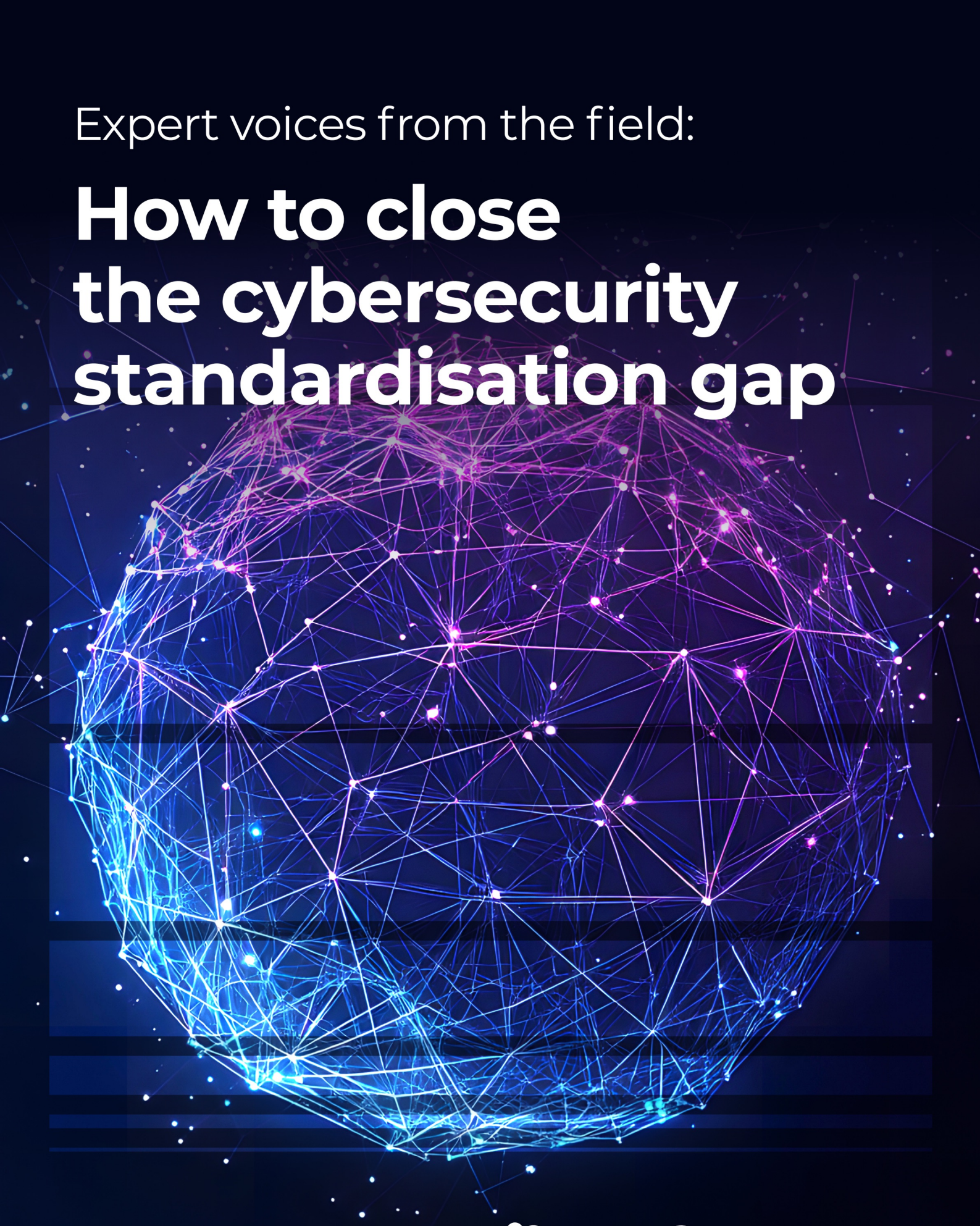
Expert voices from the field:

How to close the cybersecurity standardisation gap



standICT.eu2026
ICT Standardisation Observatory and Support Fac

CYBERSTAND.eu

HSbooster.eu
Horizon Standardisation Booster

INSTAR

NERO

6 October 2025

Funded by
the European Union

Authors

Luigi Colucci,
Project Manager at Trust-IT Services
(StandICT.eu; CYBERSTAND.eu; INSTAR; HSbooster)

Acknowledgement

Erik Andersen, Consultant at Andersen's L-Service (CYBERSTAND.eu; INSTAR; StandICT.eu)
Peter Baard, Epic Owner Digital Grid & Chair Energy ISAC Netherlands at Alliander (Volunteer at DIVD) (CYBERSTAND.eu)
Rob Brennan, Assistant Professor at University College Dublin (INSTAR)
Julien Bringer, CEO at Kallistech (CYBERSTAND.eu; INSTAR; StandICT.eu)
Alex Cadzow, Cybersecurity and Human Factors Researcher at Cadzow Communications Consulting (HSBooster.eu; StandICT.eu)
Scott Cadzow, Standards Expert at Cadzow Communications Consulting Ltd (HSBooster.eu; INSTAR; StandICT.eu)
Paolo Campegiani, Head of Innovation at Namirial (StandICT.eu)
Argyro Chatzopoulou, Senior Policy Consultant at APIROPLUS Solutions Ltd (Other)
Tasos Dagiuklas, Professor in Computer Science at London South Bank University (INSTAR)
Stefano Dalmiani, Chief Digital Officer at Monasterio Foundation Research Hospitals (HSBooster.eu)
Angelo D'Amato, Founder at Vulnir B.V. (CYBERSTAND.eu; INSTAR)
James Davenport, Professor and Incident Commander at University of Bath (StandICT.eu)
Sebastian Elfors, Senior Architect and Trust Services CSO at IDnow (INSTAR; Other)
Gorry Fairhurst, IETF Area Director at University of Aberdeen (StandICT.eu)
Nicola Filosa, Certification Engineer at Eliwell by Schneider Electric (CYBERSTAND.eu)
Sandra Feliciano, Head of Research Engagement - AI & Cybersecurity at MENAPS (CYBERSTAND.eu; StandICT.eu)
Fotios Giannakopoulos, Director at Bavarian Consultants (HSBooster.eu; INSTAR; StandICT.eu)
Jose Luis Hernandez Ramos, Associate Professor at University of Murcia (CYBERSTAND.eu)
Axel Hoehnke, Business Advisor Compliance and Cybersecurity at Axel Hoehnke Consulting (CYBERSTAND.eu)
Raul Sanchez-Reillo, Full Professor and R&D Director at Universidad Carlos III de Madrid (INSTAR; StandICT.eu)
Antonio Jara, CSO at Libelium (StandICT.eu)
Anna Maria Mandalari, Assistant Professor and CTO at UL/Mulini SRL (CYBERSTAND.eu)
Paolo Marcheschi, Electronic Engineer specialised in Biomedical Technologies and Standardisation at Monasterio.it (HSBooster.eu)

Francisco Medeiros, Director at FM Tech Consult BV (CYBERSTAND.eu; HSBooster.eu; StandICT.eu

Elmustapha Ouchamch, Ambassador NICE / NIST Program at IEEE Morocco Chapter (Other)

Nicolae Paladi, CEO at Canary Bit AB (HSBooster.eu; StandICT.eu)

Octavian Popescu, Consultant at EUCOMREG SRL (CYBERSTAND.eu; StandICT.eu)

Robin Renwick, Analyst at Erk Media Ltd (StandICT.eu; Other)

Pawel Rybicki, President of the Management Board and Forensic Science Programme Director at Homeland Security Institute - EFIC (INSTAR)

Farhan Sahito, Director General at Privanova (CYBERSTAND.eu; HSBooster.eu; StandICT.eu)

Antoine Sciberras, Senior Lecturer (Visiting) at University of Malta (INSTAR)

Jean-Francois Sulzer, Consultant at JF Sulzer Conseil (CYBERSTAND.eu; StandICT.eu)

Predrag Tasevski, Founder & CEO at Unicis.Tech OÜ (Other)

Iva Tasheva, CEO at CYEN (CYBERSTAND.eu)

Javier Tallón, Freelance at Freelance (StandICT.eu)

Karim Tobich, Director at CyberSecurity & Technology Consultancy (INSTAR; StandICT.eu)

Constantinos Tsiourtos, Managing Director at KINEAS LLC (CYBERSTAND.eu; INSTAR)

Gill Whitney, Independent Expert at ANEC (StandICT.eu)

Evgeni Yordanov, CEO at Adamanta (CYBERSTAND.eu; StandICT.eu)

About this report

This report was developed by the EU-funded project StandICT.eu 2026 in collaboration with the EU-funded projects CYBERSTAND.eu, INSTAR, HSbooster.eu, and NERO. The insights and recommendations shared here come directly from the communities built through these projects, reflecting the hands-on experience of experts actively shaping cybersecurity standards. These perspectives are unique and not available anywhere else online, as they stem from real-world engagement rather than theory. This report gathers expert insights and recommendations to help close this gap and strengthen Europe's role in global cybersecurity standardisation.

About StandICT.eu

The StandICT.eu 2026 Coordination and Support Action project is funded by the European Union under grant agreement no. 101091933. The project is coordinated by Trust-IT Srl (IT) in quality of Technical Coordinator and Dublin City University (IE) in quality of Financial Coordinator, supported by the partners European Digital SME Alliance (BE), OpenForum Europe (BE), Australo (ES) and Fraunhofer ISI (DE). The content of the present report does not represent the opinion of the European Union, and the European Union is not responsible for any use that might be made of such content.

Experts insights

Q: What should early-career professionals do today to close their cybersecurity standardisation skills gap?

A: ***By blending education, practice, and community involvement, early-career professionals can bridge the gap and grow into effective contributors to cybersecurity standardisation. In short: learn, apply, engage, and repeat.***

Early-career professionals can close their cybersecurity standardisation skills gap by combining structured learning, hands-on practice, and community engagement. Start by building a solid foundation. Complete as many cybersecurity courses as possible, participate in challenges such as “Hack The Flag” (HTF), Join cybersecurity communities (LinkedIn groups, Women in Cybersecurity (WiCyS), Cyber Security Europe, etc.), and learn core frameworks such as ISO/IEC 27001, NIST Cybersecurity Framework, and ETSI EN standards. Understand the EU landscape: NIS2 Directive, Cyber Resilience Act, and ENISA guidance. Subscribe to newsletters, follow technology news, and track emerging vulnerabilities to stay current. Then, apply what you learn. Practice by implementing a standard in a small project or workplace task. Create checklists, policies, or Software Bill of Materials (SBOM) to turn theory into tangible results. Participate in audits or compliance exercises when possible, seeing standards in action accelerates understanding. Get involved with the standardisation community early. Join your national standardisation body or mirror committee as an observer. Attend working group meetings, ETSI events, or IETF hackathons to see how standards are created and debated. Even small contributions, like commenting on draft documents, build confidence and credibility. Seek mentorship and peer support. challenge your department and institutional leaders to allow you to get involved in standardization and to recognize your contributions to standardization. Find experienced professionals who can explain the “unwritten rules” of standardisation. Coffee breaks at conferences or informal chats often provide more insight than presentations. Networking also opens doors to projects, collaborations, and funding opportunities. Finally, adopt a continuous learning mindset. Cybersecurity evolves fast, plan for regular training every 2–3 years. Explore cross-domain knowledge: combine technical skills with understanding of governance, law, and policy. Stay curious, ask questions, and focus on real-world impact rather than just theory or buzzwords.

Q: From your perspective, why does the cybersecurity standardisation skills gap exist, and why is it still here?

A: ***In short, the skills gap persists because standards are undervalued, hard to access, slow to evolve, and rarely taught. Without stronger incentives, clearer career paths, and more inclusive processes, standardisation will remain a niche domain, even as cybersecurity itself becomes ever more critical to our digital society.***

The cybersecurity standardization skills gap is a joint reflection of two different problems need to be addressed separately: cybersecurity skills gap and standardization skills gap. The cybersecurity standardisation skills gap has persisted for years despite growing awareness. Historically, cyber threats evolve rapidly and keep increasing, while education lags behind, failing to train new professionals. Standardisation remains mostly absent from curricula at every level, because most educators are not familiar with the standardization world. Cybersecurity developed reactively, with experts focused on stopping attacks rather than building long-term frameworks. This created a "firefighting" culture where immediate technical fixes are valued more than prevention and governance. As a result, many professionals are trained to configure systems or defend networks, but not to translate technical actions into compliance language or to navigate the complex world of standards. The landscape itself is fragmented and confusing. For newcomers, the "regulation framework sprawl" can be overwhelming, especially when many standards are behind paywalls or require expensive memberships to access. Education systems rarely teach standardisation. Most universities focus on technical skills, leaving graduates unprepared to understand how standards are developed or why they matter. There are almost no dedicated courses or career pathways in this field, so young professionals usually discover it by accident, often only after a regulatory incident forces their company to comply. Without structured training or mentorship, entry into the standardisation world is slow and intimidating. Industry practices also play a major role. Companies tend to prioritise speed-to-market over governance, treating standards as a checkbox for contracts rather than a strategic tool. Senior staff or regulatory teams usually handle compliance, while early-career professionals are kept away from standardisation work. This lack of exposure limits skill growth and makes the field seem inaccessible. Meanwhile, the pace of technological change far outstrips the speed of standardisation processes. Standards take years to develop through consensus, while technologies like cloud, IoT, and AI evolve in months. This lag leaves gaps between what the standards say and what practitioners face in real life. Finally, participation in standardisation is costly and time-intensive. Travel to meetings, reviewing drafts, or developing prototypes all require management support and budget. SMEs, law enforcement agencies, and even universities often lack the resources to actively engage, which keeps the pool of experts small and ageing.

Q: What recommendations would you give now to policymakers to close the gap?

A: ***By streamlining frameworks, investing in education, removing barriers, incentivising participation, and raising awareness, policymakers can turn standardisation from a niche activity into a core pillar of Europe's digital resilience.***

To close the cybersecurity standardisation skills gap, policymakers should focus on simplifying the landscape, building capacity, and removing barriers that prevent professionals and organisations from engaging. First, harmonise standards and regulations. Right now, cybersecurity is fragmented across NIS2, CRA, GDPR, sector-specific rules, and multiple international frameworks. This "framework sprawl" confuses professionals. Clear mapping guides and a coherent EU-wide framework would make compliance simpler and reduce duplication. Second, make it mandatory for European standardization organizations (ETSI, CEN and CENELEC), as well as national standardization bodies of European countries ,to identify the names of contributors to standards inside published standards, the same way authors of academic papers are identified when these are published. Third, integrate standardisation into education and training. Cybersecurity degrees rarely teach how standards are made or applied. Universities, technical schools, and bootcamps should include modules on governance, risk, and compliance, ensuring graduates enter the workforce with baseline knowledge of ISO/IEC 27001, ETSI and CEN-CENELEC standards, and EU regulations. Hands-on labs, sandboxes, and cross-sector testbeds would turn theory into practice. In parallel, European Quality Assurance Forum (ENQA) and its members should make it mandatory to require and recognise participation in standardisation technical committees and contributions to published standards. This recognition should be equal to that given to research activities, such as publishing academic articles, supporting career advancement and incentivising active engagement in the standardisation process. Fourth, make participation accessible and affordable. Many SMEs, researchers, and young professionals are excluded by paywalls and high costs to attend meetings or access standards. Policymakers should fund free or low-cost access to essential cybersecurity standards and provide travel grants or fellowships for early-career experts to join SDOs like ETSI or ISO, as has been done through EU-funded projects such as StandICT and CYBERSTAND.eu. This would expand the pool of contributors and bring fresh talent into the field. Fifth, incentivise involvement and adoption. Tax credits, compliance vouchers, and funding tied to Horizon Europe or Digital Europe projects could reward SMEs and innovators who actively implement and contribute to standards. Public procurement rules should also favour companies that demonstrate strong compliance and engagement in standardisation. Finally, promote awareness and collaboration. Most people see standards as abstract or bureaucratic. Public campaigns, case studies, and simple "how-to" guides can show their value and impact. At the same time, closer cooperation between regulators, industry, and standards bodies is needed to align policy with real-world practice and accelerate the development of effective, relevant standards.

Q: If you could choose, what bold or unconventional actions would you take to close this gap in 1-2 years?

A: ***Together, the three steps below would remove access barriers, build capacity, and turn theory into practice, dramatically reducing the gap within 1–2 years.***

To close the cybersecurity standardisation skills gap quickly, bold actions are needed to cut through bureaucracy and lower barriers to entry. Make standards and compliance tools open and free. Today, many essential cybersecurity standards are locked behind paywalls, accessible only to large organisations. By making these standards freely available, along with open-source compliance toolkits and templates, SMEs and individuals could learn and apply requirements without costly consultants. This would immediately expand participation and speed up adoption. Revise the ETSI Directives and CEN Internal Regulations to include the names of contributors directly in published standards, similar to how authors are credited in academic papers. This recognition would not affect the copyright held by standardisation organisations over the published standards. Launch an EU-wide Cyber Standards Academy and Fellowship. Promote existing efforts and create a centralised online academy offering plain-language courses on NIS2, CRA, ISO, and CEN-CENELEC and ETSI standards, plus hands-on labs and sandbox environments. At the same time, fund a European fellowship programme placing early-career professionals directly inside ETSI, CEN/CENELEC, and leading companies for 6-12 months. Immersive, real-world exposure would rapidly train a new generation of standardisation experts. Finally, mandate “standardisation sprints” in EU-funded projects. Like hackathons, these rapid cycles would bring together engineers, lawyers, policymakers, and SMEs to apply standards in real time to live products and systems. Every EU-funded cybersecurity project would be required to deliver a tangible standards contribution, a draft, a mapping guide, or a technical annex. This would create both practical resources for others to use and a fast track for developing skills through action.

Q: What are the top five emerging skills that are currently missing in cybersecurity standardisation?

A: ***The cybersecurity standardisation field is evolving quickly, but many critical skills are missing. These gaps span both technical expertise and cross-disciplinary abilities, making it harder to develop standards that keep up with innovation, regulation, and real-world needs.***

One of the most urgent gaps is AI and Generative AI security. As AI becomes embedded in everything from cloud systems to consumer devices, professionals need to understand how AI can be attacked, how to respond to AI-driven incidents, and how to align systems with the EU AI Act. This also includes AI risk assessment and governance, as well as the ability to handle AI-related cyber threat intelligence. Closely linked to this is post-quantum cryptography. Quantum computing threatens to break today's cryptographic methods, so experts must develop and deploy quantum-resistant algorithms and manage the complex transition period between classical and quantum-safe systems. Another missing area is compliance-as-code and automation. Most standards today are still human-readable PDFs. Professionals need to move towards machine-readable, API-based standards that integrate directly into Continuous Integration / Continuous Delivery pipelines. Automated checks and continuous validation would make compliance faster, cheaper, and more scalable, especially for SMEs. There is also a lack of policy-to-code translation skills. Many organisations have strong technical security but still fail audits because they cannot map what they do to legal requirements like NIS2, CRA, or GDPR. Experts are needed who can interpret complex regulations and turn them into clear, testable technical controls and guidance that engineers can implement. SBOM (Software Bill of Materials) lifecycle management is another growing need. SBOMs are essential for supply chain security, allowing companies to track all software components and dependencies. Skills are needed to generate, validate, and use SBOMs effectively, ensuring rapid response when vulnerabilities like Log4j emerge. Cloud security and DevSecOps automation are also underdeveloped. Many current standards were built for on-premises systems and don't fit modern cloud-native environments. Professionals must learn to design and test cloud security controls, automate compliance checks, and prevent vendor lock-in while maintaining interoperability across platforms.

A: The rise of cyber-physical systems, like IoT, smart cities, industrial control systems, and autonomous vehicles, creates a pressing need for expertise at the intersection of safety and cybersecurity. This includes digital twins, connected vehicles, and critical infrastructure where a security failure can have physical, even life-threatening consequences. Another gap lies in data space and interoperability security. Very few professionals understand how to secure federated data exchange systems and sovereign data connectors. Beyond technology, there is a shortage of standardisation negotiation and collaboration skills. Developing standards isn't just technical, it requires diplomacy, communication, and the ability to reach consensus among diverse stakeholders, including regulators, companies, and civil society. Plain-language communication of standards is also missing. Many standards are written in highly technical language that is inaccessible to SMEs, policymakers, and even engineers outside the standardisation circle. Experts who can explain standards clearly are vital to increasing adoption. In addition, there is limited knowledge of forensic readiness and digital evidence handling. As cyber incidents increasingly require legal action, professionals need to know how to preserve evidence, maintain chain of custody, and produce cross-border, admissible documentation. This is especially urgent for law enforcement, healthcare, and critical infrastructure. Zero Trust architectures are another area where skills are lacking. Different regions are pushing fragmented approaches, and few professionals know how to build interoperable, harmonised Zero Trust solutions. From a structural perspective, there is a lack of cross-domain knowledge. Standards now cut across multiple sectors, cloud, IoT, AI, telecoms, but most professionals specialise in only one domain. Understanding overlaps and interoperability is essential to avoid fragmentation. Finally, soft skills are just as important as technical ones. There is a need for critical thinking, abstraction and concretisation, risk-based prioritisation, and systems-level thinking to address complex, interconnected problems. Professionals also need leadership, communication, and mentoring skills to guide new contributors and keep standardisation aligned with real-world innovation. Without these emerging skills, from AI governance to forensic readiness, from compliance automation to negotiation, Europe risks falling behind, relying on external frameworks, and leaving the gap between innovation and regulation unfilled. Building these capabilities now is essential for a secure, resilient digital future.

Recommendations

This section distils the collective insights of 38 experts actively engaged in cybersecurity standardisation across theprojects like StandICT.eu, CYBERSTAND.eu, HSbooster.eu, INSTAR, and NERO projects. These recommendations are rooted in real-world experience, offering concrete actions to help close the cybersecurity standardisation skills gap. Each recommendation includes a clear definition of the action, the value and expected impact, and actionable steps to make it happen.

Make essential cybersecurity standards free or low-cost

Provide free or heavily subsidised access to core cybersecurity standards (e.g., ISO/IEC 27001, ETSI cybersecurity norms).

Why it matters: Today, many SMEs, researchers, and early-career professionals are excluded from participating due to high paywalls. Free access would democratise knowledge and accelerate adoption across Europe.

Actionable Implementation Guidelines:

- Allocate EU or national funding to cover standard publication costs.
- Create an open portal hosting key cybersecurity standards.
- Partner with SDOs (ISO, ETSI, CEN/CENELEC) to negotiate discounted or free licences for academia and SMEs.
- Promote awareness campaigns on the availability of these free resources.

Fund participation and training for early-career professionals

Provide financial support and structured training programmes to bring young experts into standardisation work.

Why it matters: The current expert pool is ageing, and younger professionals face travel, time, and resource barriers that prevent them from joining SDOs.

Actionable Implementation Guidelines:

- Launch fellowships similar to StandICT.eu and CYBERSTAND.eu to cover travel and participation costs.
- Introduce scholarships for students to attend standards meetings as observers.
- Partner with universities to embed standardisation modules into ICT degrees.
- Create mentorship schemes connecting young professionals with experienced experts.

Integrate standardisation into education and skills frameworks

Make cybersecurity standardisation a core part of formal education and lifelong learning programmes.

Why it matters: Universities and training institutions rarely cover standardisation processes, leaving graduates unprepared for compliance-driven roles.

Actionable Implementation Guidelines:

- Add compulsory courses on cybersecurity standards in undergraduate and master's programmes.
- Include practical labs using "compliance sandboxes" to test real-world scenarios.
- Develop online training modules (e.g., through ENISA and the Cybersecurity Skills Academy).
- Align education content with EU frameworks such as NIS2, CRA, and AI Act.

Simplify and harmonise EU regulations and frameworks

Create a unified, clear set of guidelines mapping different regulations to existing standards.

Why it matters: Today's regulation frameworks landscape creates confusion, especially for SMEs that must navigate GDPR, NIS2, CRA, and multiple sector-specific rules.

Actionable Implementation Guidelines:

- Develop official mapping guides between EU laws and CEN-CENELEC/ETSI standards.
- Publish free compliance toolkits with checklists and templates.
- Require all new EU legislation to include a standardisation roadmap at launch.
- Provide plain-language summaries aimed at SMEs and non-specialists.

Build hands-on testbeds and compliance sandboxes

Create physical and virtual labs where organisations can experiment with applying standards in realistic environments.

Why it matters: Practical application is essential for learning. Many professionals understand theory but lack real-world practice in deploying standards.

Actionable Implementation Guidelines:

- Fund cross-sector labs at EU and national level (e.g., cloud security, IoT, healthcare).
- Allow SMEs to access these facilities free or at minimal cost.
- Run simulation events such as hackathons or "standardisation sprints".
- Collect and publish anonymised case studies to share lessons learned.

Expert voices from the field:

How to close the cybersecurity standardisation gap

standICT.eu2026
ICT Standardisation Observatory and Su

CYBERSTAND.eu

HSbooster.eu
Horizon Standardisation Booster

INSTAR

NERO

6 October 2025

Funded by
the European Union