COMMENTS ON THE DRAFT NIST AI RMF

Gary Allan Bannister.

I have focussed only on General Comments, the reasons will be clear why? I have used your Comments Template edited in Word and copied into PDF format.

NIST AI RISK MANAGEMENT FRAMEWORK

NAME: GARY ALLAN BANNISTER

ORGANISATION : GLOBAL SUCCESS SYSTEMS

ROLE. SENIOR MANAGER AND CONSULTANT GOVERNANCE RISK AND COMPLIANCE. I have been working in this area for over 50 years.

Topics	Response #	RATIONALE	SUGGESTED CHANGE
General	I am not convinced that NIST needs another framework?	Businesses and Organaisations are suffering framework fatigue. They are overloaded. Existing frameworks can mange new technologies just as organisations manage new products and services, they do not create a new ERM. They add process, practices, controls, categories, threats and vulnerabilities to their existing frameworks.	See below more comments but change the title to **Guidance on setting up and using AI.**
	It is not a Risk Framework	It is incomplete, much of what you outline is more about a governance process. A Risk framework contains a process for calculating Likelihood, Impact, Response, Tolerance and appetite. This is already provided in numerous risk frameworks like ISO 27005, 31000, ISACA's Risk Management Framework, COSO etc.	See above
	The term Playbook was used a lot during the workshop	This confuses most stakeholders. A Risk Framework is is the structured process used to identify potential threats to an organisation and to define the strategy for managing or minimising the impact of these risks, as well as the mechanisms to effectively monitor and evaluate the strategy. It assists the organisation in integrating risk management into significant activities and functions. (ISO31000, COSO, COBIT et al). A Risk Playbook are a set of tools designed to help organisations focus on capabilities and practices. They are also designed to provide high-level key concepts for consideration when establishing a comprehensive and effective ERM program.	Be consisten in your language. As this is not considered to be a an RMF (see above) change it as recommended above to a Guidance or if you want to use the word Playbook you will need a lot more practical 'how' to do it
	The Rational explained in the workshop was that existing risk frameworks are 'too general' This is not so	Specifically the term Harm was used in the framework. I am challenging this concept, you cannot effectively monitor or measure harm. It is not possible	Reconsider this a sit alos will confuse the market place as it will not be considered helpful.