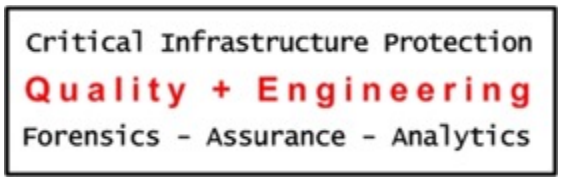

To: NIST
From: Quality + Engineering

Subject: AI Risk RMF RFI response
Date: August 11, 2021

Quality + Engineering Background and Quals:

Quality + Engineering background in AI and Risk:

- Developer of Certified Enterprise Risk Manager® certificate.
- Author of best-selling **ISO 31000: ERM** book (5 star reviews on Amazon).
- Author of **Value Added Auditing** book (risk assurance).
- Developer of Architect – Design – Deploy – Assure™ framework. Used to architect and design RMF's
- Developer of Proactive – Preventive – Predictive – Preemptive™ AI framework.
- Author of more than 30 books on supply chain risk management, quality, ISO 9001, ISO 31K, work, operational auditing, risk assurance, etc.
- More than 20 years experience in expert systems, ML, AI (Lisp, etc.), etc.
- Founder of:
    - www.WorkingIt.com
    - www.800Compete.com
    - www.QualityPlusEngineering.com

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;

Focus of these questions is largely transactional. There are overarching AI risk public policies to be addressed such as: AI geo-political risks, AI geo-economic risks, and enterprise risks. As well, there are enterprise strategies that should be addressed.

AI Risk is not mapped to international standards such as ISO 31K. The ISO 31K RMF is mature and can be easily modified (tailored) to different contexts and requirements.

Our responses focus on the specific nature of the RFI questions. The following are AI risks and challenges:

- Lack of overarching risk and AI model.
- Lack of common RMF.
- Lack of commonly used risk and AI principles.
- Lack of consistent risk and AI taxonomy.
- Lack of common risk and AI vocabulary.
- Lack of applicable risk and AI metrics and KPIs.
- Lack of risk hierarchy.
- Lack of common risk and AI processes.

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;

Trustworthiness is a hugely important. Trustworthiness needs to be expanded to include:

- 3 E's: economy, effectiveness, and efficiency.
- Develop PDCA equivalent loop for trust.
- Add GRC.
- Needs to be measurable.
- Address each of the 'lacks' in response to Question 1.
- Consider assurance such as assurance risk.
- Add risk based auditing to test, verify, and validate trustworthiness.
- Add risk based, problem solving and risk based, decision making.
- IP protections such as patent positions.

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;

AI principles to consider include:

- Confidentiality.
- Accessibility.
- Proprietary.
- Security.
- Resilience.
- Auditability.
- Measurability.

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;

AI assets are often confidential and proprietary. Depending on the size and context of the enterprise, these may be incorporated into the ERM and enterprise risk register.

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;

Associations such as IEEE and others are developing AI standards. International and national standards organizations such as ISO are developing AI standards and guidelines. Companies are developing proprietary standards such as Google.

These different approaches and standards result in diversity but also cause confusion. It would be helpful if an international standard, guideline, or benchmark could be baselines for AI risk RMF.

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;

International and national AI standards are being developed for ethics and trustworthiness. They are similar in nature.

However, there are few or no trustworthiness objectives, attributes, or characteristics that can be measured, audited, verified, and validated.

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;

As mentioned, ERM, COSO, ISO 31K and other standards and guidelines should be considered as templates. Or, new AI risk RMF can be cross walked to international standards.

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.

Equity and inclusion are hugely critical in AI design, development, and evaluation. AI risk requires objectives, criteria, principles, processes, and attributes that are measurable and auditable. Risk assurance is required if the likelihood and consequences of AI risk can be managed and measured suitably

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

See above responses.

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

NIST frameworks are good to great starting points. These frameworks can be cross walked to ISO 31K, COSO and other risk frameworks. The same can be done for AI frameworks.

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.

Future of Work and Professions are all about disruptive rules. We're living in VUCA time. Visit: **www.FutureofProfessions.com**. View **https://bit.ly/WORKING-IT-VDO**.

Nation states and criminal are using cyber strategies to cause chaos and extort monies. Many more cyber professionals need to be hired. A transparent AI RMF would induce people to work in AI and cyber.

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.

Yes, GRC should be considered in the AI RMF. Monitoring and evaluation are part of ISO 31K and COSO should also be considered.

Issues of grievance and redress are hugely critical. These issues will adjudicated in the courts. Much has to be done.

Hope this helps. Give us a holler if you need a deeper explanation. Best,

Greg Hutchins PE CERM