Dear NIST Cybersecurity Framework Team,

I hope this email finds you well. I am writing to provide feedback on the Discussion Draft of the NIST Cybersecurity Framework 2.0 Core. I appreciate the efforts made by the NIST team in incorporating the new Govern function and would like to suggest further emphasis on the interconnected nature of governance with the other core functions.

My proposal is to place Govern at the center of the diagram, visually emphasizing its central role in driving effective cybersecurity risk management across the organization. By doing so, the importance of a comprehensive governance framework in aligning cybersecurity activities with enterprise risks and legal requirements can be highlighted.

I have attached a document containing detailed descriptions of each function, including how the interconnectedness of the Govern function with the other core functions can be emphasized. I believe that by implementing these changes, the NIST Cybersecurity Framework 2.0 Core can help organizations better align their cybersecurity activities with enterprise risks and legal requirements, ultimately contributing to a more robust cybersecurity posture.

I hope you find this feedback useful and consider implementing the proposed changes. Thank you for your time and the opportunity to contribute to the development of the NIST Cybersecurity Framework 2.0 Core.

Best regards,

Yusuf

Yusuf Wilajati Purna | ユスフ ウィラジャティ プルナ
Cyber Risk Management Office, and　| サイバーリスクマネジメント室
Technology Division – Cybersecurity | テクノロジー本部（兼務）
██████████

MTI Ltd.
████████████████████████████████
████████████

Making the world *a step forward*

Strengthening Governance and Its Interconnected Role in NIST CSF 2.0 Core Functions

Yusuf Wilajati Purna
(ywpurna@ywpurna.com, purna_y@mti.co.jp)

May 2, 2023

The NIST Cybersecurity Framework 2.0 Core Discussion Draft effectively incorporates the new Govern function, which plays an essential role in establishing a robust foundation for cybersecurity risk management. By proposing to place "Govern" at the center of the diagram, the interconnected nature of governance with the other functions (Identify, Protect, Detect, Respond, and Recover) can be visually emphasized, underlining the significance of a comprehensive governance framework in driving effective cybersecurity risk management across the organization:

The descriptions for each function, considering the central role of the Govern function, are as follows:

1. **GOVERN**: Establish, maintain, and monitor risk management strategy, expectations, and policy, ensuring alignment with organizational objectives and legal/regulatory requirements. The Govern function serves as the central guiding element for all other functions, providing the necessary context, priorities, and risk tolerance to inform decision-making across the organization.
2. **IDENTIFY**: Determine the organization's current cybersecurity risk by identifying assets, understanding vulnerabilities, and assessing potential threats. This function is guided by the context and risk tolerance provided by the Govern function, helping prioritize resources and activities based on the risk landscape.

3. **PROTECT**: Implement safeguards to mitigate and reduce cybersecurity risk according to the organization's risk management strategy, expectations, and policy, as defined by the Govern function. This includes deploying security controls, managing access, and maintaining the confidentiality, integrity, and availability of assets.
4. **DETECT**: Continuously monitor and analyze the organization's assets and environments to identify potential cybersecurity attacks and compromises. This function operates within the scope and focus defined by the priorities and risk tolerance established by the Govern function.
5. **RESPOND**: Take appropriate and timely action to address detected cybersecurity incidents, based on the organization's risk management strategy and incident response plan, established by the Govern function. This includes containment, eradication, and communication with relevant stakeholders.
6. **RECOVER**: Restore assets and operations impacted by a cybersecurity incident, ensuring resilience and business continuity. The Recover function aligns with the organization's risk management strategy and priorities defined by the Govern function, focusing on minimizing the impact of incidents and restoring normal operations.

By emphasizing the interconnectedness of the governance function with the other core functions, the NIST Cybersecurity Framework 2.0 Core helps organizations to better align their cybersecurity activities with enterprise risks and legal requirements, ultimately contributing to a more robust cybersecurity posture.

EOF