TATA CONSULTANCY SERVICES

Risk & Cyber Strategy
Journey to CSF 2.0 Comments Resolution Matrix Inputs for NIST
3 March 2023

#	Document, Page #, & Line #:	POC Information:	Comment Type (C/S/A)	Comments	Rationale
1	**IDENTIFY - Business Environment (ID.BE):** The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.	Robert Watson, TCS Risk & Cyber Strategy	S	Bring this element into **new Govern Function** and modify it to Set the Business Security Ecosystem (GV: SE): The organization leaders set the vision, mission, and strategic objectives that security is a business enabler and drives growth and transformation. Leaders establish, define and enable the successful execution of security through formally established roles, responsibilities, supporting activities and synchronized risk management decisions aided by clean swim lanes and tools such as RACIs.	Many organizations still have unclear swim lanes of security and are not synchronzied.
2	Sprinkle cyber pixie dust everywhere and liberally from the **AI Risk Management Framework 1.0** document Govern Section into the new Govern Function	Robert Watson, TCS Risk & Cyber Strategy	S	Bring large swaths of the language from AI RMF 1.0 to CSF 2.0 in the Govern section. They are very good and can be absolutely mirrored as complementary. Examples below	They are very good and can be absolutely mirrored as complementary.
3		Robert Watson, TCS Risk & Cyber Strategy		Govern: Govern The GOVERN function: • cultivates and implements a culture of risk management within organizations that transcends public-private sector organizations • outlines processes, documents, and organizational schemes that anticipate, identify, and manage the risks an ecosystem can pose, including to users and others across society – and procedures to achieve those outcomes; • incorporates processes to assess potential impacts; • provides a structure by which cybersecurity risk management functions can align with organizational principles, policies, and strategic priorities; • connects technical aspects of cybersecurity system design, development and implementation to organizational values and principles, and enables organizational practices and competencies for the individuals involved in acquiring, training, deploying, and monitoring such systems; and • addresses full product lifecycle and associated processes, including legal and other issues concerning use of third-party software or hardware systems and data. NIST AI 100-1 AI RMF 1.0	
4		Robert Watson, TCS Risk & Cyber Strategy	S	GOVERN is a cross-cutting function that is infused throughout AI risk management and enables the other functions of the process. Aspects of GOVERN, especially those related to compliance or evaluation, should be integrated into each of the other functions. Attention to Governance is a continual and intrinsic requirement for effective Cybersecurity Risk Management over a organization's ecosystem including operations and hierarchy whether public or private sector. Strong governance can drive and enhance internal practices and norms to facilitate organization risk culture and drive maturity. Governing authorities can determine the overarching policies that direct an organization's mission, goals, values, culture and risk tolerance. Senior leadership sets the tone for risk management within the entire enterprise through their sponsoship and setting a culture of security which is baked into the DNA of the organization. Management aligns the technical aspects of Cybersecurity Risk Management to tactics, techniques, procedures, policies and procedures. Documentation can enhance transparency, increase compliance, improve organizational security synchronization and bolster accountability across the enterprise.	
5		Robert Watson, TCS Risk & Cyber Strategy	S	Bring elements of Govern 1-6 from the AI RMF over to this document and sprinkle cyber pixie dust into them as they relate to Governance	

6		Robert Watson, TCS Risk & Cyber Strategy	S	We concur with a strong focus on supply chain risk management in the updates to 2.0 specifically with SBOM	
7		Robert Watson, TCS Risk & Cyber Strategy	S	We would request more industry specific profiles samples in version 2.0 and would be willing to work collaboratively on those	
8		Robert Watson, TCS Risk & Cyber Strategy	S	Maintain a nice alignment and mention of International Standards and best practices from ISO, GDPR etc	
9		Robert Watson, TCS Risk & Cyber Strategy	S	Increase metrics focus through CMMI or similar maturity metrics that are simple, clear & concise	
10		Robert Watson, TCS Risk & Cyber Strategy	S	Provide more assessment based methodology linkages to RMF, 800-53 etc	