Foundation Forum 2022

Outcome Report

A Global Digital Foundation Initiative

Assured AI and Data Ecosystems:
Innovation, Standards, and Cybersecurity

Prepared by:
Catriona Gray and Rob Wortham

Global Digital Foundation — The Digital Policy Network

EUOS EU Observatory for ICT Standardisation

eit Digital

ECS European Cyber Security Organisation

AI Assurance Club — A Global Digital Foundation Initiative

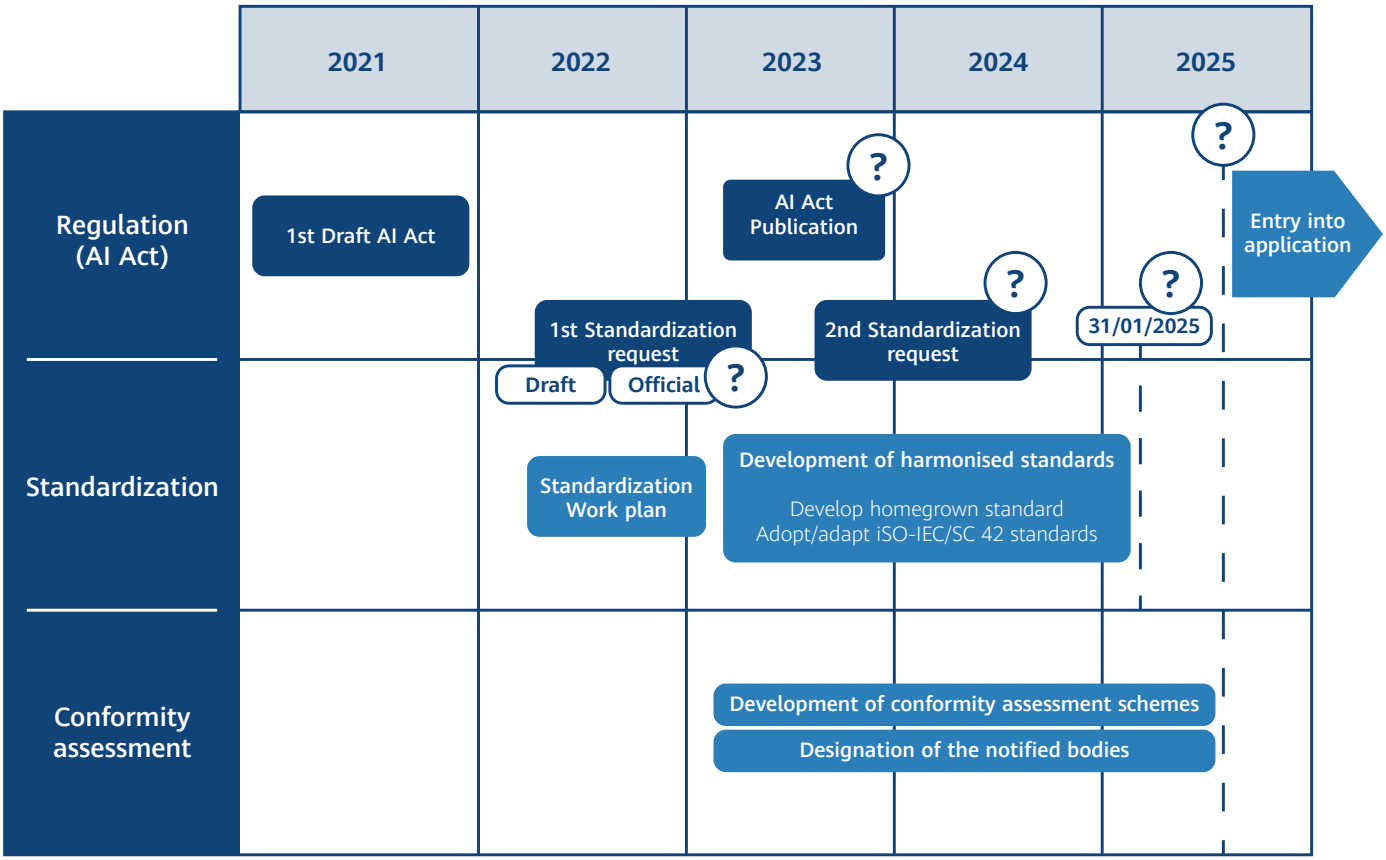
Corporate partner: HUAWEI

Table of contents

Executive summary

Executive summary

On 29 November 2022 in Brussels, Global Digital Foundation hosted its second annual Foundation Forum. This year's theme was Assured AI and Data Ecosystems: Innovation, Standards, and Cybersecurity. The AI Act is expected to become applicable by around 2025, and stakeholders must use this interim period to prepare to operationalise the provisions of the Act.



Source: AFNOR Strategie de normalisation pour d'IA CEN-CENELEC/JTC 21, December 22

Over the course of the keynotes and panels, participants had a wide-ranging set of discussions. Four interactive panels covered the topics of AI assurance, cybersecurity, innovation and standards. A final panel brought together the conclusions from each panel and enabled common themes and relationships between different policy areas to be identified. Several conclusions emerged from the Forum. Firstly, there is a need for a holistic and nuanced understanding of the interaction between different policy domains and instruments. This perspective will help businesses to utilise synergies and to avoid unnecessary proliferation of processes and compliance measures. Across all panels, there was a strong sense that SMEs should play a greater role in policy processes, governance, and in standardisation. This cooperation may take the form of working together to develop innovative assurance tools such as codes of conduct or standardised contracts. In addition, many businesses, particularly SMEs, would benefit from having more time to understand, prepare for and implement requirements and specifications set out in new standards.

Finally, we learned that there is much to be gained from multi-stakeholder governance, and that more can be done to involve representatives from all stakeholder groups. This will be key to the legitimacy and effectiveness of new regulatory frameworks.

Agenda

09:00 – 09:30 **Coffee & registration**

09:30 – 09:40 **Opening remarks**
John HIGGINS, Chair, Global Digital Foundation

09.40 -10:00 **Morning keynote: What are the challenges to build trust and confidence in AI?**
Brando BENIFEI, MEP - AI Act Rapporteur

10:00 - 11:00 **Assurance of AI through the value chain**
Moderator: Rob WORTHAM, AI Assurance Club
Panellists: Ansgar KOENE, EY | Pascal STEICHEN, House of Cybersecurity
Emanuela GIRARDI, Pop AI / Adra | Corinna SCHULZE, SAP

11:00 – 11:30 **Break**

11.30 - 12:30 **AI and cybersecurity – an evolving relationship?**
Moderator: Roberto CASCELLA, European Cyber Security Organisation
Panellists: George SHARKOV, MD, European Software Institute CEE & ETSI SAI
Iva TASHEVA, Cybersecurity Advisor CYEN | Rob VAN DER VEE, Software Improvement Group

12:30 - 13:25 **Lunch**

13.25 - 13.30 **Afternoon introduction**
John HIGGINS, Chair, Global Digital Foundation

13.30 - 13.50 **Keynote: Where should AI in EU be in 10 years?**
Calum CHACE, Author of "Surviving AI" and "The Economic Singularity"

13.50 - 14:50 **What are the implications of AI for Europe's innovation aspirations?**
Moderator: Diva TOMMEI, Chief Innovation, Education and Marketing Officer, EIT Digital
Panellists: Giovanni SOLLAZZO, AIDEM | Nick MERRITT, Vault Hill
Sergio ALVAREZ-TELENA, SCI the world | Nathanaël ACKERMAN, AI4Belgium

14:50 - 15:15 **Break**

15:15 - 16:15 **Standards and AI: are we on track?**
Moderator: Ray WALSHE, EU Standards Observatory
Panellists: Sebastian HELLENSLEBEN, CEN-Cenelec JTC 21 | Hsiao-Ying LIN, Huawei
Klaus Dieter AXT, EUnited | Nicolas MOËS, The Future Society | Karina GIBERT OLIVERAS, UPC

16:15 - 16:25 **Keynote: The EU AI Act: Will it meet its goals to both boost trust & confidence and encourage innovation?**
Edina TOTH, MEP

16:25 - 17:10 **Closing discussions: The road ahead, challenges and insights**
Moderators: John HIGGINS, Global Digital Foundation | Emanuela GIRARDI, Pop AI
Panellists: Rob WORTHAM, AI Assurance Club | Roberto CASCELLA, ECSO
Diva TOMMEI, EIT Digital | Ray WALSHE, EU Standards Observatory

17:10 - 18:30 **Networking & refreshments**

Chair

John Higgins
Global Digital Foundation

Keynote speakers

Brando Benifei
MEP - AI Act Rapporteur

Edina Toth
MEP

Calum Chace
Author of "Surviving AI" and "The Economic Singularity"

Moderators

Rob Wortham
Director, AI Assurance Club
(a Global Digital Foundation initiative)

Roberto Cascella
Head of Sector "Technology, Supply Chain & Strategic Autonomy" (ECSO)

Diva Tommei
Chief Innovation, Education and Marketing Officer, EIT Digital

Ray Walshe
Director, EU Standards Observatory

Emanuela Girardi
President, Pop AI

Policy context

John Higgins
Chair, Global Digital Foundation

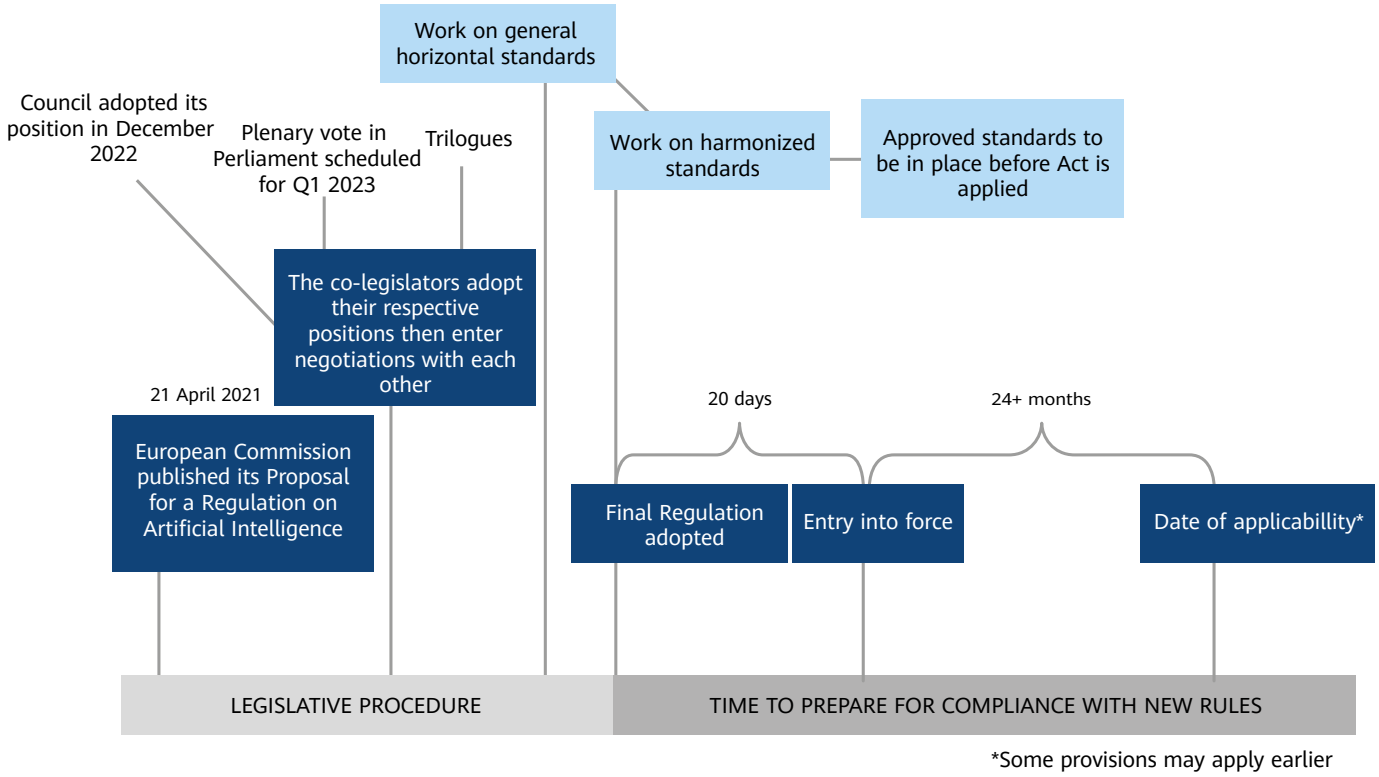
Policy context

The legal and regulatory landscape for AI is complex and quickly evolving. Across the globe, governments, industry and civil society are considering how best to respond to the risks and opportunities presented by AI technologies, including through new legislation. Policymakers are eager to strike the right balance between promoting innovation and competitiveness whilst protecting fundamental values such as safety, privacy and non-discrimination.

Source: Drafting Harmonized Standards in support AI Act CEN-CENELEC/JTC 21, November 2022

Many of the most significant AI policy developments relate to the proposed European Union AI Act. The proposed Act is the first ever attempt globally to regulate AI across all sectors of the economy, and takes a layered, risk-based approach. Legislative negotiations are ongoing and expected to continue at least until late 2023.

Just a few days after the 2022 Foundation Forum, the Council of the EU adopted its general approach to the AI Act. This agreed text includes a narrowing of the definition of AI, and adjusts some of the requirements for high-risk AI systems to make them more technically feasible, particularly for SMEs. It offers some clarification of the allocation of responsibilities and roles of various actors in AI's complex value chains.



Meanwhile, European Parliament discussions are led by two committees and co-rapporteurs, the Committee on Internal Market and Consumer Protection (IMCO) led by Italian MEP Brando Benifei, and the Committee on Civil Liberties, Justice and Home Affairs (LIBE), led by Romanian MEP Dragoș Tudorache. Brando Benifei presented the Forum's morning keynote address, a summary of which is provided below.

As reflected in the 2022 Foundation Forum programme and choice of panel topics, harmonised standards will play an integral role in the implementation of the AI Act once adopted. The European Commission has issued a draft standardisation request to the European Committee for Standardisation (CEN) and the European Committee for Electrotechnical Standardization (CENELEC). A formal standardisation request will then be made based on the requirements of the Act, and harmonised standards will be finalised before the new regulation becomes applicable. Preparatory work is already underway to develop European standards which leverage existing sources, including those from ISO, and which address the identified gaps.

Alongside the AI Act, several other European policy and legislative initiatives will shape how we use digital products and services in the years to come. Key amongst these are the Digital Services Act (DSA) which deals with illegal content, transparent advertising, and disinformation; the proposed Cyber Resilience Act (CRA) which sets out cybersecurity related requirements for products with digital elements; the Data Governance Act (DGA) which creates a framework for data sharing by strengthening mechanisms to increase data availability, particularly in the public sector, and the proposed Data Act which complements the DGA and aims to increase the availability and interoperability of non-personal data (B2B, B2C and B2G).


Foundation
Forum
2022
A Global Digital Foundation Initiative
Assured AI and Data Ecosystems
Innovation, Standards, and Cybersecurity
ECS

Keynote summaries

Brando Benifei
MEP - AI Act Rapporteur

Edina Toth
MEP

Calum Chace
Author of
“Surviving AI” and
“The Economic Singularity”

Keynote summaries

MEP Brando Benifei, one of the two European Parliament rapporteurs on the AI Act, gave an insightful keynote address on the current intra- and inter-institutional political dynamics of the Act. Brando sketched out the complex balancing act required of legislators – promoting rights and consumer protection whilst developing the market in digital products and services. While we cannot predict all evolutions of AI technology and its impacts, we must nevertheless build a legislative environment that enables us to exploit its potential without eroding trust. The way to achieve this, he argued, is through comprehensive stakeholder engagement with businesses and other organisations, and by taking a proportionate, risk-based approach drawing on the relevant evidence.

In his address, Brando went on to detail how parliamentarians have sought to strengthen the provisions of the Act. MEPs have pushed, in particular, for amendments that increase the involvement of stakeholders at all stages (including in standardisation), and for amendments that seek to expand the role of the proposed AI Board which will eventually be tasked with many of the Act's governance and enforcement functions. For the Council, on the other hand, many of the key debates focus on the extent of measures to prohibit specific AI applications, such as biometric surveillance in public and private spaces. These questions are likely to prove contentious in the upcoming negotiations between the Parliament and the Council.

As Brando highlighted, the allocation of responsibility across the AI value chain is at the core of discussions between policymakers. Many MEPs, for example, want to avoid creating loopholes that would allow general purpose AI systems to be excluded from the scope of the Act. This reflects the critical challenge facing policymakers and businesses: how to build appropriate assurance mechanisms across the value chain that meet the needs of all stakeholders, including smaller entities such as SMEs. These questions were also addressed in the first panel, Assurance of AI through the value chain, discussed below.

Brando emphasised the importance of considering markets beyond the US and Canada, including Brazil, China and India, who will be significant producers of AI systems. Rather than expecting other regions to strictly adhere to norms and practices developed in the EU, Brando suggested flexibility and common ground could be sought, for example, through the idea of risk categorization.

After lunch, Calum Chace, author of books including Surviving AI and The Economic Singularity, gave a great run-through of just how far we have come since AI technologies first began to be developed in the mid-20th century, and where we might be headed in the next decade. Calum's provocation was that Europe needs to become a more active player in AI development, not just a standard-setter for regulation.

The final keynote was given by Edina Toth MEP. Edina previously served as the Vice Chair of the Special Committee on Artificial Intelligence in a Digital Age (AIDA). Like many of the other speakers, she emphasised the need for a robust and clear regulatory environment which can help to boost trust in AI whilst encouraging innovation

Panel 1

Assurance of AI through the value chain

Moderated by

Rob Wortham	Director, AI Assurance Club

Panellists

Ansgar Koene	Global AI Ethics and Regulatory Leader, EY
Pascal Steichen	Founder and CEO, Luxembourg House of Cybersecurity
Emanuela Girardi	Founder and President of Pop AI, Board Member of Adra (AI, Data and Robotics Association), Parliamentary Candidate for Più Europa
Corinna Schulze	Director EU Government Relations, SAP

Panel 1
Assurance of AI through the value chain

The first panel had four main questions to prompt their discussions:

1. How will governance work throughout these value chains?
2. How will providers have confidence in the compliance of their sub-contractors?
3. Are compliance solutions already being developed?
4. How will this affect the power dynamics, especially between SMEs and multinationals?

Panellists were first asked to consider how governance can be made effective through the AI value chain. As the moderator, Rob Wortham gave an account of the complexity of AI value chains. AI systems comprise multiple layers, including deep learning frameworks (which may be proprietary or open source), pre-trained models such as YOLO, and datasets such as ImageNet. Any given AI system will be integrated within much larger systems, and often deployed by service providers on cloud platforms. Rarely will a single entity be behind the entire design and deployment of a system, and indeed a business may find itself within many different configurations of the value chain.

Within the AI Act itself, the concept of the value chain is mentioned in the first stated specific objective (1.4.2):

To set requirements specific to AI systems and obligations on all value chain participants in order to ensure that AI systems placed on the market and used are safe and respect existing law on fundamental rights and Union values;

Though it does not give a clear definition of the AI value chain, these value chain participants are identified elsewhere in the AI Act as including importers, distributors and authorised representatives. As the panellists noted, the AI Act looks at the concept of value chain from the perspective of market actors, rather than from a purely technical development perspective. It envisages multiple roles and potential bearers of responsibility. Crucially, this means businesses must take on different sets of requirements at different stages.

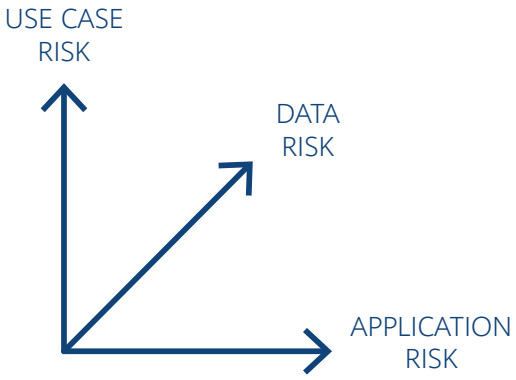
Following on from this, the panel considered how the complexity of assuring across value chains will affect power dynamics, especially between SMEs and multinationals. Panellists agreed that the pace of bringing AI to SMEs should be accelerated, and that the AI Act brings both potential enablers and burdens for SMEs. Importantly, its requirements will exist alongside obligations created by the Cyber Resilience Act, which, like the AI Act, considers responsibilities across the value chain.

As one panellist noted, one possible way of addressing the needs of SMEs could be through the use of various European Commission funding mechanisms for infrastructure, research and innovation, such as Horizon Europe, to ensure regulations are implemented by small entities, and that their specific challenges can be addressed. Digital Innovation Hubs were highlighted as one way of leveraging the power of small entities by pooling not just technical expertise, but also legal and compliance elements. European Digital Innovation Hubs (EDIH) were launched as one-stop shops to support companies to respond to digital challenges and become more competitive. They combine the benefits of a regional presence with the opportunities available as a pan-European network.

Panellists discussed the role of contracts in assigning responsibilities in addition to responsibilities explicitly set out in regulation. There was a sense that businesses need some flexibility to negotiate the terms of their contracts with each other. However, it was also recognised that where there are very few providers of large-scale pretrained models, for example, SMEs may find it difficult to hold larger firms to account through contractual agreements.

When asked about the compliance solutions already being developed, there was general agreement amongst the panel on the value of building on compliance and assurance solutions which already exist, for example in the management of subcontractor relationships to comply with GDPR. Synergies can be established with the processes already established within companies to reduce the burden and maximise the impact of new provisions on AI. One possible solution mentioned was the use of some form of assurance certificates to standardise the form in which details about assurance are given to other parties. There was support amongst the panel for the idea of a certificate or code of conduct scheme that takes a more granular approach than regulatory provisions by setting out a common standard of what compliance means.

Applying a three dimensional risk-based approach



Use case risks - High-risk AI systems as defines in the EU AI Act
Data risks - Provisions of GDPR, Data Act and Data Governance Act
Application risks - The AI technology stack

As reflected in the panel discussion, risk governance is multidimensional, and a key challenge for all organisations will be finding the right approaches and measures which address risks holistically. The Global Digital Foundation, through its initiatives including the Foundation Forum and the AI Assurance Club, aims to build a community of practice which works across these dimensions.

Key takeaways

- **Synergies with existing processes and tools, such as those used for GDPR, must be exploited.**
- **We should find ways of better leveraging the power of SMEs and targeting support and investment where it is needed.**
- **There is an appetite for multi-stakeholder cooperation to potentially develop voluntary certification schemes to standardise the format in which assurance guarantees are given to other contracting parties within the value chain.**
- **Verification, validation and testing of AI in a cost-effective and continual manner will be key to effective assurance.**

Follow up points

For each panel session, this section identifies some specific items for further investigation, particularly in preparation for Foundation Forum 2023.

- Investigate possible development of a code of conduct for AI similar to those already used for GDPR.
- Investigate current use of assurance certificates and applicability in a multi-actor environment.

Panel 2

AI and cybersecurity – an evolving relationship?

Moderated by

Roberto Cascella	Head of Sector Technology, Supply Chain & Strategic Autonomy, European Cyber Security Organisation (ECSO)

Panellists

George Sharkov	MD, European Software Institute CEE, VP ETSI SAI and ENISA WG member
Iva Tasheva	Cybersecurity Advisor CYEN (a Cyber Security SME), ENISA WG member
Rob Van Der Veer	Digital groundbreaker, Senior principal consultant, Software Improvement Group (SIG)

Panel 2
AI and cybersecurity – an evolving relationship?

The topic of the second panel was the relationship between AI and cybersecurity, and it addressed two main questions:

1. Are cybersecurity solutions keeping pace with the growing use of AI and expanding digital and data supply chains?
2. What's the place of certification systems in building trust and confidence in these cybersecurity solutions?

As all of the panellists made clear, greater use of AI techniques across sectors brings significant cybersecurity challenges. Cyber attacks are increasing in scale, cost and complexity, and we are increasingly connected, with the number of devices linked to the Internet of Things (IoT) steadily growing. When it comes to using, securing and preventing the misuse of AI, data is a key vector of risk.

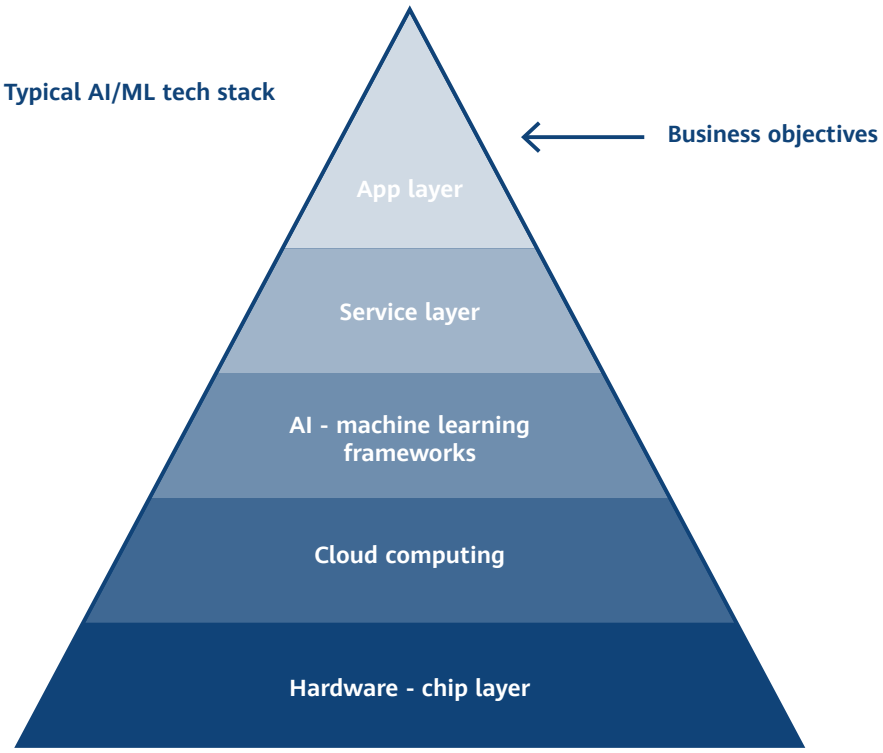
AI has been characterised as a double-edged sword for cybersecurity. The panel considered these different dimensions; how AI techniques can be used to support and automate cybersecurity operations and controls, but at the same time open many new avenues for attack methods, and expose organisations to additional risks.

The European Union Agency for Cybersecurity (ENISA) divides this complex relationship between AI and cybersecurity into three key dimensions:

- Cybersecurity for AI
- AI to support cybersecurity
- The malicious use of AI

Cybersecurity for AI	This dimension concerns potential vulnerabilities and instances of insufficient robustness in AI systems. This includes, for example, the manipulation of data used in AI systems, data poisoning, adversarial model manipulation, attacks against cyber-physical systems, and integrity in the software supply chain.
AI to support cybersecurity	AI may be used as a tool to augment cybersecurity through the development of more effective controls. These might include automated cyber threat intelligence (CTI), smart forensics, email scanning, intelligent firewalls, and automated malware analysis. AI may also be used to support law enforcement agencies to detect and respond to cybersecurity related criminal activities.
Malicious use of AI	AI can be used maliciously by adversaries to create more sophisticated attacks. Examples of this include AI powered malware, social engineering, the creation of fake social media accounts, AI-augmented distributed denial of service (DDoS) attacks, deep fakes, and AI-supported password cracking.

The second of these dimensions, the use of AI to support cybersecurity, is particularly important for SMEs, many of whom are at increased risk of business failure following a cyber attack. AI can be utilised for network management to look at threats, behaviours, and patterns that may help to identify and contain potential intrusion within the network. This also presents an effective opportunity to greatly reduce the cost of cyber-security for businesses.



Source: https://insightaas.com/how-ai-platforms-are-stacking-up/

Whilst many of the same considerations and practices relevant to other software techniques also apply to AI, the panel underlined the need to attend to the specificities of AI systems. Unlike traditional software, machine learning development involves the collection and processing of data, including very sensitive data, by developers. There are many modes of attack specific to machine learning, including data poisoning, input manipulation and reverse engineering. These model attacks require a specific understanding of AI in addition to more general cybersecurity competences. There is a need to build AI lifecycle processes that augment those we already have for classical software.

The limitations of assurance alone for securing AI systems was highlighted. Testing by vendors cannot guarantee the security and reliability of software; systems continually evolve and some of the panel argued that those deploying and using AI systems have an important role to play too.

The panel discussed the interplay of various legislative measures on cybersecurity. In September 2022, the Commission presented a proposal for a new Cyber Resilience Act which aims to protect consumers and businesses from products with inadequate security features. This is the first legislative instrument introducing EU-wide mandatory requirements for products with digital elements. The text of the proposal also highlights the interplay of cybersecurity with other EU digital policies, including the proposed AI Act.

The AI Act itself requires that high-risk AI systems have appropriate levels of robustness, accuracy and cybersecurity which must be maintained throughout the entire lifecycle. The exact technical solutions to be employed will depend on the circumstances and risks. These requirements overlap with existing legislation, namely the certification process as set out in the Cybersecurity Act. The AI Act provides that high-risk AI systems which have already been certified or had a relevant statement of conformity issued under an existing cybersecurity scheme shall be presumed to be in compliance. However, as one panellist highlighted, even systems which would not be classified as high-risk under the Act face cybersecurity risks too, and there is therefore a need to look beyond certification.

Certification for AI systems can be more complicated than those for other software systems. This stems from the nature of AI development which is continually evolving. Unlike conventional software, for which there is established industry best practice for penetration (pen) testing when a major change is implemented, AI is built to evolve at unplanned intervals. As a result, there is no obvious point at which testing would be triggered. Instead, continued assurance of behaviour and system robustness and integrity is required. Finding ways to be more efficient and reducing the cost of certification is also critical.

Key takeaways

- **Validation and explainability need to be better operationalised to foster greater trust and confidence. This will drive adoption and greater use of AI within cybersecurity.**
- **Mapping of the complex regulatory environment is required to support the supply chain. This will reduce the burden on smaller enterprises and organisations.**
- **There is a need for more multi-domain cybersecurity technology skills across European industry.**
- **Industry should leverage best practice in cybersecurity for AI risk assessment.**

Follow up points

- Supply chain plays an important role, and without appropriate controls may be a vector for cyber attacks.
- Need to develop approaches that can validate and potentially certify systems that continuously change as a result of the adoption of AI approaches.
- End users vary widely in their capabilities and this must be taken into account as AI is integrated into cybersecurity systems.

Panel 3

What are the implications of AI for Europe's innovation aspirations?

Moderated by

Diva Tommei Chief Innovation, Education and Marketing Officer, EIT Digital

Panellists

Giovanni Sollazzo Founder and Chairman, AIDEM

Nick Merritt Head of Strategy and Operations, Vault Hill

Sergio Alvarez-Telena Co-founder, CIO & Co-CTO, SCI the world

Panel 3
What are the implications of AI for Europe's innovation aspirations?

The panel was moderated by EIT Digital's Diva Tommei. EIT Digital is building a pan-European multi-stakeholder open-innovation ecosystem which includes leading European large companies, SMEs, start-ups, universities and research institutes. These stakeholders are mobilised to address the technology, talent, skills, business and capital needs of digital entrepreneurship. Since its launch in 2010, EIT Digital has equipped more than 3000 students with the skills to innovate and become entrepreneurs, supported more than 370 start-ups and scale-ups to grow internationally, and launched more than 530 products and services commercially.

For this panel, EIT Digital brought together some of the most exciting innovators and entrepreneurs, all of whom are working in different ways to innovate across the AI and deep tech ecosystems. They considered three main questions:

1. How can the value-add of innovation using AI be accelerated?
2. What will be the impact of impending regulation on this innovation?
3. How do we build the skills we need to take advantage of the AI innovation opportunity?

The panel began with a discussion of the motivations and drivers of innovation. Sergio Alvarez-Telena cited the R&D funding mechanisms within academia and in many larger companies that do not support the cutting-edge multi-year projects many innovators want to pursue, and which drive innovators like him to set up SMEs. Other panellists spoke of motivation to address gaps or problems: In the case of AIDEM, this motivation can be found in their mission to remove all personal data from advertising. For Vault Hill, their mission is to be the world's first human centric metaverse.

On the relationship between innovation and regulation, panellists had some divergent views. Some scepticism was expressed about the effectiveness of existing regulations, including GDPR, along with acknowledgement of the need for some form of regulation. On the other hand, there was still some doubt expressed about the need for regulatory interventions at all, and fears that too proactive an approach to AI or other deep tech regulation would stifle innovation.

The conversation then moved to the question of skills and talent. In July 2022, the European Commission launched the New European Innovation Agenda. This aims to position Europe at the forefront of the new wave of deep tech innovation and start-ups. The Agenda sets out 25 dedicated actions under five flagship areas:

- Funding Scale-Ups
- Enabling innovation through experimentation spaces and public procurement
- Accelerating and strengthening innovation in European Innovation Ecosystems across the EU
- Fostering, attracting and retaining deep tech talents
- Improving policy making tools

While there was considerable support for these aims amongst the panellists, it was clear from the discussion that Europe faces a huge challenge in training and retaining AI specialists. The aim of training one million deep tech talents was seen as laudable but at the same time very ambitious. Training provision must be matched with available opportunities for these specialists.

Key takeaways

- **There are many different perspectives on the role of regulation in fostering innovation.**
- **Skills and training are key parts the innovation agenda, but provision must be matched by available opportunities that appeal to businesses and potential employees.**

Panel 4

Standards and AI: are we on track?

Moderated by

Ray Walshe	Director, EU Observatory for ICT Standards (EUOS)

Panellists

Sebastian Hellensleben	Co-Chair, AI Committee CEN-Cenelec JTC 21
Hsiao-Ying Lin	Principal Researcher, Huawei Paris Research Center
Klaus-Dieter Axt	Executive Director, EUnited
Nicolas Moës	Director, European AI Governance, The Future Society
Karina Gibert Oliveras	Head of Intelligence and AI Research Centre, UPC

Panel 4
Standards and AI: are we on track?

The questions to be considered by the fourth and final panel were:

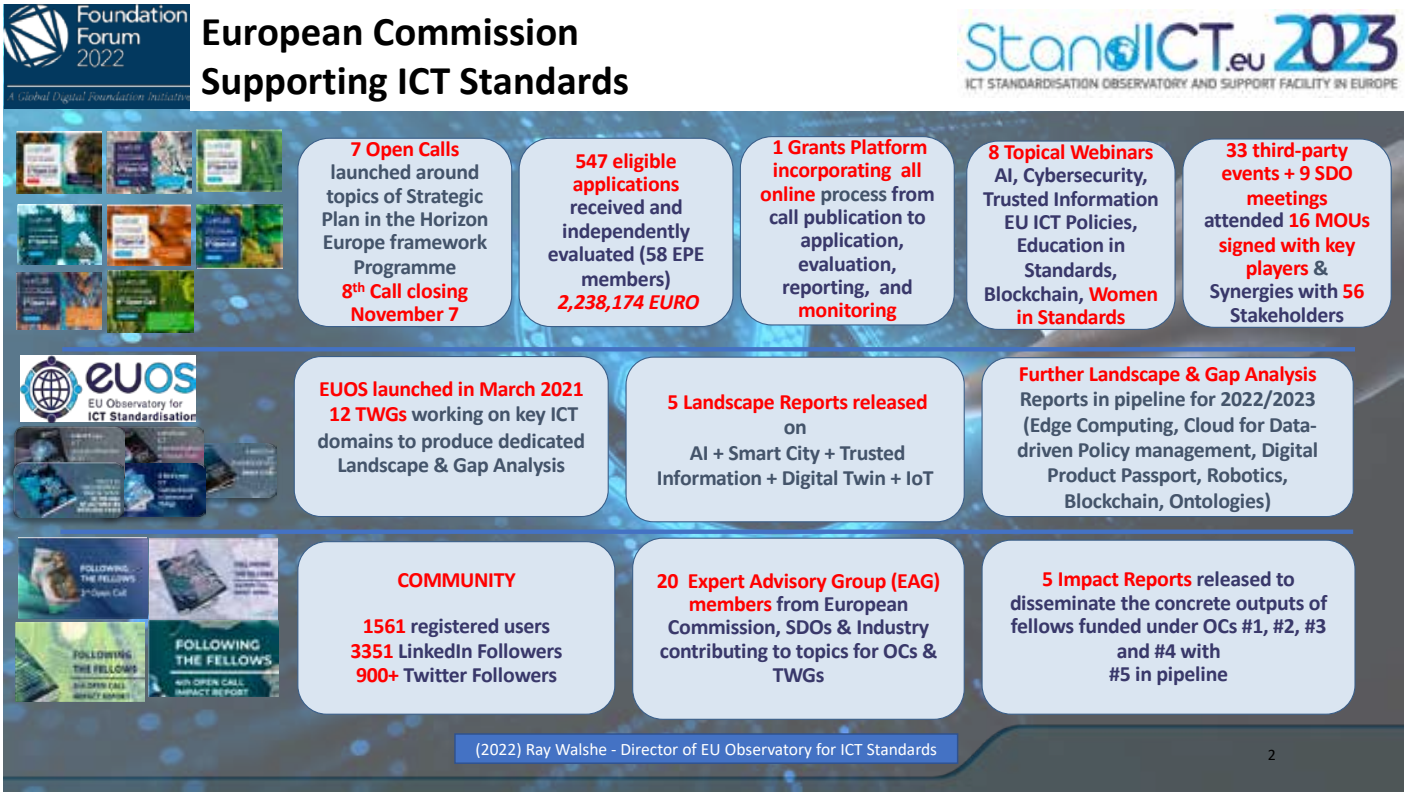
1. How will standards help Europe maximise the benefits and reduce the risks of AI?
2. How will standards help AI-driven innovation?
3. Are European standards bodies on track to deliver the right standards at the right time?

Ray Walshe, as the panel moderator, gave a brief introduction to the work of the EU Standards Observatory. As well as providing a funding platform to support international engagement in standardisation, the Observatory convenes technical working groups that produce landscape reports, including an influential report on the Landscape of Artificial Intelligence Standards published in May 2021.

Standards	Legislation
Voluntary	Mandatory
Consensual	Imposed by law
Developed by independent organisations	Established by public authorities
Reviewed every 5 years	Revised when legislators decide
Provide specifications and test methods (interoperability, safety, quality, etc.)	Gives requirements to protect public interests

Source: Ray Walshe, 2022

Ray then gave a short overview of the AI standards landscape, including the key committees and the important distinctions to be drawn between AI standards and legislation.



As Sebastian Hellensleben explained, the EU legislation relies heavily on harmonised standards for its implementation. Under the AI Act, manufacturers are incentivised to follow standards because of the presumption of conformity established in Article 40. European Standardisation Organisations (ESOs) will be responsible for setting these standards following standardisation requests (SR) from the European Commission.

In 2019, CEN and CENELEC established the new CEN-CENELEC Joint Technical Committee (JTC) 21 Artificial Intelligence. CEN-CLC/JTC 21 is responsible for the development and adoption of standards for AI and related data and the provision of guidance to other Technical Committees concerned with AI. It identifies and adopts international standards already available, or under development, from other organisations like ISO/IEC JTC 1 and its subcommittees, namely SC 42 Artificial Intelligence.

The discussion returned to the intersection of AI and cybersecurity and, in particular, how this is addressed in standards. Hsiao-Ying Lin outlined the work of the ETSI Securing AI (SAI) Working Group. This group examines how to identify threats and countermeasures, and has now published five reports. She also explained the role of the OCG AI which facilitates and coordinates activities in ETSI.

Offering an SME perspective, Klaus Dieter Axt explained how SMEs are engaging in standardisation, including generic standards development work, but also in European and international technical committees on specific issues for products. When it comes to AI, very few SMEs have the resources needed to engage in international standardisation. For the most part, SMEs receive standards and use them as tools that allow them to enter the Single Market. The timeliness of standards is arguably the key question for SMEs. Standards need to be available before the Act becomes applicable. SMEs and manufacturers must be informed about what is coming, and how they can meet the requirements.

Panellists agreed that standards are essential for ensuring market efficiency and building synergies. However, they are not just tools for market efficiency, but have a social and cultural dimension. As Karina Gibert Oliveras observed, we can trace the origins of the AI Act to ethical frameworks and principles. For standards to have the level of legitimacy needed to build trust in the new regulatory regime for AI, policymakers must pay close attention to these dimensions.

The European Commission has directed the work programme for the normalised standards to CEN and CENELEC, with ETSI being consulted. Based on the draft standardisation request, the JTC 21 is currently analysing many international pieces of work, including existing standards and standards under development at the international level. This includes work on risk management and the possible adoption of ISO/IEC DIS 42001 on AI management systems which would provide a standard framework for AI governance. However, some of the work undertaken by JTC 21 is so specific to the situation in Europe, and to the requirements of the AI Act, that it cannot be achieved by modifying other sources and existing standards. Such work includes deliberations about how we characterise the trust requirements of an AI system, as well as the structure and content conformity assessments that are particular to the EU's regulatory regime.

Once the finalised standardisation request is received, JTC 13 will analyse cybersecurity and data protection requirements and progress the consultation with the ETSI Secure AI (SAI) Work Group.

Key takeaways

- **There was strong support for inclusive approaches which involve and empower civil society as well as industry and SMEs.**

- **Without a more inclusive approach, there is a risk of significant political push-back against the AI Act that will in turn weaken legitimacy and potentially delay its adoption.**

- **Timeliness is key. Even with a relatively long grace period of 24 months under the proposed AI Act, ESOs need time to create quality standards and SMEs may need more time to conform to new requirements.**

Follow up points

- SMEs in particular, but also larger organisations, currently lack concise guidance on how to ensure they comply with regulatory requirements. There is an urgent need to develop what might be termed a one-stop-shop compliance checklist.

- The rapid creation of cybersecurity and AI standards, combined with increasing regulation in these areas, is creating a standards expertise problem for organisations of all sizes.There is an urgent need for organisations to develop staff with domain expertise combined with training in the application of standards.

Conclusions

Now in its second year, the Foundation Forum has emerged as an important opportunity for dialogue on digital policy at the European level. The Forum welcomed stakeholders from across industry, civil society, academia, and political institutions, and this diversity was reflected in the wide range of perspectives shared by the panellists. It was very apparent from all panels that considerable common ground exists, even amongst political groups. Europe stands to benefit greatly from further digital transformation, including wider adoption of trustworthy AI across sectors. Though there are many different views on how we should get there, there was much consensus that any vision for a Digital Europe should be ambitious, achievable, and should strike an acceptable balance between innovation and competition, and fundamental values.

A recurrent theme throughout the Forum discussions was the complex interplay between different policy domains and instruments. In other words, we cannot look at AI or cybersecurity, or any aspect of digital policy, in isolation. Many of the relevant instruments refer to, and will interact with, other laws. This is exemplified in the AI Act, which explicitly refers to the Cybersecurity Act and existing cybersecurity schemes. Under the AI Act, high-risk AI systems which have already been certified or had a relevant statement of conformity issued under an existing cybersecurity scheme shall be presumed to be in compliance.

There was some support for leveraging processes designed for existing regulatory requirements, including those under GDPR. More can be done now to identify and make use of these synergies and to avoid unnecessary proliferation of entirely new process measures to comply with regulations. There is, however, a need to recognise that the development, deployment, and use of AI brings specific challenges. This point was addressed by many panellists, particularly during the discussion on cybersecurity. This reinforces the necessity of understanding not just discrete policy domains and instruments, but also their interaction.

The third panel on the topic of innovation demonstrated that there are many fantastic SMEs already developing and using AI and having a positive impact on society. Across all panels there was a sense that SMEs and other smaller entities could play a much stronger role in AI policy processes, governance, and in standardisation. SME leaders can bring a more grounded, less abstract view of current market trends and can help to anticipate potential implementation challenges. There is much scope for closer collaboration and increased pooling of resources by SMEs, including through associations. Like other stakeholders, SMEs can work together to ensure their perspectives are considered, and that they have real impact on policy. There is also considerable scope for businesses to collaborate in their efforts to operationalise regulation, including by working together to develop new assurance tools such as codes of conduct or standardised contractual schemes.

Though the timeline of the proposed AI Act is still provisional, concerns were raised about the feasibility of full compliance by the time of applicability. The development of quality process standards, which will complement the Act, takes time and careful consideration. For businesses to be able to conform to these new requirements on time, and without making any trade-offs in innovation, a clearer indication of expected content may be required. As one participant suggested, the regulation should ideally coevolve to some extent with standards development.

Questions remain about exactly how the new regulatory regime will be overseen and how different powers and governance responsibilities will be arranged. There is, however, strong support for multi-stakeholder involvement. In addition, policy actors must recognise the need for alignment with Member State national strategies.

A huge amount is at stake in efforts to find the right responses to the policy challenges of the digital age. Europe's future competitiveness and prosperity will depend on its leadership in this area. Policymakers, businesses and leaders from across all stakeholder groups must be decisive, while safeguarding fundamental values, and placing security at the centre. Technologies like AI are transforming how we do business and live our lives. By addressing their potential risks now, we can overcome the greater risk of missing the opportunities they offer.

Key concepts

from panels

Key concepts from panels

Panel 1: Assurance of AI through the value chain

Concept	Requirements	Added value
AI Code of Conduct	The development of binding best practice, rules and defined levels of performance. These specifications would be more granular than legislative requirements and could reference standards	This could potentially become accepted as best practice across the AI value chain ecosystem and could reduce the cost and time involved in doing business
AI Assurance Certificates	The development of uniform schemas and mechanisms for documenting AI assurance in the supply chain	This would support businesses to demonstrate how they conform and to have some confidence that they are conducting assurance activities in similar ways
AI Operational Framework (Multi-actor Governance Framework, MAGF)	The development of a comprehensive framework for operationalising AI assurance across the value chain	This could be operationally useful but the timeline would need to be aligned with the needs of businesses using a multi-dimensional risk approach
Technical verification and validation tools	Provision of common structured methodologies	This underpins and provides the evidential basis for assurance

Key concepts from panels

Panel 2: AI and cybersecurity – an evolving relationship?

Concept	Requirements	Added value
Operationalising cybersecurity validation and explainability	Explaining systems and leveraging software best practice	This would foster greater trust and confidence to drive adoption and use to the cybersecurity community and users
Mapping the regulatory complexity to support the supply chain	Identifying and utilising the complex interplay between the various legislative instruments in the Digital Strategy	This would reduce the burden on smaller enterprises and organisations to understand and comply with requirements
The need for multi-domain cybersecurity technology skills	Addressing AI, data and cyber skills as well as combinations of skill sets, and diversity across the workforce	This would help address the technology skills shortages across European industry
Leverage best practice in cybersecurity for AI risk assessment	Identifying relevant existing processes and resources (including data) for risk assessments, systems validation and building synergies	This could improve the robustness of risk assessment processes and reduce cost burdens, particularly for SMEs

Key concepts from panels

Panel 3: What are the implications of AI for Europe's innovation aspirations?

Concept	Requirements	Added value
The need for Innovation and Entrepreneurial skills	Fostering combined and horizontal skill sets as well as subject specialisms, and ensuring relevant positions exist within Europe	This would help address the technology skills shortage across European industry and develop future leaders
A balanced, proportionate approach to regulation	Drawing on leading innovators to find the appropriate regulatory mix, e.g. through AI regulatory sandboxes	This would help to avoid any thwarting of innovation while levelling the playing field enough to encourage competition and respect for fundamental values
Accelerate the European industrial AI leaders	Accelerating AI in the enterprise base across selected key verticals	This could have the effect of increasing the importance of European policy around the world. This would help to create a common playing field beyond the EU

Key concepts from panels

Panel 4: Standards and AI: are we on track?

Concept	Requirements	Added value
Continued and further support for programmes which fund standards engagement work	Encouragement and funding for experts to consider standards engagement	This could help to address the standards and certification skills shortage
Simplification of AI standards mapping	Measures to make the current complex AI landscape more understandable to all stakeholders	Simplifying the presentation of and entry points to the AI standards landscape could make the landscape more accessible for SMEs and other stakeholders with limited capacity and resources
Engaging in standards bodies via industry associations and umbrella organisations	Leadership and closer cooperation amongst relevant organisations, including JTC 21, JTC 13, ETSI, SAI and ISO	Closer and more focused cooperation both by SMEs and by civil society would help broaden perspectives and strengthen the quality of standards deliverables
Some earlier indications of AI Standards, Validation and Certification Frameworks	ESOs working with businesses, civil society and policymakers to shape expectations	Regulated entities and stakeholders could more fully prepare for the long-term implications of legislation, and have the legal certainty needed to continue innovating

Next steps

Next Steps

Following the Transport, Telecommunications and Energy Council (Telecommunications) on 6 December 2022, the position of the Council of the EU has now been agreed. This means the Council can enter negotiations with the European Parliament, once the latter adopts its own position by around mid-2023. The two co-legislators will attempt to reach an agreement on the proposed regulation. Based on current projections, this will be no earlier than the second half of 2023. During this time, relevant European Standards Organisations (ESOs) will continue their work to prepare for the standardisation request that will be sent upon adoption of the Act. This gives stakeholders time to actively engage with policymakers and to help shape the regulatory regime they will be subject to.

Given that the AI Act is not expected to become applicable until 2025 or 2026, stakeholders can use this time to begin to anticipate, plan and experiment with methods and tools for AI assurance. The AI Assurance Club, an initiative of the Global Digital Foundation, brings together different actors from across the AI ecosystem to share best practice and to operationalise regulatory requirements and standards on AI. By joining, members gain access to a community of business and organisations working to make better AI governance a reality, in addition to insights and analysis of the evolving AI landscape. As many contributions to the 2022 Forum highlighted, these opportunities to collaborate and to find practical solutions to AI assurance are invaluable.

Foundation Forum 2023

Whilst preparing this report, some key ideas have come to the fore that are worth capturing in preparation for Foundation Forum 2023.

- Much of the value coming from the Foundation Forum arises from the contributions made by speakers and moderators during the panels. In future years it is proposed that this event become invitation only, with the expectation that all attendees will participate in discussions. This expectation will prompt attendees to read the advance briefing and be ready to bring a perspective from their own professional situation.

- The importance of the contribution of SMEs to policy was once again highlighted this year. We suggest a panel dedicated specifically to the perspectives and needs of SMEs at next year's forum.

- Looking ahead, to fully operationalise AI assurance, stakeholders will need to work together to promote validation and verification in various environments, including Cloud, Edge and Open Source for Enterprise Intelligence (EI).

Acknowledgements

The authors would particularly like to thank the following people for their feedback and subsequent input during the preparation of this report:

Roberto Cascella
John Higgins
Patrick McCarthy
Diva Tommei
Ray Walshe

We would also like to thank Willem van Vugt and the team at LEF marketing & events for their assistance with graphic design, photography and figure preparation.

Global Digital Foundation
The Digital Policy Network

EUOS
EU Observatory for ICT Standardisation

eit Digital

ECS
EUROPEAN CYBER SECURITY ORGANISATION

AI Assurance Club
A Global Digital Foundation Initiative

Corporate partner: HUAWEI