1. The greatest challenges in improving how AI actors manage AI-related risks—where “manage” means identify, assess, prioritize, respond to, or communicate those risks;

The lack of knowledge of certain AI actors about what the AI actually does, how it does it (black box mystery) and why, often results in shortcomings in risk management. Also, the lack of knowledge about the actual dataset the AI system learned from could result in a risk.

2. How organizations currently define and manage characteristics of AI trustworthiness and whether there are important characteristics which should be considered in the Framework besides: Accuracy, explainability and interpretability, reliability, privacy, robustness, safety, security (resilience), and mitigation of harmful bias, or harmful outcomes from misuse of the AI;

We agree with the list of mentioned characteristics of the AI trustworthiness, but we would also consider the dataset quality, supply chain security (e.g. trustworthiness of the vendor/suppliers,…) and updating/patching/service policy throughout the whole life cycle.

3. How organizations currently define and manage principles of AI trustworthiness and whether there are important principles which should be considered in the Framework besides: Transparency, fairness, and accountability;

Again, we agree with the list of principles of AI trustworthiness, but we would also consider whether the risk-based approach was followed when developing the AI.

4. The extent to which AI risks are incorporated into different organizations' overarching enterprise risk management—including, but not limited to, the management of risks related to cybersecurity, privacy, and safety;

We would incorporate AI risks into cybersecurity, privacy and safety risk management and also business continuity management and interoperability.

5. Standards, frameworks, models, methodologies, tools, guidelines and best practices, and principles to identify, assess, prioritize, mitigate, or communicate AI risk and whether any currently meet the minimum attributes described above;

We think that the framework suggested in the draft regulation of the EU laying down harmonised rules on Artificial intelligence – (AI Act, focusing on high-risk AI systems) and ENISA’s document “AI Cybersecurity Challenges - Threat Landscape of AI” meet the attributes.

6. How current regulatory or regulatory reporting requirements (*e.g.*, local, state, national, international) relate to the use of AI standards, frameworks, models, methodologies, tools, guidelines and best practices, and principles;

As yet, there is no regulation on AI on the national level. The draft AI Act is based upon several standards, guidelines, etc. (e.g. HLEG ethics guidelines for Trustworthy AI, work of the AI Alliance and the EU White paper on AI).

7. AI risk management standards, frameworks, models, methodologies, tools, guidelines and best practices, principles, and practices which NIST should consider to ensure that the AI RMF aligns with and supports other efforts;

Draft regulation of the EU laying down harmonised rules on Artificial intelligence (focused on high-risk AI systems); and ENISA’s document AI Cybersecurity challenges - Threat landscape of AI.

8. How organizations take into account benefits and issues related to inclusiveness in AI design, development, use and evaluation—and how AI design and development may be carried out in a way that reduces or manages the risk of potential negative impact on individuals, groups, and society.

9. The appropriateness of the attributes NIST has developed for the AI Risk Management Framework. (See above, “AI RMF Development and Attributes”);

From our point of view, the most important attributes are to provide common definitions (number 2) and be risk-based, outcome-focused, voluntary, and non-prescriptive (number 5); on the other hand in regard to the adaptability of the Framework (number 4) we are of the opinion that adaptability should be balanced with the need for details and the Framework should avoid being too general and not to the point.

10. Effective ways to structure the Framework to achieve the desired goals, including, but not limited to, integrating AI risk management processes with organizational processes for developing products and services for better outcomes in terms of trustworthiness and management of AI risks. Respondents are asked to identify any current models which would be effective. These could include—but are not limited to—the NIST Cybersecurity Framework or Privacy Framework, which focus on outcomes, functions, categories and subcategories and also offer options for developing profiles reflecting current and desired approaches as well as tiers to describe degree of framework implementation; and

11. How the Framework could be developed to advance the recruitment, hiring, development, and retention of a knowledgeable and skilled workforce necessary to perform AI-related functions within organizations.

12. The extent to which the Framework should include governance issues, including but not limited to make up of design and development teams, monitoring and evaluation, and grievance and redress.

There are some aspects which should be clearly be subject to governance (e.g. making sure the use of AI does not undermine democratic values and the rule of law). A human should always be kept in the loop when designing and monitoring the most critical uses of AI.