Infosec & Quality [ENG] - May 2023

16 May 2023

Juvenilia. Before the match. May 2023. I'm not the author of the photo.

Index

****

01- Status of ISO/IEC 270xx standards - April 2023

In April, the semi-annual meetings of ISO/IEC JTC 1 SC 27 WG 1 and WG 5 were concluded. These are the groups that draft ISO/IEC 27001, 27002, 27005 etc. and privacy standards, including ISO/IEC 27701.

As for WG 1, the activities took place online and the meeting served to summarize the activities carried out in other meetings since October.

Work has begun on the revision of ISO/IEC 27000 (overview on ISMS), 27003 (guide to 27001) and 27004 (on measurements). These are very important standards.

It was then decided not to start to work on a new edition of the ISO/IEC 27001, even though the 2022 version had been quickly prepared to update Annex A (following the new ISO/IEC 27002) and incorporate the changes to the HLS.

We have been informed that, at IAF level (i.e. the body that promotes and controls accreditation activities), ISO/IEC 27001 and ISO/IEC 20000 groups have been merged to achieve greater consistency in accreditations related to data security and information technology. I wonder that many would like ISO/IEC 20000-1 to deal with services in general and that ISO/IEC 27001 does not only deal with computer security (or cybersecurity).

With regard to the activities of WG 5, which deals with privacy, work continued on ISO/IEC 27006-2 (i.e. accreditation requirements). Work has started on a standard on privacy and artificial intelligence (ISO/IEC 27091). I also noticed a lot of work on age verification standards.

Important, in my opinion, is the work being concluded for ISO/IEC 27701, i.e. the standard for the certification of privacy management systems (extension of ISO/IEC 27001). In fact, the standard passes into FDIS status and therefore by the end of the year the updated edition should come out. This new edition will not have any new or improved requirement, the changes are only for alignment with ISO/IEC 27001:2022 and ISO/IEC 27002:2022.

On this front, work on updating ISO/IEC 27018 (privacy for cloud service providers, extension of ISO/IEC 27002) is progressing slowly.

A new version of ISO/IEC 29134 on DPIA will be soon published. It is a minor revision (on this I had already written in the past that it is a shame, since the standard would require a significant update, based on the experience gained in recent years).

****

02- Information security: the new ISO/IEC 27005 on risk management

I wrote an article on the new ISO/IEC 27005 on information security risk management: https://www.linkedin.com/pulse/new-isoiec-27005-information-security-risk-assessment-cesare-gallotti.

I summarized thoughts that I wrote before on other occasions.

As always, I am open to discussion in case someone wants to discuss my positions.

****

03- UKAS accreditation no longer valid for public procurement in Italy

The title in English is "Public procurement, UKAS accredited entities no more recognized for certifications because of Brexit": https://ntplusdiritto.ilsole24ore.com/art/appalti-pubblici-brexit-taglia-fuori-soggetti-accreditati-ukas-le-certificazioni-AELxQIND (in Italian).

Thanks to Fabrizio Cirilli and Franco Vincenzo Ferrari for having recommended this article.

Short version: certificates accredited by non-European bodies are not considered valid to participate in public tenders in Italy. The interpretation should also cover certificates accredited in Albania, India, USA, Switzerland, etc. I have not investigated whether EEA but not EU accreditation bodies are also excluded (Iceland, Liechtenstein and Norway).

****

04- CISA Security-by-Design and Default Principles

Excellent document of CISA (Cybersecurity & infrastructure security agency) with title "Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Security-by-Design and -Default": https://www.cisa.gov/news-events/alerts/2023/04/13/shifting-balance-cybersecurity-risk-security-design-and-default-principles.

In a few pages (15 in all, including index and introductory fluff) the principles of secure development and engineering are explained.

****

05- Italian Supreme Court: Poste Italiane not liable for phishing

Article (in Italian) with title "Phishing, why did the Supreme Court considers Poste Italiane not liable and condemn account holders?": https://www.cybersecitalia.it/phishing-la-cassazione-se-cliente-truffato-la-banca-non-responsabile/24214/.

I thank Maurizio Tardanico who recommended me this article.

This is a part of the text to give a first idea: "the Supreme Court has established that the bank or credit institution has no responsibility for the theft of money of account holders caused by phishing, if it has adopted a security system such as to prevent third parties from accessing the account and if the customers themselves have provided access codes to other people, obviously, without being aware of it, because they were cheated".

****

06- Privacy: Interpretation of the EU Court of Justice on pseudonymised and anonymous data

Post (in Italian) on the decision T-557/20 of 26 April 2023 of the EU Court of Justice on pseudonymous and anonymous data: https://www.linkedin.com/posts/maria-grassetto-1a8bb25b_cge-activity-7060175275069779968-LAWc.

I translate from the newsletter of Project:IN Lawyers: according to the Court it is necessary to reason on the position of the "recipient" of the personal data, to investigate if it is - or not - able to identify the data subjects, and, therefore, if it carries out a "treatment" of personal data.

****

07- Privacy: Dark Patterns

Version 2 of the EDPB Guidelines 03/2022 on deceptive design patterns in social media platform interfaces: how to recognize and avoid them: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-032022-deceptive-design-patterns-social-media_en.

On this topic I was completely unaware. Unfortunately, the document does not give concrete examples and therefore, in some cases, some things are obscure to me.

However, dark patterns are more general things and are not just about privacy. There are some articles in Internet about this.

****

08- Men can do everything (May 2023)

May 15. Today I started a course late. I accompany the little one to school, then I meet a mother of a classmate of the big one and we exchange ideas on how to deal with homework. The discussion interests me and time passes...

I hope that course participants do not send a complaint (the course will end on Wednesday).

PS: in the picture there are not my children.

****

EONL

Translation with the help of Microsoft Translator