Comments to the Discussion Draft of the NIST Cybersecurity Framework 2.0 Core (April 24, 2023)

Juan Carlos Angarita, CEO, IMS Global, [redacted]

Element of the Discussion Draft of the NIST Cybersecurity Framework 2.0 Core	Comment
Page 3, Table 1: Function and Category Names and Identifiers. CSF 2.0 Category "Improvement" ID.IM Page 13, Table 3. Category "Improvement (ID.IM)".	**Improvement category** should be moved to the **Govern** (GV) CSF 2.0 Function, considering that continuous improvement involves any kind of organizational leadership, direction, or organizational government, as well as the active participation of other levels, functions, and processes in the organization. Justification: • The continuous improvement approach should be responsibility of the direction or governance structure, as a mean to ensure the incorporation of improvements resulting of cybersecurity management in order to achieve business goals. Not doing this will render the cybersecurity process in a highly reactive profile. • Moving this Category to the Govern function will improve and easy the integration with other technical management systems (such as the provided by ISO/IEC 27001:2022) which involves context, assets, and risk management in its planning stage, and monitoring, measurement, auditing, review, and improvement activities in the verification and acting stages.
Page 6, Table 3: Functions, Categories, and Subcategories. CSF 2.0 Category "Organizational Context"	The description text should include the word "*requirements*" as is shown in the following paragraph: "*The organization's risk context, including mission, mission priorities, objectives and direction stakeholders,* ***requirements****, is understood (formerly ID.BE)*". Justification: • GV.OC-03 CSF 2.0 Subcategory includes the identification, understanding, and management of requirements. • The requirements framework – in each case – helps to define how to understand and classify information and IT assets, risks, and controls. In some cases, the requirements can also establish a minimum set of controls to be implemented.
Page 6, Table 3 CSF 2.0 Subcategory GV.OC-01	This subcategory should include a reference to the participation or relationship of the organization with a critical infrastructure sector as is shown in the following paragraph: "*GV.OC-01: Organizational mission* ***as well as the participation or relationship in a critical infrastructure sector, or several of them****, are understood in order to prioritize cybersecurity risk management (formerly ID.BE-2 and ID.BE-3)*". Note: The classification of critical infrastructure sectors, defined by current regulation and kept by CISA, can be used as an informative reference (not requirement) for that classification. Justification: • Even though an organization may participate in the value chain of several critical infrastructures, it is also true that they usually belong to a specific critical infrastructure sector. • This classification helps to identify specific interested parties, requirements, assets, risks and control solutions, This does not imply ruling out that the organization has parallel roles in other sectors.

Page 6, Table 3 CSF 2.0 Subcategory GV.OC-02	The description text of this subcategory could include the word "*needs*" as is shown in the following paragraph: "*GV.OC-02: Internal and external stakeholders, and their **needs and** expectations regarding cybersecurity risk management, are determined*". Justification: • Stakeholders are usually the source of requirements. • Adding the word "needs" will improve the integration with other key technical management systems (such as ISO/IEC 27001:2022, ISO 22301:2019, or ISO/IEC 27032:2012)
Page 7, Table 3 CSF 2.0 Subcategories GV.RM-01 and GV.RM-02	The description text of these two subcategories should have a reference to "strategy" and include the "processes approach": "*GV.RM-01: Cybersecurity risk management **strategy and** objectives**, and the specific risk management processes and methodologies,** are established and agreed to by organizational stakeholders (formerly ID.RM-1)*". "*GV.RM-02: Cybersecurity supply chain risk management **strategy and objectives, and the specific risk management processes, are** established, agreed to by organizational stakeholders, and managed (formerly ID.SC-1)*". Note: Subcategory GV.RM-02 should reference CSF 1.1 ID.BE-1 given its direct relationship with supply chain. Justification: • Strategies (high profile level) and its direction (objectives) in the organization usually are deployed through the several processes running in the organization.
Page 7, Table 3 CSF 2.0 Subcategory GV.RM-05	The description of this subcategory could be re-arranged for a better understanding as is shown in the following paragraph: "*GV.RM-05: Strategic direction **and investments, describing appropriate cyber-security risk response options, risk transfer mechanisms (e.g., insurance, outsourcing), mitigations**, and risk acceptance, are established and communicated*".
Page 7, Table 3 CSF 2.0 Subcategory GV.RM-06	This subcategory should include "*authorities*" for risk management strategy, as is shown in the following text: "*GV.RM-06: **Authority,** responsibility**,** and accountability are determined and communicated for ensuring that the risk management strategy and program are resourced, implemented, assessed, and maintained*". Justification: • This will clearly define who is responsible for decision making.
Page 8, Table 3 CSF 2.0 Subcategory GV.RM-07	This subcategory should include rules about when this review should take place, as is shown in the following text: "*GV.RM-07: Risk management strategy is reviewed and adjusted to ensure coverage of organizational requirements and risks**, periodically, at least once a year, in the face of changes in the context, or in the event of a cybersecurity incident in the organization or in the critical infrastructure sector***". Justification: • It is important to have baseline rules for the review of the risk approach to ensure its continuous improvement in face of a dynamic and complex cyber risk environment.

Page 8, Table 3 CSF 2.0 Category "Roles and Responsibilities" (GV.RR)	This category should be renamed as "***Authorities,*** *Roles, and Responsibilities (GV.RR)*" Justification: • Organizational leadership make decisions about cyber-security management in exercise of its authority.
Page 9, Table 3 CSF 2.0 Subcategory GV.RR-07	The description of this subcategory should include "*development and strengthening of skills and awareness*" as well as the "*provisioning*" of human resources as is shown in the following paragraph: "*GV.RR-07: Cybersecurity is included in human resources practices (e.g., **provisioning,** training, **development and strengthening of skills and awareness**, deprovisioning, **and** personnel screening) (formerly PR.IP-11)*". Justification: • The development and strengthening of skills and awareness is a key factor to ensure cybersecurity performance considering that the human being is the one who ultimately interacts and makes decisions regarding information.
Page 9, Table 3 CSF 2.0 Subcategory GV.PO-03	This subcategory should include rules about when this review should take place, as is shown in the following text: "*GV.PO-03: Policies and procedures are reviewed, updated, and communicated to reflect changes in requirements, threats, technology, and organizational mission**, periodically, at least once a year, in the face of changes in the context, or in the event of a cybersecurity incident in the organization or in the critical infrastructure sector***". Justification: • It is important to have baseline rules for the review of policies and procedures to ensure its continuous improvement in face of a dynamic and complex cyber risk environment.
Page 10, Table 3 CSF 2.0 Subcategory ID.AM-05	The description of this subcategory could be rearranged for clarity as is shown in the following paragraph: "*ID.AM-05: Assets are prioritized based on its classification **based on its sensitivity**, criticality, resources **and dependencies**, as well as organizational value*". Justification: • It is necessary to have clear rules about how to classify assets considering that it is the input for prioritization.
Page 10, Table 3 CSF 2.0 Subcategory ID.AM-08	The description of this subcategory should improve the detail of the life cycle of assets, as is shown in the following paragraph: "*ID.AM-08: Systems, **Services,** Devices, **Networks**, and Software are managed throughout their life cycle**, including the design (and the application of precepts such as cybersecurity by design or by default)**, pre-deployment ~~checks~~, **deployment**, ~~preventive~~ maintenance **and upgrading or updating**, integration, transfers, end-of-life with disposition **or re-use** (formerly PR.DS-3, PR.IP-2, PR.MA-1, and PR.MA-2)*". Justification: • A complete perspective of the life cycle of assets will improve the performance and effectiveness of cybersecurity controls and the cyber-security framework, and it will generate a baseline of a comprehensive asset protection throughout its life cycle.

Page 11, Table 3 Category "Risk Assessment" (ID.RA)	The description of this category could be rearranged for a better understanding as is shown in the following paragraph: "*Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission,* ***objectives,*** *functions* ***and process;*** *or image or reputation), organizational assets* ***(and economic losses)****, and individuals*". <u>Justification</u>: • Risks can materialize generating impacts on the objectives of the organization and/or its processes, as well as in its operations.
Page 12, Table 3 Subcategory ID.RA-05	The description of this subcategory could be enhanced by adding the expression "risk" as is proposed in the following paragraph: "*ID.RA-05: Threats, vulnerabilities, likelihoods, and impacts are used to determine* ***risk as well as risk*** *exposure and inform risk prioritization*". <u>Justification</u>: • Risk and risk exposure are two different expressions.
Page 12, Table 3 Subcategory ID.RA-06	The description of this subcategory should be enhanced by adding the expressions "effectiveness", "implemented", "controls", and "measures" as is proposed in the following paragraph: "*ID.RA-06: Risk responses* ***or measures (controls)*** *are chosen, prioritized, planned,* ***implemented,*** *tracked, communicated****, and evaluated for its effectiveness*** *(formerly ID.RA-6 and RS.MI-3)*" <u>Justification</u>: • It is basic to know if the implemented controls are operational and can treat risk in the desired way, achieving the expected results (effectiveness). This element is an input for continuous improvement at the level of the risk management process.
Page 12, Table 3 Subcategory ID.RA-07	The description of this subcategory should be enhanced by adding the expression "treated" as is shown in the following paragraph: "*ID.RA-07: Changes are managed, assessed for risk impact, recorded****, and treated*** *(formerly part of PR.IP-3)*" <u>Justification</u>: • Risks associated with changes must also be treated according to the responses (controls) identified in Subcategory ID.RA-06.
Page 12, Table 3 Subcategory ID.RA-08	The description of this subcategory should be enhanced by adding the expression "treated" as is shown in the following paragraph: "*ID.RA-08: Risks associated with technology suppliers and their supplied products and services are identified, recorded, prioritized, monitored****, and treated*** *(formerly ID.SC-2 and PR.DS-8)*" <u>Justification</u>: • Risks associated with products and services supplied by third-party providers must also be treated according to the responses (controls) identified in Subcategory ID.RA-06.
Page 12, Table 3 Subcategory ID.RA-10	The description of this subcategory should be enhanced by adding references to "risks", as is shown in the following paragraph: "*ID.RA-10: Exceptions to security measures are* ***formally authorized****, reviewed, tracked, and compensated for****, being clear about the associated risks***". <u>Justification</u>: • Before granting exceptions to controls (measures), the risks related to each of them must be clearly understood.

Page 13, Table 3 Subcategory ID.SC-04	The description of this subcategory should be enhanced by adding references to "inspections" as is shown in following paragraph: "*ID.SC-04: Suppliers and third-party partners are routinely assessed using audits, tests ~~results~~,* ***inspections,*** *or other forms of evaluations to confirm they are meeting their contractual obligations****, which must be included in contractual agreements with third-party providers***". Justification: • Inspections are other suitable technical mechanism to assess the degree of commitment and compliance on suppliers. • It is important to include the option of carrying out audits, tests, and inspections in formal agreements with external providers, to prevent that they refuse in the future such evaluations.
Page 15, Table 3 Subcategory PR.AA-01	The description of this subcategory should be enhanced by adding explicit references to the "life cycle" of identities and credentials, as is shown in following paragraph: "*PR.AA-01: Identities and credentials for authorized users, processes, and devices are managed by the organization (formerly PR.AC-1)****, throughout the life cycle of identities and credentials, including their assignment, verification, adjustment, transition, and revocation***". Justification: • Since identity and credential management is a central aspect of cybersecurity, it is important to establish a minimum rule about the life cycle of identities and credentials.
Page 16, Table 3 Category "Awareness and Training (PR.AT)"	This category should have an initial subcategory as is described in the following paragraph: "***PR.AT-00: The organization must identify and keep updated the group of general technical competencies in cybersecurity, as well as the specific ones according to the position, role, function, or tasks to be performed, based on the requirements framework, the information and technology assets to be protected, the risks identified in the organization, and the incident records***". In addition, the same category should also have an ending sub-category as is shown in the following paragraph: "***PR.AT-06: All the awareness and training (technical training) activities must be evaluated regarding their effectiveness in terms of the achievement of the expected competencies and the improvement of the performance of cybersecurity***". Justification: • It is important that organizations build a baseline of technical cybersecurity competencies to guide the better development of competencies and awareness around cybersecurity, as well as the evaluation of the effectiveness of such actions to determine if they really achieved their objective.
Page 16, Table 3 Subcategory PR.AT-01	This subcategory should include when such actions should happen: "*PR.AT-01: Awareness and training are provided for users****, at the start of your job and on a regular basis,*** *so they possess the knowledge and skills to perform relevant tasks (formerly PR.AT-1 and RS.CO-1)*". Justification: • It is key to establish the minimum frequency of training.

Page 16, Table 3 Category "Data Security (PR.DS)"	The description of this category should be enhanced by adding a reference to the applicable requirements, as is shown as follows: "*Information and records (data) are managed consistent with the organization's risk strategy* ***and the applicable requirements*** *to protect the confidentiality, integrity, and availability of information* ***and related assets***". Justification: • The specific requirements for the organization or its information assets can establish specific data security measures (controls).
Page 17, Table 3 Subcategory PR.DS-11 Page 20, Table 3 Subcategory PR.PS-06	These subcategories should be enhanced by adding a requirement stablished in ISO/IEC 27701 as is shown in the following paragraph: "*PR.DS-11: Backups of data are conducted, protected* ***(including encryption),*** *maintained, and tested (formerly PR.IP-4)*". "PR.PS-06: Backups of platform software are conducted, protected ***(including encryption),*** maintained, and tested". Justification: • A common practice for the protection of backups when they can contain PII (Personally identifiable information) is cyphering.
Page 19, Table 3 Category "Platform Security (PR.PS)"	The description of this category should be enhanced by adding a reference to the applicable requirements, as is shown as follows: "The hardware and software (e.g., firmware, operating systems, applications) of physical and virtual platforms are managed consistent with the organization's risk strategy ***and the applicable requirements*** to protect their confidentiality, integrity, and availability **of information and related assets**". Justification: • The specific requirements for the organization or its information assets can establish platform security measures (controls).
Page 20, Table 3	The description of this category should be enhanced by adding a reference to the applicable requirements, as is shown as follows: "*Security architectures are managed with the organization's risk strategy* ***and the applicable requirements*** *to protect asset confidentiality, integrity, and availability* **of information and related assets***, and organization resilience*". Justification: • The specific requirements for the organization or its information assets can establish specific technology infrastructure resilience measures (controls).
Category "Technology Infrastructure Resilience (PR.IR)"	This category should have an initial subcategory as is proposed in the following paragraph: "***PR.IR-00: The processes, technologies, and assets that support the provision of products and/or services in the organization, or must be managed according to the applicable requirements, are evaluated regarding the impact of their disruption, especially in the event of cybersecurity incidents, as a basis for the definition of response and recovery plans***". Justification: • Responses and other recovery mechanisms must always be defined in the face of disruptive incidents, in this case associated with cybersecurity.

Page 20, Table 3 Subcategory PR.IR-01	This subcategory should be complemented by including actions related to "testing" and "evaluation" as is shown: "*PR.IR-01: Response and recovery plans (e.g., incident response plan, business continuity plan, disaster recovery plan, contingency plan) are communicated and maintained**, as well as regularly tested and evaluated for their effectiveness** (formerly PR.IP-9)*". Justification: • It is important to test periodically any kind of plans of response and/or recovery in order to determine its suitability.
Page 20, Table 3 Subcategory PR.IR-02	This subcategory could be improved by including actions related to "physical access" as is shown: "*PR.IR-02: The organization's networks and environments are protected from unauthorized logical access**, physical access,** and usage (formerly PR.AC-3, PR.AC-5, PR.DS-7, and PR.PT-4)*" Justification: • Physical access is another key facet of security that can seriously affect availability of infrastructures.
Page 23, Table 3 Subcategory RS.MA-01	This subcategory should be the last one in this category, and its description should be improved by including a direct reference to "lessons learnt" as is shown in the following paragraph: "RS.MA-**06**: The incident response plan is executed (formerly RS.RP-1) **and the produced lessons learnt recorded and analyzed**". Justification: • The lessons learnt are an important input for improvement, and it is necessary to explicitly require that record.
Page 24, Table 3 Subcategory RS.MA-05	This subcategory should be the first in this category, and its description should be enhanced by including the terms "risks" and "requirements" as is described in the following paragraph: "*RS.MA-**00**: Criteria for initiating incident recovery defined and applied **based on risks and applicable requirements as well as reviewed at least yearly of after any critical incident considering the effectiveness of incident management***". Justification: • Criteria definition is a key input for risk methodologies and, in this case, for incident management, in order to make decisions in an orderly and informed manner.
Page 24, Table 3 Subcategory RS.AN-03	This subcategory can be enhanced by adding "lessons learnt" as is shown in the following paragraph: "*RS.AN-03: Analysis is performed to determine what has taken place during an incident and the root cause of the incident, **and the produced lessons learnt recorded and analyzed***". Justification: • This subcategory can produce additional data for lessons learnt.
Page 24, Table 3 Subcategory RS.AN-06	This subcategory can be enhanced by adding "lessons learnt" as is shown in the following paragraph: "*RS.AN-06: Actions performed during an investigation are recorded and the record's integrity and provenance are preserved (formerly part of RS.AN-3), **and the produced lessons learnt recorded and analyzed***". Justification: • This subcategory can produce additional data for lessons learnt.

Page 25, Table 3 Subcategory RC.RP-01	This subcategory can be enhanced by adding a reference to the originating incident as is shown in the following paragraph: "*RC.RP-01: The incident recovery plan is executed* ***according to the corresponding incident***". Justification: • Recovery plans must be designed for specific incidents under the approach of response flexibility.
Page 26, Table 3 Subcategory RC.RP-04	This subcategory should be moved to the category improvement. Justification: • The establishment of post-incident operational norms, besides being part of lessons learnt, it conforms improvement.
Page 26, Table 3 Subcategory RC.RP-06	This subcategory should be moved to the beginning of category. Justification: • Criteria definition is a key input for risk methodologies and, in this case, for incident recovery.