-skills-framework.

You can download the ECSF Role Profiles document, where the 12 typical cybersecurity profiles are specified. As we know, these can be useful for sharing the terminology used for professional qualifications.

****

08- New version of NIST SP 800-82 on OT

I point out the publication of the r3 of the NIST SP 800-82 entitled "Guide to Operational Technology (OT) Security": https://csrc.nist.gov/pubs/sp/800/82/r3/final.

I had read version 2 and found it very interesting. It reports many things that are found in IEC 62443, but in free format.

The changes made by this version 3 are numerous and are summarized on the last page.

However, I note with some disappointment that NIST is continuing to have longer and longer documents and in fact this version is 316 pages long, while the previous one was 247 pages long.

****

09- New Machinery and Cybersecurity Regulation

Regulation (EU) 2023/1230 on machinery has been published. It withdraws the Machinery Directive, i.e. the Directive on the safety of industrial machinery (my explanation is very imprecise and serves only to contextualize).

In very few words, the Regulation introduces the need to evaluate the safety of machines also with regard to hardware and software. This is very important because hardware and software that don't work properly can lead to unexpected operations and, therefore, dangers to people.

The text of the Regulation can be found here: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32023R1230.

The Regulation shall apply from 14 January 2027.

Once again, details on how to evaluate machines will be further specified in the harmonisation legislation.

****

10- Threats and attacks: ENISA Cybersecurity Threat Landscape 2023

ENISA published the Cybersecurity Threat Landscape 2023: https://www.enisa.europa.eu/news/eu-elections-at-risk-with-rise-of-ai-enabled-information-manipulation.

ENISA's main focus is on: information manipulation campaigns (fake news), social engineering toward specific people, Trojans in known software packages (which are downloaded from counterfeit sites), and exploitation of misconfigurations of systems, networks, and cloud services.

The first two threats (information manipulation and social engineering) are becoming more effective due to the use of artificial intelligence-based tools, which allow old techniques to be applied, but more efficiently and effectively.

I have only highlighted a few things from the executive summary here, but the document is much broader.

Unfortunately, the part on mitigation measures is extremely brief and does not add anything significant (it is mainly a list of ISO/IEC 27002 and NIST CSF controls).

****

11- Threats and attacks: Detecting AI-generated text

From Crypto-gram of October 2023, I recommend the article "Detecting AI-Generated Text": https://www.schneier.com/blog/archives/2023/09/detecting-ai-generated-text.html.

Short version: it seems that there are not tools to automatically detect AI-generated text.

One comment (ironic, I think...) points out that perhaps this same response was generated by AI.

****

12- Men can do everything (October 2023)

This summer my wife had to attend a training course. I went with children (or teenagers) to the beach for 5 days in an apartment. We kept it tidy and clean, we cooked, we kept ourselves tidy and clean.

They called me "Mr. mom" and I complained about it: "Mr. Mom" makes it seem that certain things can only be done by moms and dads should do them only in extraordinary cases. I tried to be a dad (maybe badly, but that's another story).

****

Translation done with the help of https://www.deepl.com/.

EONL