NIST Informative References for NIST Privacy Framework: An Enterprise Risk Management Tool Discussion Draft

Note to Reviewers

NIST welcomes feedback on the appropriateness of the listed guidance, as well as additional relevant NIST guidance. Feedback may be sent to privacyframework@nist.gov, but will not be posted online.

The NIST Privacy Framework: An Enterprise Risk Management Tool (Privacy Framework) permits any organization or industry sector to map the outcome-based subcategories in the Core to standards, guidelines, and practices to support the achievement of the outcomes associated with each subcategory. In the following table, NIST provides a mapping of the Core subcategories to key relevant NIST guidance. Appendix A provides a complete listing of NIST guidance used in this mapping. This mapping is not intended to be comprehensive.

Table 1: NIST Informative References

	Function	Category	Subcategory	NIST Informative References
	IDENTIFY-P (ID)	**Inventory and Mapping (ID.IM-P):** Data processing and individuals' interactions with systems, products, or services are understood and inform the management of privacy risk.	**ID.IM-P1:** Systems/products/services that process data, or with which individuals are interacting, are inventoried.	**NISTIR 8062** **NIST PRAM:** Worksheet 2 **NIST SP 800-37 Rev. 2:** Task P-10 **NIST SP 800-53 Rev. 5 (draft):** CM-8 (10), CM-12
			ID.IM-P2: The owners or operators of systems/products/services that process data, or with which individuals are interacting, are identified.	**NISTIR 8062** **NIST PRAM:** Worksheet 2 **NIST SP 800-37 Rev. 2:** Task P-9, P-10 **NIST SP 800-53 Rev. 5 (draft):** CM-8 (10)
			ID-IM-P3: Data elements that systems/products/services are processing are inventoried.	**NISTIR 8062** **NIST PRAM:** Worksheet 2 **NIST SP 800-37 Rev. 2:** Task P-12 **NIST SP 800-53 Rev. 5 (draft):** CM-8(10), CM-12, PM-29

	Function	Category	Subcategory	NIST Informative References
			ID.IM-P4: Data actions are identified.	**NISTIR 8062** **NIST PRAM:** Worksheet 2 **NIST SP 800-37 Rev. 2:** Task P-13 **NIST SP 800-53 Rev. 5 (draft):** CM-8(10)
			ID.IM-P5: The data processing environment is identified (e.g., internal, cloud).	**NISTIR 8062** **NIST PRAM:** Worksheet 2 **NIST SP 800-37 Rev. 2:** Task P-16 **NIST SP 800-53 Rev. 5 (draft):** CM-8(10), RA-2
			ID.IM-P6: Data processing is mapped, illustrating the processing of data elements by system components and their owner/operators, and interactions of individuals and organizations with the systems/products/services.	**NISTIR 8062** **NIST PRAM:** Worksheet 2 **NIST SP 800-37 Rev. 2:** Task P-13 **NIST SP 800-53 Rev. 5 (draft):** CM-8(10)
		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 supply chain is identified and communicated.	**NIST SP 800-37 Rev. 2:** Section 2.8 Supply Chain Risk Management, Task P-9 **NIST SP 800-53 Rev. 5 (draft):** CP-2, SA-12 **NIST SP 800-161** **NISTIR 7622**
			ID.BE-P2: Priorities for organizational mission, objectives, and activities are established and communicated.	**NIST PRAM:** Worksheet 1 **NIST SP 800-37 Rev. 2:** Task P-8 **NIST SP 800-53 Rev. 5 (draft):** PM-11
			ID.BE-P3: Systems/products/services that support organizational priorities are identified and key functional requirements communicated.	**NIST PRAM:** Worksheet 1 **NIST SP 800-37 Rev. 2:** Task P-8 **NIST SP 800-53 Rev. 5 (draft):** RA-9

	Function	Category	Subcategory	NIST Informative References
		Governance (ID.GV-P): The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of privacy risk.	**ID.GV-P1:** Organizational privacy policies are established and communicated.	**NIST PRAM:** Worksheet 1 **NIST SP 800-53 Rev. 5 (draft):** all -1 controls, PM-23 **NIST SP 800-39**
			ID.GV-P2: Processes to instill organizational privacy values within system/product/service development operations are in place.	**NIST PRAM:** Worksheet 1 **NIST SP 800-53 Rev. 5 (draft):** PM-6
			ID.GV-P3: Privacy roles and responsibilities for the entire workforce are established.	**NIST SP 800-37 Rev. 2:** Task P-1, Appendix D **NIST SP 800-53 Rev. 5 (draft):** PM-3
			ID.GV-P4: Privacy roles and responsibilities are coordinated and aligned with third-party stakeholders (e.g., suppliers, customers, partners).	**NIST SP 800-37 Rev. 2:** Task P-1, Appendix D **NIST SP 800-53 Rev. 5 (draft):** IR-4, PM-3, PM-18 , PM-19
			ID.GV-P5: Legal, regulatory, and contractual requirements regarding privacy are understood and managed.	**NIST PRAM:** Worksheet 1 **NIST SP 800-37 Rev. 2:** Task P-4, P-15 **NIST SP 800-53 Rev. 5 (draft):** PM-30
			ID.GV-P6: Governance and risk management processes address privacy risks.	**NIST PRAM:** Worksheet 1 **NIST SP 800-37 Rev. 2:** Task P-15, P-16 **NIST SP 800-53 Rev. 5 (draft):** PM-3, PM-7, PM-9, PM-10, PM-11, PM-18, PM-19, PM-21, PM-22, PM-23, PM-24, PM-25, PM-26, PM-28, PM-29, PM-30 **NIST SP 800-39**

	Function	Category	Subcategory	NIST Informative References
		Risk Assessment (ID.RA-P): The organization understands the privacy risks to individuals and how such privacy risks may create secondary impacts on organizational operations (including mission, functions, reputation, or workforce culture).	**ID.RA-P1:** The purposes for the data actions are identified.	**NIST SP 800-37 Rev. 2:** Task P-13 **NIST SP 800-53 Rev. 5 (draft):** CM-8(10), PA-1, PA-2, PA-3
			ID.RA-P2: Contextual factors related to the systems/products/services and the data actions are identified (e.g., individuals' privacy interests and perceptions, demographics, data sensitivity).	**NISTIR 8062** **NIST PRAM:** Worksheet 2 **NIST SP 800-37 Rev. 2:** Task P-9
			ID.RA-P3: Potential problematic data actions and associated problems are identified.	**NISTIR 8062** **NIST PRAM:** Worksheet 3, Catalog of Problematic Data Actions and Problems **NIST SP 800-37 Rev. 2:** Task P-9 **NIST SP 800-53 Rev. 5 (draft):** CM-4, RA-3 **NIST SP 800-30 Rev. 1**
			ID.RA-P4: Problematic data actions, likelihoods, and impacts are used to determine and prioritize risk.	**NISTIR 8062** **NIST PRAM:** Worksheet 3, Catalog of Problematic Data Actions and Problems **NIST SP 800-37 Rev. 2:** Task P-14 **NIST SP 800-53 Rev. 5 (draft):** RA-3 **NIST SP 800-30 Rev. 1** **NIST SP 800-39**
			ID.RA-P5: Risk responses are identified and prioritized.	**NISTIR 8062** **NIST PRAM:** Worksheet 4 **NIST SP 800-37 Rev. 2:** Task P-14, R-3 **NIST SP 800-53 Rev. 5 (draft):** RA-7 **NIST SP 800-30 Rev. 1** **NIST SP 800-39**
			ID.RA-P6: Risk is re-evaluated as data	**NISTIR 8062** **NIST SP 800-37 Rev. 2:** Task P-14, S-5, M-1, M-2

	Function	Category	Subcategory	NIST Informative References
			processing or individuals' interactions with systems/products/services change.	**NIST SP 800-53 Rev. 5 (draft):** CA-7
		Risk Management Strategy (ID.RM-P): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	**ID.RM-P1:** Risk management processes are established, managed, and agreed to by organizational stakeholders.	**NIST SP 800-37 Rev. 2:** Task P-2 **NIST SP 800-53 Rev. 5 (draft):** PM-9 **NIST SP 800-39**
			ID.RM-P2: Organizational risk tolerance is determined and clearly expressed.	**NIST SP 800-37 Rev. 2:** Task P-2 **NIST SP 800-53 Rev. 5 (draft):** PM-9, PM-32 **NIST SP 800-39**
			ID.RM-P3: The organization's determination of risk tolerance is informed by its role in the ecosystem.	**NIST SP 800-37 Rev. 2:** Task P-2 **NIST SP 800-53 Rev. 5 (draft):** PM-32 **NIST SP 800-39**
		Supply Chain Risk Management (ID.SC-P): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing privacy supply chain risk. The organization has established and implemented the processes to identify, assess, and manage privacy supply chain risks.	**ID.SC-P1:** Supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders.	**NIST SP 800-37 Rev. 2:** Section 2.8, Task P-2 **NIST SP 800-53 Rev. 5 (draft):** SA-12, PM-31 **NIST SP 800-161** **NISTIR 7622**
			ID.SC-P2: Service providers/suppliers/third-party partners of data processing systems, products, and services are identified, prioritized, and assessed using a supply chain risk assessment process.	**NIST SP 800-53 Rev. 5 (draft):** RA-3(1), SA-12 **NIST SP 800-30 Rev. 1** **NIST SP 800-161** **NISTIR 7622**
			ID.SC-P3: Contracts with service	**NIST SP 800-53 Rev. 5 (draft):** PM-31, SA-12(1) **NIST SP 800-161**

	Function	Category	Subcategory	NIST Informative References
			providers/suppliers/third-party partners are used to implement appropriate measures designed to meet the objectives of an organization's privacy program and supply chain risk management plan.	**NISTIR 7622**
			ID.SC-P4: Service providers/suppliers/third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations.	**NIST SP 800-53 Rev. 5 (draft):** SA-12(2) **NIST SP 800-161** **NISTIR 7622**
			ID.SC-P5: Response planning and testing are conducted with service providers/suppliers/third-party providers.	**NIST SP 800-53 Rev. 5 (draft):** IR-8(1), SA-12(12) **NIST SP 800-161** **NISTIR 7622**
	PROTECT-P (PR)	**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.	**NIST SP 800-63 Rev. 3** **NIST SP 800-53 Rev. 5 (draft):** IA-4(4)
			PR.AC-P2: Physical access to data and devices is managed.	**NIST SP 800-53 Rev. 5 (draft):** PE-2, PE-3, PE-4, PE-5, PE-6, PE-18, PE-20
			PR.AC-P3: Remote access is managed.	**NIST SP 800-53 Rev. 5:** AC-17, AC-20 **NISTIR 7966** **NIST SP 800-46 Rev. 2**

	Function	Category	Subcategory	NIST Informative References
				NIST SP 800-77 **NIST SP 800-113** **NIST SP 800-114 Rev. 2** **NIST SP 800-121 Rev. 2** **FIPS Publication 199**
			PR.AC-P4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties.	**NIST SP 800-53 Rev. 5 (draft):** AC-1, AC-2, AC-3, AC-5 **NIST SP 800-162**
			PR.AC-P5: Network integrity is protected (e.g., network segregation, network segmentation).	**NIST SP 800-53 Rev. 5 (draft):** AC-4, SC-7
			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).	**NIST SP 800-63 Rev. 3** **NIST SP 800-53 Rev. 5 (draft):** IA-12
			PR.AC-P7: Attribute references are used instead of attribute values.	**NISTIR 8062** **NISTIR 8112** **NIST SP 800-63 Rev. 3** **NIST SP 800-53 Rev. 5 (draft):** AC-16, IP-2(1)
		Awareness and Training (PR.AT-P): The organization's personnel and partners are provided privacy awareness education and are trained to	**PR.AT-P1:** All users are informed and trained.	**NIST SP 800-53 Rev. 5 (draft)**: AT-2, PM-13
			PR.AT-P2: Privileged users understand their roles and responsibilities.	**NIST SP 800-53 Rev. 5 (draft):** AT-3, PM-13

	Function	Category	Subcategory	NIST Informative References
		perform their privacy-related duties and responsibilities consistent with related policies, procedures, and agreements.	**PR.AT-P3:** Third-party stakeholders (e.g., service providers, customers, partners) understand their roles and responsibilities.	**NIST SP 800-53 Rev. 5 (draft):** PS-7, SA-9, SA-12 (1) **NIST SP 800-161** **NISTIR 7622**
			PR.AT-P4: Senior executives understand their roles and responsibilities.	**NIST SP 800-37 Rev. 2:** Task P-1 **NIST SP 800-53 Rev. 5 (draft):** AT-3, PM-13
			PR.AT-P5: Privacy personnel understand their roles and responsibilities.	**NIST SP 800-37 Rev. 2:** Task P-1 **NIST SP 800-53 Rev. 5 (draft):** AT-3, PM-13
		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 is protected.	**NIST SP 800-53 Rev 5 (draft):** MP-8, SC-12, SC-28 **NIST SP 800-175B**
			PR.DS-P2: Data-in-transit is protected.	**NIST SP 800-53 Rev. 5 (draft):** SC-8, SC-11, SC-12 **NIST SP 800-175B**
			PR.DS-P3: Systems/products/services and associated data are formally managed throughout removal, transfers, and disposition.	**NIST SP 800-53 Rev. 5 (draft):** CM-8, MP-6, PE-16
			PR.DS-P4: Adequate capacity to ensure availability is maintained.	**NIST SP 800-53 Rev. 5 (draft):** AU-4, CP-2, SC-5
			PR.DS-P5: Protections against data leaks are implemented.	**NIST SP 800-53 Rev. 5 (draft):** AC-4, AC-5, AC-6, PE-19, PS-3, PS-6, SC-7, SC-8, SC-, SC-31, SI-4
			PR.DS-P6: Integrity checking mechanisms are used to verify software, firmware, and information integrity.	**NIST SP 800-53 Rev. 5 (draft):** SC-16, SI-7 **NIST SP 800-175B**

	Function	Category	Subcategory	NIST Informative References
			PR.DS-P7: The development and testing environment(s) are separate from the production environment.	**NIST SP 800-53 Rev. 5 (draft):** CM-2(6)
			PR.DS-P8: Integrity checking mechanisms are used to verify hardware integrity.	**NIST SP 800-53 Rev. 5 (draft):** SA-10, SI-7
		Data Protection Processes and Procedures (PR.DP-P): Security and privacy policies (that address purpose, 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-P1:** A baseline configuration of security and privacy controls is created and maintained.	**NIST SP 800-37, Rev 2:** Task I-2 **NIST SP 800-53 Rev. 5 (draft):** CM-2, CM-, CM-4 S, CM-5
			PR.DP-P2: A system development life cycle to manage systems and an information life cycle to manage data are aligned and implemented.	**NIST SP 800-37, Rev. 2:** Task P-13 **NIST SP 800-53 Rev. 5 (draft):** PL-8 SA-3, PM-23,PM-24, PM-25, SA-8, SA-12, SA-15, SA-17 SI-12 **NIST SP 800-160 Vol. 1**
			PR.DP-P3: Configuration change control processes are in place.	**NIST SP 800-53 Rev. 5 (draft):** CM-3, CM-4, SA-10
			PR.DP-P4: Backups of information are conducted, maintained, and tested.	**NIST SP 800-53 Rev. 5 (draft):** CP-4, CP-6, CP-9 **NIST SP 800-34 Rev. 1** **NIST SP 800-84**
			PR.DP-P5: Policy and regulations regarding the physical operating environment for organizational assets are met.	**NIST SP 800-53 Rev. 5 (draft):** PE-10, PE-12, PE-13, PE-15, PE-18
			PR.DP-P6: Data are destroyed according to policy.	**NIST SP 800-53 Rev. 5 (draft):** MP-6 **NIST SP 800-88 Rev. 1**

	Function	Category	Subcategory	NIST Informative References
			PR.DP-P7: Protection processes are improved.	**NIST SP 800-37, Rev. 2:** all steps and tasks **NIST SP 800-53 Rev. 5 (draft):** CA-2, CA-7, CP-2, IR-8, PL-2, PM-6 **NIST SP 800-39**
			PR.DP-P8: Effectiveness of protection technologies is shared.	**NIST SP 800-53 Rev. 5 (draft):** AC-21, CA-7, SI-4
			PR.DP-P9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed.	**NIST SP 800-53 Rev. 5 (draft):** CP-2, CP-7, CP-12, CP-13, IR-7, IR-8, IR-9, PE-17 **NIST SP 800-34 Rev. 1** **NIST SP 800-61 Rev. 2**
			PR.DP-P10: Response and recovery plans are tested.	**NIST SP 800-53 Rev. 5 (draft):** CP-4, IR-3, PM-14 **NIST SP 800-34 Rev. 1** **NIST SP 800-84**
			PR.DP-P11: Privacy procedures are included in human resources practices (e.g., deprovisioning, personnel screening).	**NIST SP 800-53 Rev. 5 (draft):** PS-1 , PS-2, PS-3, PS-4, PS-5, PS-6, PS-7, PS-8, SA-21
			PR.DP-P12: A vulnerability management plan is developed and implemented.	**NIST SP 800-53 Rev. 5 (draft):** RA-3, RA-5, SI-2 **NIST SP 800-30 Rev. 1**
		Maintenance (PR.MA-P): System maintenance and repairs are performed consistent with policies and procedures.	**PR.MA-P1:** Maintenance and repair of organizational assets are performed and logged, with approved and controlled tools.	**NIST SP 800-53 Rev. 5 (draft):** MA-2, MA-3, MA-5, MA-6

	Function	Category	Subcategory	NIST Informative References
			PR.MA-P2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access.	**NIST SP 800-53 Rev. 5 (draft):** MA-4
		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, 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.	**NIST SP 800-53 Rev. 5 (draft):** AU Control Family
			PR.PT-P2: Removable media is protected and its use restricted according to policy.	**NIST SP 800-53 Rev. 5 (draft):** MP-2, MP-3, MP-4, MP-5, MP-7, MP-8
			PR.PT-P3: The principle of least functionality is incorporated by configuring systems to provide only essential capabilities.	**NIST SP 800-53 Rev. 5 (draft):** AC-3, CM-7
			PR.PT-P4: Communications and control networks are protected.	**NIST SP 800-53 Rev. 5 (draft):** AC-4, AC-17, AC-18, CP-8, SC-7 SC-20, SC-21, SC-22, SC-23, SC-24, SC-25, SC-29, SC-32, SC-36, SC-37, SC-38, SC-39, SC-40, SC-41, SC-43
			PR.PT-P5: Mechanisms (e.g., failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations.	**NIST SP 800-53 Rev. 5 (draft):** CP-7, CP-8, CP-11, CP-13, PL-8, RA-9

	Function	Category	Subcategory	NIST Informative References
		Protected Processing (PR.PP-P): Technical data processing solutions increase disassociability consistent with related policies, procedures, and agreements and the organization's risk strategy to protect individuals' privacy.	**PR.PP-P1:** Data are processed in an unobservable or unlinkable manner.	**NIST SP 800-63 Rev. 3** **NIST SP 800-53 Rev. 5 (draft):** IA-8(6), MP-6 **NIST SP 800-188 (draft)** **NISTIR 8053**
			PR.PP-P2: Data are processed to limit the identification of individuals.	**NIST SP 800-63 Rev. 3** **NIST SP 800-53 Rev. 5 (draft):** AC-23, IA-4(8), MP-6, SI-20 **NIST SP 800-188 (draft)** **NISTIR 8053**
			PR.PP-P3: Data are processed to restrict the formulation of inferences about individuals' behavior or activities.	**NIST SP 800-63 Rev. 3** **NIST SP 800-53 Rev. 5 (draft):** AC-23, IA-8(6), MP-6, SI-20 **NIST SP 800-188 (draft)** **NISTIR 8053**
			PR.PP-P4: Data are processed through a distributed system architecture.	**NIST SP 800-63 Rev. 3** **NIST SP 800-53 Rev. 5 (draft):** AC-23, SC-2, IA-8(6)
			PR.PP-P5: Data are processed on local devices.	**NIST SP 800-53 Rev. 5 (draft):** CM-12
	CONTROL-P (CT)	**Data Management Processes and Procedures (CT.PO-P):** Policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage data consistent with the organization's risk	**CT.PO-P1:** Policies and procedures for authorizing data processing and maintaining authorizations are in place.	**NIST SP 800-53 Rev. 5 (draft):** AC-21, IP-2, PA-1, PA-2, PA-3, PA-4
			CT.PO-P2: Processes for enabling data review, transmission/disclosure, alteration, or deletion are in place.	**NIST SP 800-53 Rev. 5 (draft):** MP-6, MP-6(9), PM-23, PM-24, PM-26, PM-28, SI-12, SI-18, SI-19
			CT.PO-P3: Processes and procedures for enabling	**NIST SP 800-63 Rev. 3**

	Function	Category	Subcategory	NIST Informative References
		strategy to protect individuals' privacy.	individuals' data processing preferences and requests (e.g., individual participation) are in place.	**NIST SP 800-53 Rev. 5 (draft):** AC-1, IP-1, IP-2, IP-3, IP-4, IP-6, PM-27
		Data Management (CT.DM-P): Data are managed consistent with the organization's risk strategy to protect individuals' privacy and increase manageability.	**CT.DM-P1:** System or device configurations permit selective collection or disclosure of data elements to allow for implementation of privacy principles (e.g., data minimization).	**NIST SP 800-63 Rev 3.** **NIST SP 800-53 Rev. 5 (draft):** AC-21, SI-12, SI-12(1), SI-12(2), SC-42(5) **NIST SP 800-188 (draft)** **NISTIR 8053**
			CT.DM-P2: Individuals' authorization for the data action is obtained.	**NIST SP 800-63 Rev 3.** **NIST SP 800-53 Rev. 5 (draft):** AC-21, IP-2
			CT.DM-P3: Data elements can be accessed for review.	**NIST SP 800-53 Rev. 5 (draft):** IP-6, PM-23, SI-12, SI-19
			CT.DM-P4: Data elements can be accessed for transmission or disclosure.	**NIST SP 800-53 Rev. 5 (draft):** IP-6, PM-23, SI-12, SI-19
			CT.DM-P5: Data elements can be accessed for alteration.	**NIST SP 800-53 Rev. 5 (draft):** PM-23, SI-12, SI-19
			CT.DM-P6: Data elements can be accessed for deletion.	**NIST SP 800-53 Rev. 5 (draft):** MP-6, MP-6(9), PM-23, SI-12, SI-19
			CT.DM-P7: Metadata containing processing permissions and related data values are transmitted with data elements.	**NISTIR 8112** **NIST SP 800-53 Rev. 5 (draft):** AC-16, IP-1, PA-1, PA-2, PA-3, PA-3(2), PM-23(1), PM-23(2), SC-16, SI-19(2)
			CT.DM-P8: Processing permissions are transmitted using standardized formats.	**NISTIR 8112**

	Function	Category	Subcategory	NIST Informative References
	INFORM-P (IN)	**Transparency Processes and Procedures (IN.TP-P):** Policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to increase transparency of the organization's data processing practices.	**IN.TP-P1:** Transparency procedures and mechanisms (e.g., internal or public reports) for data processing practices are in place.	**NIST SP 800-37 Rev. 2:** Task M-5 **NIST SP 800-53 Rev. 5 (draft):** CA-5 P, CM-4 S, PM-21, PM-30, RA-8
			IN.TP-P2: Processes for communicating data processing purposes are in place.	**NIST SP 800-53 Rev. 5 (draft):** PA-3, IP-4
		Data Processing Awareness (IN.AW-P): Individuals and organizations have an awareness of data processing practices, and processes and procedures are used and maintained to increase predictability consistent with the organization's risk strategy to protect individuals' privacy.	**IN.AW-P1:** Records of data disclosures are maintained and can be shared.	**NIST SP 800-53 Rev. 5 (draft):** PM-22
			IN.AW-P2: Individuals are informed about data processing practices.	**NIST SP 800-53 Rev. 5 (draft):** AC-8, IP-4 , IP-5, PM-21, SC-42(4)
			IN.AW-P3: System/product/service design enhances data processing visibility.	**NIST SP 800-53 Rev. 5 (draft):** SC-42(4), IP-4
			IN.AW-P4: Data sources are informed of data deletion and correction.	**NISTIR 8112** **NIST SP 800-53 Rev. 5 (draft):** PM-23, SI-19
			IN.AW-P5: Individuals are informed when data are corrected or deleted.	**NIST SP 800-53 Rev. 5 (draft):** PM-23, SI-19
			IN.AW-P6: Data provenance is maintained and can be shared.	**NISTIR 8112**
			IN.AW-P7: Data analytic inputs and outputs are	

	Function	Category	Subcategory	NIST Informative References
			understood and evaluated for bias.	
	RESPOND-P (RS)	**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.	**NIST SP 800-53 Rev. 5 (draft):** IR-1, IR-4 IR-8 **NIST SP 800-61 Rev. 2**
		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.	**NIST SP 800-53 Rev. 5 (draft):** IR-2, IR-3, IR-8 **NIST SP 800-34 Rev. 1** **NIST SP 800-50** **NIST SP 800-61 Rev. 2** **NIST SP 800-84**
			RS.CO-P2: Privacy breaches and events are reported consistent with established criteria.	**NIST SP 800-37 Rev. 2:** Task M-5 **NIST SP 800-53 Rev. 5 (draft):** IR-4, PM-21 **NIST SP 800-61 Rev. 2**
			RS.CO-P3: Information is shared consistent with response plans.	**NIST SP 800-53 Rev. 5 (draft):** CP-2, IR-4, IR-8, PM-21 **NIST SP 800-61 Rev. 2**
			RS.CO-P4: Coordination with stakeholders occurs consistent with response plans.	**NIST SP 800-53 Rev. 5 (draft):** CP-2, IR-4, SA-12 (12)
			RS.CO-P5: Data for voluntary information sharing is restricted to what is necessary for understanding the privacy breach or event.	**NIST SP 800-53 Rev. 5 (draft):** IR-6, PA-4, PM-15, SI-5 **NIST SP 800-61 Rev. 2**
			RS.CO-P6: Impacted individuals are notified	**NIST SP 800-53 Rev. 5 (draft):** IR-1, IR-7, IR-8

	Function	Category	Subcategory	NIST Informative References
			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.	**NIST SP 800-53 Rev. 5 (draft):** AU-6, CA-7, IR-4, IR-5, SI-4
			RS.AN-P2: The impact of the privacy breach or event on individuals, the organization, and the ecosystem is understood.	**NIST SP 800-53 Rev. 5 (draft):** IR-8(1) **NIST SP 800-61 Rev. 2**
			RS.AN-P3: Forensics are performed.	**NIST SP 800-53 Rev. 5 (draft):** AU-7, IR-4
			RS.AN-P4: Privacy breaches and events are categorized consistent with response plan.	**NIST SP 800-53 Rev. 5 (draft):** CP-2, IR-4, IR-5, IR-8
			RS.AN-P5: Processes are established to receive, analyze, and respond to problematic data actions disclosed to the organization from internal and external sources (e.g., internal testing, privacy researchers).	**NIST SP 800-37 Rev. 2:** Task A-6, M-3 **NIST SP 800-53 Rev. 5 (draft):** CA-5, PM-15, SI-20(8)
		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.	**NIST SP 800-53 Rev. 5 (draft):** IR-4
			RS.MI-P2: Privacy breaches and events are mitigated.	**NIST SP 800-53 Rev. 5 (draft):** IR-4
			RS.MI-P3: Newly identified problematic data actions are mitigated or documented as accepted risks.	**NIST SP 800-37 Rev. 2:** Task A-6, M-3 **NIST SP 800-53 Rev. 5 (draft):** CA-5

	Function	Category	Subcategory	NIST Informative References
		Improvements (RS.IM-P): Organizational privacy practices are improved by incorporating lessons learned from privacy breaches and events.	**RS.IM-P1:** Policies and processes incorporate lessons learned.	**NIST SP 800-53 Rev. 5 (draft):** all -1 controls, CP-2, IR-4, IR-8
		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 and responding to complaints, concerns, and questions from individuals about organizational privacy practices are in place.	**NIST SP 800-53 Rev. 5 (draft):** IP-3, PM-28
			RS.RE-P2: Individuals are provided with mitigation mechanisms.	**NIST SP 800-53 Rev. 5 (draft):** IP-3

Appendix A: NIST Guidance References

1. Federal Information Processing Standards (FIPS) Publication 199, Standards for Security Categorization of Federal Information and Information Systems, https://doi.org/10.6028/NIST.FIPS.199

2. NIST Interagency Report (NISTIR) 7622, Notional Supply Chain Risk Management Practices for Federal Information Systems https://doi.org/10.6028/NIST.IR.7622

3. NIST Internal Report (NISTIR) 7966, Security of Interactive and Automated Access Management Using Secure Shell (SSH), https://doi.org/10.6028/NIST.IR.7966

4. NISTIR 8053, De-Identification of Personal Information, https://doi.org/10.6028/NIST.IR.8053

5. NISTIR 8062, An Introduction to Privacy Engineering and Risk Management in Federal Systems, https://doi.org/10.6028/NIST.IR.8062

6. NISTIR 8112, Attribute Metadata: A Proposed Schema for Evaluating Federated Attributes, https://doi.org/10.6028/NIST.IR.8112

7. NIST Privacy Risk Assessment Methodology (PRAM), https://www.nist.gov/itl/applied-cybersecurity/privacy-engineering/resources

8. NIST Special Publication (SP) 800-30, Revision 1, Guide for Conducting Risk Assessments, https://doi.org/10.6028/NIST.SP.800-30r1

9. NIST SP 800-34, Revision 1, Contingency Planning Guide for Federal Information Systems, https://doi.org/10.6028/NIST.SP.800-34r1

10. NIST SP 800-37, Revision 2, Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy, https://doi.org/10.6028/NIST.SP.800-37r2

11. NIST SP 800-39, Managing Information Security Risk: Organization, Mission, and Information System View, https://doi.org/10.6028/NIST.SP.800-39

12. NIST SP 800-46, Revision 2, Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security, https://doi.org/10.6028/NIST.SP.800-46r2

13. NIST SP 800-50, Building an Information Technology Security Awareness and Training Program, https://doi.org/10.6028/NIST.SP.800-50

14. NIST SP 800-53, Revision 5 (draft), Security and Privacy Controls for Information Systems and Organizations, https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/draft

15. NIST SP 800-61, Revision 2, Computer Security Incident Handling Guide, https://doi.org/10.6028/NIST.SP.800-61r2

16. NIST SP 800-77, Guide to IPsec VPNs, https://doi.org/10.6028/NIST.SP.800-77

17. NIST SP 800-84, Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities, https://doi.org/10.6028/NIST.SP.800-84

18. NIST SP 800-88, Revision 1, Guidelines for Media Sanitization, https://doi.org/10.6028/NIST.SP.800-88r1

19. NIST SP 800-113, Guide to SSL VPNs, https://doi.org/10.6028/NIST.SP.800-113

20. NIST SP 800-114, Revision 1, User's Guide to Telework and Bring Your Own Device (BYOD) Security, https://doi.org/10.6028/NIST.SP.800-114r1

21. NIST SP 800-121, Revision 2, Guide to Bluetooth Security, https://doi.org/10.6028/NIST.SP.800-121r2

22. NIST SP 800-160, Volume 1, Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems, https://doi.org/10.6028/NIST.SP.800-160v1

23. NIST SP 800-161, Supply Chain Risk Management Practices for Federal Information Systems and Organizations, https://doi.org/10.6028/NIST.SP.800-161

24. NIST SP 800-162, Guide to Attribute Based Access Control (ABAC) Definition and Considerations, https://doi.org/10.6028/NIST.SP.800-162

25. NIST SP 800-175B, Guideline for Using Cryptographic Standards in the Federal Government: Cryptographic Mechanisms, https://doi.org/10.6028/NIST.SP.800-175B

26. NIST SP 800-188, De-Identifying Government Datasets (draft), https://csrc.nist.gov/CSRC/media/Publications/sp/800-188/draft/documents/sp800_188_draft2.pdf