Proposed Integrated Core

Proposed Version of the NIST Privacy Framework Core with Data Security Integrated

Note to Reviewers

The Proposed Integrated Core is provided for discussion purposes to promote the development of the NIST Privacy Framework: An Enterprise Risk Management Tool (Privacy Framework). In response to stakeholder feedback received on the Privacy Framework Discussion Draft (Discussion Draft), released April 30, 2019, NIST has prepared two different, updated versions of the Core for feedback.

The two proposed Cores offer different levels of alignment with the Framework for Improving Critical Infrastructure Cybersecurity (Cybersecurity Framework). For this Integrated Core, NIST has maintained a number of data security Functions, Categories, and Subcategories that overlap with the Cybersecurity Framework. In contrast, for the Separated Core, NIST has removed the overlapping Cybersecurity Framework Functions, Categories, Subcategories that pertain to data security. Organizations that want to manage the data security aspect of privacy risk should use the Cybersecurity Framework Core.

In addition, each Core contains the same updates based on specific feedback on the Discussion Draft Core. See below for a summary of material changes.

NIST is particularly interested in feedback on: (i) which proposed Core is preferred by stakeholders, (ii) why that proposed Core is preferred; and (iii) any additional changes to either of the proposed Cores to support organizations' needs with respect to managing privacy risk.

Please send feedback on the proposed Core versions to privacyframework@nist.gov. NIST will use feedback on this document to inform the development of a preliminary draft of the Privacy Framework.

Summary of Material Changes from the Discussion Draft Core

The Integrated Core retains all of the Functions presented in the Discussion Draft with some modifications: creation of a new Function, *Govern,* that splits off some Categories from *Identify*, and renaming *Inform* to *Communicate*. **Figure 1** was added to show the general categorical relationships between the Functions. Detect and Recover from the Cybersecurity Framework are greyed out in this figure as they are not part of the Privacy Framework, but organizations can find these Functions in the Cybersecurity Framework, and use them to further support the management of the data security aspect of privacy risk. Throughout the Core's Categories and Subcategories, NIST added several examples in the form of parentheticals to make the outcome statements more readily understood by organizations. The table below provides a summary of material changes only. Clarifying or editorial edits to the text are not included.

Function	Material Changes
Identify (ID-P)	*Inventory and Mapping* (ID.IM-P) • Added two Subcategories: ID.IM-P3 and ID.IM-P5 (previously ID.RA-P1)

Function	Material Changes
	Business Environment (ID.BE-P) • Changed use of the term "supply chain risk management" to "data processing ecosystem" in ID.BE-P1; "data processing ecosystem" is now a defined term in the updated Glossary
	Risk Assessment (ID.RA-P) • Relocated and modified ID.RA-P2 (previously IN.AW-P7) from Inform • Relocated ID.RA-P1 to Inventory and Mapping (ID.IM-P) (see above)
	Data Processing Ecosystem Risk Management (ID.DE-P) • Changed use of the term "supply chain" to "data processing ecosystem" throughout the Core and changed identifiers from SC to DE; "data processing ecosystem" is now a defined term in the updated Glossary • Added new Subcategory ID.DE-P4 • Removed previous ID.SC-P5 because it is sufficiently addressed by ID.DE-P5
Govern (GV-P) **[New Function]**	*Governance Policies, Processes, and Procedures* (GV.PP-P) • Relocated this Category from Identify (previously Governance [ID.GV-P])
	Risk Management Strategy (GV.RM-P) • Relocated this Category from Identify (previously ID.RM-P)
	Awareness and Training (GV.AT-P) • Relocated this Category from Protect (previously PR.AT-P)
	Monitoring (GV.MT-P) **[New Category]** • Created new Category statement • Created four Subcategories: GV.MT-P1 (previously ID.RA-P6) was relocated from Identify and three new Subcategories: GV.MT-P2 through P4

Protect (PR-P)	• Retained five of seven previous Categories: Identity Management, Authentication and Access Control (PR.AC-P), Data Security (PR.DS-P), Data Protection Processes and Procedures (PR.DP-P), Maintenance (PR.MA-P), and Protective Technology (PR.PT-P) with minor modifications
	• Relocated:
	  ○ Awareness and Training Category (previously PR.AT-P) to Govern (GV.AT-P) (see above)
	  ○ Protected Processing Category (previously PR.PP-P) to Control (renamed Data Minimization [CT.MN-P]) (see below)
	  ○ previous PR.AC-P7 to Data Minimization Category (now CT.MN-P7) (see below)
	• Modified PR.DP.P1 to conform to corresponding Cybersecurity Framework Subcategory

Control (CT-P)	*Data Management Policies, Processes, and Procedures* (CT.PO-P) • Modified CT.PO-P1 to address individual consent and revocation and incorporate previous CT.DM-P2 • Relocated and modified CT.PO-P4 (previously PR.DP-P2) from Protect

Function	Material Changes
	Data Minimization (CT.MN-P) **[New Category]** • Renamed Category (previously Protected Processing [PR.PP-P]) • Created seven Subcategories: CT.MN-P1 through P5 (previously PR.PP-P1 through P5) were relocated from Protected Processing in Protect; CT.MN-P6 (previously CT.DM-P1) was relocated from Data Management in Control; and CT.MN-P7 (previously PR.AC-P7) was relocated from Identity Management, Authentication, and Access Control in Protect.
Communicate (CM-P) **[Previously Inform (IN-P)]**	*Communication Policies, Processes, and Procedures* (CM.PP-P) • Renamed Category and maintained two Subcategories from previous Category (Transparency Processes and Procedures [IN.TP-P]) • Modified CM.PP-P1 to incorporates policies, processes and procedures for communicating (previously addressed by two Subcategories, IN.TP-P1 and P2) • Added new Subcategory CM.PP-P2 to address communication roles and responsibilities
	Data Processing Awareness (CM.AW-P) • Modified CM.AW-P1 (previously IN.AW-P2) to focus on mechanisms for communicating and included examples of such mechanisms • Modified CM.AW-P4 (previously IN.AW-P1) to include records of data disclosures can be accessed for review or transmission/disclosure • Modified CM.AW-P5 and combined two Subcategories (previous IN.AW-P4 and P5) to include communication of data corrections or deletions to both individuals and organizations (e.g., data sources) • Modified CM.AW-P6 to add data lineage and capability for access for review or transmission/disclosure
Respond (RS-P)	• Retained all previous Respond Function Categories, with only minor changes to Subcategory RS.RE-P2 to provide additional specificity on mitigation mechanisms "to address impacts to individuals that arise from data processing."

Appendix A: Privacy Framework Core

This appendix presents the Core: a table of Functions, Categories, and Subcategories that describe specific privacy activities that can support managing privacy risks when systems, products, and services are processing data.

Notes to Users

Under the Privacy Framework's risk-based approach:

1. An organization may not need to achieve every outcome or activity reflected in the Core. It is expected that an organization will use Profiles to select and prioritize the Functions, Categories, and Subcategories that best meet its specific needs by considering its organizational or industry sector goals, legal/regulatory requirements and industry best practices, the organization's risk management priorities, and the privacy needs of individuals who are directly or indirectly served or affected by the organization's systems, products, or services. **Thus, the Subcategories should not be read as a checklist in isolation from their Categories, which often provide a risk-based modifier on Subcategory selection.**

2. It is not obligatory to achieve an outcome in its entirety. An organization may use its Profiles to express partial achievement of an outcome, as not all aspects of an outcome may be relevant for the organization to manage privacy risk, or the organization may use a Target Profile to express an aspect of an outcome that it doesn't currently have the capability to achieve.

3. It may be necessary to consider multiple outcomes in combination to appropriately manage privacy risk. For example, an organization that responds to individuals' requests for data access may select for its Profile both the Subcategory: *CT.DM-P1: Data elements can be accessed for review* and the Category: *Identity Management, Authentication, and Access Control (PR.AC-P)* to ensure that only the individual to whom the data pertain gets access.

Implementation: The table format of the Core is not intended to suggest a specific implementation order or imply a degree of importance between the Functions, Categories, and Subcategories. Implementation may be non-sequential, simultaneous, or iterative, depending on the SDLC stage, status of the privacy program, or scale of the workforce. In addition, the Core is not exhaustive; it is extensible, allowing organizations, sectors, and other entities to adapt or add additional Functions, Categories, and Subcategories to their Profiles.

Roles:

- Workforce: Different parts of an organization's workforce may take responsibility for different Categories or Subcategories. For example, the legal department may be responsible for carrying out activities under Governance Processes and Procedures while the IT department is working on Inventory and Mapping. Ideally, the Core encourages cross-organization collaboration to develop Profiles and achieve outcomes.

- Ecosystem: The Core is intended to be usable by any organization or entity regardless of its role in the data processing ecosystem. Although the Privacy Framework does not classify ecosystem roles, an organization should review the Core from its standpoint in the ecosystem. An organization's role(s) may be legally codified – for example, some laws classify organizations as data controllers or data processors – or classifications may be derived from industry designations. Since Core elements are not assigned by ecosystem role, an organization can use its Profiles to select Functions, Categories, and Subcategories that are relevant to its role(s).

Scalability: Certain aspects of outcomes may be ambiguously worded. For example, outcomes may include terms like "communicated" or "disclosed" without stating to whom the communications or disclosures are being made. The ambiguity is intentional to allow for a wide range of organizations with different use cases to determine what is appropriate or required in a given context.

Resource Repository: Additional supporting resources, including informative references that can provide more guidance on how to achieve an outcome can be found on the NIST website at https://www.nist.gov/privacy-framework.

Cybersecurity Framework Alignment:

- **Figure 1** shows the general categorical relationships between the Functions: Identify and Govern are primarily organizational-level or contain foundational outcomes and activities, Control, Communicate, and Protect are primarily system/product/service-level and contain outcomes and activities that may not be applicable for all systems, products, and services or to the same degree, and Detect, Respond, and Recover are primarily incident-related. The Functions Detect and Recover are greyed out in **Figure 1** and **Table 1** as they are not part of the Privacy Framework, but organizations can find these Functions in the Cybersecurity Framework, and use them to further support the management of the data security aspect of privacy risk.

- Certain Functions, Categories, or Subcategories are identical to or have been adapted from the Cybersecurity Framework. The following legend can be used to identify this relationship in Table 2.

  The Function, Category, or Subcategory aligns with the Cybersecurity Framework, but the text has been adapted for the Privacy Framework.

  The Category or Subcategory is identical to the Cybersecurity Framework.

Core Identifiers: For ease of use, each component of the Core is given a unique identifier. Functions and Categories each have a unique alphabetic identifier, as shown in **Table 1**. Subcategories within each Category have a number added to the alphabetic identifier; the unique identifier for each Subcategory is included in **Table 2**.

Figure 1: Privacy and Cybersecurity Framework Functions

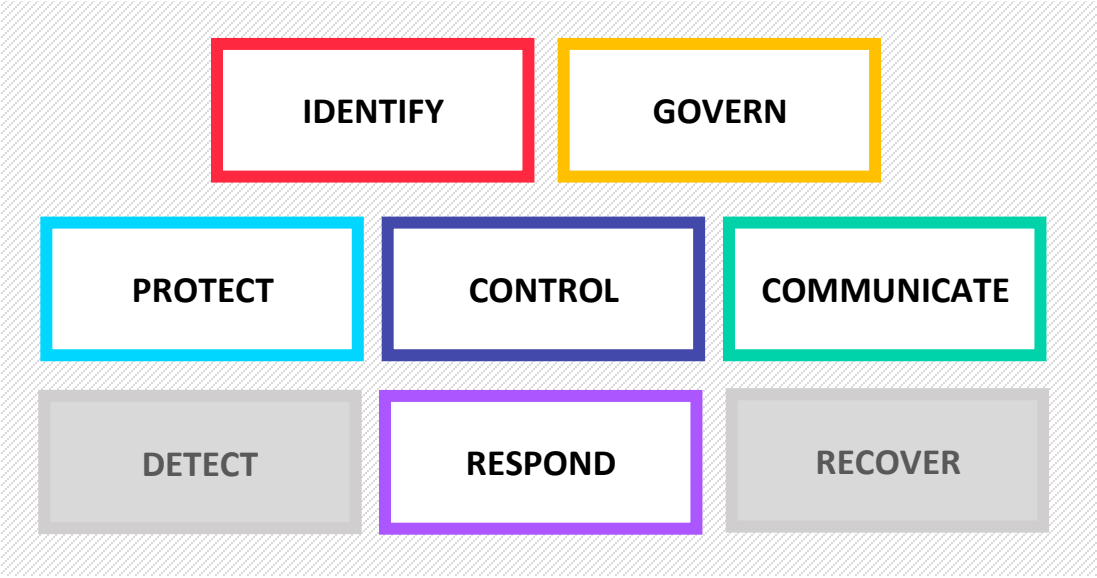

Table 1: Privacy and Cybersecurity Framework Function and Category Unique Identifiers

	Function Unique Identifier	Function	Category Unique Identifier	Category
	ID-P	Identify-P	ID.IM-P	Inventory and Mapping
			ID.BE-P	Business Environment
			ID.RA-P	Risk Assessment
			ID.DE-P	Data Processing Ecosystem Risk Management
	GV-P	Govern-P	GV.PP-P	Governance Policies, Processes, and Procedures
			GV.RM-P	Risk Management Strategy
			GV.AT-P	Awareness and Training

			GV.MT-P	Monitoring
	PR-P	Protect-P	PR.AC-P	Identity Management, Authentication, and Access Control
			PR.DS-P	Data Security
			PR.DP-P	Data Protection Processes and Procedures
			PR.MA-P	Maintenance
			PR.PT-P	Protective Technology
	CT-P	Control-P	CT.PO-P	Data Management Policies, Processes, and Procedures
			CT.DM-P	Data Management
			CT.MN-P	Data Minimization
	CM-P	Communicate-P	CM.PP-P	Communication Policies, Processes, and Procedures
			CM.AW-P	Data Processing Awareness
	RS-P	Respond-P	RS.RP-P	Response Planning
			RS.CO-P	Communications
			RS.AN-P	Analysis
			RS.MI-P	Mitigation
			RS.IM-P	Improvements
			RS.RE-P	Redress
	DE	Detect	DE.AE	Anomalies and Events
			DE.CM	Security Continuous Monitoring
			DE.DP	Detection Processes
	RC	Recover	RC.RP	Recovery Planning
			RC.IM	Improvements
			RC.CO	Communications

Table 2: Privacy Framework Core

Function	Category	Subcategory
IDENTIFY-P (ID-P): Develop the organizational understanding to manage privacy risk for individuals arising from system, product, or service data processing.	**Inventory and Mapping (ID.IM-P):** Data processing by systems, products, or services are understood and inform the management of privacy risk.	**ID.IM-P1:** Systems/products/services that process data are inventoried.
		ID.IM-P2: Owners or operators (e.g., the organization or third parties such as service providers, partners, customers, developers, etc.) and their roles with respect to the systems/products/services and components (e.g., internal or external) that process data are inventoried.
		ID.IM-P3: Categories of individuals (e.g., customers, employees or prospective employees, consumers, second tier customers) whose data are being processed are inventoried.
		ID.IM-P4: Data actions of the systems/products/services are inventoried.
		ID.IM-P5: The purposes for the data actions are inventoried.
		ID.IM-P6: Data elements within the data actions are inventoried.
		ID.IM-P7: The data processing environment is understood (e.g., geographic location, internal, cloud, third parties).
		ID.IM-P8: Data processing is mapped, illustrating the data actions and associated data elements by systems/products/services, including components (e.g., internal or external); roles of the component owners/operators; and interactions of individuals or third parties with the systems/products/services.
	Business Environment (ID.BE-P): The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform privacy roles, responsibilities, and risk management decisions.	**ID.BE-P1:** The organization's role in the data processing ecosystem is identified and communicated.
		ID.BE-P2: Priorities for organizational mission, objectives, and activities are established and communicated.
		ID.BE-P3: Systems/products/services that support organizational priorities are identified and key functional requirements communicated.
	Risk Assessment (ID.RA-P): The organization understands the privacy risks to individuals and how such privacy risks may create secondary impacts on	**ID.RA-P1:** Contextual factors related to the systems/products/services and the data actions are identified (e.g., individuals' demographics and privacy interests or perceptions, data sensitivity, visibility of data processing to individuals and third parties).

	Function	Category	Subcategory
		organizational operations (including mission, functions, reputation, other risk management priorities (e.g. compliance, financial), workforce, and culture).	**ID.RA-P2:** Data analytic inputs and outputs are identified and evaluated for bias.
			ID.RA-P3: Potential problematic data actions and associated problems are identified.
			ID.RA-P4: Problematic data actions, likelihoods, and impacts are used to determine and prioritize risk.
			ID.RA-P5: Risk responses are identified, prioritized, and implemented.
		Data Processing Ecosystem Risk Management (ID.DE-P): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing privacy risk and third parties within the data processing ecosystem. The organization has established and implemented the processes to identify, assess, and manage privacy risks within the data processing ecosystem.	**ID.DE-P1:** Data processing ecosystem risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders.
			ID.DE-P2: Data processing ecosystem parties (e.g., service providers, customers, partners, product manufacturers, application developers) are identified, prioritized, and assessed using a privacy risk assessment process.
			ID.DE-P3: Contracts with data processing ecosystem parties are used to implement appropriate measures designed to meet the objectives of an organization's privacy program.
			ID.DE-P4: Interoperability frameworks or similar multi-party approaches are used to manage data processing ecosystem privacy risks.
			ID.DE-P5: Data processing ecosystem parties are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual or framework obligations.
	GOVERN-P (GV-P): Develop and implement the organizational governance structure to enable an	**Governance Policies, Processes, and Procedures (GV.PP-P):** The policies, processes, and procedures to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of privacy risk.	**GV.PP-P1:** Organizational privacy values and policies (e.g., conditions on data processing, individuals' prerogatives with respect to data processing) are established and communicated.
			GV.PP-P2: Processes to instill organizational privacy values within system/product/service development and operations are established and in place.
			GV.PP-P3: Roles and responsibilities for the workforce are established with respect to privacy.

	Function	Category	Subcategory
	ongoing understanding of the organization's risk management priorities that are informed by privacy risk.		**GV.PP-P4:** Privacy roles and responsibilities are coordinated and aligned with third-party stakeholders (e.g., service providers, customers, partners).
			GV.PP-P5: Legal, regulatory, and contractual requirements regarding privacy are understood and managed.
			GV.PP-P6: Governance and risk management policies, processes, and procedures address privacy risks.
		Risk Management Strategy (GV.RM-P): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	**GV.RM-P1:** Risk management processes are established, managed, and agreed to by organizational stakeholders.
			GV.RM-P2: Organizational risk tolerance is determined and clearly expressed.
			GV.RM-P3: The organization's determination of risk tolerance is informed by its role in the data processing ecosystem.
		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.
		Monitoring (GV.MT-P): The policies, processes, and procedures for ongoing review of the organization's privacy posture are understood and inform the management of privacy risk.	**GV.MT-P1:** Privacy risk is re-evaluated on an ongoing basis and as key factors, including the organization's business environment, governance (e.g., legal obligations, risk tolerance), data processing, and systems/products/services change.
			GV.MT-P2: Privacy values and policies are reviewed and any updates are communicated.
			GV.MT-P3: Policies, processes, and procedures for auditing compliance with legal requirements and privacy policies are established and in place.

	Function	Category	Subcategory
			GV.MT-P4: Policies, processes, and procedures for communicating progress on managing privacy risks are established and in place.
	PROTECT-P (PR-P): Develop and implement appropriate data processing safeguards.	**Identity Management, Authentication, and Access Control (PR.AC-P):** Access to data and devices is limited to authorized individuals, processes, and devices, and is managed consistent with the assessed risk of unauthorized access.	**PR.AC-P1:** Identities and credentials are issued, managed, verified, revoked, and audited for authorized individuals, processes, and devices.
			PR.AC-P2: Physical access to data and devices is managed.
			PR.AC-P3: Remote access is managed.
			PR.AC-P4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties.
			PR.AC-P5: Network integrity is protected (e.g., network segregation, network segmentation).
			PR.AC-P6: Individuals and devices are proofed and bound to credentials, and authenticated commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks).
		Data Security (PR.DS-P): Data are managed consistent with the organization's risk strategy to protect individuals' privacy and maintain data confidentiality, integrity, and availability.	**PR.DS-P1:** Data-at-rest are protected.
			PR.DS-P2: Data-in-transit are protected.
			PR.DS-P3: Systems/products/services and associated data are formally managed throughout removal, transfers, and disposition.
			PR.DS-P4: Adequate capacity to ensure availability is maintained.
			PR.DS-P5: Protections against data leaks are implemented.
			PR.DS-P6: Integrity checking mechanisms are used to verify software, firmware, and information integrity.
			PR.DS-P7: The development and testing environment(s) are separate from the production environment.
			PR.DS-P8: Integrity checking mechanisms are used to verify hardware integrity.
		Data Protection Processes and Procedures (PR.DP-P): Security and privacy policies (that address purpose,	**PR.DP-P1:** A baseline configuration of information technology is created and maintained incorporating security principles (e.g. concept of least functionality).

	Function	Category	Subcategory
		scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage the protection of data.	**PR.DP-P2:** A system development life cycle to manage systems and an information life cycle to manage data are aligned and implemented.
			PR.DP-P3: Configuration change control processes are established and in place.
			PR.DP-P4: Backups of information are conducted, maintained, and tested.
			PR.DP-P5: Policy and regulations regarding the physical operating environment for organizational assets are met.
			PR.DP-P6: Data are destroyed according to policy.
			PR.DP-P7: Protection processes are improved.
			PR.DP-P8: Effectiveness of protection technologies is shared.
			PR.DP-P9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are established, in place, and managed.
			PR.DP-P10: Response and recovery plans are tested.
			PR.DP-P11: Privacy procedures are included in human resources practices (e.g., deprovisioning, personnel screening).
			PR.DP-P12: A vulnerability management plan is developed and implemented.
		Maintenance (PR.MA-P): System maintenance and repairs are performed consistent with policies, processes, and procedures.	**PR.MA-P1:** Maintenance and repair of organizational assets are performed and logged, with approved and controlled tools.
			PR.MA-P2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access.
		Protective Technology (PR.PT-P): Technical security solutions are managed to ensure the security and resilience of systems/products/services and associated data, consistent with related policies, processes, procedures, and agreements.	**PR.PT-P1:** Audit/log records are determined, documented, implemented, and reviewed in accordance with policy and incorporating the principle of data minimization.
			PR.PT-P2: Removable media is protected and its use restricted according to policy.
			PR.PT-P3: The principle of least functionality is incorporated by configuring systems to provide only essential capabilities.

	Function	Category	Subcategory
			PR.PT-P4: Communications and control networks are protected.
			PR.PT-P5: Mechanisms (e.g., failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations.
	CONTROL-P (CT-P): Develop and implement appropriate activities to enable organizations or individuals to manage data with sufficient granularity to manage privacy risks.	**Data Management Policies, Processes, and Procedures (CT.PO-P):** Policies, processes, and procedures are maintained and used to manage data processing (e.g., purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities) consistent with the organization's risk strategy to protect individuals' privacy.	**CT.PO-P1:** Policies, processes, and procedures for authorizing data processing (e.g., organizational decisions, individual consent), revoking authorizations, and maintaining authorizations are established and in place.
			CT.PO-P2: Policies, processes, and procedures for enabling data review, transmission or disclosure, alteration, and deletion are established and in place.
			CT.PO-P3: Policies, processes, and procedures for enabling individuals' data processing preferences and requests are established and in place.
		Data Management (CT.DM-P): Data are managed consistent with the organization's risk strategy to protect individuals' privacy and increase manageability and enable the implementation of privacy principles (e.g., individual participation, data quality, data minimization).	**CT.DM-P1:** Data elements can be accessed for review.
			CT.DM-P2: Data elements can be accessed for transmission or disclosure.
			CT.DM-P3: Data elements can be accessed for alteration.
			CT.DM-P4: Data elements can be accessed for deletion.
			CT.DM-P5: Data are transmitted using standardized formats.
			CT.DM-P6: Metadata containing processing permissions and related data values are transmitted with data elements.
		Data Minimization (CT.MN-P): Technical data processing solutions increase disassociability consistent with related policies, processes, procedures, and agreements and the organization's risk strategy to protect individuals' privacy.	**CT.MN-P1:** Data are processed in an unobservable or unlinkable manner.
			CT.MN-P2: Data are processed to limit the identification of individuals.
			CT.MN-P3: Data are processed to restrict the formulation of inferences about individuals' behavior or activities.
			CT.MN-P4: Data processing is decentralized.
			CT.MN-P5: Data actions take place on local devices.
			CT.MN-P6: System or device configurations permit selective collection or disclosure of data elements.
			CT.MN-P7: Attribute references are substituted for attribute values.

	Function	Category	Subcategory
	COMMUNICATE-P (CM-P): Develop and implement appropriate activities to enable organizations and individuals to have a reliable understanding about how data are processed and associated privacy risks.	**Communication Policies, Processes, and Procedures (CM.PP-P):** Policies, processes, and procedures are maintained and used to increase transparency of the organization's data processing practices (e.g., purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities) and associated privacy risks.	**CM.PP-P1:** Transparency policies, processes, and procedures for communicating data processing purposes, practices, and associated privacy risks are established and in place.
			CM.PP-P2: Roles and responsibilities (e.g., public relations) for communicating data processing purposes, practices, and associated privacy risks are established.
		Data Processing Awareness (CM.AW-P): Individuals and organizations have reliable knowledge about data processing practices and associated privacy risks, and processes and procedures are used and maintained to increase predictability consistent with the organization's risk strategy to protect individuals' privacy.	**CM.AW-P1:** Mechanisms (e.g., notices, internal or public reports) for communicating data processing purposes, practices, associated privacy risks, and options for enabling individuals' data processing preferences and requests are established and in place.
			CM.AW-P2: Mechanisms for obtaining feedback from individuals (e.g., surveys or focus groups) about data processing and associated privacy risks are established and in place.
			CM.AW-P3: System/product/service design enables data processing visibility.
			CM.AW-P4: Records of data disclosures are maintained and can be accessed for review or transmission/disclosure.
			CM.AW-P5: Data corrections or deletions can be communicated to individuals or organizations (e.g., data sources).
			CM.AW-P6: Data lineage and provenance are maintained and can be accessed for review or transmission/disclosure.
	RESPOND-P (RS-P): Develop and implement appropriate activities to take timely action regarding a	**Response Planning (RS.RP-P):** Response processes and procedures are executed and maintained to ensure response to privacy breaches and events.	**RS.RP-P1:** Response plan is executed during or after a privacy breach or event.
		Communications (RS.CO-P): Response activities are coordinated with internal and external stakeholders (e.g., external support from law enforcement agencies).	**RS.CO-P1:** Personnel know their roles and order of operations when a response is needed.
			RS.CO-P2: Privacy breaches and events are reported consistent with established criteria.
			RS.CO-P3: Information is shared consistent with response plans.

	Function	Category	Subcategory
	privacy breach or event.		**RS.CO-P4:** Coordination with stakeholders occurs consistent with response plans.
			RS.CO-P5: Data for voluntary information sharing are restricted to what is necessary for understanding the privacy breach or event.
			RS.CO-P6: Impacted individuals and organizations are notified about a privacy breach or event.
		Analysis (RS.AN-P): Analysis is conducted to ensure effective response to privacy breaches and events.	**RS.AN-P1:** Notifications from detection systems or processes are investigated.
			RS.AN-P2: The impact of the privacy breach or event on individuals, the organization, and the ecosystem is understood.
			RS.AN-P3: Forensics are performed.
			RS.AN-P4: Privacy breaches and events are categorized consistent with response plans.
			RS.AN-P5: Processes are established and in place to receive, analyze, and respond to problematic data actions disclosed to the organization from internal and external sources (e.g., internal testing, privacy researchers).
		Mitigation (RS.MI-P): Activities are performed to prevent expansion of, mitigate, and resolve privacy breaches and events.	**RS.MI-P1:** Privacy breaches and events are contained.
			RS.MI-P2: Privacy breaches and events are mitigated.
			RS.MI-P3: Newly identified problematic data actions are mitigated or documented as accepted risks.
		Improvements (RS.IM-P): Organizational privacy practices are improved by incorporating lessons learned from privacy breaches and events.	**RS.IM-P1:** Policies, processes, and procedures incorporate lessons learned.
		Redress (RS.RE-P): Organizational response activities include processes or mechanisms to address impacts to individuals that arise from data processing.	**RS.RE-P1:** Processes for receiving, tracking, and responding to complaints, concerns, and questions from individuals about organizational privacy practices are established and in place.
			RS.RE-P2: Individuals are provided with mitigation mechanisms to address impacts to individuals that arise from data processing.