

Cartography of cybersecurity standardisation

12 mars 2026

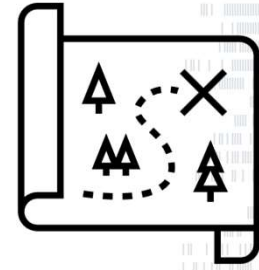
JP. Quemard

ACN

Alliance pour la confiance numérique ■ ■ ■

www.confiance-numerique.fr

Why a cartography ?



- Complexity of the environment:
 - European regulations are large, numerous and complex :
 - European regulation UE 1025/2012 under revision
 - CSA, CRA, NIS2, IA act DATA act DSA, DORA, ...
 - The standardisation stakeholders are various :
 - International bodies ISO, IEC, ITU
 - European bodies CEN, CENELEC, ETSI
 - European agencies ENISA JRC and DG's CNCT, GROW,
 - National bodies NIST, AFNOR, DIN, ...
 - Industrial Forums OASIS, Open Forum, OACI, W3C, IEEE, Global platform, Fido,
 - There is no clear delineation between the scope of each standardisation body, there is therefore a high of duplication of effort, inconsistency or contradiction.
- To find your way you need a map : a cartography action has been started by ACN (**A**lliance pour la **C**onfiance **N**umérique) French professional syndicate

An exemple : IA standardisation ?

- ISO/IEC SC 27 is providing its expertise in cybersecurity and privacy protection on emerging technological topics like Artificial Intelligence. SC 27 is now starting AI security evaluation standardization. :
 - ISO/IEC PWI 25240 Evaluation of AI-based Technology
 - ISO/IEC DIS 27090 Guidance for addressing security threats to AI systems
 - ISO/IEC CD 27091 Artificial intelligence, privacy protection
 - ISO/IEC NP 25959 Artificial Intelligence, Machine learning model evaluation metrics.
 - ISO/IEC NP 26160: Enhancing the ISO/IEC 15408 series and ISO/IEC 18045 for the Evaluation of Artificial Intelligence (AI) Functionality
- ISO/IEC SC 42 is dedicated on AI standard development and is leading the international AI standardization. It creates the foundational rules used across all industries (healthcare, finance, etc.) to ensure AI is safe, trustworthy, and interoperable.
 - ISO/IEC 42001:2023 Artificial Intelligence Management System - AIMS
 - ISO/IEC 23894:2023 AI Risk Management.
- ITU-T SG 17 positions itself as the lead Study Group for AI security within ITU-T.

An exemple : IA standardisation ?

- At European level the situation is the same :
 - ETSI TC SAI addresses 4 main aspects of AI security standardization :
 - Securing AI from attack e.g. where AI is a component in the system that needs defending.
 - Mitigating against AI e.g. where AI is the 'problem' (or used to improve and enhance other more conventional attack vectors)
 - Using AI to enhance security measures against attack from other things e.g. AI is part of the 'solution' (or used to improve and enhance more conventional countermeasures)
 - Societal security and safety aspects of the use and application of AI.
- CEN/CLC JTC21
 - WG 5: Joint standardization on Cybersecurity for AI systems. Strong coordination with CEN/CLC JTC13 Cybersecurity and data privacy :
 - EN 18282 Cybersecurity specifications for AI Systems
- CEN/CLC JTC13
 - Is mirroring ISO/IEC SC27 and potentially will transpose SC27 standards in EN

An exemple : IA standardisation ?

- More than four different standardisation bodies involved on common topics : high risk on the results
- Multiplying the Standardisation TC will increase the workload, and the expert resource is scarce
- Scope of the different TC shall be very well defined,
- Coordination and liaison management has to be dramatically improved
- Large use of Vienna, Frankfurt and Dresden agreement to avoid NIH syndrome and maximize the reuse of material.

Conclusions on cartography ?



- Cartography is a tool to map the different initiatives and help to identify gaps, overlap and contradictions in order to set up a global road **map**
- It will help, producing the big picture, to simplify and rationalise the efforts in standardisation work
- It will minimize the necessary workload because one of our main concern is the lack of experts
- It will ease the access by SME's to standardisation world
- Access cost has to be taken into account and reducing the number of standards goes in the right direction