ISACA

ISACA Vision Paper

Empowering Europe's Digital Future with Cyber Resilience, Competitiveness and Digital Trust

Introduction

As Europe continues in its efforts to make the digital transition a success for its economy and society and tackle the evolving cybersecurity threats, the need for a multi-faceted approach to create a trustworthy EU digital ecosystem has never been more urgent.

The majority of companies feel their cybersecurity teams are understaffed, and the EU is set to fall far short of the number of ICT specialists that it needs by 2030 unless new action is taken.

In order to provide a secure and resilient digital future for the European Union and achieve the EU's "Digital Decade" objectives, ISACA provides recommendations to:

- **Boost EU efforts on digital skills** by setting clear, auditable targets for businesses and providing funding to support them in seizing the opportunities offered by emerging technologies like AI and promoting gender inclusion and the participation of underserved individuals in the tech sector.
- **Put a strong focus on skills when drafting and implementing cybersecurity laws** by setting clear and auditable expectations via NIS2 and similar laws and including a "skills test" for future laws.
- **Reinforce bodies which can help the EU to develop digital skills** including ENISA and the EU Cybersecurity Skills Academy.
- **Put digital skills on the international agenda** by including it as a recurring point in EU cyber dialogues and fora such as the EU-US TTC, in order to share best practices and promote coordination.

ISACA from Global Legacy to Digital Trust

A longstanding partner of the EU and a leading certification body for European professionals

In its role of constructive partner for EU policymakers, ISACA has consistently aimed to bolster the skills essential for achieving a secure and resilient digital Europe. To this end, and to continue nurturing emerging talents, ISACA has sponsored international initiatives, such as the ENISA's International Cybersecurity Challenge, and also mapped its certifications to the professional profiles of the European Cybersecurity Skills Framework (ECSF), elaborated by ENISA. This alignment ensures that individuals can identify the relevant certifications to progress their careers and organizations can create structured upskilling and reskilling pathways for their employees. ISACA's involvement extends to participation in the European Cybersecurity Skills Academy, where ISACA has pledged

Team Europe wins ENISA's International Cybersecurity Challenge

to offer free ISACA memberships and free resources to citizens across Europe, and ISACA's participation in relevant international debates and events, such as the ENISA European Cybersecurity Skills Conferences. Intersecting with policy, ISACA has advocated through various EU regulations, like NIS 2 and the Cyber Resilience Act, for the crucial role of well-trained professionals in inspections, supervision, and risk management. ISACA's overarching goal is to contribute meaningfully to closing the skills gap that is pivotal for Europe's digital future.

Additionally, ISACA works with schools, universities and research centres across Europe to help prepare the next generation of European young professionals with the digital skills and literacy they will need to seize the opportunities offered by the digital transition as well as promote gender diversity and women in leadership roles.

Digital trust as a comprehensive approach

There could be no secure and effective digital transformation of the European economy without digital trust, namely an adequate level of confidence by individuals and businesses in the integrity of the relationships, interactions and transactions among actors within an associated digital ecosystem. Such confidence can be achieved only by the seamless combination of several inter-related functions and professions, such as cybersecurity, audit, risk, and privacy, using a comprehensive, systems-based thinking approach. Governance of digital technology should therefore be addressed in a holistic way that combines different approaches into a coherent framework with the ultimate goal of digital trust in mind. This is why I trust in digital technology is the cornerstone of ISACA's global mission.

In the 2024 ISACA State of Digital Trust report[1], almost 80% of respondents said that organisations that commit to digital trust will be more successful, while 50% of them identified a lack of skills and training in the workforce as an obstacle to achieving high levels of trust. Importantly, 65% of organisations stated that it is important to be independently and publicly graded on digital trust practices – a recognition of the value of credentialing. While 84% of organisations recognise the importance of digital trust, only 15% currently have such a framework established, further highlighting the skills supply and demand mismatch. As Europe continues pursuing its digital ambitions, skills cannot be ignored and left behind. To this end, ISACA stands committed to ensuring that the underlying systems, data, and networks are secure and governed by sound ethical and regulatory principles underpinning this transformation, in sync with the EU's latest legislations.

> Europe's digital transformation needs digital trust, as they are mutually dependent and should therefore proceed in unison. Siloed cybersecurity approaches are failing, professionals need to be trained more holistically by cross-fertilizing content from several different adjacent domains such as cybersecurity, audit, risk, privacy and governance/business in order for cybersecurity and overall trust efforts to be aligned within the context of the needs of a specific organization in a specific industry.

How to win the race to the EU Digital Decade

The state of the digital and cybersecurity landscape

As we look ahead to the next five years of EU work, it is worth appreciating how much progress Europe has made so far on digitization and cybersecurity issues. Forced by global competition, escalating cyber threats and geopolitical turmoil, the European Union has taken substantial regulatory and non-regulatory initiatives. Landmark regulations, such as the AI Act, the Digital Governance Act and the Data Act paved the way for a more digitized Europe, while cybersecurity regulations such as the Cybersecurity Act, the Cyber Resilience Act, NIS 2, DORA and the Cyber Solidarity Act have laid the groundwork for an increasingly cybersecure digital ecosystem.

ISACA Europe Conference 2023: Digital Trust World

1 ISACA State of Digital Trust

The persisting lack of skilled and holistically trainedprofessionals in both the private and public sectors, however, still represents a substantial obstacle to a successful implementation of these crucial legal frameworks across Europe.

The skills gap issue is even more evident and worrisome in the case of EU cybersecurity policies. According to the 2023 ISACA State of Cybersecurity2, 62% of companies declared that their cyber teams are understaffed, with the consequence that, at the current pace, complying fully with new sweeping cybersecurity regulations will become increasingly unlikely. Despite this, 47% of companies have job openings for more advanced cyber roles, with 20% for more entry-level positions. In other words, the demand is there, but supply is lacking. This is reflected in the fluidity of the market, with 68% of organisations finding it difficult to retain cyber professionals. Such instability does not support a resilient Europe delivering cybersecurity and trust for its citizens and businesses.

The scale of this gap is already exposing European countries to unprecedented risks, as we have seen in the recent cases of cyberattacks targeting critical infrastructure, such as hospitals and transportation providers. Moreover, the growing use of emerging technologies, like artificial intelligence, is introducing a range of complexities and risks that existing frameworks and skill sets are not fully equipped to control. In fact, while the uptake and roll-out of emerging technologies will surely create new opportunities for the EU economy and society, new and more sophisticated cyber threats are likely to emerge, making it imperative for businesses to be equipped with the right expertise and for future cybersecurity strategies to be as agile and forward-looking as possible in order to control these risks.

As recently forecast by the European Commission's State of the Digital Decade, the EU is on a path to equipping 59% of the population with basic digital skills along with 12 million ICT specialists, a considerable shortfall from the targets (80% digital skills and 20 million ICT specialists).[3] Among the Commission's recommendations is a call for greater female participation in STEM (science, technology, engineering and mathematics). It is essential to ensure ongoing, comprehensive access to cybersecurity for women as they progress in their careers, addressing the widening talent gap due to increasing demand. Failing to fully utilise nearly half of the working population will lead to a failure in closing the cyber skills gap. Ensuring that women have an equitable stake in the digital and cybersecurity landscape will enrich the field with diverse perspectives and solutions, contributing to a more robust defence framework. This will require educating? cyber professionals about unconscious bias, which is one of the biggest barriers to female entry into the cyber market.[4]

A skilled cybersecurity workforce is not just an operational requirement, but a vital and strategic imperative for the European Union, its citizens and businesses.

2 State of Cybersecurity 2023 | ISACA

3 2023 Report on the State of the Digital Decade| European Commission

4 Empowering Women to Work in Cybersecurity Is a Win-Win | BCG

ISACA's policy recommendations

Boost EU-level efforts to enhance digital skills with quantifiable targets for businesses

ISACA urges the European Commission and EU co-legislators to prioritize the enhancement of digital skills and the upskilling of European professionals. This is urgently needed to achieve the objectives of the Digital Decade, which includes the target of having 20 million employed ICT specialists in the EU and ensuring that at least 80% of all Europeans possess basic digital skills by 2030, among other goals.

Given the skills gap highlighted in our reports and its implications for the European security and regional competitiveness, ISACA recommends the establishment of clear, quantifiable targets for certified cybersecurity (and adjacent domain) professionals in the EU by 2030 as part of a new EU initiative dedicated to digital and cyber skills and proposed by the European Commission in the first year of its new mandate. These targets should also include a maturity score for businesses as a measurable objective, providing a roadmap for continuous improvement for European companies. Of course, these maturity scores would not necessarily be disclosed publicly but would rather be used in dialogue with the relevant authorities. This goes hand-in-hand with the reinforced role for ENISA that we discuss below.

Address the cyber skill gap in critical entities and sectors while implementing recent laws

The EU has passed several important laws in furtherance of this mandate which address cybersecurity in a general way.

These laws now need to be transposed to national level and implemented. This is an opportunity to properly address digital skills as a vital element of cybersecurity, without waiting for new initiatives.

NIS2 requires Member States to promote education and training on cybersecurity (article 7.f). It further requires Member States to ensure that essential and important entities put in place risk management measures which include cybersecurity training (article 21.g). ISACA urges Member States to transpose these rules effectively and in manner that holds critical entities to a high standard for cybersecurity skills which should be monitored closely by national authorities. ISACA further urges the NIS2 cooperation group to promote high standards and place a strong emphasis on developing the skills, using its guiding role (article 14.a).

The recently proposed Cyber Solidarity Act complements other cybersecurity laws, including by coordinated preparedness testing across sectors. Appropriately trained staff are a key element of firms' cybersecurity and should be assessed as part of the preparedness exercise, with effective remedial measures for sectors and entities where understaffing contributes to their vulnerability.

Monitor how recent cybersecurity laws affect the cyber-maturity of organisations

It has become clear that no digital regulation, no matter how clear, comprehensive and in line with technological advancements, can succeed in the EU without a sufficiently skilled and trained workforce. For this reason, it is of paramount importance for the EU to develop qualified and trained EU professionals with the right skillsets to comply with the EU digital and cybersecurity regulations that are already in effect or will soon will be. In this regard, trainings and professional certifications prove to play a pivotal role in providing individuals and businesses with the expertise to fully and successfully comply with the relevant digital and cybersecurity regulations. Such training and certifications should therefore be better integrated by the EU and Member states in the workforce development strategies as well as in the EU legal framework.

To the same end, in line with ISACA's commitment to effective governance, we recommend an auditable tracking system for the implementation of NIS 2, the Cyber Resilience Act and the forthcoming cybersecurity legislations. This should include regular audits focusing on the cybersecurity maturity of enterprises.

As demonstrated by the success of the Cybersecurity Skills Academy, the involvement and engagement of key stakeholders in dialogue with the public sector are also integral to achieving this aim. The high expertise of industry, academia, and the private sector can, in fact, be leveraged to benefit regulators and policymakers, serving as essential tools in cultivating the expertise and capabilities necessary for effective cybersecurity implementation.

Implement a "skills test" into digital and cybersecurity regulation

ISACA recommends that future digital legislation requires a "skills test" as part of its impact assessment, in the same manner and potentially even streamlined with the competitiveness test proposed by President von der Leyen.[5]

When this test identifies significant deficiencies in the labour force which would be required to meet the objectives of the law, such law should include targeted measures seeking to redress this problem.

Reinforce ENISA's mandate to improve EU cybersecurity skills

ENISA plays an important role coordinating, advising, and supporting European cybersecurity capacities. This includes making a relevant contribution to improve digital skills in Europe, including the development of the European Cybersecurity Skills Framework (ECSF), as well as being responsible for providing regular recommendations on the development of cybersecurity capacities across the EU under NIS2 (article 18).

It is clear that cybersecurity will remain a topic with major national importance, where Member States naturally reserve certain competences to the national level.

ISACA suggests reinforcing ENISA's mandate in regard to digital skills, as an element of the cybersecurity framework where there is a clear value to cross-border coordination and European-level action. This could concretely be achieved by allowing ENISA to make urgent recommendations, for example following cybersecurity exercises, backed by a (confidential) "comply-or-explain" mechanism to balance national and European interests.

Strengthen the role of the EU Cybersecurity Skills Academy

Roundtable of the Cybersecurity Skills Academy

ISACA calls on the EU to develop further the Cybersecurity Skills Academy into a fully structured programme, including dedicated funding and acting as a hub connecting individuals and organisations to relevant training, certification, and educational programmes, thereby bridging the existing skills gap.

Since public funding for cyber skills comes from a wide range of EU funding programmes, managed either at EU or at national / regional levels, it is not necessarily obvious for potential beneficiaries to track them or even being aware of their existence. To make sure that public funding usefully reaches as many beneficiaries as possible, the Digital Skills and Jobs Platform should be further developed and related information days targeting possible beneficiaries as well as multipliers should be organised.

Create public-private partnerships for impartial audits

ISACA proposes the creation of public-private partnerships for carrying out impartial cybersecurity audits. Building on globally recognised certifications and programmes on the market, these partnerships would not only uphold the highest standards, but also ensure high-quality auditing services. Additionally, public-private partnerships can help governments and public sector enhancing their internal expertise and capacity for addressing challenges in software and systems engineering and service operations. This will also help bolster the cyber resilience of critical infrastructure.

Targeted measures should be taken for gender and diversity inclusion

Following ISACA's SheLeadsTech programme's commitment to advance gender diversity and female empowerment in cyber leadership, we encourage targeted funding and initiatives allocated to promote the inclusion of women. The exclusion of various parts of the population adversely impacts the cyber labour market, both for the skills gap and threat detection, which is improved through diverse perspectives. There cannot be digital trust without greater reflection of the wider EU population in key cyber roles.

5 2023 State of the Union |European Commission President von der Leyen

SheLeadsTech™
ENGAGE. EMPOWER. ELEVATE.

Through its SheLeadsTech[6] initiative, ISACA is committed to empower women by offering under-represented professionals access to education, skills development and career opportunities, while highlighting gender disparities in the tech labour market. This initiative includes comprehensive resources, services, events, and learning materials to make leadership roles accessible to all.

Establish a small and medium enterprises (SMEs) cybersecurity support scheme

Acknowledging the vital role that SMEs play in the European economy, we recommend an easily accessible support scheme dedicated to boosting their cybersecurity resilience, offering financial incentives for SMEs to obtain certified cybersecurity assessments and implement necessary measures.

Support AI literacy and training for emerging technologies as a forward-looking step

In its 2024 AI Pulse Poll, ISACA found that more than 80% of digital trust professionals will need training within two years if they wish to retain their current roles or advance their careers. To prepare for the complexities introduced by emerging technologies like AI, ISACA recommends the support of AI literacy programmes. This is recognised in the Commission's Digital Education Action Plan (2021-2027), which seeks to support AI traineeships for university students, vocational education students and teaching staff. ISACA calls for the AI Act to require the Commission and Member States to promote literacy through education, training, skilling and reskilling programmes, while AI developers and deployers should ensure their staff are sufficiently AI literate. These efforts should aim at equipping both current and future professionals with the skills and the understanding to manage AI ethics, governance, and security effectively.

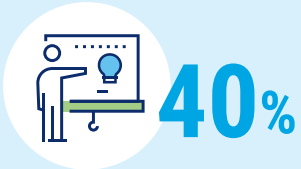
Integrate skills considerations into the EU's digital diplomacy efforts

The EU engages in a number of cyber dialogues with partners such as the US and the UK, as well as engaging with them in fora such as the EU-US trade and technology council.

Developing digital skills is a common goal between countries. Sharing best practices, and aligning on key concepts and expectations towards firms, could help each partner to strengthen its own efforts as well as helping companies to focus their resources on effectively developing the skills they need.

More AI Guidance and Training Needed

OF THOSE SURVEYED
are extremely or very familiar with AI. **46% would classify** themselves as a beginner.



40% OF ORGANIZATIONS OFFER
no AI training at all. **32% say training** is limited to staff who work in tech-related positions.

6 ISACA SheLeadsTech

ISACA Certifications

CISA
Certified Information Systems Auditor.

CISM
Certified Information Security Manager.

CRISC
Certified in Risk and Information Systems Control.

CDPSE
Certified Data Privacy Solutions Engineer.

CGEIT
Certified in the Governance of Enterprise IT.

ISACA Trainings & Certificates

- AI Essentials
- AI Governance: Principles, Strategies and Business Alignment
- Auditing Generative AI: Strategy, Analysis and Risk Mitigation
- Cybersecurity Fundamentals
- Cybersecurity Audit
- IT Risk Fundamentals
- IT Audit Fundamentals
- Introduction to Digital Trust Ecosystem Framework

Capability Maturity Model Integration (CMMI)

As recognised by EU policymakers, organisations are increasingly dependent on interconnected digital technologies, which heightens their susceptibility to cyberattacks from an ever-evolving threat landscape. Proactive measures are therefore crucial to boost resilience. A cybersecurity maturity assessment examines an organisation's posture and enables a comprehensive understanding of cybersecurity risks, prioritisation of vulnerabilities, and the development of effective controls. It evaluates employee readiness and process adequacy at addressing cyber risks.

Assessing an organisation's maturity level informs focused training to address weaknesses, fostering a stronger security culture. Tailored recommendations are then provided, safeguarding the organisation's data, systems, and assets. Consequently, resources are allocated appropriately, cyber awareness is enhanced, and compliance with regulations is improved, ultimately reducing the risk and cost associated with cyberattacks. These efficiency gains are equally important for public and private organisations.

ISACA's CMMI offers a distinct cybersecurity risk assessment framework by allowing organisations to identify and analyse gaps in their security systems. It facilitates the assessment, optimisation, and reporting of cyber capabilities, assisting organisations in implementing leading frameworks and staying current in the evolving cybersecurity landscape. Its flexibility can accommodate organisations of all sizes. Indeed, many SMEs have adopted it. It is also a suitable framework for government departments and agencies, servicing the needs of the US Department of Defence, Treasury, and Social Security.

In light of the recent EU Regulation on the Cybersecurity of the EU institutions, bodies and agencies, CMMI can also support the institutions in complying with their obligations. In particular, the Regulation stipulates a biennial all-hazard maturity assessment for all components of the institutions' ICT environment. These assessments must be comprehensive, encompassing on-premises and operational technology networks to third-party hosted assets and services in cloud computing, as well as mobile and corporate networks. ISACA's CMMI is ideally suited to support this compliance effort.

CMMI not only harmonises with leading frameworks, like NIST Cybersecurity Framework and ISO/IEC (27001, 27002) standards, but is also updated biannually to ensure alignment with changing best practices that seek to counter emerging cyber threats. Learning from implementing CMMI in both the public and private sector feeds back into how CMMI is delivered. This generates synergies between each sector, which could also support the EU's efforts to close the cyber skills gap. CMMI ultimately provides a roadmap of concrete deliverables that are prioritised according to the organisation's most relevant risks.

Medical Device Discovery Appraisal Program (MDDAP)

The ISACA's Medical Device Discovery Appraisal Program aims to streamline the regulatory process for medical devices by assessing and improving the quality management systems (QMS) of medical device manufacturers.

MDDAP utilizes a risk-based approach to assess the maturity and effectiveness of a manufacturer's QMS. The program aligns with international quality system standards and regulatory requirements, such as ISO 13485 and the FDA's Quality System Regulation (QSR). Through a comprehensive appraisal process, MDDAP evaluates various aspects of a manufacturer's operations, including design controls, production and process controls, risk management, and post-market surveillance.

Participating in MDDAP can provide manufacturers with several benefits, including a more efficient regulatory pathway, enhanced product quality, and a competitive advantage in the market. The program encourages continuous improvement and collaboration between manufacturers, regulatory authorities, and other stakeholders in the medical device industry.

Control Objectives for Information Technologies (COBIT)

ISACA's COBIT is a comprehensive framework designed to enhance information and technology (I&T) governance and management practices within organizations. With a focus on developing, implementing, monitoring, and improving I&T processes, COBIT aligns I&T objectives with broader business goals, ensuring optimal use of technology resources.

Structured around a governance and management model, COBIT emphasizes a holistic approach to enterprise information and technology. The framework comprises three key components: the Governance System, the Management System, and the Components.

The Governance System centers on addressing stakeholder needs through effective governance practices, encompassing principles, policies, and a governance system aligning I&T with business strategy. Meanwhile, the Management System oversees day-to-day I&T operations, incorporating enablers like processes, organizational structures, information, and culture to achieve IT-related objectives.

COBIT integrates seven components, including Processes; Organizational Structures; Information Flows; People, Skills and Competencies; Principles, Policies and Procedures; Culture, Ethics and Behavior; and Services, Infrastructure, and Applications, supporting the implementation of governance and management objectives. This dynamic framework allows organizations to customize their approach based on unique needs and risks, providing a common language and toolset for IT professionals and business leaders to collaborate successfully in achieving strategic objectives while managing and mitigating I&T-related risks.

Mapping of ISACA professional certifications and trainings to support implementation of EU regulations

EU Regulation	ISACA relevant certifications & trainings to support implementation of EU regulations
Cyber Resilience Act	■ CISM combined with CISA, CRISC and CDPSE for creating holistic professionals and preparing the workforce to implement cyber resilience. ■ CMMI as a capability and maturity benchmarking assessment method.
Regulation on 'managed security services' (amending the Cybersecurity Act)	■ CISM combined with CISA, CRISC and CDPSE for creating holistic professionals and preparing the workforce to implement cyber resilience. ■ CMMI as a capability and maturity benchmarking assessment method.
Digital Operational Resilience Act (DORA)	■ COBIT and CGEIT on Governance of ICT (Financial entities shall have in place an internal governance and control framework that ensures an effective and prudent management of ICT risk). ■ CISM/Cybersecurity Fundamentals on building the cyber workforce (Members of the management body of the financial entity shall actively keep up to date with sufficient knowledge and skills to understand and assess ICT risk and its impact on the operations of the financial entity, including by following specific training on a regular basis, commensurate to the ICT risk being managed). ■ CISA/CRISC on risk management and assurance related workforce development (Financial entities shall have a sound, comprehensive and well-documented ICT risk management framework as part of their overall risk management system).
Network and Information Security 2 (NIS 2) Directive	■ CISM/Cybersecurity Fundamentals on building the Cyber workforce ■ CISA/CRISC on risk management and assurance related workforce development ■ CMMI for measuring the maturity of the entities involved and complying with legal requirements.
Artificial Intelligence Act (AI Act)	■ Combination of CISA+CET/AI and CRISC+CET/AI towards creating the workforce of risk and audit (assurance) professionals. ■ CMMI as the solution towards AI system maturity assessment and for measuring the maturity of vendors and user organizations throughout the lifecycle of an AI system. ■ Dedicated ISACA trainings on AI, such as AI Essentials, Auditing Generative AI and AI Governance ■ In view of the development of AI Act-related standards: ■ CRISC could contribute to standards development by helping equip individuals in companies developing high-risk AI to implement the risk management system. ■ AI Fundamentals could provide guidance on how organisations concretely train their staff on AI. ■ CISM could contribute to standards development by helping to support AI-focused companies in upskilling their cybersecurity capacity. ■ CMMI Safety View could feed into standards guidelines around quality assurance in the AI Act.
Regulation for a high cybersecurity level at the EU institutions, bodies, offices and agencies (EUIBAs)	■ CMMI as a necessary compliance solution to carry out maturity assessment for every component of the EUIBAs ICT environment, spanning on-premises, operational technology networks, third-party hosted assets, cloud services, mobile and corporate networks.
EU 5G Toolbox	■ CRISC, CISM, CISA to create holistic professionals focusing on risk management and assurance, as well as security management and preparing the workforce towards 5G networks' rollout and 5G adoption ■ CMMI to measure the maturity of the 5G networks' users and operators.
General Data Protection Regulation (GDPR)	■ CDPSE to create competent privacy technologists to fully comply with the GDPR legal requirements.

ISACA

For more information:

AI Resources
www.isaca.org/resources/artificial-intelligence

Digital Trust Resources
www.isaca.org/digital-trust

About ISACA

ISACA® is a global leader with more than 50 years of experience offering knowledge, certifications, community, advocacy, and education in cybersecurity, information systems audit, governance of digital technology, risk and privacy. We have a worldwide network of 180,000 members in 188 countries, with a new European office in Ireland as well as 44 European chapters. ISACA offers globally recognized professional certifications, which are considered the gold standard in the aforementioned domains, as well as solutions to help businesses train and build quality teams to ensure their ICT ecosystem is trusted. This makes ISACA a one-stop shop with services marked by reliability, efficiency and excellence. ISACA is committed to using its deep expertise to support policymakers as they work to make Europe more secure and competitive.