Santander

March 3, 2023

Santander appreciates the opportunity to submit comments in response to **NIST´s Cybersecurity Framework 2.0 Concept Paper: Potential Significant Updates to the Cybersecurity Framework.**

Santander supports NIST's efforts to evaluate and improve its existing cybersecurity resources, including the NIST Cybersecurity Framework (CSF), seeking diverse stakeholder feedback in the update process.

General Observations:

After our response to the NIST Cybersecurity Request for Information (RFI) and our participation on the second workshop on CSF 2.0, we have reviewed and evaluated the significant changes provided in the Concept Paper, divided in six sections:

1. CSF 2.0 will explicitly recognize the CSF's broad use to clarify its potential applications

2. CSF 2.0 will remain a framework, providing context and connections to existing standards and resources.

3. CSF 2.0 (and companion resources) will include updated and expanded guidance on Framework implementation

4. CSF 2.0 will emphasize the importance of cybersecurity governance

5. CSF 2.0 will emphasize the importance of cybersecurity supply chain risk management (CSCRM)

6. CSF 2.0 will advance understanding of cybersecurity measurement and assessment

Santander welcomes the changes proposed (six sections including the subsections proposals), as they are aligned with the feedback provided on the RIF by Santander. However we would like to highlight and share our opinion on the following sections:

Proposed Considerations:

1) CSF 2.0 will emphasize the importance of cybersecurity governance - 4th Section

Adding a new Govern function will highlight that the cybersecurity governance is critical to managing and reducing cybersecurity risk and will help organizations to comply with European and International regulations and guidelines such as DORA, NIS2, EBA Guidelines, SEC (Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure Proposed rule), etc.

Our recommendation is to move the following categories to the Govern Function: Business Environment (ID.BE), Governance (ID.GV), Risk Management Strategy (ID.RM) and Awareness and Training (PR.AT).

The following governance-related topics should be considered (as subcategories under the existing categories or with the creation of new ones):

- Internal governance and internal control framework
- Cyber Security Strategy aligned with Business Strategy (including Resilience strategy)
- Budget & Resources (including staff & qualifications)
- Legal & Regulatory requirements
- Policies, standards, guidelines (creation and maintenance)
- Roles & Responsibilities
- Oversight & Regular Reviews (organization, policies, controls, metrics, indicators, etc.)
- Reporting Channels & Committees (including the Board, Business Areas, etc.)

2) CSF 2.0 will emphasize the importance of cybersecurity supply chain risk management (CSCRM) – 5th Section

Given the relevance of the supply chain processes, it might be appropriate to include a new Supply Chain Function that includes on C-SCRM specific outcomes (oversight and management) instead of expanding ID. SC Category in the Identify Function.

3) Additional suggestions on the current subcategories were provided on the RFI for your review and consideration for the final draft.

Santander looks forward to collaborating and providing our perspectives on the CSF 2.0 draft.