NIST PRIVACY FRAMEWORK VERSION 1.1 CONCEPT PAPER

June 18, 2024

Note to Reviewers

This Concept Paper supports updating the NIST Privacy Framework to Version 1.1. It introduces the basic approach to updating the framework, using illustrative examples, but it is not intended to describe the complete update.

NIST welcomes all feedback on the concepts within this paper and is interested in answers to the following questions:

- Do the topics introduced in this concept paper identify key focus areas for updating the NIST Privacy Framework? If not, are there additional focus areas NIST should consider?
- The examples introduced in this concept paper were designed to elicit consistent principles which NIST will use to guide the complete update for public comment. Are there other principles or approaches that NIST should consider to increase the efficacy of using the NIST Privacy Framework and Cybersecurity Framework together?
- Apart from addressing alignment between the Privacy Framework and Cybersecurity Framework, are there other updates NIST should make to ensure the Privacy Framework remains responsive to current privacy risk management needs?

1. Introduction

Since the release of NIST Privacy Framework (PF) Version 1.0 in January of 2020, NIST has released NIST Cybersecurity Framework (CSF) Version 2.0, with significant revisions to content and structure. PF 1.0 was modeled on the CSF so the two frameworks could be used together more easily. NIST seeks to maintain the connection by making appropriate PF adjustments based on CSF 2.0 changes. In addition, organizations have had a few years to use the PF, therefore, NIST is interested in any areas where targeted improvements can be made. Given these developments, NIST has determined to make a modest PF update to Version 1.1. In summary, the goals for this update are to support realignment with CSF 2.0, facilitate ease and effectiveness of use, and ensure the tool is responsive to current privacy risk management needs.

This concept paper outlines key topics for discussion about potential PF 1.1 updates. For each topic, a non-exhaustive set of examples is provided to illustrate the issues for stakeholder feedback and inform the principles that NIST can use in updating the PF to version 1.1.

This paper will support discussion sessions at the NIST public workshop, Ready, Set, Update! Privacy Framework 1.1 + Data Governance and Management Profile Workshop. If you would like to provide informal feedback on this material in addition to or in lieu of participating in the workshop, please send it to privacyframework@nist.gov by July 31, 2024.

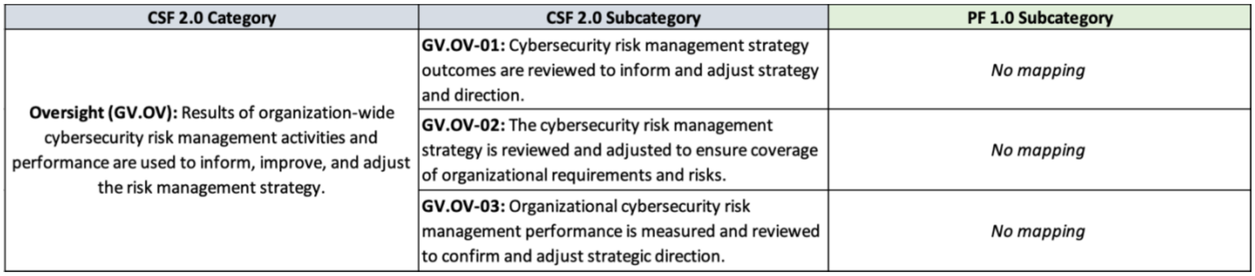
More information on the PF 1.1 development process can be found in the New Projects section of the NIST Privacy Framework website.

2. Topic 1: CSF 2.0 Revisions That Do Not Map to Analogous PF 1.0 Content

Many new CSF 2.0 Categories/Subcategories lack a mapping to analogous PF 1.0 content, which may hinder effective use of the frameworks together. This section highlights a few examples and explores options for PF 1.1 updates to address resulting issues.

2.1. Example 1: The New CSF 2.0 Oversight Category (GV.OV)

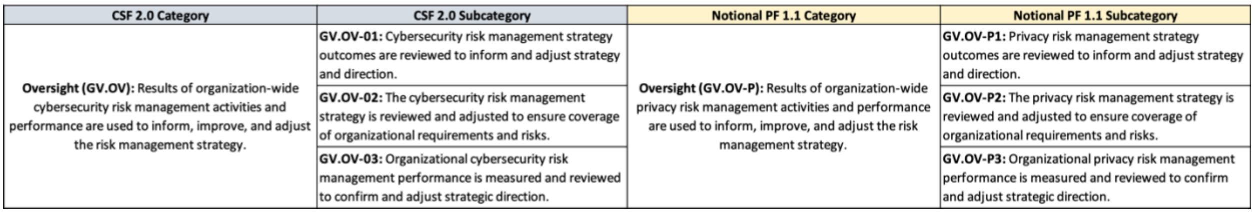
CSF 2.0 introduces an Oversight Category (GV.OV) dedicated to oversight of organizational cybersecurity risk management strategy. This new Category does not map to PF 1.0 as illustrated below:[1]



CSF 2.0 Category	CSF 2.0 Subcategory	PF 1.0 Subcategory
Oversight (GV.OV): Results of organization-wide cybersecurity risk management activities and performance are used to inform, improve, and adjust the risk management strategy.	**GV.OV-01:** Cybersecurity risk management strategy outcomes are reviewed to inform and adjust strategy and direction.	*No mapping*
	GV.OV-02: The cybersecurity risk management strategy is reviewed and adjusted to ensure coverage of organizational requirements and risks.	*No mapping*
	GV.OV-03: Organizational cybersecurity risk management performance is measured and reviewed to confirm and adjust strategic direction.	*No mapping*

Table 1: CSF 2.0 Oversight Category with Lack of PF 1.0 Mapping

NIST proposes creating a new Oversight Category in the Govern-P Function:



CSF 2.0 Category	CSF 2.0 Subcategory	Notional PF 1.1 Category	Notional PF 1.1 Subcategory
Oversight (GV.OV): Results of organization-wide cybersecurity risk management activities and performance are used to inform, improve, and adjust the risk management strategy.	**GV.OV-01:** Cybersecurity risk management strategy outcomes are reviewed to inform and adjust strategy and direction.	**Oversight (GV.OV-P):** Results of organization-wide privacy risk management activities and performance are used to inform, improve, and adjust the risk management strategy.	**GV.OV-P1:** Privacy risk management strategy outcomes are reviewed to inform and adjust strategy and direction.
	GV.OV-02: The cybersecurity risk management strategy is reviewed and adjusted to ensure coverage of organizational requirements and risks.		**GV.OV-P2:** The privacy risk management strategy is reviewed and adjusted to ensure coverage of organizational requirements and risks.
	GV.OV-03: Organizational cybersecurity risk management performance is measured and reviewed to confirm and adjust strategic direction.		**GV.OV-P3:** Organizational privacy risk management performance is measured and reviewed to confirm and adjust strategic direction.

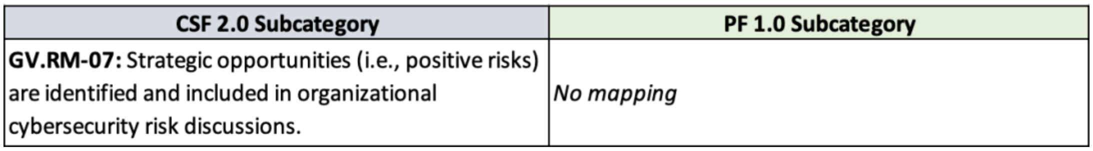
Table 2: Notional PF 1.1 Oversight Category and Subcategories with CSF 2.0 Mapping

Given the lack of a dedicated privacy risk management Category in PF 1.0, NIST is interested in whether this change is responsive to stakeholder needs and helps support use of the PF and CSF together. NIST is also interested in what effect, if any, this proposed change would have on the utility of the existing Monitoring and Review Category (GV.MT-P). Potential changes to GV.MT-P are discussed in Section 3.3 below.

2.2. Example 2: CSF 2.0 Subcategories that do not Map to PF 1.0 (GV.RM-07 and GV.RR-01)

CSF 2.0 also adds Subcategories which do not map to PF 1.0, but which may be replicated or adapted for the PF Core. Some new CSF 2.0 Subcategories are added to existing CSF Categories, such as GV.RM-07:

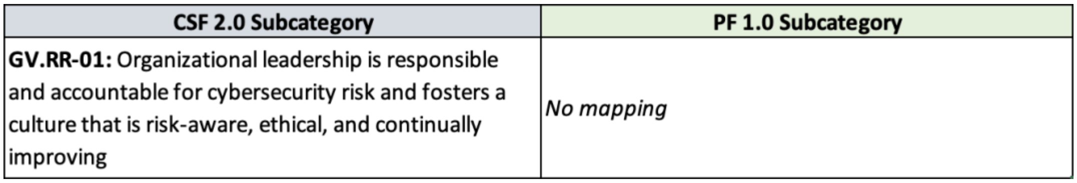
[1] We note that *GV.RM-P1: Risk management processes are established, managed, and agreed to by organizational stakeholders*, is concerned with overall risk management processes, not privacy risk management processes.



CSF 2.0 Subcategory	PF 1.0 Subcategory
GV.RM-07: Strategic opportunities (i.e., positive risks) are identified and included in organizational cybersecurity risk discussions.	*No mapping*

Table 3: CSF 2.0 Subcategory added to existing GV.RM Category

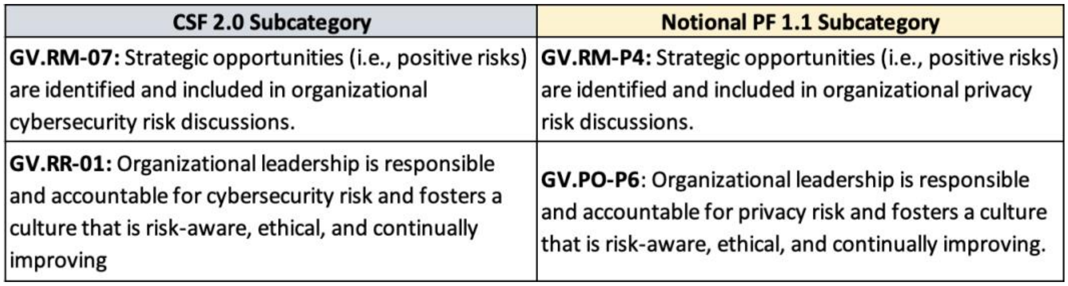
Other CSF 2.0 Subcategories are part of new CSF 2.0 Categories, such as GV.RR-01:[2]



CSF 2.0 Subcategory	PF 1.0 Subcategory
GV.RR-01: Organizational leadership is responsible and accountable for cybersecurity risk and fosters a culture that is risk-aware, ethical, and continually improving	*No mapping*

Table 4: CSF 2.0 Subcategory added to new GV.RR Category

As illustrated in Table 5 below, NIST Proposes creating new PF 1.1 Subcategories that map to the new CSF 2.0 Subcategories. In the case of CSF 2.0 Subcategories within new CSF 2.0 Categories (e.g., GV.RR-01), NIST proposes adding them to existing and analogous PF Categories:[3]



CSF 2.0 Subcategory	Notional PF 1.1 Subcategory
GV.RM-07: Strategic opportunities (i.e., positive risks) are identified and included in organizational cybersecurity risk discussions.	**GV.RM-P4:** Strategic opportunities (i.e., positive risks) are identified and included in organizational privacy risk discussions.
GV.RR-01: Organizational leadership is responsible and accountable for cybersecurity risk and fosters a culture that is risk-aware, ethical, and continually improving	**GV.PO-P6**: Organizational leadership is responsible and accountable for privacy risk and fosters a culture that is risk-aware, ethical, and continually improving.

Table 5: Notional PF 1.1 Subcategories mapped to CSF 2.0

NIST is interested in whether it is useful to create new replicated or adapted PF 1.1 Subcategories that map to new CSF 2.0 Categories. To the extent that the CSF 2.0 Subcategory is in a new CSF 2.0 Category, NIST is also interested in whether a similar new PF 1.1 Category is necessary, or whether the new PF 1.1 Subcategory should simply be added to an existing, analogous Category where feasible.

3. Topic 2: CSF 2.0 Revisions that Map to Analogous PF 1.0 Content

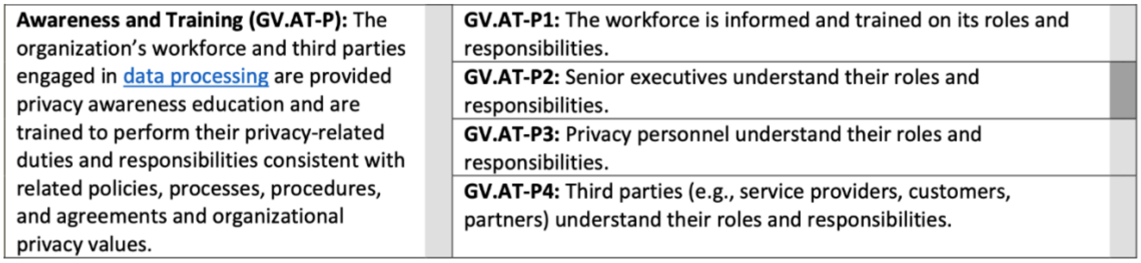
This section highlights a few examples of CSF 2.0 Categories/Subcategories that map to PF 1.0 but nonetheless create differences in content or structure. It also explores options for PF 1.1 updates to address these issues.

[2] GV.RR is the new CSF 2.0 Roles, Responsibilities, and Authorities Category.

[3] GV.PO-P is the existing Privacy Framework Governance Policies, Processes, and Procedures Category.

3.1. Example 1: The Awareness and Training Categories (PR.AT and GV.AT-P)

As illustrated by Table 6 below, the PF 1.0 Awareness and Training Category contains Subcategories that were mostly adapted from CSF 1.1.[4] Despite this similarity in content, PF stakeholders expressed a preference to include the PF 1.0 Awareness and Training Category in the Govern-P Function because privacy awareness and training programs cover more than data protection. This contrasts with the CSF 1.1 Awareness and Training Category, which is in the Protect Function.

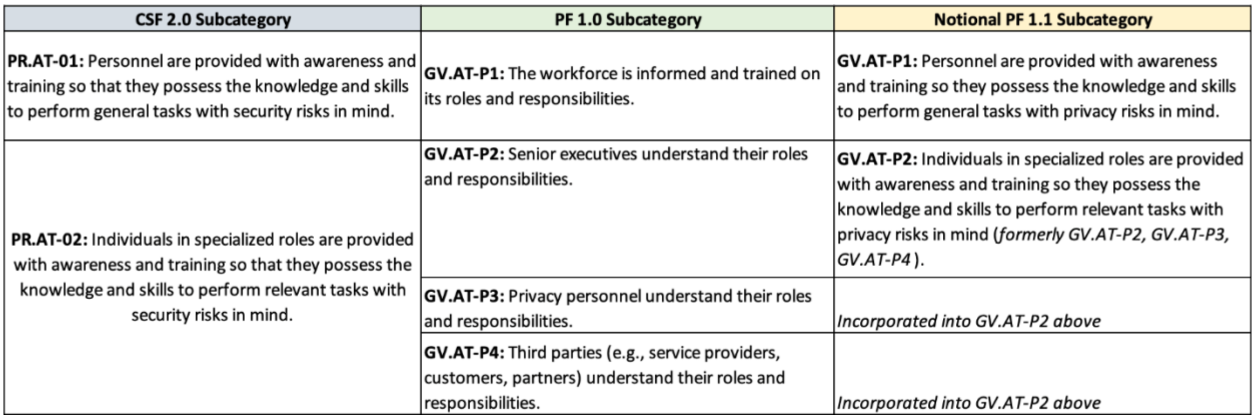


Awareness and Training (GV.AT-P): The organization's workforce and third parties engaged in data processing are provided privacy awareness education and are trained to perform their privacy-related duties and responsibilities consistent with related policies, processes, procedures, and agreements and organizational privacy values.	**GV.AT-P1:** The workforce is informed and trained on its roles and responsibilities.
	GV.AT-P2: Senior executives understand their roles and responsibilities.
	GV.AT-P3: Privacy personnel understand their roles and responsibilities.
	GV.AT-P4: Third parties (e.g., service providers, customers, partners) understand their roles and responsibilities.

Table 6: PF 1.0 Awareness and Training Category with CSF 1.1 alignment shaded gray

CSF 2.0 revises the language of PR.AT and keeps the Category in the Protect Function. As illustrated in the left and center columns below, the CSF 2.0 update creates language and location differences with PF 1.0. NIST is interested in the extent to which these differences create issues in using the frameworks together.

NIST proposes adopting the same approach as was taken for PF 1.0 which is to prioritize the needs of privacy programs when using the PF over one-to-one mappings (i.e., adapt CSF language and keep GV.AT-P in the Govern-P Function):



CSF 2.0 Subcategory	PF 1.0 Subcategory	Notional PF 1.1 Subcategory
PR.AT-01: Personnel are provided with awareness and training so that they possess the knowledge and skills to perform general tasks with security risks in mind.	**GV.AT-P1:** The workforce is informed and trained on its roles and responsibilities.	**GV.AT-P1:** Personnel are provided with awareness and training so they possess the knowledge and skills to perform general tasks with privacy risks in mind.
PR.AT-02: Individuals in specialized roles are provided with awareness and training so that they possess the knowledge and skills to perform relevant tasks with security risks in mind.	**GV.AT-P2:** Senior executives understand their roles and responsibilities.	**GV.AT-P2:** Individuals in specialized roles are provided with awareness and training so they possess the knowledge and skills to perform relevant tasks with privacy risks in mind (*formerly GV.AT-P2, GV.AT-P3, GV.AT-P4*).
	GV.AT-P3: Privacy personnel understand their roles and responsibilities.	*Incorporated into GV.AT-P2 above*
	GV.AT-P4: Third parties (e.g., service providers, customers, partners) understand their roles and responsibilities.	*Incorporated into GV.AT-P2 above*

Table 7: Notional PF 1.1 update of GV.AT-P

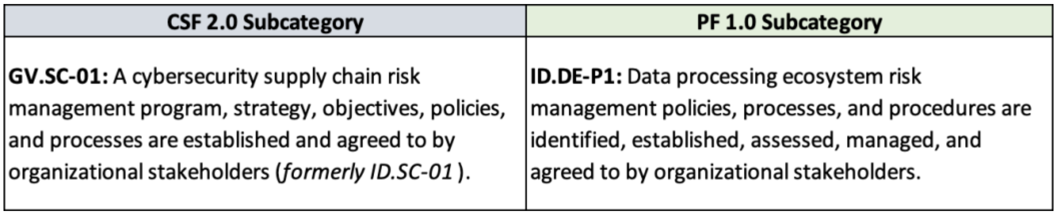
NIST is interested in knowing whether this notional approach strikes an appropriate balance between aligning more closely with CSF 2.0 language while adhering to privacy stakeholder needs.

[4] The dark gray shading indicates language that is identical between the two frameworks. The light gray shading indicated language that was adapted for the PF.

3.1.1 Example 2: The Cybersecurity Supply Chain Risk Management and Data Processing Ecosystem Risk Management Categories (GV.SC and ID.DE-P)

The PF 1.0 Data Processing Ecosystem Risk Management Category (ID.DE-P) was adapted from the CSF 1.1 Supply Chain Cybersecurity Risk Management Category (ID.SC). The CSF 1.1 Subcategory text used the term "identify," so for the PF 1.0, NIST opted to keep the Category in Identify-P instead of the new Govern-P. NIST coined the term "data processing ecosystem" because it resonated more than "supply chain" with privacy stakeholders.

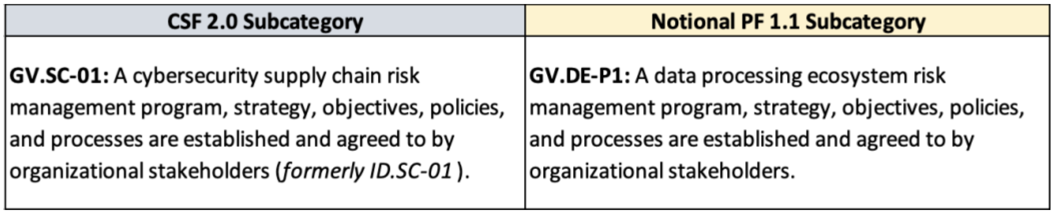
CSF 2.0 revises the Cybersecurity Supply Chain Risk Management Category (GV.SC) and relocates it to the new Govern Function. This creates both content and structural misalignment with PF 1.0:



CSF 2.0 Subcategory	PF 1.0 Subcategory
GV.SC-01: A cybersecurity supply chain risk management program, strategy, objectives, policies, and processes are established and agreed to by organizational stakeholders (*formerly ID.SC-01*).	**ID.DE-P1:** Data processing ecosystem risk management policies, processes, and procedures are identified, established, assessed, managed, and agreed to by organizational stakeholders.

Table 8: Mapping of new GV.SC Subcategory GV.SC-01 to ID.DE-P1

NIST proposes revising both language and location of ID.DE-P1 as follows:



CSF 2.0 Subcategory	Notional PF 1.1 Subcategory
GV.SC-01: A cybersecurity supply chain risk management program, strategy, objectives, policies, and processes are established and agreed to by organizational stakeholders (*formerly ID.SC-01*).	**GV.DE-P1:** A data processing ecosystem risk management program, strategy, objectives, policies, and processes are established and agreed to by organizational stakeholders.

Table 9: Notional PF 1.1 Update to create GV.DE-P1

NIST plans to continue using the term "data processing ecosystem." This proposal follows the rationale that PF 1.1 revisions should seek to maximize alignment with CSF 2.0 unless there are functional privacy reasons *not* to do so (see section 3.1 above for a functional privacy example). NIST is interested in whether this is a useful approach, noting that that in some cases, this will create artifacts in the PF 1.1 Core.

3.2. Example 3: The CSF 2.0 Technology Infrastructure Resilience Category (PR.IR)

Figure 5 below demonstrates how PF 1.0 and CSF 1.1 Functions could be used in varying combinations to manage different aspects of privacy and cybersecurity risks depending on the degree of collaboration between an organizations' cybersecurity and privacy programs:[5]

[5] *See* National Institute of Standards and Technology. (2020). *NIST Privacy Framework: A Tool for Improving Privacy Through Enterprise Risk Management, Version 1.0* (National Institute of Standards and Technology, Gaithersburg, MD) at 7. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.01162020.pdf.
When developing Version 1.0, NIST found that stakeholders were divided between those who wanted to replicate the overlap Functions in the Privacy Framework and those who did not. As a compromise, NIST opted to replicate Protect with a few privacy adaptions because of the importance of Protect outcomes and

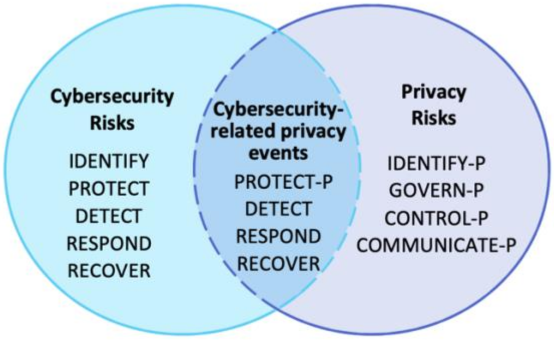
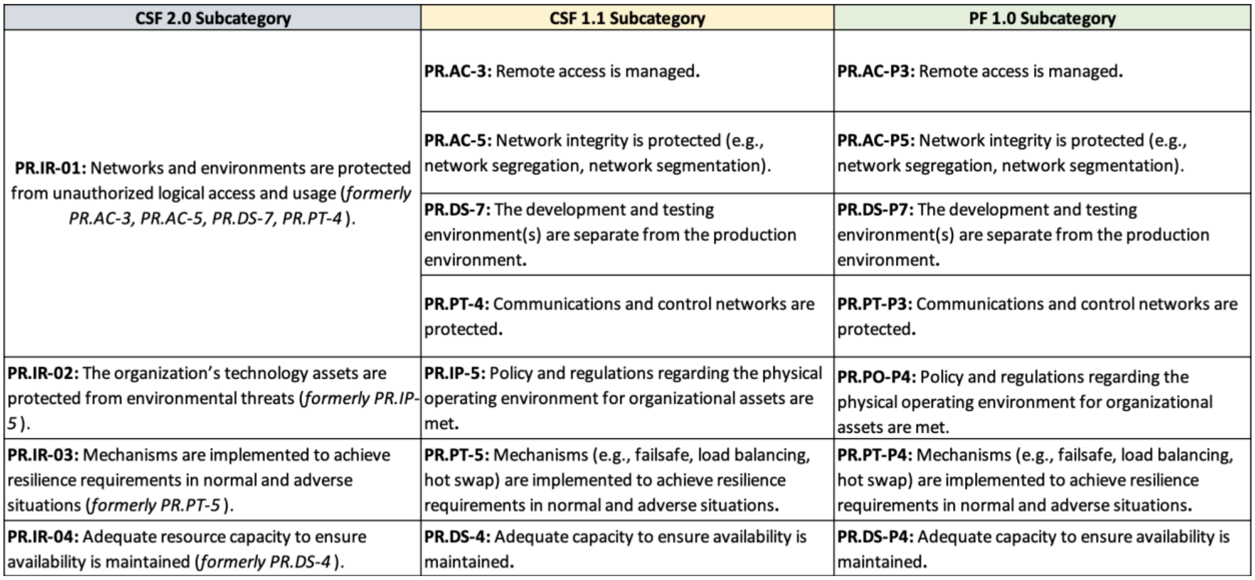


Figure 5: Using Functions to Manage Cybersecurity and Privacy Risks

CSF 2.0 makes numerous revisions which affect the Protect-P Function. For example, the Technology Infrastructure Resilience Category (PR.IR) is a new CSF 2.0 Category that contains CSF 1.1 Subcategories with varying degrees of revision. The relationship among these CSF 2.0 Subcategories and associated CSF 1.1 and PF 1.0 Subcategories is as follows:

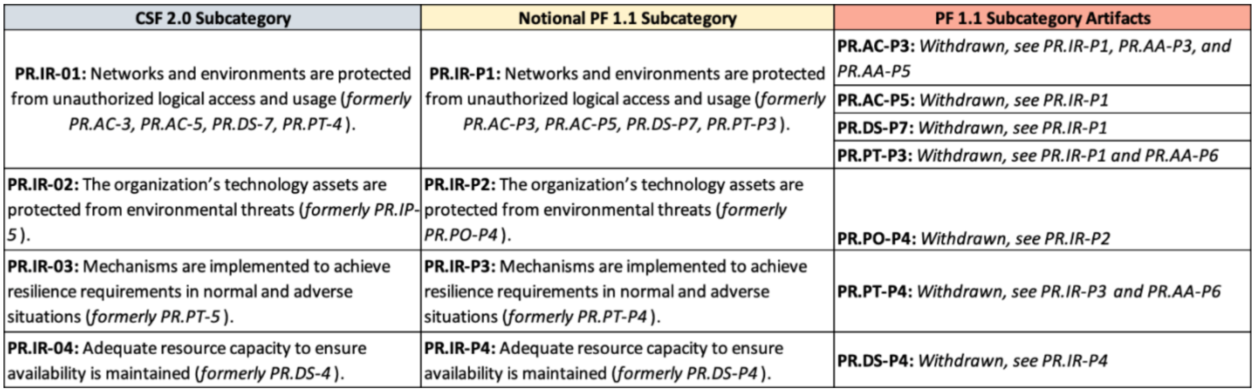


CSF 2.0 Subcategory	CSF 1.1 Subcategory	PF 1.0 Subcategory
PR.IR-01: Networks and environments are protected from unauthorized logical access and usage (*formerly PR.AC-3, PR.AC-5, PR.DS-7, PR.PT-4*).	**PR.AC-3:** Remote access is managed.	**PR.AC-P3:** Remote access is managed.
	PR.AC-5: Network integrity is protected (e.g., network segregation, network segmentation).	**PR.AC-P5:** Network integrity is protected (e.g., network segregation, network segmentation).
	PR.DS-7: The development and testing environment(s) are separate from the production environment.	**PR.DS-P7:** The development and testing environment(s) are separate from the production environment.
	PR.PT-4: Communications and control networks are protected.	**PR.PT-P3:** Communications and control networks are protected.
PR.IR-02: The organization's technology assets are protected from environmental threats (*formerly PR.IP-5*).	**PR.IP-5:** Policy and regulations regarding the physical operating environment for organizational assets are met.	**PR.PO-P4:** Policy and regulations regarding the physical operating environment for organizational assets are met.
PR.IR-03: Mechanisms are implemented to achieve resilience requirements in normal and adverse situations (*formerly PR.PT-5*).	**PR.PT-5:** Mechanisms (e.g., failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations.	**PR.PT-P4:** Mechanisms (e.g., failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations.
PR.IR-04: Adequate resource capacity to ensure availability is maintained (*formerly PR.DS-4*).	**PR.DS-4:** Adequate capacity to ensure availability is maintained.	**PR.DS-P4:** Adequate capacity to ensure availability is maintained.

Table 10: Relationship among Protect and Protect-P Subcategories associated with PR.IR in CSF 2.0

NIST proposes updating the PF 1.1 Protect-P Function in accordance with the PF 1.0 approach of replicating CSF Categories/Subcategories where practicable and adapting other Subcategories where a privacy focus is required or useful. Table 11 below illustrates how this approach applies in the context of the PR.IR Category:

activities in preventing data breaches, but otherwise allow flexibility in the ways that organizations might use the two frameworks together.



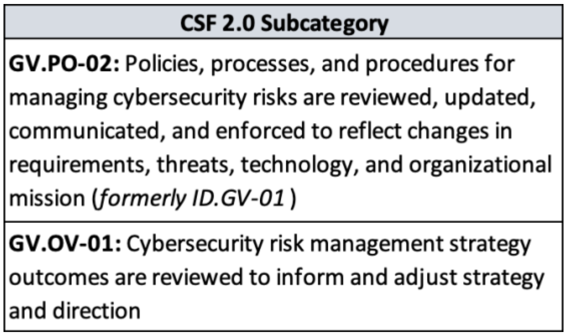
CSF 2.0 Subcategory	Notional PF 1.1 Subcategory	PF 1.1 Subcategory Artifacts
PR.IR-01: Networks and environments are protected from unauthorized logical access and usage (*formerly PR.AC-3, PR.AC-5, PR.DS-7, PR.PT-4*).	**PR.IR-P1:** Networks and environments are protected from unauthorized logical access and usage (*formerly PR.AC-P3, PR.AC-P5, PR.DS-P7, PR.PT-P3*).	**PR.AC-P3:** *Withdrawn, see PR.IR-P1, PR.AA-P3, and PR.AA-P5*
		PR.AC-P5: *Withdrawn, see PR.IR-P1*
		PR.DS-P7: *Withdrawn, see PR.IR-P1*
		PR.PT-P3: *Withdrawn, see PR.IR-P1 and PR.AA-P6*
PR.IR-02: The organization's technology assets are protected from environmental threats (*formerly PR.IP-5*).	**PR.IR-P2:** The organization's technology assets are protected from environmental threats (*formerly PR.PO-P4*).	**PR.PO-P4:** *Withdrawn, see PR.IR-P2*
PR.IR-03: Mechanisms are implemented to achieve resilience requirements in normal and adverse situations (*formerly PR.PT-5*).	**PR.IR-P3:** Mechanisms are implemented to achieve resilience requirements in normal and adverse situations (*formerly PR.PT-P4*).	**PR.PT-P4:** *Withdrawn, see PR.IR-P3 and PR.AA-P6*
PR.IR-04: Adequate resource capacity to ensure availability is maintained (*formerly PR.DS-4*).	**PR.IR-P4:** Adequate resource capacity to ensure availability is maintained (*formerly PR.DS-P4*).	**PR.DS-P4:** *Withdrawn, see PR.IR-P4*

Table 11: Notional PF 1.1 PR.IR-P Category with artifacts

Note this approach requires creating an entirely new PF 1.1 Category (PR.IR-P) and generates seven artifacts in the PF 1.1 Core.[6] NIST is interested in whether this approach facilitates continued flexibility and effective use of the PF and CSF together to manage the full spectrum of privacy and cybersecurity risks. NIST is also interested in whether the original reasons for creating the Protect-P Function (see fn. 5) still exist. For example, making major changes to language and structure as well as creating numerous artifacts could be avoided by simply removing the Protect-P Function from PF 1.1. In this scenario, organizations could use the CSF 2.0 Protect (along with Detect, Respond, and Recover) to manage risks associated with cybersecurity-related privacy events.

3.3. Example 4: The Monitoring and Review Category (GV.MT-P)

Unlike PF 1.0, CSF 2.0 lacks a dedicated Monitoring and Review Category. Analogous Subcategories are found instead within the same Categories as the original activity. For example, from the CSF 2.0 Oversight and Policies, Processes, and Procedures Categories respectively:



CSF 2.0 Subcategory
GV.PO-02: Policies, processes, and procedures for managing cybersecurity risks are reviewed, updated, communicated, and enforced to reflect changes in requirements, threats, technology, and organizational mission (*formerly ID.GV-01*)
GV.OV-01: Cybersecurity risk management strategy outcomes are reviewed to inform and adjust strategy and direction

Table 12: Example CSF 2.0 Subcategories that address review activities

NIST is interested in whether mapping between analogous PF and CSF Categories/Subcategories is sufficient to support joint frameworks use. Relocating GV.MT-P activities to the Categories where the original activities take place would improve structural alignment with CSF 2.0 but would also create artifacts within the PF 1.1 Core.

[6] Note as well that more than one PF 1.1 Protect-P Category would be impacted following this approach as the artifacts indicate (i.e., revision of the Identity Management, Authentication, and Access Control Category (PR.AA-P), formerly PR.AC-P).

Alternatively, if GV.MT-P were kept, it could be expanded as needed based on the creation of new PF 1.1 Subcategories to align with CSF 2.0. NIST is also interested in whether the creation of a new Oversight Category (i.e., GV.OV-P), would influence the need for GV.MT-P.

4. Topic 3: Other Potential Updates

In addition to the alignment changes discussed in this paper, NIST is interested in other potential PF 1.1 updates to increase usability and address current privacy risk management needs. Revisions of Core outcomes may be needed to better reflect current privacy risk management practices, even in cases where CSF 2.0 alignment is not implicated. For example, the use and understanding of Artificial Intelligence (AI) technology has evolved since the PF 1.0 release in 2020. AI-related PF Subcategories (e.g., ID.RA-P2)[7] could be revised to better reflect the current state of AI or removed given the subsequent publication of the NIST AI Risk Management Framework.[8]

NIST is also interested in stylistic improvements to Core outcomes that could improve readability, usability, or accessibility.

[7] ID.RA-P2: Data analytic inputs and outputs are identified and evaluated for bias.

[8] *See* National Institute of Standards and Technology. (2023). *Artificial Intelligence Risk Management Framework (AI RMF 1.0)* (National Institute of Standards and Technology, Gaithersburg, MD). https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf