NIST Cybersecurity White Paper
CSWP 38 ipd

NIST Privacy Workforce Taxonomy

Initial Public Draft

Authors

NIST Privacy Workforce Public Working Group (PWWG)

Editors

Dylan Gilbert
Meghan Anderson
Applied Cybersecurity Division
Information Technology Laboratory

This publication is available free of charge from:
https://doi.org/10.6028/NIST.CSWP.38.ipd

November 21, 2024

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

Certain equipment, instruments, software, or materials, commercial or non-commercial, are identified in this paper in order to specify the experimental procedure adequately. Such identification does not imply recommendation or endorsement of any product or service by NIST, nor does it imply that the materials or equipment identified are necessarily the best available for the purpose.

NIST Technical Series Policies

Publication History
Approved by the NIST Editorial Review Board on YYYY-MM-DD [Will be added to final publication.]

How to Cite this NIST Technical Series Publication:

NIST Privacy Workforce Public Working Group (2024) NIST Privacy Workforce Taxonomy. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Cybersecurity White Paper (CSWP) NIST CSWP 38 ipd. https://doi.org/10.6028/NIST.CSWP.38.ipd

Author ORCID iDs
Meghan Anderson: 0009-0004-2875-5672
Dylan Gilbert: 0009-0003-6061-3757

Public Comment Period

November 21, 2024 – January 17, 2025

Submit Comments

pwwg@nist.gov

National Institute of Standards and Technology
Attn: Applied Cybersecurity Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 2000) Gaithersburg, MD 20899-2000

Additional Information

Additional information about this publication is available at https://csrc.nist.gov/publications/cswp, including related content, potential updates, and document history.

All comments are subject to release under the Freedom of Information Act (FOIA).

Abstract

This document provides a taxonomy of Task, Knowledge, and Skill (TKS) Statements aligned with the NIST Privacy Framework, Version 1.0 and the NICE Workforce Framework for Cybersecurity model of TKS Statement building blocks. It contains a mapping of the Taxonomy's TKS Statements to the NIST Privacy Framework Core Subcategories as well as a compilation of all TKS Statements organized in alphabetical order. The Taxonomy is voluntary and designed for flexible use. It can help organizations better achieve their desired privacy outcomes, support recruitment with more consistent position descriptions, and inform the education and training of professionals to produce a more skilled and knowledgeable workforce capable of managing privacy risks.

Keywords

Privacy Framework; Privacy Workforce Public Working Group; PWWG; privacy workforce; NICE Framework; Task, Knowledge, and Skill Statements; TKS Statements; task; knowledge; skill; privacy; privacy risk; privacy risk management; taxonomy.

Note to Reviewers

The NIST Privacy Workforce Taxonomy Initial Public Draft (IPD) was developed by the NIST Privacy Workforce Public Working Group (PWWG). The PWWG convened a global stakeholder community representing industry, the public sector, civil society, and academia with the shared goal to identify and document tasks, knowledge, and skills aligned with the NIST Privacy Framework, Version 1.0 (Privacy Framework 1.0) and the NICE Workforce Framework for Cybersecurity (NICE Framework). The Privacy Workforce Taxonomy can help organizations better achieve their desired privacy outcomes, support recruitment, and inform workforce education and training.

More information on the PWWG can be found here: *https://www.nist.gov/privacy-framework/workforce-advancement/privacy-workforce-public-working-group*

More information on the Privacy Framework can be found here: *https://www.nist.gov/privacy-framework*

More information on the NICE Framework can be found here: *https://www.nist.gov/itl/applied-cybersecurity/nice/nice-framework-resource-center*

This Initial Public Draft contains the following sections:

- **1. Mapping of Privacy Framework 1.0 to TKS Statements:** Maps Privacy Framework 1.0 Core Subcategories to Task, Knowledge, and Skill (TKS) Statements, excluding the Protect-P Function. The NICE Framework will be leveraged to map Protect-P Subcategories to TKS Statements
- **2. TKS Statements Inventory:** Lists the NIST Privacy Workforce Taxonomy IPD TKS Statements in alphabetical order and organized by Statement type
- **Appendix A: TKS Statements Cheat Sheet:** Highlights general principles, rules, and definitions for creating TKS Statements
- **Appendix B: NIST Privacy Framework Glossary:** Defines selected terms used for the purposes of Privacy Framework 1.0 and the Privacy Workforce Taxonomy IPD

NIST welcomes feedback on all aspects of this Initial Public Draft. NIST is particularly interested in answers to the following questions:

1. Are these TKS Statements drafted at a helpful level of detail?
    a. Task Statements are drafted at a high level to support the intent of the Privacy Framework 1.0 Subcategories. Would it be useful to include more detailed "step-by-step" Task Statements?
2. Are any TKS Statements missing? Are any TKS Statements unnecessary or irrelevant?
3. Is the "Notes" section that is included in certain Subcategory mappings (e.g., ID.BE-P2) useful?

   a. Are there other Subcategories that would benefit from notes? If so, what Subcategories? What information would be useful to include in these additional notes?

4. Are the TKS Statements mapped to the appropriate Subcategories?
5. Do the organization-defined parameters bracketed within TKS Statements provide helpful flexibility for organizations seeking to tailor TKS Statements to their needs?
6. Should Task Statements focused on creating documentation (i.e., T155 - T182) be included? If so, are any changes to these Task Statements necessary (i.e., additions, subtractions, revisions)?

Table of Contents

List of Tables

Acknowledgments

NIST would like to recognize the contributions made by the members of the NIST Privacy Workforce Public Working Group (PWWG). PWWG members committed significant time and expertise to help craft the Taxonomy’s Task, Knowledge, and Skill Statements. In particular, NIST thanks the PWWG Project Team Leads and Co-Chairs for their collaborative efforts and dedication in creating this Taxonomy.

1. Mapping of Privacy Framework 1.0 to TKS Statements

This section maps Privacy Framework 1.0 Core Subcategories to Privacy Workforce Taxonomy TKS Statements to assist organizations seeking tasks, knowledge, and skills aligned with a Subcategory outcome(s). The TKS Statements mapping is not intended to be used as a check list, and the Task Statements are not a series of chronological steps. Organization-defined parameters in brackets provide flexibility for organizations to adapt and apply TKS Statements based on their unique context and needs.

Table 1. Mapping of Privacy Framework 1.0 to TKS Statements

Statement Type	ID	Description	Subcategory Mapping
Subcategory	**ID.IM-P1**	**Systems/products/services that process data are inventoried.**	
Task	T129	Determine the methodology for taking inventory of data.	ID.IM-P1; ID.IM-P2; ID.IM-P3; ID.IM-P4; ID.IM-P5; ID.IM-P6; ID.IM-P7
Task	T139	Determine what the data inventory will be used for.	ID.IM-P1; ID.IM-P2; ID.IM-P3; ID.IM-P4; ID.IM-P5; ID.IM-P6; ID.IM-P7
Task	T168	Document systems/products/services that process data.	ID.IM-P1
Task	T238	Identify systems/products/services that process data.	ID.IM-P1
Task	T292	Select a system or data store for inventory information.	ID.IM-P1; ID.IM-P2; ID.IM-P3; ID.IM-P4; ID.IM-P5; ID.IM-P6; ID.IM-P7
Task	T295	Select an inventory tool option.	ID.IM-P1; ID.IM-P2; ID.IM-P3; ID.IM-P4; ID.IM-P5; ID.IM-P6; ID.IM-P7
Knowledge	K044	Knowledge of data elements that are legally defined terms.	ID.IM-P1; ID.IM-P2; ID.IM-P3; ID.IM-P4; ID.IM-P5; ID.IM-P6; ID.IM-P7; ID.IM-P8
Knowledge	K064	Knowledge of document accessibility requirements.	ID.IM-P1; ID.IM-P2; ID.IM-P3; ID.IM-P4; ID.IM-P5; ID.IM-P6; ID.IM-P7; ID.IM-P8; CM.AW-P4
Knowledge	K084	Knowledge of inventory (and other data management system) options and tools.	ID.IM-P1; ID.IM-P2; ID.IM-P3; ID.IM-P4; ID.IM-P5; ID.IM-P6; ID.IM-P7; ID.IM-P8
Knowledge	K118	Knowledge of organizational stakeholders with expertise on systems/products/services.	ID.IM-P1
Knowledge	K166	Knowledge of risk assessment and analysis systems.	ID.IM-P1; ID.IM-P2; ID.IM-P3; ID.IM-P4; ID.IM-P5; ID.IM-P6; ID.IM-P7; ID.IM-P8
Knowledge	K257	Knowledge of the organization's data processing.	ID.IM-P1; ID.IM-P2; ID.IM-P3; ID.IM-P4; ID.IM-P5; ID.IM-P6; ID.IM-P7; ID.IM-P8; CT.PO-P1; CT.PO-P2; CT.PO-P3; CT.PO-P4; CT.DM-P1; CT.DM-P2; CT.DM-P3; CT.DM-P4; CT.DM-P5; CT.DM-P6; CT.DM-P7; CT.DM-P8; CT.DM-P9; CT.DM-P10; CM.AW-P1; CM.AW-P2; CM.AW-P3; CM.AW-P4; CM.AW-P5; CM.AW-P6; CM.AW-P7; CM.AW-P8
Knowledge	K275	Knowledge of the organization's needs for information that can be provided from inventory and mapping.	ID.IM-P1; ID.IM-P2; ID.IM-P3; ID.IM-P4; ID.IM-P5; ID.IM-P6; ID.IM-P7; ID.IM-P8
Knowledge	K303	Knowledge of the organization's systems/products/services.	GV.MT-P1; ID.IM-P1; ID.IM-P2; ID.IM-P3; ID.IM-P4; ID.IM-P5; ID.IM-P6; ID.IM-P7; ID.IM-P8; ID.BE-P3; ID.RA-P1
Knowledge	K318	Knowledge of the structure of your organization's technology-related functions.	ID.IM-P1; ID.IM-P2; ID.IM-P3; ID.IM-P4; ID.IM-P5; ID.IM-P6; ID.IM-P7; ID.IM-P8
Skill	S152	Skill in evaluating the quality of information received.	ID.IM-P1; ID.IM-P2; ID.IM-P3; ID.IM-P4; ID.IM-P5; ID.IM-P6; ID.IM-P7; ID.IM-P8
Skill	S168	Skill in identifying data elements that are legally defined terms.	ID.IM-P1; ID.IM-P2; ID.IM-P3; ID.IM-P4; ID.IM-P5; ID.IM-P6; ID.IM-P7; ID.IM-P8
Skill	S169	Skill in identifying data elements that are organization-defined terms or classifications.	ID.IM-P1; ID.IM-P2; ID.IM-P3; ID.IM-P4; ID.IM-P5; ID.IM-P6; ID.IM-P7; ID.IM-P8
Skill	S183	Skill in identifying the organization’s systems/products/services that process data.	ID.IM-P1

Statement Type	ID	Description	Subcategory Mapping
Skill	S189	Skill in implementing inventory (and other data management system) options and tools.	ID.IM-P1; ID.IM-P2; ID.IM-P3; ID.IM-P4; ID.IM-P5; ID.IM-P6; ID.IM-P7; ID.IM-P8
Skill	S261	Skill in querying inventory management systems.	ID.IM-P1; ID.IM-P2; ID.IM-P3; ID.IM-P4; ID.IM-P5; ID.IM-P6; ID.IM-P7; ID.IM-P8
Skill	S264	Skill in reporting from inventory management systems.	ID.IM-P1; ID.IM-P2; ID.IM-P3; ID.IM-P4; ID.IM-P5; ID.IM-P6; ID.IM-P7; ID.IM-P8
Subcategory	**ID.IM-P2**	**Owners or operators (e.g., the organization or third parties such as service providers, partners, customers, and developers) and their roles with respect to the systems/products/services and components (e.g., internal or external) that process data are inventoried.**	
Task	T129	Determine the methodology for taking inventory of data.	ID.IM-P1; ID.IM-P2; ID.IM-P3; ID.IM-P4; ID.IM-P5; ID.IM-P6; ID.IM-P7
Task	T139	Determine what the data inventory will be used for.	ID.IM-P1; ID.IM-P2; ID.IM-P3; ID.IM-P4; ID.IM-P5; ID.IM-P6; ID.IM-P7
Task	T164	Document owners and operators, including their roles with respect to the systems/products/services and components that process data.	ID.IM-P2
Task	T231	Identify owners and operators of systems/products/services and components that process data.	ID.IM-P2
Task	T232	Identify owners' and operators' roles with respect to the systems/products/services and components that process data.	ID.IM-P2
Task	T292	Select a system or data store for inventory information.	ID.IM-P1; ID.IM-P2; ID.IM-P3; ID.IM-P4; ID.IM-P5; ID.IM-P6; ID.IM-P7
Task	T295	Select an inventory tool option.	ID.IM-P1; ID.IM-P2; ID.IM-P3; ID.IM-P4; ID.IM-P5; ID.IM-P6; ID.IM-P7
Knowledge	K004	Knowledge of [*organization-selected, regulation-defined*] roles of system/product/service and component owners or operators.	ID.IM-P2
Knowledge	K044	Knowledge of data elements that are legally defined terms.	ID.IM-P1; ID.IM-P2; ID.IM-P3; ID.IM-P4; ID.IM-P5; ID.IM-P6; ID.IM-P7; ID.IM-P8
Knowledge	K045	Knowledge of data elements that are organization-defined terms or classifications.	ID.IM-P1; ID.IM-P2; ID.IM-P3; ID.IM-P4; ID.IM-P5; ID.IM-P6; ID.IM-P7; ID.IM-P8
Knowledge	K064	Knowledge of document accessibility requirements.	ID.IM-P1; ID.IM-P2; ID.IM-P3; ID.IM-P4; ID.IM-P5; ID.IM-P6; ID.IM-P7; ID.IM-P8; CM.AW-P4
Knowledge	K084	Knowledge of inventory (and other data management system) options and tools.	ID.IM-P1; ID.IM-P2; ID.IM-P3; ID.IM-P4; ID.IM-P5; ID.IM-P6; ID.IM-P7; ID.IM-P8
Knowledge	K166	Knowledge of risk assessment and analysis systems.	ID.IM-P1; ID.IM-P2; ID.IM-P3; ID.IM-P4; ID.IM-P5; ID.IM-P6; ID.IM-P7; ID.IM-P8
Knowledge	K244	Knowledge of the organization's components.	ID.IM-P2; ID.IM-P7; ID.IM-P8; ID.BE-P1; ID.BE-P2; ID.BE-P3
Knowledge	K257	Knowledge of the organization's data processing.	ID.IM-P1; ID.IM-P2; ID.IM-P3; ID.IM-P4; ID.IM-P5; ID.IM-P6; ID.IM-P7; ID.IM-P8; CT.PO-P1; CT.PO-P2; CT.PO-P3; CT.PO-P4; CT.DM-P1; CT.DM-P2; CT.DM-P3; CT.DM-P4; CT.DM-P5; CT.DM-P6; CT.DM-P7; CT.DM-P8; CT.DM-P9; CT.DM-P10; CM.AW-P1; CM.AW-P2; CM.AW-P3; CM.AW-P4; CM.AW-P5; CM.AW-P6; CM.AW-P7; CM.AW-P8

Statement Type	ID	Description	Subcategory Mapping
Knowledge	K275	Knowledge of the organization's needs for information that can be provided from inventory and mapping.	ID.IM-P1; ID.IM-P2; ID.IM-P3; ID.IM-P4; ID.IM-P5; ID.IM-P6; ID.IM-P7; ID.IM-P8
Knowledge	K303	Knowledge of the organization's systems/products/services.	GV.MT-P1; ID.IM-P1; ID.IM-P2; ID.IM-P3; ID.IM-P4; ID.IM-P5; ID.IM-P6; ID.IM-P7; ID.IM-P8; ID.BE-P3; ID.RA-P1
Knowledge	K315	Knowledge of the set of organizational roles.	ID.IM-P2
Knowledge	K318	Knowledge of the structure of your organization's technology-related functions.	ID.IM-P1; ID.IM-P2; ID.IM-P3; ID.IM-P4; ID.IM-P5; ID.IM-P6; ID.IM-P7; ID.IM-P8
Knowledge	K328	Knowledge of third parties.	ID.IM-P2
Skill	S152	Skill in evaluating the quality of information received.	ID.IM-P1; ID.IM-P2; ID.IM-P3; ID.IM-P4; ID.IM-P5; ID.IM-P6; ID.IM-P7; ID.IM-P8
Skill	S168	Skill in identifying data elements that are legally defined terms.	ID.IM-P1; ID.IM-P2; ID.IM-P3; ID.IM-P4; ID.IM-P5; ID.IM-P6; ID.IM-P7; ID.IM-P8
Skill	S169	Skill in identifying data elements that are organization-defined terms or classifications.	ID.IM-P1; ID.IM-P2; ID.IM-P3; ID.IM-P4; ID.IM-P5; ID.IM-P6; ID.IM-P7; ID.IM-P8
Skill	S174	Skill in identifying owners and operators with respect to the systems/products/services and components that process data.	ID.IM-P2
Skill	S189	Skill in implementing inventory (and other data management system) options and tools.	ID.IM-P1; ID.IM-P2; ID.IM-P3; ID.IM-P4; ID.IM-P5; ID.IM-P6; ID.IM-P7; ID.IM-P8
Skill	S261	Skill in querying inventory management systems.	ID.IM-P1; ID.IM-P2; ID.IM-P3; ID.IM-P4; ID.IM-P5; ID.IM-P6; ID.IM-P7; ID.IM-P8
Skill	S264	Skill in reporting from inventory management systems.	ID.IM-P1; ID.IM-P2; ID.IM-P3; ID.IM-P4; ID.IM-P5; ID.IM-P6; ID.IM-P7; ID.IM-P8
Subcategory	**ID.IM-P3**	**Categories of individuals (e.g., customers, employees or prospective employees, consumers) whose data are being processed are inventoried.**	
Task	T158	Document categories of individuals whose data are being processed, including their role within a system/product/service.	ID.IM-P3
Task	T139	Determine what the data inventory will be used for.	ID.IM-P1; ID.IM-P2; ID.IM-P3; ID.IM-P4; ID.IM-P5; ID.IM-P6; ID.IM-P7
Task	T129	Determine the methodology for taking inventory of data.	ID.IM-P1; ID.IM-P2; ID.IM-P3; ID.IM-P4; ID.IM-P5; ID.IM-P6; ID.IM-P7
Task	T069	Define categories of individuals whose data are being processed.	ID.IM-P3
Task	T295	Select an inventory tool option.	ID.IM-P1; ID.IM-P2; ID.IM-P3; ID.IM-P4; ID.IM-P5; ID.IM-P6; ID.IM-P7
Task	T292	Select a system or data store for inventory information.	ID.IM-P1; ID.IM-P2; ID.IM-P3; ID.IM-P4; ID.IM-P5; ID.IM-P6; ID.IM-P7
Knowledge	K044	Knowledge of data elements that are legally defined terms.	ID.IM-P1; ID.IM-P2; ID.IM-P3; ID.IM-P4; ID.IM-P5; ID.IM-P6; ID.IM-P7; ID.IM-P8
Knowledge	K045	Knowledge of data elements that are organization-defined terms or classifications.	ID.IM-P1; ID.IM-P2; ID.IM-P3; ID.IM-P4; ID.IM-P5; ID.IM-P6; ID.IM-P7; ID.IM-P8
Knowledge	K064	Knowledge of document accessibility requirements.	ID.IM-P1; ID.IM-P2; ID.IM-P3; ID.IM-P4; ID.IM-P5; ID.IM-P6; ID.IM-P7; ID.IM-P8; CM.AW-P4

Statement Type	ID	Description	Subcategory Mapping
Knowledge	K084	Knowledge of inventory (and other data management system) options and tools.	ID.IM-P1; ID.IM-P2; ID.IM-P3; ID.IM-P4; ID.IM-P5; ID.IM-P6; ID.IM-P7; ID.IM-P8
Knowledge	K166	Knowledge of risk assessment and analysis systems.	ID.IM-P1; ID.IM-P2; ID.IM-P3; ID.IM-P4; ID.IM-P5; ID.IM-P6; ID.IM-P7; ID.IM-P8
Knowledge	K257	Knowledge of the organization's data processing.	ID.IM-P1; ID.IM-P2; ID.IM-P3; ID.IM-P4; ID.IM-P5; ID.IM-P6; ID.IM-P7; ID.IM-P8; CT.PO-P1; CT.PO-P2; CT.PO-P3; CT.PO-P4; CT.DM-P1; CT.DM-P2; CT.DM-P3; CT.DM-P4; CT.DM-P5; CT.DM-P6; CT.DM-P7; CT.DM-P8; CT.DM-P9; CT.DM-P10; CM.AW-P1; CM.AW-P2; CM.AW-P3; CM.AW-P4; CM.AW-P5; CM.AW-P6; CM.AW-P7; CM.AW-P8
Knowledge	K275	Knowledge of the organization's needs for information that can be provided from inventory and mapping.	ID.IM-P1; ID.IM-P2; ID.IM-P3; ID.IM-P4; ID.IM-P5; ID.IM-P6; ID.IM-P7; ID.IM-P8
Knowledge	K303	Knowledge of the organization's systems/products/services.	GV.MT-P1; ID.IM-P1; ID.IM-P2; ID.IM-P3; ID.IM-P4; ID.IM-P5; ID.IM-P6; ID.IM-P7; ID.IM-P8; ID.BE-P3; ID.RA-P1
Knowledge	K318	Knowledge of the structure of your organization's technology-related functions.	ID.IM-P1; ID.IM-P2; ID.IM-P3; ID.IM-P4; ID.IM-P5; ID.IM-P6; ID.IM-P7; ID.IM-P8
Skill	S121	Skill in developing taxonomies.	ID.IM-P3; ID.IM-P4; ID.IM-P5
Skill	S152	Skill in evaluating the quality of information received.	ID.IM-P1; ID.IM-P2; ID.IM-P3; ID.IM-P4; ID.IM-P5; ID.IM-P6; ID.IM-P7; ID.IM-P8
Skill	S168	Skill in identifying data elements that are legally defined terms.	ID.IM-P1; ID.IM-P2; ID.IM-P3; ID.IM-P4; ID.IM-P5; ID.IM-P6; ID.IM-P7; ID.IM-P8
Skill	S169	Skill in identifying data elements that are organization-defined terms or classifications.	ID.IM-P1; ID.IM-P2; ID.IM-P3; ID.IM-P4; ID.IM-P5; ID.IM-P6; ID.IM-P7; ID.IM-P8
Skill	S189	Skill in implementing inventory (and other data management system) options and tools.	ID.IM-P1; ID.IM-P2; ID.IM-P3; ID.IM-P4; ID.IM-P5; ID.IM-P6; ID.IM-P7; ID.IM-P8
Skill	S205	Skill in maintaining taxonomies.	ID.IM-P3; ID.IM-P4; ID.IM-P5
Skill	S261	Skill in querying inventory management systems.	ID.IM-P1; ID.IM-P2; ID.IM-P3; ID.IM-P4; ID.IM-P5; ID.IM-P6; ID.IM-P7; ID.IM-P8
Skill	S264	Skill in reporting from inventory management systems.	ID.IM-P1; ID.IM-P2; ID.IM-P3; ID.IM-P4; ID.IM-P5; ID.IM-P6; ID.IM-P7; ID.IM-P8
Subcategory	**ID.IM-P4**	**Data actions of the systems/products/services are inventoried.**	
Task	T124	Determine the level of granularity for illustrating or documenting data actions.	ID.IM-P4
Task	T129	Determine the methodology for taking inventory of data.	ID.IM-P1; ID.IM-P2; ID.IM-P3; ID.IM-P4; ID.IM-P5; ID.IM-P6; ID.IM-P7
Task	T139	Determine what the data inventory will be used for.	ID.IM-P1; ID.IM-P2; ID.IM-P3; ID.IM-P4; ID.IM-P5; ID.IM-P6; ID.IM-P7
Task	T160	Document data actions of systems/products/services.	ID.IM-P4
Task	T210	Examine system design documentation/artifacts.	ID.IM-P4
Task	T241	Identify the data actions of the systems/products/services.	ID.IM-P4

Statement Type	ID	Description	Subcategory Mapping
Task	T292	Select a system or data store for inventory information.	ID.IM-P1; ID.IM-P2; ID.IM-P3; ID.IM-P4; ID.IM-P5; ID.IM-P6; ID.IM-P7
Task	T295	Select an inventory tool option.	ID.IM-P1; ID.IM-P2; ID.IM-P3; ID.IM-P4; ID.IM-P5; ID.IM-P6; ID.IM-P7
Knowledge	K040	Knowledge of data actions of the systems/products/services.	ID.IM-P4
Knowledge	K044	Knowledge of data elements that are legally defined terms.	ID.IM-P1; ID.IM-P2; ID.IM-P3; ID.IM-P4; ID.IM-P5; ID.IM-P6; ID.IM-P7; ID.IM-P8
Knowledge	K045	Knowledge of data elements that are organization-defined terms or classifications.	ID.IM-P1; ID.IM-P2; ID.IM-P3; ID.IM-P4; ID.IM-P5; ID.IM-P6; ID.IM-P7; ID.IM-P8
Knowledge	K064	Knowledge of document accessibility requirements.	ID.IM-P1; ID.IM-P2; ID.IM-P3; ID.IM-P4; ID.IM-P5; ID.IM-P6; ID.IM-P7; ID.IM-P8; CM.AW-P4
Knowledge	K084	Knowledge of inventory (and other data management system) options and tools.	ID.IM-P1; ID.IM-P2; ID.IM-P3; ID.IM-P4; ID.IM-P5; ID.IM-P6; ID.IM-P7; ID.IM-P8
Knowledge	K160	Knowledge of requirements related to data actions.	ID.IM-P4
Knowledge	K166	Knowledge of risk assessment and analysis systems.	ID.IM-P1; ID.IM-P2; ID.IM-P3; ID.IM-P4; ID.IM-P5; ID.IM-P6; ID.IM-P7; ID.IM-P8
Knowledge	K186	Knowledge of system design documentation/artifacts.	ID.IM-P4; ID.IM-P8
Knowledge	K192	Knowledge of system/product/service data life cycle operations.	ID.IM-P4
Knowledge	K257	Knowledge of the organization's data processing.	ID.IM-P1; ID.IM-P2; ID.IM-P3; ID.IM-P4; ID.IM-P5; ID.IM-P6; ID.IM-P7; ID.IM-P8; CT.PO-P1; CT.PO-P2; CT.PO-P3; CT.PO-P4; CT.DM-P1; CT.DM-P2; CT.DM-P3; CT.DM-P4; CT.DM-P5; CT.DM-P6; CT.DM-P7; CT.DM-P8; CT.DM-P9; CT.DM-P10; CM.AW-P1; CM.AW-P2; CM.AW-P3; CM.AW-P4; CM.AW-P5; CM.AW-P6; CM.AW-P7; CM.AW-P8
Knowledge	K275	Knowledge of the organization's needs for information that can be provided from inventory and mapping.	ID.IM-P1; ID.IM-P2; ID.IM-P3; ID.IM-P4; ID.IM-P5; ID.IM-P6; ID.IM-P7; ID.IM-P8
Knowledge	K303	Knowledge of the organization's systems/products/services.	GV.MT-P1; ID.IM-P1; ID.IM-P2; ID.IM-P3; ID.IM-P4; ID.IM-P5; ID.IM-P6; ID.IM-P7; ID.IM-P8; ID.BE-P3; ID.RA-P1
Knowledge	K318	Knowledge of the structure of your organization's technology-related functions.	ID.IM-P1; ID.IM-P2; ID.IM-P3; ID.IM-P4; ID.IM-P5; ID.IM-P6; ID.IM-P7; ID.IM-P8
Skill	S121	Skill in developing taxonomies.	ID.IM-P3; ID.IM-P4; ID.IM-P5
Skill	S152	Skill in evaluating the quality of information received.	ID.IM-P1; ID.IM-P2; ID.IM-P3; ID.IM-P4; ID.IM-P5; ID.IM-P6; ID.IM-P7; ID.IM-P8
Skill	S168	Skill in identifying data elements that are legally defined terms.	ID.IM-P1; ID.IM-P2; ID.IM-P3; ID.IM-P4; ID.IM-P5; ID.IM-P6; ID.IM-P7; ID.IM-P8
Skill	S169	Skill in identifying data elements that are organization-defined terms or classifications.	ID.IM-P1; ID.IM-P2; ID.IM-P3; ID.IM-P4; ID.IM-P5; ID.IM-P6; ID.IM-P7; ID.IM-P8
Skill	S189	Skill in implementing inventory (and other data management system) options and tools.	ID.IM-P1; ID.IM-P2; ID.IM-P3; ID.IM-P4; ID.IM-P5; ID.IM-P6; ID.IM-P7; ID.IM-P8
Skill	S205	Skill in maintaining taxonomies.	ID.IM-P3; ID.IM-P4; ID.IM-P5

Statement Type	ID	Description	Subcategory Mapping
Skill	S261	Skill in querying inventory management systems.	ID.IM-P1; ID.IM-P2; ID.IM-P3; ID.IM-P4; ID.IM-P5; ID.IM-P6; ID.IM-P7; ID.IM-P8
Skill	S264	Skill in reporting from inventory management systems.	ID.IM-P1; ID.IM-P2; ID.IM-P3; ID.IM-P4; ID.IM-P5; ID.IM-P6; ID.IM-P7; ID.IM-P8
Skill	S268	Skill in reviewing and interpreting system design documentation/artifacts to identify data actions.	ID.IM-P4
Subcategory	**ID.IM-P5**	**The purposes for the data actions are inventoried.**	
Task	T129	Determine the methodology for taking inventory of data.	ID.IM-P1; ID.IM-P2; ID.IM-P3; ID.IM-P4; ID.IM-P5; ID.IM-P6; ID.IM-P7
Task	T139	Determine what the data inventory will be used for.	ID.IM-P1; ID.IM-P2; ID.IM-P3; ID.IM-P4; ID.IM-P5; ID.IM-P6; ID.IM-P7
Task	T159	Document categories of the purposes for the data actions of systems/products/services.	ID.IM-P5
Task	T219	Identify categories of purposes for the data actions of systems/products/services.	ID.IM-P5
Task	T292	Select a system or data store for inventory information.	ID.IM-P1; ID.IM-P2; ID.IM-P3; ID.IM-P4; ID.IM-P5; ID.IM-P6; ID.IM-P7
Task	T295	Select an inventory tool option.	ID.IM-P1; ID.IM-P2; ID.IM-P3; ID.IM-P4; ID.IM-P5; ID.IM-P6; ID.IM-P7
Knowledge	K022	Knowledge of categories of purposes for data actions.	ID.IM-P5
Knowledge	K044	Knowledge of data elements that are legally defined terms.	ID.IM-P1; ID.IM-P2; ID.IM-P3; ID.IM-P4; ID.IM-P5; ID.IM-P6; ID.IM-P7; ID.IM-P8
Knowledge	K045	Knowledge of data elements that are organization-defined terms or classifications.	ID.IM-P1; ID.IM-P2; ID.IM-P3; ID.IM-P4; ID.IM-P5; ID.IM-P6; ID.IM-P7; ID.IM-P8
Knowledge	K064	Knowledge of document accessibility requirements.	ID.IM-P1; ID.IM-P2; ID.IM-P3; ID.IM-P4; ID.IM-P5; ID.IM-P6; ID.IM-P7; ID.IM-P8; CM.AW-P4
Knowledge	K084	Knowledge of inventory (and other data management system) options and tools.	ID.IM-P1; ID.IM-P2; ID.IM-P3; ID.IM-P4; ID.IM-P5; ID.IM-P6; ID.IM-P7; ID.IM-P8
Knowledge	K161	Knowledge of requirements related to purposes for data actions.	ID.IM-P5
Knowledge	K166	Knowledge of risk assessment and analysis systems.	ID.IM-P1; ID.IM-P2; ID.IM-P3; ID.IM-P4; ID.IM-P5; ID.IM-P6; ID.IM-P7; ID.IM-P8
Knowledge	K257	Knowledge of the organization's data processing.	ID.IM-P1; ID.IM-P2; ID.IM-P3; ID.IM-P4; ID.IM-P5; ID.IM-P6; ID.IM-P7; ID.IM-P8; CT.PO-P1; CT.PO-P2; CT.PO-P3; CT.PO-P4; CT.DM-P1; CT.DM-P2; CT.DM-P3; CT.DM-P4; CT.DM-P5; CT.DM-P6; CT.DM-P7; CT.DM-P8; CT.DM-P9; CT.DM-P10; CM.AW-P1; CM.AW-P2; CM.AW-P3; CM.AW-P4; CM.AW-P5; CM.AW-P6; CM.AW-P7; CM.AW-P8
Knowledge	K275	Knowledge of the organization's needs for information that can be provided from inventory and mapping.	ID.IM-P1; ID.IM-P2; ID.IM-P3; ID.IM-P4; ID.IM-P5; ID.IM-P6; ID.IM-P7; ID.IM-P8
Knowledge	K303	Knowledge of the organization's systems/products/services.	GV.MT-P1; ID.IM-P1; ID.IM-P2; ID.IM-P3; ID.IM-P4; ID.IM-P5; ID.IM-P6; ID.IM-P7; ID.IM-P8; ID.BE-P3; ID.RA-P1
Knowledge	K318	Knowledge of the structure of your organization's technology-related functions.	ID.IM-P1; ID.IM-P2; ID.IM-P3; ID.IM-P4; ID.IM-P5; ID.IM-P6; ID.IM-P7; ID.IM-P8

Statement Type	ID	Description	Subcategory Mapping
Skill	S121	Skill in developing taxonomies.	ID.IM-P3; ID.IM-P4; ID.IM-P5
Skill	S152	Skill in evaluating the quality of information received.	ID.IM-P1; ID.IM-P2; ID.IM-P3; ID.IM-P4; ID.IM-P5; ID.IM-P6; ID.IM-P7; ID.IM-P8
Skill	S168	Skill in identifying data elements that are legally defined terms.	ID.IM-P1; ID.IM-P2; ID.IM-P3; ID.IM-P4; ID.IM-P5; ID.IM-P6; ID.IM-P7; ID.IM-P8
Skill	S169	Skill in identifying data elements that are organization-defined terms or classifications.	ID.IM-P1; ID.IM-P2; ID.IM-P3; ID.IM-P4; ID.IM-P5; ID.IM-P6; ID.IM-P7; ID.IM-P8
Skill	S189	Skill in implementing inventory (and other data management system) options and tools.	ID.IM-P1; ID.IM-P2; ID.IM-P3; ID.IM-P4; ID.IM-P5; ID.IM-P6; ID.IM-P7; ID.IM-P8
Skill	S205	Skill in maintaining taxonomies.	ID.IM-P3; ID.IM-P4; ID.IM-P5
Skill	S261	Skill in querying inventory management systems.	ID.IM-P1; ID.IM-P2; ID.IM-P3; ID.IM-P4; ID.IM-P5; ID.IM-P6; ID.IM-P7; ID.IM-P8
Skill	S264	Skill in reporting from inventory management systems.	ID.IM-P1; ID.IM-P2; ID.IM-P3; ID.IM-P4; ID.IM-P5; ID.IM-P6; ID.IM-P7; ID.IM-P8
Subcategory	**ID.IM-P6**	**Data elements within the data actions are inventoried.**	
Task	T029	Classify data elements with their risk classification in context.	ID.IM-P6
Task	T129	Determine the methodology for taking inventory of data.	ID.IM-P1; ID.IM-P2; ID.IM-P3; ID.IM-P4; ID.IM-P5; ID.IM-P6; ID.IM-P7
Task	T139	Determine what the data inventory will be used for.	ID.IM-P1; ID.IM-P2; ID.IM-P3; ID.IM-P4; ID.IM-P5; ID.IM-P6; ID.IM-P7
Task	T156	Document categories of data elements within the data actions of systems/products/services.	ID.IM-P6
Task	T161	Document data elements that can be used to identify data subjects (i.e., direct and indirect identifiers).	ID.IM-P6
Task	T218	Identify categories of data elements within the data actions of systems/products/services.	ID.IM-P6
Task	T292	Select a system or data store for inventory information.	ID.IM-P1; ID.IM-P2; ID.IM-P3; ID.IM-P4; ID.IM-P5; ID.IM-P6; ID.IM-P7
Task	T295	Select an inventory tool option.	ID.IM-P1; ID.IM-P2; ID.IM-P3; ID.IM-P4; ID.IM-P5; ID.IM-P6; ID.IM-P7
Knowledge	K044	Knowledge of data elements that are legally defined terms.	ID.IM-P1; ID.IM-P2; ID.IM-P3; ID.IM-P4; ID.IM-P5; ID.IM-P6; ID.IM-P7; ID.IM-P8
Knowledge	K045	Knowledge of data elements that are organization-defined terms or classifications.	ID.IM-P1; ID.IM-P2; ID.IM-P3; ID.IM-P4; ID.IM-P5; ID.IM-P6; ID.IM-P7; ID.IM-P8
Knowledge	K059	Knowledge of databases.	ID.IM-P6
Knowledge	K062	Knowledge of definitions of direct and indirect identifiers.	ID.IM-P6
Knowledge	K064	Knowledge of document accessibility requirements.	ID.IM-P1; ID.IM-P2; ID.IM-P3; ID.IM-P4; ID.IM-P5; ID.IM-P6; ID.IM-P7; ID.IM-P8; CM.AW-P4
Knowledge	K078	Knowledge of guidance and resources on identifiers.	ID.IM-P6
Knowledge	K084	Knowledge of inventory (and other data management system) options and tools.	ID.IM-P1; ID.IM-P2; ID.IM-P3; ID.IM-P4; ID.IM-P5; ID.IM-P6; ID.IM-P7; ID.IM-P8
Knowledge	K152	Knowledge of re-identification techniques research.	ID.IM-P6
Knowledge	K166	Knowledge of risk assessment and analysis systems.	ID.IM-P1; ID.IM-P2; ID.IM-P3; ID.IM-P4; ID.IM-P5; ID.IM-P6; ID.IM-P7; ID.IM-P8
Knowledge	K222	Knowledge of the difference between structured and unstructured data.	ID.IM-P6

Statement Type	ID	Description	Subcategory Mapping
Knowledge	K257	Knowledge of the organization's data processing.	ID.IM-P1; ID.IM-P2; ID.IM-P3; ID.IM-P4; ID.IM-P5; ID.IM-P6; ID.IM-P7; ID.IM-P8; CT.PO-P1; CT.PO-P2; CT.PO-P3; CT.PO-P4; CT.DM-P1; CT.DM-P2; CT.DM-P3; CT.DM-P4; CT.DM-P5; CT.DM-P6; CT.DM-P7; CT.DM-P8; CT.DM-P9; CT.DM-P10; CM.AW-P1; CM.AW-P2; CM.AW-P3; CM.AW-P4; CM.AW-P5; CM.AW-P6; CM.AW-P7; CM.AW-P8
Knowledge	K275	Knowledge of the organization's needs for information that can be provided from inventory and mapping.	ID.IM-P1; ID.IM-P2; ID.IM-P3; ID.IM-P4; ID.IM-P5; ID.IM-P6; ID.IM-P7; ID.IM-P8
Knowledge	K303	Knowledge of the organization's systems/products/services.	GV.MT-P1; ID.IM-P1; ID.IM-P2; ID.IM-P3; ID.IM-P4; ID.IM-P5; ID.IM-P6; ID.IM-P7; ID.IM-P8; ID.BE-P3; ID.RA-P1
Knowledge	K318	Knowledge of the structure of your organization's technology-related functions.	ID.IM-P1; ID.IM-P2; ID.IM-P3; ID.IM-P4; ID.IM-P5; ID.IM-P6; ID.IM-P7; ID.IM-P8
Knowledge	K332	Knowledge of types of data elements.	ID.IM-P6
Skill	S075	Skill in classifying data.	ID.IM-P6
Skill	S152	Skill in evaluating the quality of information received.	ID.IM-P1; ID.IM-P2; ID.IM-P3; ID.IM-P4; ID.IM-P5; ID.IM-P6; ID.IM-P7; ID.IM-P8
Skill	S159	Skill in explaining recent documented exploits or attacks to technical and non-technical staff, to facilitate classification of data elements as direct or indirect identifiers.	ID.IM-P6
Skill	S168	Skill in identifying data elements that are legally defined terms.	ID.IM-P1; ID.IM-P2; ID.IM-P3; ID.IM-P4; ID.IM-P5; ID.IM-P6; ID.IM-P7; ID.IM-P8
Skill	S169	Skill in identifying data elements that are organization-defined terms or classifications.	ID.IM-P1; ID.IM-P2; ID.IM-P3; ID.IM-P4; ID.IM-P5; ID.IM-P6; ID.IM-P7; ID.IM-P8
Skill	S189	Skill in implementing inventory (and other data management system) options and tools.	ID.IM-P1; ID.IM-P2; ID.IM-P3; ID.IM-P4; ID.IM-P5; ID.IM-P6; ID.IM-P7; ID.IM-P8
Skill	S261	Skill in querying inventory management systems.	ID.IM-P1; ID.IM-P2; ID.IM-P3; ID.IM-P4; ID.IM-P5; ID.IM-P6; ID.IM-P7; ID.IM-P8
Skill	S264	Skill in reporting from inventory management systems.	ID.IM-P1; ID.IM-P2; ID.IM-P3; ID.IM-P4; ID.IM-P5; ID.IM-P6; ID.IM-P7; ID.IM-P8
Skill	S267	Skill in retrieving information on data elements from databases, unstructured data stores, and other stores of data.	ID.IM-P6
Subcategory	**ID.IM-P7**	**The data processing environment is identified (e.g., geographic location, internal, cloud, third parties).**	
Task	T068	Define categories of data processing environments.	ID.IM-P7
Task	T129	Determine the methodology for taking inventory of data.	ID.IM-P1; ID.IM-P2; ID.IM-P3; ID.IM-P4; ID.IM-P5; ID.IM-P6; ID.IM-P7
Task	T139	Determine what the data inventory will be used for.	ID.IM-P1; ID.IM-P2; ID.IM-P3; ID.IM-P4; ID.IM-P5; ID.IM-P6; ID.IM-P7
Task	T157	Document categories of data processing environments.	ID.IM-P7
Task	T292	Select a system or data store for inventory information.	ID.IM-P1; ID.IM-P2; ID.IM-P3; ID.IM-P4; ID.IM-P5; ID.IM-P6; ID.IM-P7

Statement Type	ID	Description	Subcategory Mapping
Task	T295	Select an inventory tool option.	ID.IM-P1; ID.IM-P2; ID.IM-P3; ID.IM-P4; ID.IM-P5; ID.IM-P6; ID.IM-P7
Knowledge	K044	Knowledge of data elements that are legally defined terms.	ID.IM-P1; ID.IM-P2; ID.IM-P3; ID.IM-P4; ID.IM-P5; ID.IM-P6; ID.IM-P7; ID.IM-P8
Knowledge	K045	Knowledge of data elements that are organization-defined terms or classifications.	ID.IM-P1; ID.IM-P2; ID.IM-P3; ID.IM-P4; ID.IM-P5; ID.IM-P6; ID.IM-P7; ID.IM-P8
Knowledge	K054	Knowledge of data processing environments.	ID.IM-P7; ID.DE-P2
Knowledge	K064	Knowledge of document accessibility requirements.	ID.IM-P1; ID.IM-P2; ID.IM-P3; ID.IM-P4; ID.IM-P5; ID.IM-P6; ID.IM-P7; ID.IM-P8; CM.AW-P4
Knowledge	K065	Knowledge of documentation related to the organization’s data processing environment.	ID.IM-P7
Knowledge	K084	Knowledge of inventory (and other data management system) options and tools.	ID.IM-P1; ID.IM-P2; ID.IM-P3; ID.IM-P4; ID.IM-P5; ID.IM-P6; ID.IM-P7; ID.IM-P8
Knowledge	K166	Knowledge of risk assessment and analysis systems.	ID.IM-P1; ID.IM-P2; ID.IM-P3; ID.IM-P4; ID.IM-P5; ID.IM-P6; ID.IM-P7; ID.IM-P8
Knowledge	K244	Knowledge of the organization's components.	ID.IM-P2; ID.IM-P7; ID.IM-P8; ID.BE-P1; ID.BE-P2; ID.BE P3
Knowledge	K257	Knowledge of the organization's data processing.	ID.IM-P1; ID.IM-P2; ID.IM-P3; ID.IM-P4; ID.IM-P5; ID.IM-P6; ID.IM-P7; ID.IM-P8; CT.PO-P1; CT.PO-P2; CT.PO-P3; CT.PO-P4; CT.DM-P1; CT.DM-P2; CT.DM-P3; CT.DM-P4; CT.DM-P5; CT.DM-P6; CT.DM-P7; CT.DM-P8; CT.DM-P9; CT.DM-P10; CM.AW-P1; CM.AW-P2; CM.AW-P3; CM.AW-P4; CM.AW-P5; CM.AW-P6; CM.AW-P7; CM.AW-P8
Knowledge	K275	Knowledge of the organization's needs for information that can be provided from inventory and mapping.	ID.IM-P1; ID.IM-P2; ID.IM-P3; ID.IM-P4; ID.IM-P5; ID.IM-P6; ID.IM-P7; ID.IM-P8
Knowledge	K303	Knowledge of the organization's systems/products/services.	GV.MT-P1; ID.IM-P1; ID.IM-P2; ID.IM-P3; ID.IM-P4; ID.IM-P5; ID.IM-P6; ID.IM-P7; ID.IM-P8; ID.BE-P3; ID.RA-P1
Knowledge	K318	Knowledge of the structure of your organization's technology-related functions.	ID.IM-P1; ID.IM-P2; ID.IM-P3; ID.IM-P4; ID.IM-P5; ID.IM-P6; ID.IM-P7; ID.IM-P8
Skill	S152	Skill in evaluating the quality of information received.	ID.IM-P1; ID.IM-P2; ID.IM-P3; ID.IM-P4; ID.IM-P5; ID.IM-P6; ID.IM-P7; ID.IM-P8
Skill	S168	Skill in identifying data elements that are legally defined terms.	ID.IM-P1; ID.IM-P2; ID.IM-P3; ID.IM-P4; ID.IM-P5; ID.IM-P6; ID.IM-P7; ID.IM-P8
Skill	S169	Skill in identifying data elements that are organization-defined terms or classifications.	ID.IM-P1; ID.IM-P2; ID.IM-P3; ID.IM-P4; ID.IM-P5; ID.IM-P6; ID.IM-P7; ID.IM-P8
Skill	S189	Skill in implementing inventory (and other data management system) options and tools.	ID.IM-P1; ID.IM-P2; ID.IM-P3; ID.IM-P4; ID.IM-P5; ID.IM-P6; ID.IM-P7; ID.IM-P8
Skill	S261	Skill in querying inventory management systems.	ID.IM-P1; ID.IM-P2; ID.IM-P3; ID.IM-P4; ID.IM-P5; ID.IM-P6; ID.IM-P7; ID.IM-P8
Skill	S264	Skill in reporting from inventory management systems.	ID.IM-P1; ID.IM-P2; ID.IM-P3; ID.IM-P4; ID.IM-P5; ID.IM-P6; ID.IM-P7; ID.IM-P8

Statement Type	ID	Description	Subcategory Mapping
Subcategory	**ID.IM-P8**	**Data processing is mapped, illustrating the data actions and associated data elements for systems/products/services, including components; roles of the component owners/operators; and interactions of individuals or third parties with the systems/products/services.**	
Task	T009	Apply the data map model to all data processing activities of systems/products/services.	ID.IM-P8
Task	T033	Create a data map model.	ID.IM-P8
Task	T128	Determine the methodology for data mapping, including level of granularity/detail.	ID.IM-P8
Task	T138	Determine what system design artifacts should support the data mapping.	ID.IM-P8
Task	T140	Determine what the data map(s) will be used for.	ID.IM-P8
Task	T267	Interpret system design documentation/artifacts.	ID.IM-P8
Task	T293	Select a system or data store for mapping information.	ID.IM-P8
Knowledge	K044	Knowledge of data elements that are legally defined terms.	ID.IM-P1; ID.IM-P2; ID.IM-P3; ID.IM-P4; ID.IM-P5; ID.IM-P6; ID.IM-P7; ID.IM-P8
Knowledge	K045	Knowledge of data elements that are organization-defined terms or classifications.	ID.IM-P1; ID.IM-P2; ID.IM-P3; ID.IM-P4; ID.IM-P5; ID.IM-P6; ID.IM-P7; ID.IM-P8
Knowledge	K046	Knowledge of data flow mapping.	ID.IM-P8
Knowledge	K064	Knowledge of document accessibility requirements.	ID.IM-P1; ID.IM-P2; ID.IM-P3; ID.IM-P4; ID.IM-P5; ID.IM-P6; ID.IM-P7; ID.IM-P8; CM.AW-P4
Knowledge	K069	Knowledge of entity relationship diagramming.	ID.IM-P8
Knowledge	K084	Knowledge of inventory (and other data management system) options and tools.	ID.IM-P1; ID.IM-P2; ID.IM-P3; ID.IM-P4; ID.IM-P5; ID.IM-P6; ID.IM-P7; ID.IM-P8
Knowledge	K166	Knowledge of risk assessment and analysis systems.	ID.IM-P1; ID.IM-P2; ID.IM-P3; ID.IM-P4; ID.IM-P5; ID.IM-P6; ID.IM-P7; ID.IM-P8
Knowledge	K186	Knowledge of system design documentation/artifacts.	ID.IM-P4; ID.IM-P8
Knowledge	K244	Knowledge of the organization's components.	ID.IM-P2; ID.IM-P7; ID.IM-P8; ID.BE-P1; ID.BE-P2; ID.BE P3
Knowledge	K257	Knowledge of the organization's data processing.	ID.IM-P1; ID.IM-P2; ID.IM-P3; ID.IM-P4; ID.IM-P5; ID.IM-P6; ID.IM-P7; ID.IM-P8; CT.PO-P1; CT.PO-P2; CT.PO-P3; CT.PO-P4; CT.DM-P1; CT.DM-P2; CT.DM-P3; CT.DM-P4; CT.DM-P5; CT.DM-P6; CT.DM-P7; CT.DM-P8; CT.DM-P9; CT.DM-P10; CM.AW-P1; CM.AW-P2; CM.AW-P3; CM.AW-P4; CM.AW-P5; CM.AW-P6; CM.AW-P7; CM.AW-P8
Knowledge	K275	Knowledge of the organization's needs for information that can be provided from inventory and mapping.	ID.IM-P1; ID.IM-P2; ID.IM-P3; ID.IM-P4; ID.IM-P5; ID.IM-P6; ID.IM-P7; ID.IM-P8
Knowledge	K303	Knowledge of the organization's systems/products/services.	GV.MT-P1; ID.IM-P1; ID.IM-P2; ID.IM-P3; ID.IM-P4; ID.IM-P5; ID.IM-P6; ID.IM-P7; ID.IM-P8; ID.BE-P3; ID.RA-P1
Knowledge	K310	Knowledge of the relationship among data inventory elements (i.e., ID.IM-P1 - P7) and how they apply to the creation of data maps.	ID.IM-P8
Knowledge	K318	Knowledge of the structure of your organization's technology-related functions.	ID.IM-P1; ID.IM-P2; ID.IM-P3; ID.IM-P4; ID.IM-P5; ID.IM-P6; ID.IM-P7; ID.IM-P8
Skill	S152	Skill in evaluating the quality of information received.	ID.IM-P1; ID.IM-P2; ID.IM-P3; ID.IM-P4; ID.IM-P5; ID.IM-P6; ID.IM-P7; ID.IM-P8

Statement Type	ID	Description	Subcategory Mapping
Skill	S168	Skill in identifying data elements that are legally defined terms.	ID.IM-P1; ID.IM-P2; ID.IM-P3; ID.IM-P4; ID.IM-P5; ID.IM-P6; ID.IM-P7; ID.IM-P8
Skill	S169	Skill in identifying data elements that are organization-defined terms or classifications.	ID.IM-P1; ID.IM-P2; ID.IM-P3; ID.IM-P4; ID.IM-P5; ID.IM-P6; ID.IM-P7; ID.IM-P8
Skill	S189	Skill in implementing inventory (and other data management system) options and tools.	ID.IM-P1; ID.IM-P2; ID.IM-P3; ID.IM-P4; ID.IM-P5; ID.IM-P6; ID.IM-P7; ID.IM-P8
Skill	S201	Skill in interpreting system design documentation/artifacts.	ID.IM-P8
Skill	S218	Skill in mapping data flows.	ID.IM-P8
Skill	S219	Skill in mapping entity relationships.	ID.IM-P8
Skill	S223	Skill in mapping processes.	ID.IM-P8
Skill	S261	Skill in querying inventory management systems.	ID.IM-P1; ID.IM-P2; ID.IM-P3; ID.IM-P4; ID.IM-P5; ID.IM-P6; ID.IM-P7; ID.IM-P8
Skill	S264	Skill in reporting from inventory management systems.	ID.IM-P1; ID.IM-P2; ID.IM-P3; ID.IM-P4; ID.IM-P5; ID.IM-P6; ID.IM-P7; ID.IM-P8
Subcategory	**ID.BE-P1**	**The organization’s role(s) in the data processing ecosystem are identified and communicated.**	
Task	T047	Create a process for exchanging information relevant to the organization’s role(s) in the data processing ecosystem.	ID.BE-P1
Task	T133	Determine the organization's non-regulation-defined role(s) in the data processing ecosystem.	ID.BE-P1; GV.RM-P3
Task	T134	Determine the organization's regulation-defined role(s) in the data processing ecosystem.	ID.BE-P1; GV.RM-P3
Task	T265	Inform [*organization-defined stakeholders*] of the organization's role(s) in the data processing ecosystem following the applicable process(es).	ID.BE-P1
Knowledge	K002	Knowledge of [*organization-defined stakeholders*] that need to understand the organization's role(s) in the data processing ecosystem.	ID.BE-P1
Knowledge	K066	Knowledge of effective strategies for communicating with [*organization-defined stakeholders*].	ID.BE-P1
Knowledge	K072	Knowledge of external party expectations regarding the organization's role(s).	ID.BE-P1
Knowledge	K153	Knowledge of relationship dynamics with relevant external parties.	ID.BE-P1
Knowledge	K163	Knowledge of resources required for risk management.	ID.BE-P1; ID.BE-P2; ID.BE-P3; GV.RM-P1; GV.RM-P2; GV.RM-P3
Knowledge	K218	Knowledge of the data assets.	ID.BE-P1
Knowledge	K244	Knowledge of the organization's components.	ID.IM-P2; ID.IM-P7; ID.IM-P8; ID.BE-P1; ID.BE-P2; ID.BE P3
Knowledge	K254	Knowledge of the organization's data processing ecosystem.	ID.BE-P1; ID.DE-P1; ID.DE-P2; ID.DE-P3; ID.DE-P4; ID.DE-P5; CT.PO-P1; CT.PO-P2; CT.PO-P3; CT.PO-P4; CM.AW-P1; CM.AW-P2; CM.AW-P3; CM.AW-P4; CM.AW-P5; CM.AW-P6; CM.AW-P7; CM.AW-P8
Knowledge	K262	Knowledge of the organization's external products and services that use personal data.	ID.BE-P1
Knowledge	K276	Knowledge of the organization's operations, including associated revenue streams if applicable.	ID.BE-P1
Knowledge	K299	Knowledge of the organization's structure.	ID.BE-P1
Skill	S034	Skill in applying the organization's privacy policies to match its role(s) in the data processing ecosystem with its data processing.	ID.BE-P1
Skill	S054	Skill in assessing the impact of changes to organizational operations on its role(s) in the data processing ecosystem.	ID.BE-P1

Statement Type	ID	Description	Subcategory Mapping
Skill	S076	Skill in communicating [*organization-defined stakeholder*] expectations.	ID.BE-P1
Skill	S079	Skill in communicating privacy legal requirements/principles to [*organization-defined stakeholders*] and decision-makers.	ID.BE-P1; GV.MT-P2; GV.MT-P3; GV.MT-P4; GV.MT-P5; GV.MT-P7
Skill	S083	Skill in conducting exploratory or investigative activities.	ID.BE-P1
Skill	S142	Skill in evaluating how privacy laws and regulations apply to the organization's data processing goals.	ID.BE-P1
Skill	S144	Skill in evaluating how privacy standards and best practices apply to the organization's data processing goals.	ID.BE-P1
Skill	S217	Skill in managing stakeholder expectations.	ID.BE-P1
Skill	S242	Skill in performing a data discovery exercise manually or via tool(s) for digital and non-digital data.	ID.BE-P1
Skill	S251	Skill in performing analysis of the organization's role(s) under applicable privacy laws and regulations.	ID.BE-P1
Subcategory	**ID.BE-P2**	**Priorities for organizational mission, objectives, and activities are established and communicated.**	
Notes: Organizations may choose to evaluate existing priorities for gaps (e.g., incompleteness, outdated information) and determine necessary actions to address identified gaps.			
Task	T004	Align mission/objectives/activities with [*organization-defined stakeholder*] priorities.	ID.BE-P2
Task	T005	Align priorities for mission/objectives/activities with privacy risk management decisions.	ID.BE-P2
Task	T006	Align priorities for mission/objectives/activities with privacy role(s) and responsibilities.	ID.BE-P2
Task	T015	Assess internal and external stakeholder priorities.	ID.BE-P2
Task	T045	Create a process for communicating priorities for mission/objectives/activities.	ID.BE-P2
Task	T049	Create a process for prioritizing mission/objectives/activities.	ID.BE-P2
Task	T234	Identify priorities for mission/objectives/activities.	ID.BE-P2
Task	T264	Inform [*organization-defined stakeholders*] of priorities for organizational mission/objectives/activities, following the applicable process(es).	ID.BE-P2
Knowledge	K003	Knowledge of [*organization-defined stakeholders*] to whom priorities for mission/objectives/activities must be communicated.	ID.BE-P2
Knowledge	K163	Knowledge of resources required for risk management.	ID.BE-P1; ID.BE-P2; ID.BE-P3; GV.RM-P1; GV.RM-P2; GV.RM-P3
Knowledge	K241	Knowledge of the organization's budget approval process.	ID.BE-P2
Knowledge	K244	Knowledge of the organization's components.	ID.IM-P2; ID.IM-P7; ID.IM-P8; ID.BE-P1; ID.BE-P2; ID.BE P3
Knowledge	K261	Knowledge of the organization's expansion or consolidation plans.	ID.BE-P2; GV.RM-P1; GV.RM-P2; GV.RM-P3
Knowledge	K264	Knowledge of the organization's future roadmap.	ID.BE-P2; GV.RM-P1; GV.RM-P2; GV.RM-P3
Knowledge	K274	Knowledge of the organization's mission/objectives/activities.	ID.BE-P2
Knowledge	K286	Knowledge of the organization's privacy risk management decisions.	ID.BE-P2
Knowledge	K288	Knowledge of the organization's privacy risks.	ID.BE-P2; ID.BE-P3
Knowledge	K290	Knowledge of the organization's privacy roles and responsibilities.	ID.BE-P2
Skill	S009	Skill in advocating for privacy program resources and prioritization.	ID.BE-P2
Skill	S027	Skill in applying privacy requirements to prioritize organizational mission/objectives/activities.	ID.BE-P2
Skill	S078	Skill in communicating privacy benefits and risks to the organization's mission/objectives/activities.	ID.BE-P2
Skill	S177	Skill in identifying requirements in privacy laws and regulations.	ID.BE-P2
Skill	S241	Skill in organizing stakeholder priorities.	ID.BE-P2
Skill	S256	Skill in prioritizing organizational mission/objectives/activities.	ID.BE-P2
Skill	S282	Skill in soliciting information from organizational stakeholders using a variety of communication methods.	ID.BE-P2
Skill	S294	Skill in translating privacy benefits and risks to the organization's mission/objectives/activities.	ID.BE-P2

Statement Type	ID	Description	Subcategory Mapping
Subcategory	**ID.BE-P3**	**Systems/products/services that support organizational priorities are identified and key requirements communicated.**	
Task	T046	Create a process for communicating the organization's priorities and key requirements for each system/product/service.	ID.BE-P3
Task	T097	Determine inventoried systems/products/services that support organizational priorities and key requirements.	ID.BE-P3
Task	T107	Determine requirements for each system/product/service, based on organizational priorities and privacy laws and regulations.	ID.BE-P3
Task	T266	Inform applicable system/product/service owners and operators of key requirements and organizational priorities, according to established process(es).	ID.BE-P3
Task	T305	Train system/product/service owners and operators on key requirements and organizational priorities.	ID.BE-P3
Knowledge	K028	Knowledge of communications planning.	ID.BE-P3
Knowledge	K106	Knowledge of non-legal requirements.	ID.BE-P3
Knowledge	K119	Knowledge of owners and operators of systems/products/services.	ID.BE-P3
Knowledge	K146	Knowledge of privacy-related artifacts.	ID.BE-P3
Knowledge	K163	Knowledge of resources required for risk management.	ID.BE-P1; ID.BE-P2; ID.BE-P3; GV.RM-P1; GV.RM-P2; GV.RM-P3
Knowledge	K178	Knowledge of stakeholder management practices.	ID.BE-P3
Knowledge	K193	Knowledge of system/product/service inventories.	ID.BE-P3
Knowledge	K244	Knowledge of the organization's components.	ID.IM-P2; ID.IM-P7; ID.IM-P8; ID.BE-P1; ID.BE-P2; ID.BE P3
Knowledge	K288	Knowledge of the organization's privacy risks.	ID.BE-P2; ID.BE-P3
Knowledge	K297	Knowledge of the organization's risk tolerance.	ID.BE-P3; ID.RA-P5; ID.DE-P3; GV.RM-P3; GV.MT-P1
Knowledge	K303	Knowledge of the organization's systems/products/services.	GV.MT-P1; ID.IM-P1; ID.IM-P2; ID.IM-P3; ID.IM-P4; ID.IM-P5; ID.IM-P6; ID.IM-P7; ID.IM-P8; ID.BE-P3; ID.RA-P1
Knowledge	K344	Knowledge of where the organization keeps inventories of systems/products/services.	ID.BE-P3
Skill	S011	Skill in advocating for stakeholder action.	ID.BE-P3
Skill	S052	Skill in assessing system/product/service support for organizational priorities.	ID.BE-P3
Skill	S089	Skill in crafting effective communications plans.	ID.BE-P3
Skill	S131	Skill in drafting requirements from priorities, using the organization's collaboration/communication tools if necessary.	ID.BE-P3
Skill	S155	Skill in executing a communications plan.	ID.BE-P3; GV.MT-P2
Skill	S157	Skill in explaining complex topics/ideas.	ID.BE-P3; GV.MT-P2
Subcategory	**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 and/or types, visibility of data processing to individuals and third parties).**	
Notes: Organizations can leverage their data inventory and data map to help identify categories of individuals whose data the organization processes, categories of privacy threats associated with data actions, as well as system/product/service requirements that can inform the contextual factors analysis.			
Task	T077	Define the scope of contextual factors for assessing the privacy risks of systems/products/services.	ID.RA-P1
Task	T147	Determine which contextual factors apply to the data actions of a system/product/service.	ID.RA-P1

Statement Type	ID	Description	Subcategory Mapping
Task	T162	Document factors that may influence individuals affected by the data actions of a system/product/service.	ID.RA-P1
Task	T171	Document the degree to which the data actions of a system/product/service are visible to individuals.	ID.RA-P1
Task	T172	Document the degree to which the organization controls the processing of individuals' data.	ID.RA-P1
Task	T173	Document the evaluation of the risk level of privacy threat actors/threat actor communities associated with the data actions of a system/product/service.	ID.RA-P1
Task	T174	Document the extent of information technology experience (or understanding) of individuals affected by the data actions of a system/product/service.	ID.RA-P1
Task	T177	Document the privacy interests of individuals affected by the data actions of a system/product/service.	ID.RA-P1
Task	T181	Document the set(s) of contextual factors associated with the data actions of a system/product/service.	ID.RA-P1
Task	T180	Document the scope of contextual factors for assessing the privacy risks of the organization's systems/products/services.	ID.RA-P1
Task	T202	Evaluate systems/products/services for evidence of cognitive bias in design and development that could cause privacy problems to individuals.	ID.RA-P1
Task	T208	Evaluate the risk level of privacy threat actors/threat actor communities associated with the data actions of a system/product/service.	ID.RA-P1
Task	T223	Identify factors that may influence individuals affected by the data actions of a system/product/service.	ID.RA-P1
Task	T242	Identify the degree to which the data actions of a system/product/service are visible to individuals.	ID.RA-P1
Task	T243	Identify the degree to which the organization controls the processing of individuals' data.	ID.RA-P1
Task	T244	Identify the extent of information technology experience (or understanding) of individuals affected by the data actions of a system/product/service.	ID.RA-P1
Task	T245	Identify the privacy interests of individuals affected by the data actions of a system/product/service.	ID.RA-P1
Knowledge	K016	Knowledge of business practices, processes, and related activities that may pose privacy risk to the individuals affected by the data actions of a system/product/service.	ID.RA-P1
Knowledge	K021	Knowledge of categories of individuals subject to heightened privacy risk.	ID.RA-P1
Knowledge	K081	Knowledge of individual rights within privacy laws and regulations that govern the data actions of a system/product/service.	ID.RA-P1
Knowledge	K130	Knowledge of privacy practices that may negatively impact the privacy of individuals.	ID.RA-P1
Knowledge	K131	Knowledge of privacy principles implicated by the data actions of a system/product/service.	ID.RA-P1
Knowledge	K136	Knowledge of privacy requirements in systems/products/services.	ID.RA-P1
Knowledge	K138	Knowledge of privacy risk assessment approaches (i.e., quantitative, qualitative, and semi-quantitative).	ID.RA-P1; ID.RA-P4
Knowledge	K139	Knowledge of privacy risk assessment methodologies.	ID.RA-P1; ID.RA-P4
Knowledge	K142	Knowledge of privacy threat actor/threat actor community capabilities.	ID.RA-P1
Knowledge	K143	Knowledge of privacy threat actors associated with a given privacy threat category.	ID.RA-P1
Knowledge	K162	Knowledge of research related to information/power imbalances and their applicability to privacy risk.	ID.RA-P1
Knowledge	K179	Knowledge of stakeholders from whom to gather contextual factors related to the data actions of a system/product/service.	ID.RA-P1
Knowledge	K214	Knowledge of the contextual nature of privacy regarding how the data actions of a system/product/service impact individuals.	ID.RA-P1
Knowledge	K223	Knowledge of the different roles privacy threat actors may play in a system/product/service.	ID.RA-P1
Knowledge	K303	Knowledge of the organization's systems/products/services.	GV.MT-P1; ID.IM-P1; ID.IM-P2; ID.IM-P3; ID.IM-P4; ID.IM-P5; ID.IM-P6; ID.IM-P7; ID.IM-P8; ID.BE-P3; ID.RA-P1

Statement Type	ID	Description	Subcategory Mapping
Knowledge	K331	Knowledge of types of cognitive biases that could cause privacy problems to individuals during the design and development of systems/products/services.	ID.RA-P1
Knowledge	K333	Knowledge of types of privacy threat actors.	ID.RA-P1
Knowledge	K334	Knowledge of types of privacy threat categories.	ID.RA-P1
Knowledge	K348	Knowledge of why information/power imbalances related to the data processing of a system/product/service exist.	ID.RA-P1
Skill	S050	Skill in assessing privacy threat actor/threat actor community capabilities.	ID.RA-P1
Skill	S055	Skill in assessing the impact of information/power imbalances on the severity of privacy problems.	ID.RA-P1
Skill	S058	Skill in assessing the impact of privacy threat categories on a system/product/service.	ID.RA-P1
Skill	S118	Skill in determining which privacy laws and regulations apply to the data actions of a system/product/service.	ID.RA-P1
Skill	S119	Skill in determining which privacy principles are implicated by the data actions of a system/product/service.	ID.RA-P1
Skill	S123	Skill in differentiating user roles within the system/product/service.	ID.RA-P1
Skill	S135	Skill in engaging with development teams to identify privacy requirements of systems/products/services.	ID.RA-P1
Skill	S143	Skill in evaluating how privacy requirements affect the risk/benefit calculus within privacy risk assessment.	ID.RA-P1
Skill	S147	Skill in evaluating privacy requirements documentation for a system/product/service.	ID.RA-P1
Skill	S153	Skill in evaluating the risk tolerance of individuals affected by the data actions of a system/product/service.	ID.RA-P1
Skill	S165	Skill in gathering correct, accurate, and relevant information.	ID.RA-P1; GV.PO-P5
Skill	S175	Skill in identifying privacy practices that negatively impact the privacy of an individual.	ID.RA-P1
Skill	S236	Skill in negotiating with [*organization-defined stakeholders*] to meet privacy risk assessment goals.	ID.RA-P1
Skill	S262	Skill in recognizing cognitive biases related to the system/product/service life cycle.	ID.RA-P1
Skill	S263	Skill in recognizing information/power imbalances related to data processing.	ID.RA-P1
Skill	S270	Skill in selecting an effective approach to gather contextual information from [*organization-defined stakeholders*].	ID.RA-P1
Subcategory	**ID.RA-P2**	**Data analytic inputs and outputs are identified and evaluated for bias.**	
Task	T032	Conduct fairness assessments of potential computational/statistical biases in the AI system.	ID.RA-P2
Task	T067	Define acceptable levels of difference in AI system performance in accordance with established organizational governance policies, business requirements, regulatory compliance, legal frameworks, and ethical standards within the context of use.	ID.RA-P2
Task	T072	Define the actions to be taken if disparity levels in AI system performance rise above acceptable levels.	ID.RA-P2
Task	T073	Define the AI system's goals/objectives in collaboration with human factors and socio-technical stakeholders.	ID.RA-P2
Task	T074	Define the AI system's learning tasks, including known assumptions and limitations.	ID.RA-P2
Task	T091	Determine how system performance varies across groups, within groups, or for intersecting groups, using context specific fairness metrics.	ID.RA-P2
Task	T109	Determine sources of bias in test, evaluation, verification, and validation (TEVV) data.	ID.RA-P2
Task	T163	Document methods used for training data processing, including known limitations.	ID.RA-P2
Task	T169	Document the AI system's goals/objectives in collaboration with human factors and socio-technical stakeholders.	ID.RA-P2
Task	T170	Document the AI system's learning tasks, including known assumptions and limitations.	ID.RA-P2
Task	T187	Establish a process for third parties to report potential biases in the AI system.	ID.RA-P2
Task	T188	Establish a process(es) for determining sources of bias in training data.	ID.RA-P2

Statement Type	ID	Description	Subcategory Mapping
Task	T189	Establish a process(es) for evaluating (i.e., monitor, test, and verify) the degree to which initial AI system conditions remain representative, accurate, and unbiased in the operational environment over time and under changing sociotechnical conditions.	ID.RA-P2
Task	T190	Establish a process(es) for monitoring AI system outputs for performance or bias issues that exceed established tolerance levels.	ID.RA-P2
Task	T192	Establish mechanisms for regular communication and feedback among interdisciplinary AI actors and [*organization-defined stakeholders*].	ID.RA-P2
Task	T196	Evaluate AI systems in regards to disability inclusion, including consideration of disability status in bias testing, and discriminatory screen out processes that may arise from non-inclusive design or deployment decisions.	ID.RA-P2
Task	T197	Evaluate biases in the presentation of system output to end users, operators, and practitioners, in collaboration with human factors experts.	ID.RA-P2
Task	T228	Identify groups within the target population (i.e., user base and training data) that may require disaggregated analysis, in collaboration with impacted communities.	ID.RA-P2
Task	T233	Identify potential sources of human-cognitive bias across the AI system life cycle.	ID.RA-P2
Task	T255	Implement mechanisms for confirming/supporting AI system output and end user perspectives about that output.	ID.RA-P2
Task	T275	Model results in close collaboration with impact assessors, socio-technical experts, and other AI actors with expertise in the context of use.	ID.RA-P2
Task	T294	Select AI system performance and validation metrics that are interpretable and unambiguous for downstream decision-making tasks, taking socio-technical factors into consideration.	ID.RA-P2
Knowledge	K033	Knowledge of contextual factors associated with the AI system.	ID.RA-P2
Knowledge	K074	Knowledge of forms of systemic bias in images, text (or word embeddings), audio, or other complex or unstructured data.	ID.RA-P2
Knowledge	K076	Knowledge of general fairness metrics.	ID.RA-P2
Knowledge	K105	Knowledge of non-AI solutions to achieve system goals.	ID.RA-P2
Knowledge	K176	Knowledge of safeguards in place for human use of the AI system's output.	ID.RA-P2
Knowledge	K183	Knowledge of statistical methods for data cleaning, transformation, and balancing.	ID.RA-P2
Knowledge	K184	Knowledge of statistical techniques for mitigating underrepresentation in data.	ID.RA-P2
Knowledge	K200	Knowledge of testing modules that can be incorporated throughout the AI life cycle and corroborated by independent evaluators.	ID.RA-P2
Knowledge	K201	Knowledge of the AI system's data collection.	ID.RA-P2
Knowledge	K202	Knowledge of the AI system's minimum functionality.	ID.RA-P2
Knowledge	K203	Knowledge of the AI system's potential benefits.	ID.RA-P2
Knowledge	K204	Knowledge of the AI systems' technical specifications and requirements.	ID.RA-P2
Knowledge	K211	Knowledge of the completeness, representativeness, and balance of data sources for the AI system.	ID.RA-P2
Knowledge	K230	Knowledge of the extent to which, for a given task, humans can utilize and oversee the AI system's outputs.	ID.RA-P2
Knowledge	K327	Knowledge of third parties associated with the AI system(s).	ID.RA-P2
Skill	S248	Skill in performing analysis of quantified harms from computational/statistical bias for contextually significant differences across groups, within groups, and among intersecting groups.	ID.RA-P2
Skill	S025	Skill in applying mathematical/computational techniques (i.e., pre-, in-, and post-processing) to balance model performance quality with bias considerations based on data characteristics, model performance, and sociotechnical context.	ID.RA-P2

Statement Type	ID	Description	Subcategory Mapping
Skill	S032	Skill in applying test, evaluation, verification, and validation (TEVV) protocols for models, systems and their subcomponents, deployment, and operation.	ID.RA-P2
Skill	S043	Skill in assessing data labels for evidence of bias.	ID.RA-P2
Skill	S045	Skill in assessing differences in distributions of AI system outcomes across and within groups, including intersecting groups.	ID.RA-P2
Skill	S053	Skill in assessing the AI system's technical specifications and requirements for alignment with its goals/objectives.	ID.RA-P2
Skill	S094	Skill in creating custom, context-specific fairness metrics, in collaboration with affected communities.	ID.RA-P2
Skill	S099	Skill in customizing fairness metrics to specific context of use.	ID.RA-P2
Skill	S100	Skill in data cleaning and balancing.	ID.RA-P2
Skill	S122	Skill in differentiating between causal/inferential relationships and correlated relationships, as well as selection of proxies used in measurement models.	ID.RA-P2
Skill	S167	Skill in identifying assumptions and decisions made for data and metadata selection.	ID.RA-P2
Skill	S172	Skill in identifying input data features that may serve as proxies for demographic group membership or otherwise give rise to emergent bias within AI systems.	ID.RA-P2
Skill	S185	Skill in identifying types of harms from computational/statistical bias.	ID.RA-P2
Skill	S224	Skill in marking outputs to clearly show they came from an AI.	ID.RA-P2
Skill	S259	Skill in process mapping.	ID.RA-P2
Skill	S288	Skill in tracing data lineage.	ID.RA-P2
Subcategory	**ID.RA-P3**	**Potential problematic data actions and associated problems are identified.**	
Task	T185	Enumerate potential problems for identified problematic data actions.	ID.RA-P3
Task	T066	Define a set of problematic data actions and problems for assessing systems/products/services.	ID.RA-P3
Task	T150	Determine which problematic data actions and associated problems apply to the data actions of systems/products/services.	ID.RA-P3
Task	T155	Document a set of problematic data actions and problems associated with the data actions of systems/products/services.	ID.RA-P3
Task	T176	Document the organization's set of problematic data actions and associated problems for assessing systems/products/services.	ID.RA-P3
Task	T284	Provide [*organization-defined stakeholders*] with access to documentation of privacy risk assessments.	ID.RA-P3; ID.RA-P4
Knowledge	K147	Knowledge of privacy-related social norms.	ID.RA-P3
Knowledge	K169	Knowledge of risk management system options.	ID.RA-P3; ID.RA-P4
Knowledge	K216	Knowledge of the correlation between the organization's data actions and potential problems to individuals.	ID.RA-P3
Knowledge	K316	Knowledge of the set of problematic data actions and problems for assessing an organization's systems/products/services.	ID.RA-P3
Skill	S028	Skill in applying privacy threat modeling methods.	ID.RA-P3
Skill	S232	Skill in modeling privacy threats.	ID.RA-P3
Skill	S283	Skill in surveying or interviewing [*organization-defined stakeholders*].	ID.RA-P3
Skill	S300	Skill in using risk management systems or document repositories to create documentation of privacy risk assessments.	ID.RA-P3; ID.RA-P4
Subcategory	**ID.RA-P4**	**Problematic data actions, likelihoods, and impacts are used to determine and prioritize risk.**	
Task	T019	Assess the impact should identified problematic data actions of systems/products/services create problems.	ID.RA-P4

Statement Type	ID	Description	Subcategory Mapping
Task	T165	Document privacy risk assessments, including privacy risk prioritization.	ID.RA-P4
Task	T204	Evaluate the effectiveness of the applied privacy risk assessment approach (i.e., quantitative, qualitative, and semi-quantitative).	ID.RA-P4
Task	T206	Evaluate the likelihood that identified problematic data actions of systems/products/services will create problems to individuals.	ID.RA-P4
Task	T239	Identify the appropriate privacy risk assessment approach (i.e., quantitative, qualitative, and semi-quantitative) for evaluating the data actions of systems/products/services.	ID.RA-P4
Task	T282	Prioritize risks based on the likelihood and impact of the problematic data actions, accounting for organizational values, stakeholder expectations, and costs.	ID.RA-P4
Task	T284	Provide [*organization-defined stakeholders*] with access to documentation of privacy risk assessments.	ID.RA-P3; ID.RA-P4
Task	T290	Select a method for visualizing and demonstrating privacy risk prioritization.	ID.RA-P4
Task	T291	Select a privacy risk assessment information repository tool.	ID.RA-P4
Knowledge	K035	Knowledge of contextual privacy risk factors that affect impact.	ID.RA-P4
Knowledge	K036	Knowledge of contextual privacy risk factors that affect likelihood.	ID.RA-P4
Knowledge	K097	Knowledge of methods to measure or estimate [*Select: the impact of problems for individuals from privacy events; the likelihood of privacy events; the likelihood of problems arising from privacy events; the likelihood of problems for individuals from privacy events; the severity of problems for individuals*].	ID.RA-P4
Knowledge	K138	Knowledge of privacy risk assessment approaches (i.e., quantitative, qualitative, and semi-quantitative).	ID.RA-P1; ID.RA-P4
Knowledge	K139	Knowledge of privacy risk assessment methodologies.	ID.RA-P1; ID.RA-P4
Knowledge	K169	Knowledge of risk management system options.	ID.RA-P3; ID.RA-P4
Knowledge	K173	Knowledge of risk scoring based on industry and organizational processes.	ID.RA-P4
Knowledge	K205	Knowledge of the applied privacy risk assessment methodology.	ID.RA-P4
Knowledge	K206	Knowledge of the applied privacy risk model's requirements.	ID.RA-P4
Skill	S068	Skill in assigning risk based upon likelihood of it being realized.	ID.RA-P4
Skill	S069	Skill in assigning risk using industry standard tools and techniques.	ID.RA-P4
Skill	S081	Skill in conducting a privacy risk assessment.	ID.RA-P4; GV.MT-P1
Skill	S088	Skill in correlating problematic data actions with potential problems.	ID.RA-P4; GV.MT-P6
Skill	S148	Skill in evaluating privacy risk models.	ID.RA-P4
Skill	S173	Skill in identifying objective data points or information to measure or estimate privacy risk factors.	ID.RA-P4
Skill	S184	Skill in identifying training needs related to privacy risk measurement or estimation.	ID.RA-P4
Skill	S226	Skill in measuring or estimating the impact of privacy events on individuals.	ID.RA-P4
Skill	S227	Skill in measuring or estimating the impact of problems for individuals from privacy events.	ID.RA-P4
Skill	S228	Skill in measuring or estimating the likelihood of privacy events.	ID.RA-P4
Skill	S229	Skill in measuring or estimating the likelihood of problems for individuals arising from privacy events.	ID.RA-P4
Skill	S230	Skill in measuring or estimating the likelihood of problems for individuals from privacy events.	ID.RA-P4
Skill	S253	Skill in performing gap analysis related to privacy risk measurement or estimation.	ID.RA-P4
Skill	S300	Skill in using risk management systems or document repositories to create documentation of privacy risk assessments.	ID.RA-P3; ID.RA-P4
Skill	S301	Skill in using tools to assess privacy risk.	ID.RA-P4
Subcategory	**ID.RA-P5**	**Risk responses are identified, prioritized, and implemented.**	
Task	T153	Develop a privacy risk response plan in consultation with [*organization-defined stakeholders*].	ID.RA-P5
Task	T166	Document selected privacy controls.	ID.RA-P5
Task	T175	Document the mitigation strategy for privacy risk findings that require ongoing attention or remediation.	ID.RA-P5

Statement Type	ID	Description	Subcategory Mapping
Task	T178	Document the privacy risk response decision(s) of the authorizing official or decision-maker.	ID.RA-P5
Task	T256	Implement risk responses in accordance with privacy risk response plan.	ID.RA-P5
Task	T281	Prioritize risk responses to the problematic data actions of systems/products/services in consultation with [*organization-defined stakeholders*].	ID.RA-P5
Task	T283	Prioritize selected privacy controls in consultation with [*organization-defined stakeholders*].	ID.RA-P5
Task	T296	Select privacy controls.	ID.RA-P5
Task	T303	Test the effectiveness of privacy controls.	ID.RA-P5
Task	T304	Test the effectiveness of privacy risk responses.	ID.RA-P5
Knowledge	K007	Knowledge of applicable privacy controls, based on the organization's needs.	ID.RA-P5
Knowledge	K034	Knowledge of contextual factors that affect mitigation efforts.	ID.RA-P5
Knowledge	K077	Knowledge of governance, risk, and compliance (GRC) tools used by the organization.	ID.RA-P5
Knowledge	K100	Knowledge of mitigation strategies for applying privacy controls to address privacy risks.	ID.RA-P5
Knowledge	K101	Knowledge of mitigation strategies for applying privacy controls to systems/products/services.	ID.RA-P5
Knowledge	K126	Knowledge of privacy control baselines.	ID.RA-P5
Knowledge	K127	Knowledge of privacy control categorization practices (i.e., common/inherited, hybrid, and system-specific).	ID.RA-P5
Knowledge	K140	Knowledge of privacy risk mitigation controls.	ID.RA-P5
Knowledge	K170	Knowledge of risk response measurement techniques.	ID.RA-P5
Knowledge	K171	Knowledge of risk response prioritization.	ID.RA-P5
Knowledge	K172	Knowledge of risk responses.	ID.RA-P5
Knowledge	K217	Knowledge of the costs of implementing privacy controls.	ID.RA-P5
Knowledge	K219	Knowledge of the data life cycle stages.	ID.RA-P5
Knowledge	K221	Knowledge of the difference between a risk mitigation strategy and a privacy risk control.	ID.RA-P5
Knowledge	K227	Knowledge of the enterprise methodology used to test and evaluate privacy controls.	ID.RA-P5
Knowledge	K228	Knowledge of the extent to which privacy controls can be implemented within the organization.	ID.RA-P5
Knowledge	K280	Knowledge of the organization's prioritized privacy outcomes.	ID.RA-P5; GV.PO-P1; GV.PO-P3; GV.RM-P1; GV.MT-P1; GV.MT-P2
Knowledge	K297	Knowledge of the organization's risk tolerance.	ID.BE-P3; ID.RA-P5; ID.DE-P3; GV.RM-P3; GV.MT-P1
Knowledge	K311	Knowledge of the relationship between privacy controls and risk factors.	ID.RA-P5
Knowledge	K313	Knowledge of the relationships between privacy risk mitigating controls and privacy risks.	ID.RA-P5
Skill	S004	Skill in adjusting controls to privacy risks based on risk responses.	ID.RA-P5
Skill	S017	Skill in applying an appropriate privacy control baseline to the data actions of systems/products/services.	ID.RA-P5
Skill	S039	Skill in articulating recommended privacy priorities.	ID.RA-P5
Skill	S040	Skill in articulating the relationship between privacy risk mitigating controls and privacy risk.	ID.RA-P5; GV.MT-P1
Skill	S059	Skill in assessing the impact of the privacy risk mitigation strategy on individuals.	ID.RA-P5
Skill	S060	Skill in assessing the impact of the privacy risk mitigation strategy on operations.	ID.RA-P5
Skill	S067	Skill in assigning priority to privacy risk mitigation controls.	ID.RA-P5
Skill	S074	Skill in calculating risk prioritization.	ID.RA-P5; GV.MT-P1
Skill	S098	Skill in creating tests to measure the mitigation effectiveness of privacy controls.	ID.RA-P5
Skill	S137	Skill in establishing risk prioritization.	ID.RA-P5
Skill	S138	Skill in evaluating (i.e., quantitatively, qualitatively) the impact of risk responses on privacy risk.	ID.RA-P5
Skill	S151	Skill in evaluating the effectiveness of risk responses.	ID.RA-P5
Skill	S160	Skill in explaining risk response strategies to stakeholders.	ID.RA-P5
Skill	S171	Skill in identifying effective mitigation strategies for applying privacy controls to address privacy risks.	ID.RA-P5
Skill	S193	Skill in implementing privacy risk response plans tailored to organizational needs.	ID.RA-P5

Statement Type	ID	Description	Subcategory Mapping
Skill	S194	Skill in implementing privacy risk responses in collaboration with [*organization-defined stakeholders*].	ID.RA-P5
Skill	S195	Skill in implementing risk responses based on context.	ID.RA-P5
Skill	S197	Skill in informing stakeholders of privacy risks.	ID.RA-P5
Skill	S207	Skill in making risk response decisions in consultation with [*organization-defined stakeholders*].	ID.RA-P5
Skill	S225	Skill in matching mitigation controls to privacy risk factors.	ID.RA-P5
Skill	S278	Skill in selecting privacy control(s) to address an identified privacy risk.	ID.RA-P5
Skill	S279	Skill in selecting privacy control(s) to mitigate an identified privacy risk.	ID.RA-P5
Skill	S280	Skill in selecting privacy controls in the absence of a privacy control baseline.	ID.RA-P5
Skill	S281	Skill in selecting risk responses to address identified privacy risks.	ID.RA-P5
Skill	S299	Skill in using governance, risk, and compliance (GRC) tools.	ID.RA-P5
Subcategory	**ID.DE-P1**	**Data processing ecosystem risk management policies, processes, and procedures are identified, established, assessed, managed, and agreed to by organizational stakeholders.**	
Notes: Organizations may choose to evaluate existing policies/processes/procedures for gaps (e.g., incompleteness, outdated information) and determine necessary actions to address identified gaps.			
Task	T042	Create a policy/policies that addresses the purpose, scope, roles, responsibilities, and coordination required for data processing ecosystem risk management that is consistent with applicable laws, regulations, standards, and guidelines.	ID.DE-P1
Task	T055	Create a process(es)/procedure(s) for facilitating implementation of the data processing ecosystem risk management policy/policies and associated controls.	ID.DE-P1
Knowledge	K018	Knowledge of business/sector-specific requirements for policies/processes/procedures.	ID.DE-P1
Knowledge	K048	Knowledge of data management practices.	ID.DE-P1
Knowledge	K053	Knowledge of data processing ecosystem practices.	ID.DE-P1
Knowledge	K055	Knowledge of data processing requirements.	ID.DE-P1; GV.PO-P5
Knowledge	K085	Knowledge of key organizational roles related to data processing ecosystem risk management.	ID.DE-P1
Knowledge	K168	Knowledge of risk management processes.	ID.DE-P1; ID.DE-P2; ID.DE-P3; ID.DE-P4; ID.DE-P5; GV.RM-P1; GV.RM-P2; GV.RM-P3
Knowledge	K225	Knowledge of the distinction between data management practices and policies/processes/procedures.	ID.DE-P1
Knowledge	K254	Knowledge of the organization's data processing ecosystem.	ID.BE-P1; ID.DE-P1; ID.DE-P2; ID.DE-P3; ID.DE-P4; ID.DE-P5; CT.PO-P1; CT.PO-P2; CT.PO-P3; CT.PO-P4; CM.AW-P1; CM.AW-P2; CM.AW-P3; CM.AW-P4; CM.AW-P5; CM.AW-P6; CM.AW-P7; CM.AW-P8
Knowledge	K255	Knowledge of the organization's data processing goals.	ID.DE-P1; GV.PO-P6; GV.RM-P1; GV.RM-P2; GV.RM-P3; GV.MT-P3; GV.MT-P4; GV.MT-P5; GV.MT-P6; GV.MT-P7; CT.PO-P1; CT.PO-P2; CT.PO-P3; CM.PO-P1
Knowledge	K258	Knowledge of the organization's data strategy.	ID.DE-P1; GV.PO-P6; GV.RM-P1; GV.RM-P2; GV.RM-P3; GV.MT-P3; GV.MT-P4; GV.MT-P5; GV.MT-P6; GV.MT-P7; CT.PO-P1; CT.PO-P2; CT.PO-P3; CM.PO-P1
Skill	S003	Skill in addressing gaps between current practices and policy requirements.	ID.DE-P1; GV.MT-P2
Skill	S007	Skill in advocating for data processing ecosystem risk management policies/processes/procedures to [*organization-defined stakeholders*].	ID.DE-P1
Skill	S026	Skill in applying methodologies for assigning stakeholder roles and responsibilities.	ID.DE-P1

Statement Type	ID	Description	Subcategory Mapping
Skill	S047	Skill in assessing policies/processes/procedures for efficacy.	ID.DE-P1
Skill	S070	Skill in attaining approval from organizational decision-makers.	ID.DE-P1
Skill	S087	Skill in coordinating with [*organization-defined stakeholders*] on activities related to policies/processes/procedures.	ID.DE-P1
Skill	S127	Skill in drafting policies/processes/procedures.	ID.DE-P1; GV.MT-P3; GV.MT-P4; GV.MT-P5; GV.MT-P6; GV.MT-P7; CT.PO-P1; CT.PO-P2; CT.PO-P3; CM.PO-P1
Skill	S170	Skill in identifying data processing requirements applicable to the organization.	ID.DE-P1
Skill	S178	Skill in identifying roles and decision-makers to collaborate for consensus-building.	GV.PO-P1; ID.DE-P1
Skill	S206	Skill in making privacy-related recommendations for actions.	ID.DE-P1
Skill	S240	Skill in organizing a team capable of understanding the relevance and effectiveness of policies/processes/procedures.	ID.DE-P1
Subcategory	**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.**	
Task	T076	Define the roles of data processing ecosystem parties.	ID.DE-P2
Task	T087	Determine data processing ecosystem parties on an [*organization-defined schedule*].	ID.DE-P2
Task	T194	Establish roles and responsibilities for identifying and managing information about data processing ecosystem parties on an [*organization-defined schedule*].	ID.DE-P2
Task	T200	Evaluate privacy and security controls associated with the data processing ecosystem on an [*organization-defined schedule*].	ID.DE-P2
Task	T280	Prioritize data processing ecosystem risk management parties using privacy risk assessment results in accordance with established policies/processes/procedures.	ID.DE-P2
Knowledge	K012	Knowledge of baseline privacy and security controls.	ID.DE-P2
Knowledge	K019	Knowledge of categories of data elements in systems/products/services.	ID.DE-P2
Knowledge	K054	Knowledge of data processing environments.	ID.IM-P7; ID.DE-P2
Knowledge	K154	Knowledge of relevant criteria or factors as they apply to prioritizing data processing ecosystem parties.	ID.DE-P2
Knowledge	K168	Knowledge of risk management processes.	ID.DE-P1; ID.DE-P2; ID.DE-P3; ID.DE-P4; ID.DE-P5; GV.RM-P1; GV.RM-P2; GV.RM-P3
Knowledge	K207	Knowledge of the audit common body of knowledge (CBK).	ID.DE-P2
Knowledge	K254	Knowledge of the organization's data processing ecosystem.	ID.BE-P1; ID.DE-P1; ID.DE-P2; ID.DE-P3; ID.DE-P4; ID.DE-P5; CT.PO-P1; CT.PO-P2; CT.PO-P3; CT.PO-P4; CM.AW-P1; CM.AW-P2; CM.AW-P3; CM.AW-P4; CM.AW-P5; CM.AW-P6; CM.AW-P7; CM.AW-P8
Knowledge	K260	Knowledge of the organization's documentation related to data processing ecosystem parties.	ID.DE-P2
Knowledge	K298	Knowledge of the organization's role(s) in the data processing ecosystem.	ID.DE-P2
Knowledge	K317	Knowledge of the skills matrix within the organization.	ID.DE-P2
Skill	S018	Skill in applying audit methodologies.	ID.DE-P2
Skill	S077	Skill in communicating metrics (and related insights) to ensure [*organization-defined stakeholder*] support.	ID.DE-P2
Skill	S188	Skill in implementing controls.	ID.DE-P2
Skill	S200	Skill in interpreting privacy risk assessment results.	ID.DE-P2; GV.PO-P6
Skill	S216	Skill in managing relationships with data processing ecosystem parties.	ID.DE-P2
Skill	S272	Skill in selecting controls.	ID.DE-P2

Statement Type	ID	Description	Subcategory Mapping
Subcategory	**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.**	
Task	T048	Create a process for ongoing monitoring and review of data processing ecosystem party contract performance.	ID.DE-P3
Task	T183	Draft language within data processing ecosystem party contracts incorporating identified legal, technical, and organizational measures to meet privacy objectives.	ID.DE-P3; CT.DM-P1; CT.DM-P2; CT.DM-P3; CT.DM-P4
Task	T198	Evaluate contractual terms for consistency with scope of work.	ID.DE-P3
Task	T230	Identify legal, technical, and organizational measures data processing ecosystem parties can undertake to meet the organization's privacy objectives.	ID.DE-P3
Task	T277	Negotiate privacy and security clauses in contracts.	ID.DE-P3; CT.DM-P1; CT.DM-P2; CT.DM-P3; CT.DM-P4
Knowledge	K025	Knowledge of clauses and legal terms necessary for agreements with data processing ecosystem parties.	ID.DE-P3
Knowledge	K037	Knowledge of contract enforcement mechanisms.	ID.DE-P3
Knowledge	K052	Knowledge of data processing ecosystem party privacy standards of practice.	ID.DE-P3
Knowledge	K088	Knowledge of legal, technical, and organizational measures to meet organizational privacy objectives.	ID.DE-P3
Knowledge	K132	Knowledge of privacy program objectives.	ID.DE-P3
Knowledge	K135	Knowledge of privacy program priorities.	ID.DE-P3
Knowledge	K164	Knowledge of resources to determine negotiation-specific priorities.	ID.DE-P3
Knowledge	K168	Knowledge of risk management processes.	ID.DE-P1; ID.DE-P2; ID.DE-P3; ID.DE-P4; ID.DE-P5; GV.RM-P1; GV.RM-P2; GV.RM-P3
Knowledge	K237	Knowledge of the organization's ability to mitigate privacy risk.	ID.DE-P3
Knowledge	K240	Knowledge of the organization's and other data processing ecosystem parties' relative bargaining positions/powers.	ID.DE-P3
Knowledge	K245	Knowledge of the organization's contract management practices.	ID.DE-P3
Knowledge	K246	Knowledge of the organization's contracting process.	ID.DE-P3
Knowledge	K254	Knowledge of the organization's data processing ecosystem.	ID.BE-P1; ID.DE-P1; ID.DE-P2; ID.DE-P3; ID.DE-P4; ID.DE-P5; CT.PO-P1; CT.PO-P2; CT.PO-P3; CT.PO-P4; CM.AW-P1; CM.AW-P2; CM.AW-P3; CM.AW-P4; CM.AW-P5; CM.AW-P6; CM.AW-P7; CM.AW-P8
Knowledge	K297	Knowledge of the organization's risk tolerance.	ID.BE-P3; ID.RA-P5; ID.DE-P3; GV.RM-P3; GV.MT-P1
Skill	S051	Skill in assessing risk based on the changes to the scope of work.	ID.DE-P3
Skill	S101	Skill in defining criteria for ongoing monitoring and review of contract performance.	ID.DE-P3
Skill	S125	Skill in drafting contracts.	ID.DE-P3
Skill	S132	Skill in drafting standard contractual language designed to meet an organization's privacy program objectives.	ID.DE-P3
Skill	S141	Skill in evaluating contracts based on [*organization-defined criteria*].	ID.DE-P3
Skill	S158	Skill in explaining contractual privacy responsibilities.	ID.DE-P3
Skill	S237	Skill in negotiating with external parties.	ID.DE-P3
Skill	S238	Skill in negotiating with internal stakeholders.	ID.DE-P3
Skill	S244	Skill in performing analysis of contract language for adherence to data processing and privacy requirements.	ID.DE-P3
Skill	S295	Skill in translating privacy objectives to legal/contractual language.	ID.DE-P3
Subcategory	**ID.DE-P4**	**Interoperability frameworks or similar multi-party approaches are used to manage data processing ecosystem privacy risks.**	

Statement Type	ID	Description	Subcategory Mapping
Task	T149	Determine which interoperability framework(s) or similar multi-party approaches are applicable.	ID.DE-P4
Task	T251	Implement applicable components of interoperability frameworks or similar multi-party approaches to the organization's data processing ecosystem risk management practices.	ID.DE-P4
Task	T299	Select which components of interoperability frameworks or similar multi-party approaches to apply, based on a thorough assessment.	ID.DE-P4
Knowledge	K026	Knowledge of codes of ethics, conduct, and practice associated with interoperability frameworks or similar multi-party approaches.	ID.DE-P4
Knowledge	K079	Knowledge of implementation procedures associated with interoperability frameworks or similar multi-party approaches.	ID.DE-P4
Knowledge	K080	Knowledge of implementation rules and requirements associated with interoperability frameworks or similar multi-party approaches.	ID.DE-P4
Knowledge	K083	Knowledge of interoperability frameworks or similar multi-party approaches for managing data processing ecosystem privacy risk.	ID.DE-P4
Knowledge	K168	Knowledge of risk management processes.	ID.DE-P1; ID.DE-P2; ID.DE-P3; ID.DE-P4; ID.DE-P5; GV.RM-P1; GV.RM-P2; GV.RM-P3
Knowledge	K254	Knowledge of the organization's data processing ecosystem.	ID.BE-P1; ID.DE-P1; ID.DE-P2; ID.DE-P3; ID.DE-P4; ID.DE-P5; CT.PO-P1; CT.PO-P2; CT.PO-P3; CT.PO-P4; CM.AW-P1; CM.AW-P2; CM.AW-P3; CM.AW-P4; CM.AW-P5; CM.AW-P6; CM.AW-P7; CM.AW-P8
Skill	S019	Skill in applying codes of ethics, conduct, and practice associated with interoperability frameworks or similar multi-party approaches to external processes within the data processing ecosystem.	ID.DE-P4
Skill	S049	Skill in assessing privacy gaps in the organization's implementation of interoperability framework or similar multi-party approaches.	ID.DE-P4
Skill	S150	Skill in evaluating the effectiveness of interoperability frameworks or similar multi-party approaches to address privacy risks across the organization's data processing ecosystem.	ID.DE-P4
Skill	S209	Skill in managing interoperability frameworks or similar multi-party approaches to address privacy risks across the organization's data processing ecosystem.	ID.DE-P4
Subcategory	**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, interoperability framework, or other obligations.**	
Task	T050	Create a process for routinely assessing data processing ecosystem parties for conformance to their obligations.	ID.DE-P5
Task	T063	Create assessment categories of data processing ecosystem parties based on risk.	ID.DE-P5
Task	T142	Determine whether assessment of data processing ecosystem parties will be conducted by internal or external teams based on resources.	ID.DE-P5
Task	T199	Evaluate data processing ecosystem parties for conformance to their obligations.	ID.DE-P5
Knowledge	K008	Knowledge of assessment methodologies.	ID.DE-P5
Knowledge	K009	Knowledge of assessment methods to evaluate data processing ecosystem parties for conformance to their obligations.	ID.DE-P5
Knowledge	K010	Knowledge of audit methodologies.	ID.DE-P5
Knowledge	K107	Knowledge of obligations/commitments of data processing ecosystem parties.	ID.DE-P5
Knowledge	K168	Knowledge of risk management processes.	ID.DE-P1; ID.DE-P2; ID.DE-P3; ID.DE-P4; ID.DE-P5; GV.RM-P1; GV.RM-P2; GV.RM-P3

Statement Type	ID	Description	Subcategory Mapping
Knowledge	K212	Knowledge of the components of conformance evaluation processes built around categories of risk.	ID.DE-P5
Knowledge	K254	Knowledge of the organization's data processing ecosystem.	ID.BE-P1; ID.DE-P1; ID.DE-P2; ID.DE-P3; ID.DE-P4; ID.DE-P5; CT.PO-P1; CT.PO-P2; CT.PO-P3; CT.PO-P4; CM.AW-P1; CM.AW-P2; CM.AW-P3; CM.AW-P4; CM.AW-P5; CM.AW-P6; CM.AW-P7; CM.AW-P8
Skill	S071	Skill in auditing technical and organizational privacy measures.	ID.DE-P5
Skill	S082	Skill in conducting assessments of technical and organizational privacy measures.	ID.DE-P5
Skill	S092	Skill in creating conformity assessment processes in collaboration with [*organization-defined stakeholders*].	ID.DE-P5
Skill	S285	Skill in tailoring conformity assessment processes for relevance and applicability to the organization.	ID.DE-P5
Subcategory	**GV.PO-P1**	**Organizational privacy values and policies (e.g., conditions on data processing such as data uses or retention periods, individuals' prerogatives with respect to data processing) are established and communicated.**	
Notes: Organizations may choose to evaluate existing values and policies for gaps (e.g., incompleteness, outdated information) and determine necessary actions to address identified gaps.			
Task	T034	Create an organizational privacy policy/policies for data processing that reflects the organization's privacy values and privacy risk management and is consistent with applicable laws, regulations, standards, and guidelines.	GV.PO-P1
Task	T060	Create a process(es)/procedure(s) that addresses audience, cadence, and mechanisms for communication about organizational privacy [*Select: policies; values*] among [*organization-defined stakeholders*].	GV.PO-P1
Task	T101	Determine organizational privacy values in consultation with [*organization-defined stakeholders*].	GV.PO-P1
Task	T315	Verify that organizational privacy values are established.	GV.PO-P1
Knowledge	K001	Knowledge of [*organization-defined stakeholders*] impacted by privacy policies.	GV.PO-P1
Knowledge	K015	Knowledge of business partners and the data they process for the organization.	GV.PO-P1; GV.PO-P2
Knowledge	K071	Knowledge of existing policies/processes/procedures.	GV.PO-P1; GV.MT-P3; GV.MT-P4; GV.MT-P5; GV.MT-P7
Knowledge	K120	Knowledge of policy governance procedures.	GV.PO-P1
Knowledge	K133	Knowledge of privacy program operating models.	GV.PO-P1
Knowledge	K134	Knowledge of privacy program operating principles.	GV.PO-P1
Knowledge	K145	Knowledge of privacy values documentation practices.	GV.PO-P1
Knowledge	K265	Knowledge of the organization's governance processes.	GV.PO-P1
Knowledge	K280	Knowledge of the organization's prioritized privacy outcomes.	ID.RA-P5; GV.PO-P1; GV.PO-P3; GV.RM-P1; GV.MT-P1; GV.MT-P2
Knowledge	K292	Knowledge of the organization's privacy values.	GV.PO-P1; GV.MT-P3; GV.MT-P4; GV.MT-P5; GV.MT-P7; CT.PO-P1; CT.PO-P2; CT.PO-P3; CM.PO-P1
Knowledge	K343	Knowledge of where organizational privacy values are documented.	GV.PO-P1
Skill	S095	Skill in creating organizational policies.	GV.PO-P1
Skill	S096	Skill in creating policy governance procedures.	GV.PO-P1
Skill	S163	Skill in facilitating productive privacy values discussions.	GV.PO-P1
Skill	S178	Skill in identifying roles and decision-makers to collaborate for consensus-building.	GV.PO-P1; ID.DE-P1
Skill	S204	Skill in leveraging methodologies for assigning stakeholder roles and responsibilities.	GV.PO-P1
Skill	S212	Skill in managing organizational policies.	GV.PO-P1; GV.MT-P3; GV.MT-P4; GV.MT-P5; GV.MT-P6; GV.MT-P7; CT.PO-P1; CT.PO-P2; CT.PO-P3; CM.PO-P1

Statement Type	ID	Description	Subcategory Mapping
Skill	S234	Skill in negotiating to reach agreements about organizational values and policies.	GV.PO-P1
Subcategory	**GV.PO-P2**	**Processes to instill organizational privacy values within system/product/service development and operations are established and in place.**	
Notes: Organizations may choose to evaluate existing processes for gaps (e.g., incompleteness, outdated information) and determine necessary actions to address identified gaps.			
Task	T002	Align data processing activities with system/product/service development and operations procedures.	GV.PO-P2
Task	T065	Create processes to incorporate privacy best practices and values into system/product/service development and operations in collaboration with [*organization-defined stakeholders*].	GV.PO-P2
Task	T167	Document system/product/service development and operations processes.	GV.PO-P2
Task	T221	Identify data processing activities that fall outside the scope of existing development and operations procedures.	GV.PO-P2
Task	T236	Identify privacy values implicated by the organization's inventoried data processing activities.	GV.PO-P2
Task	T306	Update all system/product/service development and operations processes with feedback and approval from leadership.	GV.PO-P2
Knowledge	K015	Knowledge of business partners and the data they process for the organization.	GV.PO-P1; GV.PO-P2
Knowledge	K095	Knowledge of methods relating to system/product/service development and operations.	GV.PO-P2
Knowledge	K347	Knowledge of whether [*organization-defined stakeholders*] process privacy-related information in conflict with the organization's privacy values.	GV.PO-P2
Skill	S030	Skill in applying templates for privacy-related system/product/service development and operations procedures.	GV.PO-P2
Skill	S091	Skill in creating activities that incorporate privacy values into systems/products/service development and operations.	GV.PO-P2
Skill	S097	Skill in creating process flows that promote clarity of privacy values and best practices.	GV.PO-P2
Skill	S120	Skill in developing relationships with [*organization-defined stakeholders*] to instill privacy values within system/product/service development and operations.	GV.PO-P2
Skill	S134	Skill in effectively leading group discussions involving the relationship between privacy values and data processing activities.	GV.PO-P2
Skill	S149	Skill in evaluating privacy values within relevant systems/products/services and operations.	GV.PO-P2
Skill	S190	Skill in implementing leadership mandates.	GV.PO-P2
Skill	S199	Skill in interpreting leadership mandates.	GV.PO-P2
Skill	S203	Skill in leading discovery activities to align privacy values with system/product/service development and operations.	GV.PO-P2
Skill	S208	Skill in managing appropriate response-related actions to inquiries that involve privacy concerns.	GV.PO-P2
Skill	S231	Skill in measuring privacy values within relevant systems/products/services and operations.	GV.PO-P2
Skill	S245	Skill in performing analysis of data used by [*organization-defined stakeholders*] to ensure privacy values are followed.	GV.PO-P2
Skill	S254	Skill in performing gap analysis to determine if privacy values are missing from system/product/service development and operations processes.	GV.PO-P2
Skill	S260	Skill in providing alternative means of using data in accord with the organization's privacy values.	GV.PO-P2
Skill	S276	Skill in selecting methods to include in documentation related to system/product/service development and operations.	GV.PO-P2
Subcategory	**GV.PO-P3**	**Roles and responsibilities for the workforce are established with respect to privacy.**	

Statement Type	ID	Description	Subcategory Mapping
Task	T025	Assign privacy risk management responsibilities to organizational roles.	GV.PO-P3; GV.RM-P1
Task	T064	Create new roles that support privacy.	GV.PO-P3; CM.PO-P2
Task	T224	Identify gaps in privacy requirements and responsibilities for all organizational roles.	GV.PO-P3
Task	T246	Identify the responsibilities necessary to support the organization's management of privacy risk.	GV.PO-P3
Knowledge	K075	Knowledge of gaps in privacy team skillsets.	GV.PO-P3
Knowledge	K150	Knowledge of RACI Assignment Matrix (Responsible, Accountable, Consulted, Informed).	GV.PO-P3; GV.PO-P4; CM.PO-P2
Knowledge	K280	Knowledge of the organization's prioritized privacy outcomes.	ID.RA-P5; GV.PO-P1; GV.PO-P3; GV.RM-P1; GV.MT-P1; GV.MT-P2
Knowledge	K284	Knowledge of the organization's privacy operating model.	GV.PO-P3
Knowledge	K289	Knowledge of the organization's privacy roadmap.	GV.PO-P3
Skill	S015	Skill in aligning organizational roles with organizational privacy objectives.	GV.PO-P3
Skill	S103	Skill in designing a privacy roadmap.	GV.PO-P3
Skill	S113	Skill in determining if existing talent can be used to fill skillset gap(s).	GV.PO-P3; CM.PO-P2
Skill	S115	Skill in determining the organization's privacy maturity level.	GV.PO-P3
Skill	S129	Skill in drafting privacy role responsibilities.	GV.PO-P3; CM.PO-P2
Subcategory	**GV.PO-P4**	**Privacy roles and responsibilities are coordinated and aligned with third-party stakeholders (e.g., service providers, customers, partners).**	
Task	T028	Categorize [*organization-defined third-party stakeholders*] based on common responsibilities.	GV.PO-P4
Task	T051	Create a process(es) to align [*organization-defined third-party stakeholder*] roles and responsibilities with privacy roles and responsibilities.	GV.PO-P4
Task	T195	Establish roles that support third-party stakeholder privacy risk management responsibilities.	GV.PO-P4
Task	T227	Identify gaps in third-party stakeholder roles and responsibilities necessary to manage organizational privacy risk.	GV.PO-P4
Task	T249	Identify third-party stakeholder roles and responsibilities to support privacy policies/processes/procedures.	GV.PO-P4
Task	T308	Update privacy roles and responsibilities in accordance with changes to third-party stakeholder relationships.	GV.PO-P4
Knowledge	K104	Knowledge of mutual processes needed to engage with [*organization-defined third-party stakeholders*].	GV.PO-P4
Knowledge	K150	Knowledge of RACI Assignment Matrix (Responsible, Accountable, Consulted, Informed).	GV.PO-P3; GV.PO-P4; CM.PO-P2
Knowledge	K208	Knowledge of the capabilities of [*organization-defined third-party stakeholders*].	GV.PO-P4
Knowledge	K283	Knowledge of the organization's privacy needs related to each [*organization-defined third-party stakeholder*].	GV.PO-P4
Knowledge	K291	Knowledge of the organization's privacy strategy.	GV.PO-P4
Knowledge	K329	Knowledge of third-party data processing activities.	GV.PO-P4
Knowledge	K330	Knowledge of third-party stakeholder risk types.	GV.PO-P4
Knowledge	K335	Knowledge of vendor management concepts.	GV.PO-P4
Skill	S031	Skill in applying templates to manage [*organization-defined third-party stakeholder*] responsibilities.	GV.PO-P4
Skill	S130	Skill in drafting privacy roles and responsibilities that relate to third-party stakeholder relationships.	GV.PO-P4
Skill	S176	Skill in identifying privacy roles and responsibilities related to new data processing activities.	GV.PO-P4
Skill	S181	Skill in identifying the most appropriate internal or external individuals involved in [*organization-defined third-party stakeholder*] engagement.	GV.PO-P4
Skill	S211	Skill in managing mutual privacy expectations with third-party stakeholders.	GV.PO-P4
Skill	S233	Skill in negotiating third-party agreements to align with organizational privacy roles and responsibilities.	GV.PO-P4
Subcategory	**GV.PO-P5**	**Legal, regulatory, and contractual requirements regarding privacy are understood and managed.**	
Task	T220	Identify contractual privacy requirements.	GV.PO-P5

Statement Type	ID	Description	Subcategory Mapping
Task	T235	Identify privacy requirements in privacy laws and regulations as they apply to the organization's data processing activities.	GV.PO-P5
Task	T268	Maintain a document repository for compliance with privacy laws and regulations.	GV.PO-P5
Knowledge	K017	Knowledge of business strategies and practices that implicate privacy.	GV.PO-P5
Knowledge	K051	Knowledge of data processing ecosystem parties, including their jurisdiction and role in relation to the organization's data processing activities.	GV.PO-P5
Knowledge	K055	Knowledge of data processing requirements.	ID.DE-P1; GV.PO-P5
Knowledge	K082	Knowledge of information or other evidence necessary for responding to regulators.	GV.PO-P5
Knowledge	K129	Knowledge of privacy guidelines and tools to aid with development of crosswalk(s) and/or compliance register(s).	GV.PO-P5
Knowledge	K341	Knowledge of where information on ecosystem parties is located.	GV.PO-P5
Knowledge	K346	Knowledge of where your organization keeps formal documentation on its current state of privacy compliance.	GV.PO-P5; GV.MT-P3; GV.MT-P4; GV.MT-P5; GV.MT-P7
Skill	S037	Skill in applying vendor risk management (VRM) methodologies to understand where and how data processing ecosystem partners process data the organization is responsible for.	GV.PO-P5
Skill	S056	Skill in assessing the impact of new laws and regulations on contract negotiation.	GV.PO-P5
Skill	S057	Skill in assessing the impact of new laws and regulations on privacy requirements.	GV.PO-P5; GV.MT-P1
Skill	S072	Skill in automating legal and regulatory requirements involving privacy operations.	GV.PO-P5
Skill	S124	Skill in documenting where information on ecosystem parties is located.	GV.PO-P5
Skill	S165	Skill in gathering correct, accurate, and relevant information.	ID.RA-P1; GV.PO-P5
Skill	S213	Skill in managing privacy compliance efforts.	GV.PO-P5
Skill	S252	Skill in performing contract negotiations and reviews that are effective for achieving privacy objectives.	GV.PO-P5
Skill	S265	Skill in researching legal opinions and related best practices in accord with laws and regulations.	GV.PO-P5
Skill	S298	Skill in translating relevant legal and regulatory requirements to the organization's needs.	GV.PO-P5; GV.MT-P2; GV.MT-P3; GV.MT-P4; GV.MT-P5; GV.MT-P7; CT.PO-P1; CT.PO-P2; CT.PO-P3
Skill	S302	Skill in utilizing legal and regulatory analysis tools.	GV.PO-P5
Subcategory	**GV.PO-P6**	**Governance and risk management policies, processes, and procedures address privacy risks.**	
Task	T003	Align governance and risk management policies/processes/procedures with privacy risk assessment results.	GV.PO-P6
Task	T120	Determine the extent to which governance and risk management policies/processes/procedures adequately address privacy risks.	GV.PO-P6
Knowledge	K238	Knowledge of the organization's activities that impact privacy.	GV.PO-P6
Knowledge	K255	Knowledge of the organization's data processing goals.	ID.DE-P1; GV.PO-P6; GV.RM-P1; GV.RM-P2; GV.RM-P3; GV.MT-P3; GV.MT-P4; GV.MT-P5; GV.MT-P6; GV.MT-P7; CT.PO-P1; CT.PO-P2; CT.PO-P3; CM.PO-P1
Knowledge	K258	Knowledge of the organization's data strategy.	ID.DE-P1; GV.PO-P6; GV.RM-P1; GV.RM-P2; GV.RM-P3; GV.MT-P3; GV.MT-P4; GV.MT-P5; GV.MT-P6; GV.MT-P7; CT.PO-P1; CT.PO-P2; CT.PO-P3; CM.PO-P1
Knowledge	K266	Knowledge of the organization's governance structure.	GV.PO-P6; GV.RM-P1
Knowledge	K314	Knowledge of the results of privacy risk assessments conducted or sanctioned by the organization.	GV.PO-P6

Statement Type	ID	Description	Subcategory Mapping
Knowledge	K342	Knowledge of where organizational governance and risk management policies/processes/procedures are documented.	GV.PO-P6
Skill	S109	Skill in determining appropriate changes to governance, risk, and privacy policies/processes/procedures.	GV.PO-P6; GV.MT-P1; GV.MT-P2
Skill	S164	Skill in fostering changes necessary to reduce risk and strengthen the organization's privacy posture.	GV.PO-P6
Skill	S187	Skill in identifying whether previously performed privacy risk assessments are still relevant to the organization.	GV.PO-P6
Skill	S196	Skill in incorporating organizational privacy priorities into governance and risk management policies/processes/procedures.	GV.PO-P6
Skill	S200	Skill in interpreting privacy risk assessment results.	ID.DE-P2; GV.PO-P6
Skill	S220	Skill in mapping governance, risk, and privacy policies/processes/procedures.	GV.PO-P6
Skill	S243	Skill in performing a gap analysis.	GV.PO-P6
Subcategory	**GV.RM-P1**	**Risk management processes are established, managed, and agreed to by organizational stakeholders.**	
Task	T025	Assign privacy risk management responsibilities to organizational roles.	GV.PO-P3; GV.RM-P1
Task	T062	Create a risk management process(es) in collaboration with [*organization-defined stakeholders*].	GV.RM-P1
Task	T179	Document the risk management process(es) in collaboration with [*organization-defined stakeholders*].	GV.RM-P1
Task	T207	Evaluate the organization's risk management process(es) for privacy gaps.	GV.RM-P1
Task	T217	Identify any existing risk management policies/processes/procedures.	GV.RM-P1
Task	T240	Identify the categories of risk that inform existing organizational risk management process(es).	GV.RM-P1
Task	T261	Incorporate privacy into the organization's risk management process(es).	GV.RM-P1
Knowledge	K068	Knowledge of enterprise risk management principles.	GV.RM-P1
Knowledge	K121	Knowledge of potential executive sponsors.	GV.RM-P1
Knowledge	K163	Knowledge of resources required for risk management.	ID.BE-P1; ID.BE-P2; ID.BE-P3; GV.RM-P1; GV.RM-P2; GV.RM-P3
Knowledge	K168	Knowledge of risk management processes.	ID.DE-P1; ID.DE-P2; ID.DE-P3; ID.DE-P4; ID.DE-P5; GV.RM-P1; GV.RM-P2; GV.RM-P3
Knowledge	K195	Knowledge of systems/products/services within scope of risk management.	GV.RM-P1
Knowledge	K229	Knowledge of the extent to which privacy is considered/addressed as a risk within the organization.	GV.RM-P1
Knowledge	K255	Knowledge of the organization's data processing goals.	ID.DE-P1; GV.PO-P6; GV.RM-P1; GV.RM-P2; GV.RM-P3; GV.MT-P3; GV.MT-P4; GV.MT-P5; GV.MT-P6; GV.MT-P7; CT.PO-P1; CT.PO-P2; CT.PO-P3; CM.PO-P1
Knowledge	K258	Knowledge of the organization's data strategy.	ID.DE-P1; GV.PO-P6; GV.RM-P1; GV.RM-P2; GV.RM-P3; GV.MT-P3; GV.MT-P4; GV.MT-P5; GV.MT-P6; GV.MT-P7; CT.PO-P1; CT.PO-P2; CT.PO-P3; CM.PO-P1
Knowledge	K261	Knowledge of the organization's expansion or consolidation plans.	ID.BE-P2; GV.RM-P1; GV.RM-P2; GV.RM-P3
Knowledge	K264	Knowledge of the organization's future roadmap.	ID.BE-P2; GV.RM-P1; GV.RM-P2; GV.RM-P3
Knowledge	K266	Knowledge of the organization's governance structure.	GV.PO-P6; GV.RM-P1
Knowledge	K280	Knowledge of the organization's prioritized privacy outcomes.	ID.RA-P5; GV.PO-P1; GV.PO-P3; GV.RM-P1; GV.MT-P1; GV.MT-P2
Skill	S006	Skill in advocating for an enterprise risk management strategy.	GV.RM-P1

Statement Type	ID	Description	Subcategory Mapping
Skill	S008	Skill in advocating for privacy equities with [*organization-defined stakeholders*], including securing executive sponsorship where necessary.	GV.RM-P1
Skill	S133	Skill in educating [*organization-defined stakeholders*] on privacy risk.	GV.RM-P1
Skill	S210	Skill in managing multi-stakeholder processes.	GV.RM-P1
Skill	S239	Skill in obtaining stakeholder engagement.	GV.RM-P1
Skill	S303	Skill in writing technical content for risk management processes.	GV.RM-P1
Subcategory	**GV.RM-P2**	**Organizational risk tolerance is determined and clearly expressed.**	
Task	T020	Assess the organization's risk tolerance for gaps between policies/processes/procedures and risks associated with current practices.	GV.RM-P2
Task	T027	Attain [*organization-defined stakeholder*] feedback on the risk tolerance assessment.	GV.RM-P2
Task	T193	Establish principles that inform risk assessment and associated decision-making.	GV.RM-P2
Task	T229	Identify how the organization conveys risk tolerance.	GV.RM-P2
Task	T262	Incorporate stakeholder responses to the risk tolerance assessment into the organization's risk-related policies/processes/procedures.	GV.RM-P2
Knowledge	K067	Knowledge of emerging technology.	GV.RM-P2
Knowledge	K108	Knowledge of organization's approach to information governance.	GV.RM-P2
Knowledge	K110	Knowledge of organization's internal and external policies.	GV.RM-P2
Knowledge	K111	Knowledge of organization's sector-specific risks.	GV.RM-P2
Knowledge	K122	Knowledge of potential impacts of risks to the organization.	GV.RM-P2
Knowledge	K163	Knowledge of resources required for risk management.	ID.BE-P1; ID.BE-P2; ID.BE-P3; GV.RM-P1; GV.RM-P2; GV.RM-P3
Knowledge	K167	Knowledge of risk assessment criteria.	GV.RM-P2
Knowledge	K168	Knowledge of risk management processes.	ID.DE-P1; ID.DE-P2; ID.DE-P3; ID.DE-P4; ID.DE-P5; GV.RM-P1; GV.RM-P2; GV.RM-P3
Knowledge	K255	Knowledge of the organization's data processing goals.	ID.DE-P1; GV.PO-P6; GV.RM-P1; GV.RM-P2; GV.RM-P3; GV.MT-P3; GV.MT-P4; GV.MT-P5; GV.MT-P6; GV.MT-P7; CT.PO-P1; CT.PO-P2; CT.PO-P3; CM.PO-P1
Knowledge	K258	Knowledge of the organization's data strategy.	ID.DE-P1; GV.PO-P6; GV.RM-P1; GV.RM-P2; GV.RM-P3; GV.MT-P3; GV.MT-P4; GV.MT-P5; GV.MT-P6; GV.MT-P7; CT.PO-P1; CT.PO-P2; CT.PO-P3; CM.PO-P1
Knowledge	K261	Knowledge of the organization's expansion or consolidation plans.	ID.BE-P2; GV.RM-P1; GV.RM-P2; GV.RM-P3
Knowledge	K264	Knowledge of the organization's future roadmap.	ID.BE-P2; GV.RM-P1; GV.RM-P2; GV.RM-P3
Knowledge	K296	Knowledge of the organization's risk management process(es).	GV.RM-P2; CM.AW-P8
Skill	S249	Skill in performing analysis of risk in a defined risk management process.	GV.RM-P2
Skill	S038	Skill in articulating how privacy incorporates into the organization's risks.	GV.RM-P2
Skill	S186	Skill in identifying undocumented/implicit risk tolerance policies/processes/procedures.	GV.RM-P2
Subcategory	**GV.RM-P3**	**The organization’s determination of risk tolerance is informed by its role(s) in the data processing ecosystem.**	
Notes: Organizations may find it useful to meet this outcome prior to, or concurrent with, meeting GV.RM-P2 above.			

Statement Type	ID	Description	Subcategory Mapping
Task	T014	Assess how the organization's role(s) in the data processing ecosystem affects its ability to manage risk.	GV.RM-P3
Task	T079	Determine acceptable actions for responding to risks that exceed the organization's risk tolerance with input from [*organization-defined stakeholders*].	GV.RM-P3
Task	T133	Determine the organization's non-regulation-defined role(s) in the data processing ecosystem.	ID.BE-P1; GV.RM-P3
Task	T134	Determine the organization's regulation-defined role(s) in the data processing ecosystem.	ID.BE-P1; GV.RM-P3
Task	T135	Determine the risks associated with each organizational role in the data processing ecosystem that exceed (or could exceed) the organization's risk tolerance.	GV.RM-P3
Knowledge	K231	Knowledge of the factors that inform the organization's risk tolerance determination.	GV.RM-P3
Knowledge	K163	Knowledge of resources required for risk management.	ID.BE-P1; ID.BE-P2; ID.BE-P3; GV.RM-P1; GV.RM-P2; GV.RM-P3
Knowledge	K168	Knowledge of risk management processes.	ID.DE-P1; ID.DE-P2; ID.DE-P3; ID.DE-P4; ID.DE-P5; GV.RM-P1; GV.RM-P2; GV.RM-P3
Knowledge	K247	Knowledge of the organization's contractual commitments.	GV.RM-P3
Knowledge	K255	Knowledge of the organization's data processing goals.	ID.DE-P1; GV.PO-P6; GV.RM-P1; GV.RM-P2; GV.RM-P3; GV.MT-P3; GV.MT-P4; GV.MT-P5; GV.MT-P6; GV.MT-P7; CT.PO-P1; CT.PO-P2; CT.PO-P3; CM.PO-P1
Knowledge	K258	Knowledge of the organization's data strategy.	ID.DE-P1; GV.PO-P6; GV.RM-P1; GV.RM-P2; GV.RM-P3; GV.MT-P3; GV.MT-P4; GV.MT-P5; GV.MT-P6; GV.MT-P7; CT.PO-P1; CT.PO-P2; CT.PO-P3; CM.PO-P1
Knowledge	K261	Knowledge of the organization's expansion or consolidation plans.	ID.BE-P2; GV.RM-P1; GV.RM-P2; GV.RM-P3
Knowledge	K264	Knowledge of the organization's future roadmap.	ID.BE-P2; GV.RM-P1; GV.RM-P2; GV.RM-P3
Knowledge	K297	Knowledge of the organization's risk tolerance.	ID.BE-P3; ID.RA-P5; ID.DE-P3; GV.RM-P3; GV.MT-P1
Knowledge	K325	Knowledge of the ways in which the organization's role(s) in the data processing ecosystem affects its ability to manage risk.	GV.RM-P3
Skill	S010	Skill in advocating for privacy risk management priorities.	GV.RM-P3
Skill	S111	Skill in determining contractual obligations that arise from the organization's role in the data processing ecosystem.	GV.RM-P3
Skill	S182	Skill in identifying the organization's role in the data processing ecosystem.	GV.RM-P3
Subcategory	**GV.AT-P1**	**The workforce is informed and trained on its roles and responsibilities.**	
Task	T022	Assess workforce learning needs at an [*organization-defined frequency*].	GV.AT-P1
Task	T030	Collect feedback on learning activities and materials from [*organization-defined stakeholders*].	GV.AT-P1
Task	T108	Determine resources to support the learning program.	GV.AT-P1
Task	T119	Determine the delivery methods for the learning program.	GV.AT-P1
Task	T186	Establish a learning program plan.	GV.AT-P1
Task	T205	Evaluate the learning program plan at an [*organization-defined frequency*] against the organization's training needs assessment.	GV.AT-P1
Task	T225	Identify gaps in the current learning program.	GV.AT-P1
Task	T253	Implement learning activities.	GV.AT-P1
Task	T254	Implement lessons learned from the evaluation of the learning plan into a revised learning plan at an [*organization-defined frequency*].	GV.AT-P1

Statement Type	ID	Description	Subcategory Mapping
Knowledge	K070	Knowledge of existing learning materials.	GV.AT-P1
Knowledge	K086	Knowledge of learning program delivery methods.	GV.AT-P1
Knowledge	K087	Knowledge of learning solutions.	GV.AT-P1
Knowledge	K165	Knowledge of resources to support learning activities.	GV.AT-P1
Knowledge	K263	Knowledge of the organization's functional areas.	GV.AT-P1
Knowledge	K326	Knowledge of the workforce population.	GV.AT-P1
Knowledge	K349	Knowledge of workforce learning preferences.	GV.AT-P1
Skill	S001	Skill in adapting learning activities and materials to meet evolving needs.	GV.AT-P1
Skill	S002	Skill in adapting training to audience knowledge level.	GV.AT-P2
Skill	S035	Skill in applying the results of training need assessments to the evaluation of learning programs.	GV.AT-P1
Skill	S041	Skill in assessing a learner's demonstrated privacy knowledge.	GV.AT-P1
Skill	S066	Skill in assessing whether knowledge is transformed into behavior.	GV.AT-P1
Skill	S085	Skill in conducting training needs assessment(s).	GV.AT-P1
Skill	S104	Skill in designing feedback mechanisms to provide insight into learning activities and materials.	GV.AT-P1
Skill	S162	Skill in facilitating communication among [*organization-defined stakeholders*] about the learning program plan, including how it supports organizational and learning goals and impacts personnel.	GV.AT-P1
Skill	S202	Skill in interpreting training data/feedback.	GV.AT-P1
Subcategory	**GV.AT-P2**	**Senior executives understand their roles and responsibilities.**	
Task	T012	Assess [*Select: senior executive; privacy personnel; third party*] privacy-related duties and responsibilities at an [*organization-defined frequency*].	GV.AT-P2; GV.AT-P3; GV.AT-P4
Knowledge	K141	Knowledge of privacy risks of greatest importance to the organization's senior executives.	GV.AT-P2
Knowledge	K270	Knowledge of the organization's leadership structure.	GV.AT-P2
Skill	S013	Skill in aligning executive roles and responsibilities to their specific business function.	GV.AT-P2
Subcategory	**GV.AT-P3**	**Privacy personnel understand their roles and responsibilities.**	
Task	T012	Assess [*Select: senior executive; privacy personnel; third party*] privacy-related duties and responsibilities at an [*organization-defined frequency*].	GV.AT-P2; GV.AT-P3; GV.AT-P4
Task	T154	Develop role-based learning materials for privacy personnel based on duties and responsibilities.	GV.AT-P3
Task	T222	Identify external training or certifications that support job performance.	GV.AT-P3
Knowledge	K149	Knowledge of professional privacy training options.	GV.AT-P3
Subcategory	**GV.AT-P4**	**Third parties (e.g., service providers, customers, partners) understand their roles and responsibilities.**	
Task	T012	Assess [*Select: senior executive; privacy personnel; third party*] privacy-related duties and responsibilities at an [*organization-defined frequency*].	GV.AT-P2; GV.AT-P3; GV.AT-P4
Task	T182	Document the specific roles and responsibilities expected from each third party.	GV.AT-P4
Task	T248	Identify third parties with privacy roles and responsibilities.	GV.AT-P4
Task	T286	Provide privacy learning materials to third parties.	GV.AT-P4
Knowledge	K322	Knowledge of the third parties' data processing activities	GV.AT-P4
Subcategory	**GV.MT-P1**	**Privacy risk is re-evaluated on an ongoing basis and as key factors, including the organization's business environment (e.g., introduction of new technologies), governance (e.g., legal obligations, risk tolerance), data processing, and systems/products/services change.**	
Task	T121	Determine the factors which will drive the re-evaluation of organizational privacy risk.	GV.MT-P1

Statement Type	ID	Description	Subcategory Mapping
Task	T144	Determine whether privacy risk re-evaluation is merited based on analysis of internal and external events at an [*organization-defined cadence*].	GV.MT-P1
Task	T146	Determine which components of privacy risk assessment should be re-evaluated based on changes to [*organization-defined key factors*].	GV.MT-P1
Task	T285	Provide [*organization-defined stakeholders*] with access to updated documentation of privacy risk assessments.	GV.MT-P1
Knowledge	K023	Knowledge of changes to [*organization-defined key factors*] that determine risk re-evaluation.	GV.MT-P1
Knowledge	K338	Knowledge of ways the organization stores/keeps privacy risk assessments.	GV.MT-P1
Knowledge	K175	Knowledge of roles and responsibilities assigned to the privacy risk re-evaluation process.	GV.MT-P1
Knowledge	K181	Knowledge of stakeholders who need to be informed of privacy risk assessments.	GV.MT-P1
Knowledge	K213	Knowledge of the components of the organization's privacy risk assessments.	GV.MT-P1
Knowledge	K280	Knowledge of the organization's prioritized privacy outcomes.	ID.RA-P5; GV.PO-P1; GV.PO-P3; GV.RM-P1; GV.MT-P1; GV.MT-P2
Knowledge	K282	Knowledge of the organization's privacy control baseline.	GV.MT-P1
Knowledge	K297	Knowledge of the organization's risk tolerance.	ID.BE-P3; ID.RA-P5; ID.DE-P3; GV.RM-P3; GV.MT-P1
Knowledge	K303	Knowledge of the organization's systems/products/services.	GV.MT-P1; ID.IM-P1; ID.IM-P2; ID.IM-P3; ID.IM-P4; ID.IM-P5; ID.IM-P6; ID.IM-P7; ID.IM-P8; ID.BE-P3; ID.RA-P1
Skill	S020	Skill in applying criteria for a privacy risk re-evaluation.	GV.MT-P1
Skill	S040	Skill in articulating the relationship between privacy risk mitigating controls and privacy risk.	ID.RA-P5; GV.MT-P1
Skill	S057	Skill in assessing the impact of new laws and regulations on privacy requirements.	GV.PO-P5; GV.MT-P1
Skill	S074	Skill in calculating risk prioritization.	ID.RA-P5; GV.MT-P1
Skill	S081	Skill in conducting a privacy risk assessment.	ID.RA-P4; GV.MT-P1
Skill	S109	Skill in determining appropriate changes to governance, risk, and privacy policies/processes/procedures.	GV.PO-P6; GV.MT-P1; GV.MT-P2
Subcategory	**GV.MT-P2**	**Privacy values, policies, and training are reviewed and any updates are communicated.**	
Task	T080	Determine actions to update privacy policies based on the results of their evaluation and any related updates/revisions to privacy values.	GV.MT-P2
Task	T081	Determine actions to update privacy training based on the results of their evaluation and any related updates/revisions to privacy values and/or policies.	GV.MT-P2
Task	T082	Determine actions to update privacy values based on the results of their evaluation.	GV.MT-P2
Task	T090	Determine factors/events that trigger a review of privacy values/policies/training, including the scope of review associated with each triggering event.	GV.MT-P2
Task	T201	Evaluate privacy values/policies/training for gaps based on [*organization-defined triggering factors/events*].	GV.MT-P2
Task	T263	Inform [*organization-defined stakeholders*] of changes and new requirements to privacy values, policies, or trainings.	GV.MT-P2
Knowledge	K073	Knowledge of factors that can create a need to update values/policies/training.	GV.MT-P2
Knowledge	K174	Knowledge of roles and responsibilities assigned to the participants in the values/policies/training review process.	GV.MT-P2
Knowledge	K277	Knowledge of the organization's policy management infrastructure.	GV.MT-P2
Knowledge	K280	Knowledge of the organization's prioritized privacy outcomes.	ID.RA-P5; GV.PO-P1; GV.PO-P3; GV.RM-P1; GV.MT-P1; GV.MT-P2
Skill	S003	Skill in addressing gaps between current practices and policy requirements.	ID.DE-P1; GV.MT-P2

Statement Type	ID	Description	Subcategory Mapping
Skill	S005	Skill in advising [*organization-defined stakeholders*] on appropriate outcomes based on gaps between legal requirements and organizational objectives.	GV.MT-P2; CT.PO-P4
Skill	S065	Skill in assessing what factors should influence changes to the organization's values/policies/training.	GV.MT-P2
Skill	S079	Skill in communicating privacy legal requirements/principles to [*organization-defined stakeholders*] and decision-makers.	ID.BE-P1; GV.MT-P2; GV.MT-P3; GV.MT-P4; GV.MT-P5; GV.MT-P7
Skill	S109	Skill in determining appropriate changes to governance, risk, and privacy policies/processes/procedures.	GV.PO-P6; GV.MT-P1; GV.MT-P2
Skill	S154	Skill in evaluating whether privacy values are aligned with operations.	GV.MT-P2
Skill	S155	Skill in executing a communications plan.	ID.BE-P3; GV.MT-P2
Skill	S157	Skill in explaining complex topics/ideas.	ID.BE-P3; GV.MT-P2
Skill	S298	Skill in translating relevant legal and regulatory requirements to the organization's needs.	GV.PO-P5; GV.MT-P2; GV.MT-P3; GV.MT-P4; GV.MT-P5; GV.MT-P7; CT.PO-P1; CT.PO-P2; CT.PO-P3
Subcategory	**GV.MT-P3**	**Policies, processes, and procedures for assessing compliance with legal requirements and privacy policies are established and in place.**	
Notes: Organizations may choose to evaluate existing policies/processes/procedures for gaps (e.g., incompleteness, outdated information) and determine necessary actions to address identified gaps.			
Task	T037	Create a policy/policies that addresses the purpose, scope, roles, responsibilities, and coordination required for assessing compliance with legal requirements that is consistent with applicable laws, regulations, standards, and guidelines.	GV.MT-P3
Task	T038	Create a policy/policies that addresses the purpose, scope, roles, responsibilities, and coordination required for assessing compliance with privacy policies that is consistent with applicable laws, regulations, standards, and guidelines.	GV.MT-P3
Task	T061	Create a process(es)/procedure(s) with objectives and associated methods and objects of assessment for assessing compliance with [*Select: legal requirements, privacy policies*].	GV.MT-P3
Knowledge	K071	Knowledge of existing policies/processes/procedures.	GV.PO-P1; GV.MT-P3; GV.MT-P4; GV.MT-P5; GV.MT-P7
Knowledge	K255	Knowledge of the organization's data processing goals.	ID.DE-P1; GV.PO-P6; GV.RM-P1; GV.RM-P2; GV.RM-P3; GV.MT-P3; GV.MT-P4; GV.MT-P5; GV.MT-P6; GV.MT-P7; CT.PO-P1; CT.PO-P2; CT.PO-P3; CM.PO-P1
Knowledge	K258	Knowledge of the organization's data strategy.	ID.DE-P1; GV.PO-P6; GV.RM-P1; GV.RM-P2; GV.RM-P3; GV.MT-P3; GV.MT-P4; GV.MT-P5; GV.MT-P6; GV.MT-P7; CT.PO-P1; CT.PO-P2; CT.PO-P3; CM.PO-P1
Knowledge	K271	Knowledge of the organization's legal requirements related to policies/processes/procedures.	GV.MT-P3; GV.MT-P4; GV.MT-P5; GV.MT-P7
Knowledge	K287	Knowledge of the organization's privacy risk management strategy.	GV.MT-P3; GV.MT-P4; GV.MT-P5; GV.MT-P7
Knowledge	K292	Knowledge of the organization's privacy values.	GV.PO-P1; GV.MT-P3; GV.MT-P4; GV.MT-P5; GV.MT-P7; CT.PO-P1; CT.PO-P2; CT.PO-P3; CM.PO-P1
Knowledge	K293	Knowledge of the organization's process for management and approval of policies/processes/procedures.	GV.MT-P3; GV.MT-P4; GV.MT-P5; GV.MT-P6; GV.MT-P7
Knowledge	K312	Knowledge of the relationships and dependencies among policies, processes, and procedures.	GV.MT-P3; GV.MT-P4; GV.MT-P5; GV.MT-P6; GV.MT-P7
Knowledge	K346	Knowledge of where your organization keeps formal documentation on its current state of privacy compliance.	GV.PO-P5; GV.MT-P3; GV.MT-P4; GV.MT-P5; GV.MT-P7

Statement Type	ID	Description	Subcategory Mapping
Skill	S297	Skill in translating relevant concepts of privacy policies to the organization's practices and activities.	GV.MT-P3; GV.MT-P4; GV.MT-P5; GV.MT-P7
Skill	S298	Skill in translating relevant legal and regulatory requirements to the organization's needs.	GV.PO-P5; GV.MT-P2; GV.MT-P3; GV.MT-P4; GV.MT-P5; GV.MT-P7; CT.PO-P1; CT.PO-P2; CT.PO-P3
Skill	S127	Skill in drafting policies/processes/procedures.	ID.DE-P1; GV.MT-P3; GV.MT-P4; GV.MT-P5; GV.MT-P6; GV.MT-P7; CT.PO-P1; CT.PO-P2; CT.PO-P3; CM.PO-P1
Skill	S212	Skill in managing organizational policies.	GV.PO-P1; GV.MT-P3; GV.MT-P4; GV.MT-P5; GV.MT-P6; GV.MT-P7; CT.PO-P1; CT.PO-P2; CT.PO-P3; CM.PO-P1
Skill	S079	Skill in communicating privacy legal requirements/principles to [*organization-defined stakeholders*] and decision-makers.	ID.BE-P1; GV.MT-P2; GV.MT-P3; GV.MT-P4; GV.MT-P5; GV.MT-P7
Subcategory	**GV.MT-P4**	**Policies, processes, and procedures for communicating progress on managing privacy risks are established and in place.**	
Notes: Organizations may choose to evaluate existing policies/processes/procedures for gaps (e.g., incompleteness, outdated information) and determine necessary actions to address identified gaps.			
Task	T040	Create a policy/policies that addresses the purpose, scope, roles, responsibilities, and coordination required for communicating progress on managing privacy risks that is consistent with applicable laws, regulations, standards, and guidelines.	GV.MT-P4
Task	T059	Create a process(es)/procedure(s) that addresses audience, cadence, and mechanisms for communicating progress on organizational privacy risk management among [*organization-defined stakeholders*].	GV.MT-P4
Knowledge	K071	Knowledge of existing policies/processes/procedures.	GV.PO-P1; GV.MT-P3; GV.MT-P4; GV.MT-P5; GV.MT-P7
Knowledge	K255	Knowledge of the organization's data processing goals.	ID.DE-P1; GV.PO-P6; GV.RM-P1; GV.RM-P2; GV.RM-P3; GV.MT-P3; GV.MT-P4; GV.MT-P5; GV.MT-P6; GV.MT-P7; CT.PO-P1; CT.PO-P2; CT.PO-P3; CM.PO-P1
Knowledge	K258	Knowledge of the organization's data strategy.	ID.DE-P1; GV.PO-P6; GV.RM-P1; GV.RM-P2; GV.RM-P3; GV.MT-P3; GV.MT-P4; GV.MT-P5; GV.MT-P6; GV.MT-P7; CT.PO-P1; CT.PO-P2; CT.PO-P3; CM.PO-P1
Knowledge	K271	Knowledge of the organization's legal requirements related to policies/processes/procedures.	GV.MT-P3; GV.MT-P4; GV.MT-P5; GV.MT-P7
Knowledge	K287	Knowledge of the organization's privacy risk management strategy.	GV.MT-P3; GV.MT-P4; GV.MT-P5; GV.MT-P7
Knowledge	K292	Knowledge of the organization's privacy values.	GV.PO-P1; GV.MT-P3; GV.MT-P4; GV.MT-P5; GV.MT-P7; CT.PO-P1; CT.PO-P2; CT.PO-P3; CM.PO-P1
Knowledge	K293	Knowledge of the organization's process for management and approval of policies/processes/procedures.	GV.MT-P3; GV.MT-P4; GV.MT-P5; GV.MT-P6; GV.MT-P7
Knowledge	K312	Knowledge of the relationships and dependencies among policies, processes, and procedures.	GV.MT-P3; GV.MT-P4; GV.MT-P5; GV.MT-P6; GV.MT-P7
Knowledge	K346	Knowledge of where your organization keeps formal documentation on its current state of privacy compliance.	GV.PO-P5; GV.MT-P3; GV.MT-P4; GV.MT-P5; GV.MT-P7
Skill	S297	Skill in translating relevant concepts of privacy policies to the organization's practices and activities.	GV.MT-P3; GV.MT-P4; GV.MT-P5; GV.MT-P7
Skill	S298	Skill in translating relevant legal and regulatory requirements to the organization's needs.	GV.PO-P5; GV.MT-P2; GV.MT-P3; GV.MT-P4; GV.MT-P5; GV.MT-P7; CT.PO-P1; CT.PO-P2; CT.PO-P3

Statement Type	ID	Description	Subcategory Mapping
Skill	S127	Skill in drafting policies/processes/procedures.	ID.DE-P1; GV.MT-P3; GV.MT-P4; GV.MT-P5; GV.MT-P6; GV.MT-P7; CT.PO-P1; CT.PO-P2; CT.PO-P3; CM.PO-P1
Skill	S212	Skill in managing organizational policies.	GV.PO-P1; GV.MT-P3; GV.MT-P4; GV.MT-P5; GV.MT-P6; GV.MT-P7; CT.PO-P1; CT.PO-P2; CT.PO-P3; CM.PO-P1
Skill	S079	Skill in communicating privacy legal requirements/principles to [*organization-defined stakeholders*] and decision-makers.	ID.BE-P1; GV.MT-P2; GV.MT-P3; GV.MT-P4; GV.MT-P5; GV.MT-P7
Subcategory	**GV.MT-P5**	**Policies, processes, and procedures 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 discovery, privacy researchers, professional events).**	
Notes: Organizations may choose to evaluate existing policies/processes/procedures for gaps (e.g., incompleteness, outdated information) and determine necessary actions to address identified gaps.			
Task	T036	Create a policy/policies that addresses the purpose, scope, roles, responsibilities, and coordination required for analysis and organizational information sharing related to problematic data actions that is consistent with applicable laws, regulations, standards, and guidelines	GV.MT-P5
Task	T054	Create a process(es)/procedure(s) for facilitating analysis and information sharing about problematic data actions among [*organization-defined stakeholders*].	GV.MT-P5
Knowledge	K071	Knowledge of existing policies/processes/procedures.	GV.PO-P1; GV.MT-P3; GV.MT-P4; GV.MT-P5; GV.MT-P7
Knowledge	K255	Knowledge of the organization's data processing goals.	ID.DE-P1; GV.PO-P6; GV.RM-P1; GV.RM-P2; GV.RM-P3; GV.MT-P3; GV.MT-P4; GV.MT-P5; GV.MT-P6; GV.MT-P7; CT.PO-P1; CT.PO-P2; CT.PO-P3; CM.PO-P1
Knowledge	K258	Knowledge of the organization's data strategy.	ID.DE-P1; GV.PO-P6; GV.RM-P1; GV.RM-P2; GV.RM-P3; GV.MT-P3; GV.MT-P4; GV.MT-P5; GV.MT-P6; GV.MT-P7; CT.PO-P1; CT.PO-P2; CT.PO-P3; CM.PO-P1
Knowledge	K271	Knowledge of the organization's legal requirements related to policies/processes/procedures.	GV.MT-P3; GV.MT-P4; GV.MT-P5; GV.MT-P7
Knowledge	K287	Knowledge of the organization's privacy risk management strategy.	GV.MT-P3; GV.MT-P4; GV.MT-P5; GV.MT-P7
Knowledge	K292	Knowledge of the organization's privacy values.	GV.PO-P1; GV.MT-P3; GV.MT-P4; GV.MT-P5; GV.MT-P7; CT.PO-P1; CT.PO-P2; CT.PO-P3; CM.PO-P1
Knowledge	K293	Knowledge of the organization's process for management and approval of policies/processes/procedures.	GV.MT-P3; GV.MT-P4; GV.MT-P5; GV.MT-P6; GV.MT-P7
Knowledge	K312	Knowledge of the relationships and dependencies among policies, processes, and procedures.	GV.MT-P3; GV.MT-P4; GV.MT-P5; GV.MT-P6; GV.MT-P7
Knowledge	K346	Knowledge of where your organization keeps formal documentation on its current state of privacy compliance.	GV.PO-P5; GV.MT-P3; GV.MT-P4; GV.MT-P5; GV.MT-P7
Skill	S297	Skill in translating relevant concepts of privacy policies to the organization's practices and activities.	GV.MT-P3; GV.MT-P4; GV.MT-P5; GV.MT-P7
Skill	S298	Skill in translating relevant legal and regulatory requirements to the organization's needs.	GV.PO-P5; GV.MT-P2; GV.MT-P3; GV.MT-P4; GV.MT-P5; GV.MT-P7; CT.PO-P1; CT.PO-P2; CT.PO-P3

Statement Type	ID	Description	Subcategory Mapping
Skill	S127	Skill in drafting policies/processes/procedures.	ID.DE-P1; GV.MT-P3; GV.MT-P4; GV.MT-P5; GV.MT-P6; GV.MT-P7; CT.PO-P1; CT.PO-P2; CT.PO-P3; CM.PO-P1
Skill	S212	Skill in managing organizational policies.	GV.PO-P1; GV.MT-P3; GV.MT-P4; GV.MT-P5; GV.MT-P6; GV.MT-P7; CT.PO-P1; CT.PO-P2; CT.PO-P3; CM.PO-P1
Skill	S079	Skill in communicating privacy legal requirements/principles to [*organization-defined stakeholders*] and decision-makers.	ID.BE-P1; GV.MT-P2; GV.MT-P3; GV.MT-P4; GV.MT-P5; GV.MT-P7
Subcategory	**GV.MT-P6**	**Policies, processes, and procedures incorporate lessons learned from problematic data actions.**	
Task	T016	Assess problematic data actions for lessons learned.	GV.MT-P6
Task	T085	Determine changes to policies/processes/procedures based on lessons learned from problematic data actions in consultation with [*organization-defined stakeholders*].	GV.MT-P6
Task	T143	Determine whether lessons learned from problematic data actions(s) require a change to policies/process/procedures.	GV.MT-P6
Task	T260	Incorporate appropriate changes to policies/processes/procedures based on lessons learned from problematic data actions and with [*organization-defined stakeholder*] consensus.	GV.MT-P6
Knowledge	K224	Knowledge of the different types of problematic data actions.	GV.MT-P6
Knowledge	K226	Knowledge of the effect of preventative policies/processes/procedures on problematic data action(s).	GV.MT-P6
Knowledge	K232	Knowledge of the impact of problematic data actions (i.e., on individuals and/or organizations).	GV.MT-P6; CM.AW-P8
Knowledge	K233	Knowledge of the impact of the organization's problematic data actions (i.e., on individuals and/or the organization).	GV.MT-P6; CM.AW-P8
Knowledge	K255	Knowledge of the organization's data processing goals.	ID.DE-P1; GV.PO-P6; GV.RM-P1; GV.RM-P2; GV.RM-P3; GV.MT-P3; GV.MT-P4; GV.MT-P5; GV.MT-P6; GV.MT-P7; CT.PO-P1; CT.PO-P2; CT.PO-P3; CM.PO-P1
Knowledge	K258	Knowledge of the organization's data strategy.	ID.DE-P1; GV.PO-P6; GV.RM-P1; GV.RM-P2; GV.RM-P3; GV.MT-P3; GV.MT-P4; GV.MT-P5; GV.MT-P6; GV.MT-P7; CT.PO-P1; CT.PO-P2; CT.PO-P3; CM.PO-P1
Knowledge	K293	Knowledge of the organization's process for management and approval of policies/processes/procedures.	GV.MT-P3; GV.MT-P4; GV.MT-P5; GV.MT-P6; GV.MT-P7
Knowledge	K312	Knowledge of the relationships and dependencies among policies, processes, and procedures.	GV.MT-P3; GV.MT-P4; GV.MT-P5; GV.MT-P6; GV.MT-P7
Skill	S084	Skill in conducting root cause analysis.	GV.MT-P6
Skill	S088	Skill in correlating problematic data actions with potential problems.	ID.RA-P4; GV.MT-P6
Skill	S110	Skill in determining appropriate changes to policies/processes/procedures to mitigate past issues from problematic data actions.	GV.MT-P6
Skill	S127	Skill in drafting policies/processes/procedures.	ID.DE-P1; GV.MT-P3; GV.MT-P4; GV.MT-P5; GV.MT-P6; GV.MT-P7; CT.PO-P1; CT.PO-P2; CT.PO-P3; CM.PO-P1

Statement Type	ID	Description	Subcategory Mapping
Skill	S212	Skill in managing organizational policies.	GV.PO-P1; GV.MT-P3; GV.MT-P4; GV.MT-P5; GV.MT-P6; GV.MT-P7; CT.PO-P1; CT.PO-P2; CT.PO-P3; CM.PO-P1
Skill	S221	Skill in mapping policies/processes/procedures to identified problems.	GV.MT-P6
Subcategory	**GV.MT-P7**	**Policies, processes, and procedures for receiving, tracking, and responding to complaints, concerns, and questions from individuals about organizational privacy practices are established and in place.**	
Notes: Organizations may choose to evaluate existing policies/processes/procedures for gaps (e.g., incompleteness, outdated information) and determine necessary actions to address identified gaps.			
Task	T044	Create a policy/policies that addresses the purpose, scope, roles, responsibilities, and coordination required for managing feedback from individuals about organizational privacy practices that is consistent with applicable laws, regulations, standards, and guidelines.	GV.MT-P7
Task	T052	Create a process(es)/procedure(s) for [*Select: receiving; responding to; tracking*] feedback from individuals about organizational privacy practices.	GV.MT-P7
Knowledge	K071	Knowledge of existing policies/processes/procedures.	GV.PO-P1; GV.MT-P3; GV.MT-P4; GV.MT-P5; GV.MT-P7
Knowledge	K255	Knowledge of the organization's data processing goals.	ID.DE-P1; GV.PO-P6; GV.RM-P1; GV.RM-P2; GV.RM-P3; GV.MT-P3; GV.MT-P4; GV.MT-P5; GV.MT-P6; GV.MT-P7; CT.PO-P1; CT.PO-P2; CT.PO-P3; CM.PO-P1
Knowledge	K258	Knowledge of the organization's data strategy.	ID.DE-P1; GV.PO-P6; GV.RM-P1; GV.RM-P2; GV.RM-P3; GV.MT-P3; GV.MT-P4; GV.MT-P5; GV.MT-P6; GV.MT-P7; CT.PO-P1; CT.PO-P2; CT.PO-P3; CM.PO-P1
Knowledge	K271	Knowledge of the organization's legal requirements related to policies/processes/procedures.	GV.MT-P3; GV.MT-P4; GV.MT-P5; GV.MT-P7
Knowledge	K287	Knowledge of the organization's privacy risk management strategy.	GV.MT-P3; GV.MT-P4; GV.MT-P5; GV.MT-P7
Knowledge	K292	Knowledge of the organization's privacy values.	GV.PO-P1; GV.MT-P3; GV.MT-P4; GV.MT-P5; GV.MT-P7; CT.PO-P1; CT.PO-P2; CT.PO-P3; CM.PO-P1
Knowledge	K293	Knowledge of the organization's process for management and approval of policies/processes/procedures.	GV.MT-P3; GV.MT-P4; GV.MT-P5; GV.MT-P6; GV.MT-P7
Knowledge	K312	Knowledge of the relationships and dependencies among policies, processes, and procedures.	GV.MT-P3; GV.MT-P4; GV.MT-P5; GV.MT-P6; GV.MT-P7
Knowledge	K346	Knowledge of where your organization keeps formal documentation on its current state of privacy compliance.	GV.PO-P5; GV.MT-P3; GV.MT-P4; GV.MT-P5; GV.MT-P7
Skill	S297	Skill in translating relevant concepts of privacy policies to the organization's practices and activities.	GV.MT-P3; GV.MT-P4; GV.MT-P5; GV.MT-P7
Skill	S298	Skill in translating relevant legal and regulatory requirements to the organization's needs.	GV.PO-P5; GV.MT-P2; GV.MT-P3; GV.MT-P4; GV.MT-P5; GV.MT-P7; CT.PO-P1; CT.PO-P2; CT.PO-P3
Skill	S127	Skill in drafting policies/processes/procedures.	ID.DE-P1; GV.MT-P3; GV.MT-P4; GV.MT-P5; GV.MT-P6; GV.MT-P7; CT.PO-P1; CT.PO-P2; CT.PO-P3; CM.PO-P1
Skill	S212	Skill in managing organizational policies.	GV.PO-P1; GV.MT-P3; GV.MT-P4; GV.MT-P5; GV.MT-P6; GV.MT-P7; CT.PO-P1; CT.PO-P2; CT.PO-P3; CM.PO-P1

Statement Type	ID	Description	Subcategory Mapping
Skill	S079	Skill in communicating privacy legal requirements/principles to [*organization-defined stakeholders*] and decision-makers.	ID.BE-P1; GV.MT-P2; GV.MT-P3; GV.MT-P4; GV.MT-P5; GV.MT-P7
Subcategory	**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.**	
Notes: Distinctions between policies/processes/procedures for authorizing, revoking and maintaining data processing authorizations respectively may depend on the organization. Some organizations may require separate activities to create and implement each one. **Organizations may choose to evaluate existing policies/processes/procedures for gaps (e.g., incompleteness, outdated information) and determine necessary actions to address identified gaps.**			
Task	T041	Create a policy/policies that addresses the purpose, scope, roles, responsibilities, and coordination required for data processing authorizations that is consistent with applicable laws, regulations, standards, and guidelines.	CT.PO-P1
Task	T056	Create a process(es)/procedure(s) for implementing policies for data processing authorizations related to [*Select: organizational decisions; individuals whose data are processed*].	CT.PO-P1
Knowledge	K254	Knowledge of the organization's data processing ecosystem.	ID.BE-P1; ID.DE-P1; ID.DE-P2; ID.DE-P3; ID.DE-P4; ID.DE-P5; CT.PO-P1; CT.PO-P2; CT.PO-P3; CT.PO-P4; CM.AW-P1; CM.AW-P2; CM.AW-P3; CM.AW-P4; CM.AW-P5; CM.AW-P6; CM.AW-P7; CM.AW-P8
Knowledge	K255	Knowledge of the organization's data processing goals.	ID.DE-P1; GV.PO-P6; GV.RM-P1; GV.RM-P2; GV.RM-P3; GV.MT-P3; GV.MT-P4; GV.MT-P5; GV.MT-P6; GV.MT-P7; CT.PO-P1; CT.PO-P2; CT.PO-P3; CM.PO-P1
Knowledge	K257	Knowledge of the organization's data processing.	ID.IM-P1; ID.IM-P2; ID.IM-P3; ID.IM-P4; ID.IM-P5; ID.IM-P6; ID.IM-P7; ID.IM-P8; CT.PO-P1; CT.PO-P2; CT.PO-P3; CT.PO-P4; CT.DM-P1; CT.DM-P2; CT.DM-P3; CT.DM-P4; CT.DM-P5; CT.DM-P6; CT.DM-P7; CT.DM-P8; CT.DM-P9; CT.DM-P10; CM.AW-P1; CM.AW-P2; CM.AW-P3; CM.AW-P4; CM.AW-P5; CM.AW-P6; CM.AW-P7; CM.AW-P8
Knowledge	K258	Knowledge of the organization's data strategy.	ID.DE-P1; GV.PO-P6; GV.RM-P1; GV.RM-P2; GV.RM-P3; GV.MT-P3; GV.MT-P4; GV.MT-P5; GV.MT-P6; GV.MT-P7; CT.PO-P1; CT.PO-P2; CT.PO-P3; CM.PO-P1
Knowledge	K292	Knowledge of the organization's privacy values.	GV.PO-P1; GV.MT-P3; GV.MT-P4; GV.MT-P5; GV.MT-P7; CT.PO-P1; CT.PO-P2; CT.PO-P3; CM.PO-P1
Knowledge	K302	Knowledge of the organization's systems that store/log authorizations.	CT.PO-P1
Skill	S127	Skill in drafting policies/processes/procedures.	ID.DE-P1; GV.MT-P3; GV.MT-P4; GV.MT-P5; GV.MT-P6; GV.MT-P7; CT.PO-P1; CT.PO-P2; CT.PO-P3; CM.PO-P1

Statement Type	ID	Description	Subcategory Mapping
Skill	S212	Skill in managing organizational policies.	GV.PO-P1; GV.MT-P3; GV.MT-P4; GV.MT-P5; GV.MT-P6; GV.MT-P7; CT.PO-P1; CT.PO-P2; CT.PO-P3; CM.PO-P1
Skill	S298	Skill in translating relevant legal and regulatory requirements to the organization's needs.	GV.PO-P5; GV.MT-P2; GV.MT-P3; GV.MT-P4; GV.MT-P5; GV.MT-P7; CT.PO-P1; CT.PO-P2; CT.PO-P3
Subcategory	**CT.PO-P2**	**Policies, processes, and procedures for enabling data review, transfer, sharing or disclosure, alteration, and deletion are established and in place (e.g., to maintain data quality, manage data retention).**	
Notes: Organizations may choose to evaluate existing policies/processes/procedures for gaps (e.g., incompleteness, outdated information) and determine necessary actions to address identified gaps.			
Task	T035	Create a policy (or policies) that addresses the purpose, scope, roles, responsibilities, and coordination required for data management that is consistent with applicable laws, regulations, standards, and guidelines.	CT.PO-P2
Task	T057	Create a process(es)/procedure(s) for tracking and managing data review, transfer, sharing, or disclosure, alteration, and deletion activities.	CT.PO-P2
Knowledge	K254	Knowledge of the organization's data processing ecosystem.	ID.BE-P1; ID.DE-P1; ID.DE-P2; ID.DE-P3; ID.DE-P4; ID.DE-P5; CT.PO-P1; CT.PO-P2; CT.PO-P3; CT.PO-P4; CM.AW-P1; CM.AW-P2; CM.AW-P3; CM.AW-P4; CM.AW-P5; CM.AW-P6; CM.AW-P7; CM.AW-P8
Knowledge	K255	Knowledge of the organization's data processing goals.	ID.DE-P1; GV.PO-P6; GV.RM-P1; GV.RM-P2; GV.RM-P3; GV.MT-P3; GV.MT-P4; GV.MT-P5; GV.MT-P6; GV.MT-P7; CT.PO-P1; CT.PO-P2; CT.PO-P3; CM.PO-P1
Knowledge	K257	Knowledge of the organization's data processing.	ID.IM-P1; ID.IM-P2; ID.IM-P3; ID.IM-P4; ID.IM-P5; ID.IM-P6; ID.IM-P7; ID.IM-P8; CT.PO-P1; CT.PO-P2; CT.PO-P3; CT.PO-P4; CT.DM-P1; CT.DM-P2; CT.DM-P3; CT.DM-P4; CT.DM-P5; CT.DM-P6; CT.DM-P7; CT.DM-P8; CT.DM-P9; CT.DM-P10; CM.AW-P1; CM.AW-P2; CM.AW-P3; CM.AW-P4; CM.AW-P5; CM.AW-P6; CM.AW-P7; CM.AW-P8
Knowledge	K258	Knowledge of the organization's data strategy.	ID.DE-P1; GV.PO-P6; GV.RM-P1; GV.RM-P2; GV.RM-P3; GV.MT-P3; GV.MT-P4; GV.MT-P5; GV.MT-P6; GV.MT-P7; CT.PO-P1; CT.PO-P2; CT.PO-P3; CM.PO-P1
Knowledge	K292	Knowledge of the organization's privacy values.	GV.PO-P1; GV.MT-P3; GV.MT-P4; GV.MT-P5; GV.MT-P7; CT.PO-P1; CT.PO-P2; CT.PO-P3; CM.PO-P1
Knowledge	K300	Knowledge of the organization's systems that store data.	CT.PO-P2
Skill	S127	Skill in drafting policies/processes/procedures.	ID.DE-P1; GV.MT-P3; GV.MT-P4; GV.MT-P5; GV.MT-P6; GV.MT-P7; CT.PO-P1; CT.PO-P2; CT.PO-P3; CM.PO-P1
Skill	S212	Skill in managing organizational policies.	GV.PO-P1; GV.MT-P3; GV.MT-P4; GV.MT-P5; GV.MT-P6; GV.MT-P7; CT.PO-P1; CT.PO-P2; CT.PO-P3; CM.PO-P1
Skill	S298	Skill in translating relevant legal and regulatory requirements to the organization's needs.	GV.PO-P5; GV.MT-P2; GV.MT-P3; GV.MT-P4; GV.MT-P5; GV.MT-P7; CT.PO-P1; CT.PO-P2; CT.PO-P3

Statement Type	ID	Description	Subcategory Mapping
Subcategory	**CT.PO-P3**	**Policies, processes, and procedures for enabling individuals' data processing preferences and requests are established and in place.**	
Notes: Organizations may choose to evaluate existing policies/processes/procedures for gaps (e.g., incompleteness, outdated information) and determine necessary actions to address identified gaps.			
Task	T043	Create a policy/policies that addresses the purpose, scope, roles, responsibilities, and coordination required for enabling individuals' data processing preferences and requests that is consistent with applicable laws, regulations, standards, and guidelines.	CT.PO-P3
Task	T053	Create a process(es)/procedure(s) for enabling individuals' data processing preferences and requests that includes relevant mechanisms to enable such preferences and requests.	CT.PO-P3
Knowledge	K180	Knowledge of stakeholders responsible for the systems that store individuals' data processing preferences and requests.	CT.PO-P3
Knowledge	K144	Knowledge of privacy tools for enabling data processing requests and preferences.	CT.PO-P3
Knowledge	K196	Knowledge of teams responsible for systems that store individuals' data processing preferences and requests.	CT.PO-P3
Knowledge	K254	Knowledge of the organization's data processing ecosystem.	ID.BE-P1; ID.DE-P1; ID.DE-P2; ID.DE-P3; ID.DE-P4; ID.DE-P5; CT.PO-P1; CT.PO-P2; CT.PO-P3; CT.PO-P4; CM.AW-P1; CM.AW-P2; CM.AW-P3; CM.AW-P4; CM.AW-P5; CM.AW-P6; CM.AW-P7; CM.AW-P8
Knowledge	K255	Knowledge of the organization's data processing goals.	ID.DE-P1; GV.PO-P6; GV.RM-P1; GV.RM-P2; GV.RM-P3; GV.MT-P3; GV.MT-P4; GV.MT-P5; GV.MT-P6; GV.MT-P7; CT.PO-P1; CT.PO-P2; CT.PO-P3; CM.PO-P1
Knowledge	K257	Knowledge of the organization's data processing.	ID.IM-P1; ID.IM-P2; ID.IM-P3; ID.IM-P4; ID.IM-P5; ID.IM-P6; ID.IM-P7; ID.IM-P8; CT.PO-P1; CT.PO-P2; CT.PO-P3; CT.PO-P4; CT.DM-P1; CT.DM-P2; CT.DM-P3; CT.DM-P4; CT.DM-P5; CT.DM-P6; CT.DM-P7; CT.DM-P8; CT.DM-P9; CT.DM-P10; CM.AW-P1; CM.AW-P2; CM.AW-P3; CM.AW-P4; CM.AW-P5; CM.AW-P6; CM.AW-P7; CM.AW-P8
Knowledge	K258	Knowledge of the organization's data strategy.	ID.DE-P1; GV.PO-P6; GV.RM-P1; GV.RM-P2; GV.RM-P3; GV.MT-P3; GV.MT-P4; GV.MT-P5; GV.MT-P6; GV.MT-P7; CT.PO-P1; CT.PO-P2; CT.PO-P3; CM.PO-P1
Knowledge	K292	Knowledge of the organization's privacy values.	GV.PO-P1; GV.MT-P3; GV.MT-P4; GV.MT-P5; GV.MT-P7; CT.PO-P1; CT.PO-P2; CT.PO-P3; CM.PO-P1
Knowledge	K301	Knowledge of the organization's systems that store individuals' data processing preferences and requests.	CT.PO-P3
Knowledge	K306	Knowledge of the privacy expectations of individuals interacting with or affected by the organization's systems/products/services.	CT.PO-P3
Skill	S029	Skill in applying privacy tools to policy/process/procedure creation.	CT.PO-P3
Skill	S127	Skill in drafting policies/processes/procedures.	ID.DE-P1; GV.MT-P3; GV.MT-P4; GV.MT-P5; GV.MT-P6; GV.MT-P7; CT.PO-P1; CT.PO-P2; CT.PO-P3; CM.PO-P1

Statement Type	ID	Description	Subcategory Mapping
Skill	S212	Skill in managing organizational policies.	GV.PO-P1; GV.MT-P3; GV.MT-P4; GV.MT-P5; GV.MT-P6; GV.MT-P7; CT.PO-P1; CT.PO-P2; CT.PO-P3; CM.PO-P1
Skill	S266	Skill in researching trends involving individual data processing preferences and request types.	CT.PO-P3
Skill	S290	Skill in translating individual data processing requests and preferences into viable organizational policies/processes/procedures.	CT.PO-P3
Skill	S298	Skill in translating relevant legal and regulatory requirements to the organization's needs.	GV.PO-P5; GV.MT-P2; GV.MT-P3; GV.MT-P4; GV.MT-P5; GV.MT-P7; CT.PO-P1; CT.PO-P2; CT.PO-P3
Subcategory	**CT.PO-P4**	**A data life cycle to manage data is aligned and implemented with the system development life cycle to manage systems.**	
Task	T001	Align data life cycle and system development life cycle target states.	CT.PO-P4
Task	T115	Determine the current state of system processes in consultation with [*organization-defined stakeholders*] .	CT.PO-P4
Task	T136	Determine the target state of system processes in consultation with [*organization-defined stakeholders*].	CT.PO-P4
Task	T270	Map data life cycle activities to the system development life cycle, noting overlaps and impacted areas.	CT.PO-P4
Task	T289	Review industry-related standards and best practices related to the data life cycle and the system development life cycle for applicability.	CT.PO-P4
Knowledge	K177	Knowledge of software development methodologies.	CT.PO-P4
Knowledge	K254	Knowledge of the organization's data processing ecosystem.	ID.BE-P1; ID.DE-P1; ID.DE-P2; ID.DE-P3; ID.DE-P4; ID.DE-P5; CT.PO-P1; CT.PO-P2; CT.PO-P3; CT.PO-P4; CM.AW-P1; CM.AW-P2; CM.AW-P3; CM.AW-P4; CM.AW-P5; CM.AW-P6; CM.AW-P7; CM.AW-P8
Knowledge	K257	Knowledge of the organization's data processing.	ID.IM-P1; ID.IM-P2; ID.IM-P3; ID.IM-P4; ID.IM-P5; ID.IM-P6; ID.IM-P7; ID.IM-P8; CT.PO-P1; CT.PO-P2; CT.PO-P3; CT.PO-P4; CT.DM-P1; CT.DM-P2; CT.DM-P3; CT.DM-P4; CT.DM-P5; CT.DM-P6; CT.DM-P7; CT.DM-P8; CT.DM-P9; CT.DM-P10; CM.AW-P1; CM.AW-P2; CM.AW-P3; CM.AW-P4; CM.AW-P5; CM.AW-P6; CM.AW-P7; CM.AW-P8
Knowledge	K268	Knowledge of the organization's internal stakeholder strategy and objectives related to data management.	CT.PO-P4
Knowledge	K269	Knowledge of the organization's internal stakeholder strategy and objectives related to system development.	CT.PO-P4
Knowledge	K148	Knowledge of process documentation and flowcharts/diagrams related to the data life cycle and system development life cycle.	CT.PO-P4
Knowledge	K320	Knowledge of the technical aspects of system development.	CT.PO-P4
Knowledge	K321	Knowledge of the technical aspects of the system development life cycle.	CT.PO-P4
Skill	S005	Skill in advising [*organization-defined stakeholders*] on appropriate outcomes based on gaps between legal requirements and organizational objectives.	GV.MT-P2; CT.PO-P4
Skill	S080	Skill in comparing/contrasting the data life cycle with the system development life cycle within the organization, applying insights from relevant documentation.	CT.PO-P4
Skill	S093	Skill in creating consistent processes across the organization for the design, delivery, and evaluation of programs.	CT.PO-P4
Skill	S166	Skill in harmonizing the design, delivery, and evaluation methodologies within system development.	CT.PO-P4
Skill	S192	Skill in implementing new methods within system management and data management based on gap analysis results.	CT.PO-P4

Statement Type	ID	Description	Subcategory Mapping
Skill	S277	Skill in selecting policy and/or technical controls in the context of stakeholder values, mission, and objectives.	CT.PO-P4
Skill	S291	Skill in translating legal and regulatory requirements to plain language/widely understandable terminology.	CT.PO-P4
Subcategory	**CT.DM-P1**	**Data elements can be accessed for review.**	
Task	T011	Archive data elements access logs.	CT.DM-P1; CT.DM-P2; CT.DM-P3; CT.DM-P4
Task	T084	Determine categories of data elements necessary to access for [*Select: review; transmission or disclosure; alteration; deletion*].	CT.DM-P1; CT.DM-P2; CT.DM-P3; CT.DM-P4
Task	T102	Determine remedial actions for systems that cannot implement [*Select: logging and monitoring data access requests; auditing data access logs; archiving data access logs*].	CT.DM-P1; CT.DM-P2; CT.DM-P3; CT.DM-P4
Task	T103	Determine remedial actions for systems that cannot support access requests to data elements for [*Select: review; transmission or disclosure; alteration; deletion*].	CT.DM-P1; CT.DM-P2; CT.DM-P3; CT.DM-P4
Task	T104	Determine remedial actions for systems that cannot support access to data elements for [*Select: review; transmission or disclosure; alteration; deletion*].	CT.DM-P1; CT.DM-P2; CT.DM-P3; CT.DM-P4
Task	T111	Determine the categories of entities that may request access to data elements for [*Select: review; transmission or disclosure; alteration; deletion*].	CT.DM-P1; CT.DM-P2; CT.DM-P3; CT.DM-P4
Task	T183	Draft language within data processing ecosystem party contracts incorporating identified legal, technical, and organizational measures to meet privacy objectives.	ID.DE-P3; CT.DM-P1; CT.DM-P2; CT.DM-P3; CT.DM-P4
Task	T211	Execute agreed-upon remedial actions for systems that cannot implement [*Select: logging and monitoring data access requests; auditing data access logs; archiving data access logs*].	CT.DM-P1; CT.DM-P2; CT.DM-P3; CT.DM-P4
Task	T212	Execute agreed-upon remedial actions for systems that cannot support access requests to data elements for [*Select: review; transmission or disclosure; alteration; deletion*].	CT.DM-P1; CT.DM-P2; CT.DM-P3; CT.DM-P4
Task	T213	Execute agreed-upon remedial actions for systems that cannot support access to data elements for [*Select: review; transmission or disclosure; alteration; deletion*].	CT.DM-P1; CT.DM-P2; CT.DM-P3; CT.DM-P4
Task	T259	Include privacy requirements for accessing data elements for [*Select: review; transmission or disclosure; alteration; deletion*] in system design.	CT.DM-P1; CT.DM-P2; CT.DM-P3; CT.DM-P4
Task	T277	Negotiate privacy and security clauses in contracts.	ID.DE-P3; CT.DM-P1; CT.DM-P2; CT.DM-P3; CT.DM-P4
Task	T323	Verify that the system implements [*Select: logging and monitoring data access requests; auditing data access logs; archiving data access logs*].	CT.DM-P1; CT.DM-P2; CT.DM-P3; CT.DM-P4
Task	T325	Verify that the system supports access requests to data elements for [*Select: review; transmission or disclosure; alteration; deletion*].	CT.DM-P1; CT.DM-P2; CT.DM-P3; CT.DM-P4
Task	T326	Verify that the system supports access to data elements for [*Select: review; transmission or disclosure; alteration; deletion*].	CT.DM-P1; CT.DM-P2; CT.DM-P3; CT.DM-P4
Knowledge	K005	Knowledge of access controls for reviewing data elements.	CT.DM-P1; CT.DM-P2; CT.DM-P3; CT.DM-P4
Knowledge	K050	Knowledge of data modeling/mapping.	CT.DM-P1; CT.DM-P2; CT.DM-P3; CT.DM-P4; CT.DM-P5; CM.AW-P4
Knowledge	K092	Knowledge of mechanisms/tools for archiving documentation associated with data elements access.	CT.DM-P1; CT.DM-P2; CT.DM-P3; CT.DM-P4
Knowledge	K093	Knowledge of mechanisms/tools for logging and monitoring access to data elements for review.	CT.DM-P1; CT.DM-P2; CT.DM-P3; CT.DM-P4
Knowledge	K137	Knowledge of privacy requirements.	CT.DM-P1; CT.DM-P2; CT.DM-P3; CT.DM-P4; CT.DM-P5; CT.DM-P6; CT.DM-P7; CM.AW-P4
Knowledge	K187	Knowledge of system design.	CT.DM-P1; CT.DM-P2; CT.DM-P3; CT.DM-P4; CT.DM-P5; CT.DM-P6; CT.DM-P7; CM.AW-P4

Statement Type	ID	Description	Subcategory Mapping
Knowledge	K199	Knowledge of techniques to facilitate accessibility of data elements in systems.	CT.DM-P1; CT.DM-P2; CT.DM-P3; CT.DM-P4; CM.AW-P4
Knowledge	K209	Knowledge of the categories of entities that may request access to an organization's data elements.	CT.DM-P1; CT.DM-P2; CT.DM-P3; CT.DM-P4
Knowledge	K257	Knowledge of the organization's data processing.	ID.IM-P1; ID.IM-P2; ID.IM-P3; ID.IM-P4; ID.IM-P5; ID.IM-P6; ID.IM-P7; ID.IM-P8; CT.PO-P1; CT.PO-P2; CT.PO-P3; CT.PO-P4; CT.DM-P1; CT.DM-P2; CT.DM-P3; CT.DM-P4; CT.DM-P5; CT.DM-P6; CT.DM-P7; CT.DM-P8; CT.DM-P9; CT.DM-P10; CM.AW-P1; CM.AW-P2; CM.AW-P3; CM.AW-P4; CM.AW-P5; CM.AW-P6; CM.AW-P7; CM.AW-P8
Skill	S064	Skill in assessing the tradeoff between utility and privacy associated with implementing mechanisms/tools.	CT.DM-P1; CT.DM-P2; CT.DM-P3; CT.DM-P4
Skill	S073	Skill in building system architecture.	CT.DM-P1; CT.DM-P2; CT.DM-P3; CT.DM-P4; CT.DM-P5; CT.DM-P6
Skill	S107	Skill in designing system architecture.	CT.DM-P1; CT.DM-P2; CT.DM-P3; CT.DM-P4; CT.DM-P5; CT.DM-P6
Skill	S145	Skill in evaluating mechanisms/tools for compatibility with existing system architecture.	CT.DM-P1; CT.DM-P2; CT.DM-P3; CT.DM-P4
Skill	S146	Skill in evaluating mechanisms/tools for effectiveness in meeting privacy requirements.	CT.DM-P1; CT.DM-P2; CT.DM-P3; CT.DM-P4
Skill	S255	Skill in performing system analysis.	CT.DM-P1; CT.DM-P2; CT.DM-P3; CT.DM-P4; CT.DM-P5; CT.DM-P6
Subcategory	**CT.DM-P2**	**Data elements can be accessed for transmission or disclosure.**	
Task	T011	Archive data elements access logs.	CT.DM-P1; CT.DM-P2; CT.DM-P3; CT.DM-P4
Task	T102	Determine remedial actions for systems that cannot implement [*Select: logging and monitoring data access requests; auditing data access logs; archiving data access logs*].	CT.DM-P1; CT.DM-P2; CT.DM-P3; CT.DM-P4
Task	T103	Determine remedial actions for systems that cannot support access requests to data elements for [*Select: review; transmission or disclosure; alteration; deletion*].	CT.DM-P1; CT.DM-P2; CT.DM-P3; CT.DM-P4
Task	T104	Determine remedial actions for systems that cannot support access to data elements for [*Select: review; transmission or disclosure; alteration; deletion*].	CT.DM-P1; CT.DM-P2; CT.DM-P3; CT.DM-P4
Task	T084	Determine categories of data elements necessary to access for [*Select: review; transmission or disclosure; alteration; deletion*].	CT.DM-P1; CT.DM-P2; CT.DM-P3; CT.DM-P4
Task	T111	Determine the categories of entities that may request access to data elements for [*Select: review; transmission or disclosure; alteration; deletion*].	CT.DM-P1; CT.DM-P2; CT.DM-P3; CT.DM-P4
Task	T183	Draft language within data processing ecosystem party contracts incorporating identified legal, technical, and organizational measures to meet privacy objectives.	ID.DE-P3; CT.DM-P1; CT.DM-P2; CT.DM-P3; CT.DM-P4
Task	T211	Execute agreed-upon remedial actions for systems that cannot implement [*Select: logging and monitoring data access requests; auditing data access logs; archiving data access logs*].	CT.DM-P1; CT.DM-P2; CT.DM-P3; CT.DM-P4
Task	T212	Execute agreed-upon remedial actions for systems that cannot support access requests to data elements for [*Select: review; transmission or disclosure; alteration; deletion*].	CT.DM-P1; CT.DM-P2; CT.DM-P3; CT.DM-P4
Task	T213	Execute agreed-upon remedial actions for systems that cannot support access to data elements for [*Select: review; transmission or disclosure; alteration; deletion*].	CT.DM-P1; CT.DM-P2; CT.DM-P3; CT.DM-P4
Task	T259	Include privacy requirements for accessing data elements for [*Select: review; transmission or disclosure; alteration; deletion*] in system design.	CT.DM-P1; CT.DM-P2; CT.DM-P3; CT.DM-P4

Statement Type	ID	Description	Subcategory Mapping
Task	T277	Negotiate privacy and security clauses in contracts.	ID.DE-P3; CT.DM-P1; CT.DM-P2; CT.DM-P3; CT.DM-P4
Task	T323	Verify that the system implements [*Select: logging and monitoring data access requests; auditing data access logs; archiving data access logs*].	CT.DM-P1; CT.DM-P2; CT.DM-P3; CT.DM-P4
Task	T325	Verify that the system supports access requests to data elements for [*Select: review; transmission or disclosure; alteration; deletion*].	CT.DM-P1; CT.DM-P2; CT.DM-P3; CT.DM-P4
Task	T326	Verify that the system supports access to data elements for [*Select: review; transmission or disclosure; alteration; deletion*].	CT.DM-P1; CT.DM-P2; CT.DM-P3; CT.DM-P4
Knowledge	K005	Knowledge of access controls for reviewing data elements.	CT.DM-P1; CT.DM-P2; CT.DM-P3; CT.DM-P4
Knowledge	K050	Knowledge of data modeling/mapping.	CT.DM-P1; CT.DM-P2; CT.DM-P3; CT.DM-P4; CT.DM-P5; CM.AW-P4
Knowledge	K092	Knowledge of mechanisms/tools for archiving documentation associated with data elements access.	CT.DM-P1; CT.DM-P2; CT.DM-P3; CT.DM-P4
Knowledge	K093	Knowledge of mechanisms/tools for logging and monitoring access to data elements for review.	CT.DM-P1; CT.DM-P2; CT.DM-P3; CT.DM-P4
Knowledge	K137	Knowledge of privacy requirements.	CT.DM-P1; CT.DM-P2; CT.DM-P3; CT.DM-P4; CT.DM-P5; CT.DM-P6; CT.DM-P7; CM.AW-P4
Knowledge	K187	Knowledge of system design.	CT.DM-P1; CT.DM-P2; CT.DM-P3; CT.DM-P4; CT.DM-P5; CT.DM-P6; CT.DM-P7; CM.AW-P4
Knowledge	K199	Knowledge of techniques to facilitate accessibility of data elements in systems.	CT.DM-P1; CT.DM-P2; CT.DM-P3; CT.DM-P4; CM.AW-P4
Knowledge	K209	Knowledge of the categories of entities that may request access to an organization's data elements.	CT.DM-P1; CT.DM-P2; CT.DM-P3; CT.DM-P4
Knowledge	K257	Knowledge of the organization's data processing.	ID.IM-P1; ID.IM-P2; ID.IM-P3; ID.IM-P4; ID.IM-P5; ID.IM-P6; ID.IM-P7; ID.IM-P8; CT.PO-P1; CT.PO-P2; CT.PO-P3; CT.PO-P4; CT.DM-P1; CT.DM-P2; CT.DM-P3; CT.DM-P4; CT.DM-P5; CT.DM-P6; CT.DM-P7; CT.DM-P8; CT.DM-P9; CT.DM-P10; CM.AW-P1; CM.AW-P2; CM.AW-P3; CM.AW-P4; CM.AW-P5; CM.AW-P6; CM.AW-P7; CM.AW-P8
Skill	S064	Skill in assessing the tradeoff between utility and privacy associated with implementing mechanisms/tools.	CT.DM-P1; CT.DM-P2; CT.DM-P3; CT.DM-P4
Skill	S073	Skill in building system architecture.	CT.DM-P1; CT.DM-P2; CT.DM-P3; CT.DM-P4; CT.DM-P5; CT.DM-P6
Skill	S107	Skill in designing system architecture.	CT.DM-P1; CT.DM-P2; CT.DM-P3; CT.DM-P4; CT.DM-P5; CT.DM-P6
Skill	S145	Skill in evaluating mechanisms/tools for compatibility with existing system architecture.	CT.DM-P1; CT.DM-P2; CT.DM-P3; CT.DM-P4
Skill	S146	Skill in evaluating mechanisms/tools for effectiveness in meeting privacy requirements.	CT.DM-P1; CT.DM-P2; CT.DM-P3; CT.DM-P4
Skill	S255	Skill in performing system analysis.	CT.DM-P1; CT.DM-P2; CT.DM-P3; CT.DM-P4; CT.DM-P5; CT.DM-P6
Subcategory	**CT.DM-P3**	**Data elements can be accessed for alteration.**	
Task	T011	Archive data elements access logs.	CT.DM-P1; CT.DM-P2; CT.DM-P3; CT.DM-P4
Task	T102	Determine remedial actions for systems that cannot implement [*Select: logging and monitoring data access requests; auditing data access logs; archiving data access logs*].	CT.DM-P1; CT.DM-P2; CT.DM-P3; CT.DM-P4
Task	T103	Determine remedial actions for systems that cannot support access requests to data elements for [*Select: review; transmission or disclosure; alteration; deletion*].	CT.DM-P1; CT.DM-P2; CT.DM-P3; CT.DM-P4

Statement Type	ID	Description	Subcategory Mapping
Task	T104	Determine remedial actions for systems that cannot support access to data elements for [*Select: review; transmission or disclosure; alteration; deletion*].	CT.DM-P1; CT.DM-P2; CT.DM-P3; CT.DM-P4
Task	T084	Determine categories of data elements necessary to access for [*Select: review; transmission or disclosure; alteration; deletion*].	CT.DM-P1; CT.DM-P2; CT.DM-P3; CT.DM-P4
Task	T111	Determine the categories of entities that may request access to data elements for [*Select: review; transmission or disclosure; alteration; deletion*].	CT.DM-P1; CT.DM-P2; CT.DM-P3; CT.DM-P4
Task	T183	Draft language within data processing ecosystem party contracts incorporating identified legal, technical, and organizational measures to meet privacy objectives.	ID.DE-P3; CT.DM-P1; CT.DM-P2; CT.DM-P3; CT.DM-P4
Task	T211	Execute agreed-upon remedial actions for systems that cannot implement [*Select: logging and monitoring data access requests; auditing data access logs; archiving data access logs*].	CT.DM-P1; CT.DM-P2; CT.DM-P3; CT.DM-P4
Task	T212	Execute agreed-upon remedial actions for systems that cannot support access requests to data elements for [*Select: review; transmission or disclosure; alteration; deletion*].	CT.DM-P1; CT.DM-P2; CT.DM-P3; CT.DM-P4
Task	T213	Execute agreed-upon remedial actions for systems that cannot support access to data elements for [*Select: review; transmission or disclosure; alteration; deletion*].	CT.DM-P1; CT.DM-P2; CT.DM-P3; CT.DM-P4
Task	T259	Include privacy requirements for accessing data elements for [*Select: review; transmission or disclosure; alteration; deletion*] in system design.	CT.DM-P1; CT.DM-P2; CT.DM-P3; CT.DM-P4
Task	T277	Negotiate privacy and security clauses in contracts.	ID.DE-P3; CT.DM-P1; CT.DM-P2; CT.DM-P3; CT.DM-P4
Task	T323	Verify that the system implements [*Select: logging and monitoring data access requests; auditing data access logs; archiving data access logs*].	CT.DM-P1; CT.DM-P2; CT.DM-P3; CT.DM-P4
Task	T325	Verify that the system supports access requests to data elements for [*Select: review; transmission or disclosure; alteration; deletion*].	CT.DM-P1; CT.DM-P2; CT.DM-P3; CT.DM-P4
Task	T326	Verify that the system supports access to data elements for [*Select: review; transmission or disclosure; alteration; deletion*].	CT.DM-P1; CT.DM-P2; CT.DM-P3; CT.DM-P4
Knowledge	K005	Knowledge of access controls for reviewing data elements.	CT.DM-P1; CT.DM-P2; CT.DM-P3; CT.DM-P4
Knowledge	K050	Knowledge of data modeling/mapping.	CT.DM-P1; CT.DM-P2; CT.DM-P3; CT.DM-P4; CT.DM-P5; CM.AW-P4
Knowledge	K092	Knowledge of mechanisms/tools for archiving documentation associated with data elements access.	CT.DM-P1; CT.DM-P2; CT.DM-P3; CT.DM-P4
Knowledge	K093	Knowledge of mechanisms/tools for logging and monitoring access to data elements for review.	CT.DM-P1; CT.DM-P2; CT.DM-P3; CT.DM-P4
Knowledge	K137	Knowledge of privacy requirements.	CT.DM-P1; CT.DM-P2; CT.DM-P3; CT.DM-P4; CT.DM-P5; CT.DM-P6; CT.DM-P7; CM.AW-P4
Knowledge	K187	Knowledge of system design.	CT.DM-P1; CT.DM-P2; CT.DM-P3; CT.DM-P4; CT.DM-P5; CT.DM-P6; CT.DM-P7; CM.AW-P4
Knowledge	K199	Knowledge of techniques to facilitate accessibility of data elements in systems.	CT.DM-P1; CT.DM-P2; CT.DM-P3; CT.DM-P4; CM.AW-P4
Knowledge	K209	Knowledge of the categories of entities that may request access to an organization's data elements.	CT.DM-P1; CT.DM-P2; CT.DM-P3; CT.DM-P4
Knowledge	K257	Knowledge of the organization's data processing.	ID.IM-P1; ID.IM-P2; ID.IM-P3; ID.IM-P4; ID.IM-P5; ID.IM-P6; ID.IM-P7; ID.IM-P8; CT.PO-P1; CT.PO-P2; CT.PO-P3; CT.PO-P4; CT.DM-P1; CT.DM-P2; CT.DM-P3; CT.DM-P4; CT.DM-P5; CT.DM-P6; CT.DM-P7; CT.DM-P8; CT.DM-P9; CT.DM-P10; CM.AW-P1; CM.AW-P2; CM.AW-P3; CM.AW-P4; CM.AW-P5; CM.AW-P6; CM.AW-P7; CM.AW-P8

Statement Type	ID	Description	Subcategory Mapping
Skill	S064	Skill in assessing the tradeoff between utility and privacy associated with implementing mechanisms/tools.	CT.DM-P1; CT.DM-P2; CT.DM-P3; CT.DM-P4
Skill	S073	Skill in building system architecture.	CT.DM-P1; CT.DM-P2; CT.DM-P3; CT.DM-P4; CT.DM-P5; CT.DM-P6
Skill	S107	Skill in designing system architecture.	CT.DM-P1; CT.DM-P2; CT.DM-P3; CT.DM-P4; CT.DM-P5; CT.DM-P6
Skill	S145	Skill in evaluating mechanisms/tools for compatibility with existing system architecture.	CT.DM-P1; CT.DM-P2; CT.DM-P3; CT.DM-P4
Skill	S146	Skill in evaluating mechanisms/tools for effectiveness in meeting privacy requirements.	CT.DM-P1; CT.DM-P2; CT.DM-P3; CT.DM-P4
Skill	S255	Skill in performing system analysis.	CT.DM-P1; CT.DM-P2; CT.DM-P3; CT.DM-P4; CT.DM-P5; CT.DM-P6
Subcategory	**CT.DM-P4**	**Data elements can be accessed for deletion.**	
Task	T011	Archive data elements access logs.	CT.DM-P1; CT.DM-P2; CT.DM-P3; CT.DM-P4
Task	T102	Determine remedial actions for systems that cannot implement [*Select: logging and monitoring data access requests; auditing data access logs; archiving data access logs*].	CT.DM-P1; CT.DM-P2; CT.DM-P3; CT.DM-P4
Task	T103	Determine remedial actions for systems that cannot support access requests to data elements for [*Select: review; transmission or disclosure; alteration; deletion*].	CT.DM-P1; CT.DM-P2; CT.DM-P3; CT.DM-P4
Task	T104	Determine remedial actions for systems that cannot support access to data elements for [*Select: review; transmission or disclosure; alteration; deletion*].	CT.DM-P1; CT.DM-P2; CT.DM-P3; CT.DM-P4
Task	T084	Determine categories of data elements necessary to access for [*Select: review; transmission or disclosure; alteration; deletion*].	CT.DM-P1; CT.DM-P2; CT.DM-P3; CT.DM-P4
Task	T111	Determine the categories of entities that may request access to data elements for [*Select: review; transmission or disclosure; alteration; deletion*].	CT.DM-P1; CT.DM-P2; CT.DM-P3; CT.DM-P4
Task	T183	Draft language within data processing ecosystem party contracts incorporating identified legal, technical, and organizational measures to meet privacy objectives.	ID.DE-P3; CT.DM-P1; CT.DM-P2; CT.DM-P3; CT.DM-P4
Task	T211	Execute agreed-upon remedial actions for systems that cannot implement [*Select: logging and monitoring data access requests; auditing data access logs; archiving data access logs*].	CT.DM-P1; CT.DM-P2; CT.DM-P3; CT.DM-P4
Task	T212	Execute agreed-upon remedial actions for systems that cannot support access requests to data elements for [*Select: review; transmission or disclosure; alteration; deletion*].	CT.DM-P1; CT.DM-P2; CT.DM-P3; CT.DM-P4
Task	T213	Execute agreed-upon remedial actions for systems that cannot support access to data elements for [*Select: review; transmission or disclosure; alteration; deletion*].	CT.DM-P1; CT.DM-P2; CT.DM-P3; CT.DM-P4
Task	T259	Include privacy requirements for accessing data elements for [*Select: review; transmission or disclosure; alteration; deletion*] in system design.	CT.DM-P1; CT.DM-P2; CT.DM-P3; CT.DM-P4
Task	T277	Negotiate privacy and security clauses in contracts.	ID.DE-P3; CT.DM-P1; CT.DM-P2; CT.DM-P3; CT.DM-P4
Task	T323	Verify that the system implements [*Select: logging and monitoring data access requests; auditing data access logs; archiving data access logs*].	CT.DM-P1; CT.DM-P2; CT.DM-P3; CT.DM-P4
Task	T325	Verify that the system supports access requests to data elements for [*Select: review; transmission or disclosure; alteration; deletion*].	CT.DM-P1; CT.DM-P2; CT.DM-P3; CT.DM-P4
Task	T326	Verify that the system supports access to data elements for [*Select: review; transmission or disclosure; alteration; deletion*].	CT.DM-P1; CT.DM-P2; CT.DM-P3; CT.DM-P4
Knowledge	K005	Knowledge of access controls for reviewing data elements.	CT.DM-P1; CT.DM-P2; CT.DM-P3; CT.DM-P4
Knowledge	K050	Knowledge of data modeling/mapping.	CT.DM-P1; CT.DM-P2; CT.DM-P3; CT.DM-P4; CT.DM-P5; CM.AW-P4

Statement Type	ID	Description	Subcategory Mapping
Knowledge	K092	Knowledge of mechanisms/tools for archiving documentation associated with data elements access.	CT.DM-P1; CT.DM-P2; CT.DM-P3; CT.DM-P4
Knowledge	K093	Knowledge of mechanisms/tools for logging and monitoring access to data elements for review.	CT.DM-P1; CT.DM-P2; CT.DM-P3; CT.DM-P4
Knowledge	K137	Knowledge of privacy requirements.	CT.DM-P1; CT.DM-P2; CT.DM-P3; CT.DM-P4; CT.DM-P5; CT.DM-P6; CT.DM-P7; CM.AW-P4
Knowledge	K187	Knowledge of system design.	CT.DM-P1; CT.DM-P2; CT.DM-P3; CT.DM-P4; CT.DM-P5; CT.DM-P6; CT.DM-P7; CM.AW-P4
Knowledge	K199	Knowledge of techniques to facilitate accessibility of data elements in systems.	CT.DM-P1; CT.DM-P2; CT.DM-P3; CT.DM-P4; CM.AW-P4
Knowledge	K209	Knowledge of the categories of entities that may request access to an organization's data elements.	CT.DM-P1; CT.DM-P2; CT.DM-P3; CT.DM-P4
Knowledge	K257	Knowledge of the organization's data processing.	ID.IM-P1; ID.IM-P2; ID.IM-P3; ID.IM-P4; ID.IM-P5; ID.IM-P6; ID.IM-P7; ID.IM-P8; CT.PO-P1; CT.PO-P2; CT.PO-P3; CT.PO-P4; CT.DM-P1; CT.DM-P2; CT.DM-P3; CT.DM-P4; CT.DM-P5; CT.DM-P6; CT.DM-P7; CT.DM-P8; CT.DM-P9; CT.DM-P10; CM.AW-P1; CM.AW-P2; CM.AW-P3; CM.AW-P4; CM.AW-P5; CM.AW-P6; CM.AW-P7; CM.AW-P8
Skill	S064	Skill in assessing the tradeoff between utility and privacy associated with implementing mechanisms/tools.	CT.DM-P1; CT.DM-P2; CT.DM-P3; CT.DM-P4
Skill	S073	Skill in building system architecture.	CT.DM-P1; CT.DM-P2; CT.DM-P3; CT.DM-P4; CT.DM-P5; CT.DM-P6
Skill	S107	Skill in designing system architecture.	CT.DM-P1; CT.DM-P2; CT.DM-P3; CT.DM-P4; CT.DM-P5; CT.DM-P6
Skill	S145	Skill in evaluating mechanisms/tools for compatibility with existing system architecture.	CT.DM-P1; CT.DM-P2; CT.DM-P3; CT.DM-P4
Skill	S146	Skill in evaluating mechanisms/tools for effectiveness in meeting privacy requirements.	CT.DM-P1; CT.DM-P2; CT.DM-P3; CT.DM-P4
Skill	S255	Skill in performing system analysis.	CT.DM-P1; CT.DM-P2; CT.DM-P3; CT.DM-P4; CT.DM-P5; CT.DM-P6
Subcategory	**CT.DM-P5**	**Data are destroyed according to policy.**	
Task	T094	Determine how to meet privacy requirements for data destruction in systems that fail to do so.	CT.DM-P5
Task	T116	Determine the data custodian responsible for data destruction.	CT.DM-P5
Task	T117	Determine the data destruction method(s).	CT.DM-P5
Task	T118	Determine the data to be destroyed in accordance with organizational policy.	CT.DM-P5
Task	T122	Determine the feasibility for updating systems to meet privacy requirements for data destruction.	CT.DM-P5
Task	T257	Include data destruction requirements in system design.	CT.DM-P5
Task	T288	Retain documentation associated with data destruction for regulatory purposes.	CT.DM-P5
Task	T313	Verify that data is destroyed according to policy.	CT.DM-P5
Task	T319	Verify that systems are designed in accordance with privacy requirements for data destruction.	CT.DM-P5
Knowledge	K038	Knowledge of contractual obligations for data destruction.	CT.DM-P5
Knowledge	K042	Knowledge of data destruction method(s).	CT.DM-P5
Knowledge	K047	Knowledge of data life cycle.	CT.DM-P5
Knowledge	K050	Knowledge of data modeling/mapping.	CT.DM-P1; CT.DM-P2; CT.DM-P3; CT.DM-P4; CT.DM-P5; CM.AW-P4
Knowledge	K056	Knowledge of data that must be retained.	CT.DM-P5
Knowledge	K063	Knowledge of destruction evidence.	CT.DM-P5

Statement Type	ID	Description	Subcategory Mapping
Knowledge	K091	Knowledge of mechanisms/tools for archiving documentation associated with data destruction.	CT.DM-P5
Knowledge	K094	Knowledge of mechanisms/tools for retaining logs associated with data destruction.	CT.DM-P5
Knowledge	K113	Knowledge of organizational data governance.	CT.DM-P5; CT.DM-P6; CT.DM-P7
Knowledge	K117	Knowledge of organizational roles related to data destruction.	CT.DM-P5
Knowledge	K137	Knowledge of privacy requirements.	CT.DM-P1; CT.DM-P2; CT.DM-P3; CT.DM-P4; CT.DM-P5; CT.DM-P6; CT.DM-P7; CM.AW-P4
Knowledge	K187	Knowledge of system design.	CT.DM-P1; CT.DM-P2; CT.DM-P3; CT.DM-P4; CT.DM-P5; CT.DM-P6; CT.DM-P7; CM.AW-P4
Knowledge	K249	Knowledge of the organization's data disposition instructions.	CT.DM-P5
Knowledge	K257	Knowledge of the organization's data processing.	ID.IM-P1; ID.IM-P2; ID.IM-P3; ID.IM-P4; ID.IM-P5; ID.IM-P6; ID.IM-P7; ID.IM-P8; CT.PO-P1; CT.PO-P2; CT.PO-P3; CT.PO-P4; CT.DM-P1; CT.DM-P2; CT.DM-P3; CT.DM-P4; CT.DM-P5; CT.DM-P6; CT.DM-P7; CT.DM-P8; CT.DM-P9; CT.DM-P10; CM.AW-P1; CM.AW-P2; CM.AW-P3; CM.AW-P4; CM.AW-P5; CM.AW-P6; CM.AW-P7; CM.AW-P8
Knowledge	K285	Knowledge of the organization's privacy requirements.	CT.DM-P5
Knowledge	K345	Knowledge of where the organization's data is located.	CT.DM-P5
Skill	S021	Skill in applying data destruction methods.	CT.DM-P5
Skill	S073	Skill in building system architecture.	CT.DM-P1; CT.DM-P2; CT.DM-P3; CT.DM-P4; CT.DM-P5; CT.DM-P6
Skill	S107	Skill in designing system architecture.	CT.DM-P1; CT.DM-P2; CT.DM-P3; CT.DM-P4; CT.DM-P5; CT.DM-P6
Skill	S255	Skill in performing system analysis.	CT.DM-P1; CT.DM-P2; CT.DM-P3; CT.DM-P4; CT.DM-P5; CT.DM-P6
Skill	S258	Skill in privacy engineering.	CT.DM-P5; CM.AW-P3
Skill	S289	Skill in translating between technical and non-technical privacy requirements.	CT.DM-P5
Subcategory	**CT.DM-P6**	**Data are transmitted using standardized formats.**	
Task	T105	Determine remedial actions for systems that cannot transmit data using standardized formats, in consultation with [*organization-defined stakeholders*].	CT.DM-P6
Task	T148	Determine which data is to be transmitted, in accordance with the organizational policy.	CT.DM-P6
Task	T152	Determine which standardized format to use for data transmission in accordance with the organizational policy.	CT.DM-P6
Task	T214	Execute agreed-upon remedial actions for systems that cannot transmit data using standardized formats.	CT.DM-P6
Task	T258	Include privacy requirements for [*Select: the transmission of data elements; transmitting processing permissions and related data values*] into system design.	CT.DM-P6; CT.DM-P7
Task	T322	Verify that the system implements [*Select: authentication, logging, monitoring, data transformation to standardized formats*] for data transmission.	CT.DM-P6
Knowledge	K030	Knowledge of considerations for transmission of data elements.	CT.DM-P6
Knowledge	K032	Knowledge of contextual factors associated with implementation of data transmission mechanisms/ tools.	CT.DM-P6
Knowledge	K113	Knowledge of organizational data governance.	CT.DM-P5; CT.DM-P6; CT.DM-P7

Statement Type	ID	Description	Subcategory Mapping
Knowledge	K137	Knowledge of privacy requirements.	CT.DM-P1; CT.DM-P2; CT.DM-P3; CT.DM-P4; CT.DM-P5; CT.DM-P6; CT.DM-P7; CM.AW-P4
Knowledge	K182	Knowledge of standardized formats for data transmission.	CT.DM-P6
Knowledge	K187	Knowledge of system design.	CT.DM-P1; CT.DM-P2; CT.DM-P3; CT.DM-P4; CT.DM-P5; CT.DM-P6; CT.DM-P7; CM.AW-P4
Knowledge	K210	Knowledge of the categories of entities that may request data transmission.	CT.DM-P6
Knowledge	K257	Knowledge of the organization's data processing.	ID.IM-P1; ID.IM-P2; ID.IM-P3; ID.IM-P4; ID.IM-P5; ID.IM-P6; ID.IM-P7; ID.IM-P8; CT.PO-P1; CT.PO-P2; CT.PO-P3; CT.PO-P4; CT.DM-P1; CT.DM-P2; CT.DM-P3; CT.DM-P4; CT.DM-P5; CT.DM-P6; CT.DM-P7; CT.DM-P8; CT.DM-P9; CT.DM-P10; CM.AW-P1; CM.AW-P2; CM.AW-P3; CM.AW-P4; CM.AW-P5; CM.AW-P6; CM.AW-P7; CM.AW-P8
Knowledge	K294	Knowledge of the organization's required formats for data transmission.	CT.DM-P6
Skill	S073	Skill in building system architecture.	CT.DM-P1; CT.DM-P2; CT.DM-P3; CT.DM-P4; CT.DM-P5; CT.DM-P6
Skill	S107	Skill in designing system architecture.	CT.DM-P1; CT.DM-P2; CT.DM-P3; CT.DM-P4; CT.DM-P5; CT.DM-P6
Skill	S140	Skill in evaluating contextual factors to implement data transmission mechanisms.	CT.DM-P6
Skill	S255	Skill in performing system analysis.	CT.DM-P1; CT.DM-P2; CT.DM-P3; CT.DM-P4; CT.DM-P5; CT.DM-P6
Skill	S273	Skill in selecting data transmission formats based on context and consistent with organizational requirements.	CT.DM-P6
Skill	S292	Skill in translating legal/business privacy requirements to technical privacy requirements.	CT.DM-P6
Subcategory	**CT.DM-P7**	**Mechanisms for transmitting processing permissions and related data values with data elements are established and in place.**	
Notes: Distinctions between mechanisms for transmitting processing permissions may depend on the organization. Some organizations may require separate activities to create and implement each one. **Organizations may choose to evaluate existing mechanisms for gaps (e.g., incompleteness, outdated information) and determine necessary actions to address identified gaps.**			
Task	T075	Define the processing permissions for data elements.	CT.DM-P7
Task	T106	Determine remedial actions for systems that cannot transmit processing permissions and related data values with data elements.	CT.DM-P7
Task	T215	Execute agreed-upon remedial actions for systems that cannot transmit processing permissions and related data values with data elements.	CT.DM-P7
Task	T258	Include privacy requirements for [*Select: the transmission of data elements; transmitting processing permissions and related data values*] into system design.	CT.DM-P6; CT.DM-P7
Task	T324	Verify that the system implements mechanisms for transmitting processing permissions and related data values with data elements.	CT.DM-P7
Knowledge	K090	Knowledge of mechanisms for transmitting processing permissions and related data values with data elements.	CT.DM-P7
Knowledge	K102	Knowledge of modes of transmission of data elements in systems.	CT.DM-P7

Statement Type	ID	Description	Subcategory Mapping
Knowledge	K103	Knowledge of modes of transmission of data processing permissions.	CT.DM-P7
Knowledge	K113	Knowledge of organizational data governance.	CT.DM-P5; CT.DM-P6; CT.DM-P7
Knowledge	K137	Knowledge of privacy requirements.	CT.DM-P1; CT.DM-P2; CT.DM-P3; CT.DM-P4; CT.DM-P5; CT.DM-P6; CT.DM-P7; CM.AW-P4
Knowledge	K187	Knowledge of system design.	CT.DM-P1; CT.DM-P2; CT.DM-P3; CT.DM-P4; CT.DM-P5; CT.DM-P6; CT.DM-P7; CM.AW-P4
Knowledge	K215	Knowledge of the contractual obligations for processing data elements.	CT.DM-P7
Knowledge	K250	Knowledge of the organization's data elements, including associated data values and processing permissions.	CT.DM-P7
Knowledge	K257	Knowledge of the organization's data processing.	ID.IM-P1; ID.IM-P2; ID.IM-P3; ID.IM-P4; ID.IM-P5; ID.IM-P6; ID.IM-P7; ID.IM-P8; CT.PO-P1; CT.PO-P2; CT.PO-P3; CT.PO-P4; CT.DM-P1; CT.DM-P2; CT.DM-P3; CT.DM-P4; CT.DM-P5; CT.DM-P6; CT.DM-P7; CT.DM-P8; CT.DM-P9; CT.DM-P10; CM.AW-P1; CM.AW-P2; CM.AW-P3; CM.AW-P4; CM.AW-P5; CM.AW-P6; CM.AW-P7; CM.AW-P8
Skill	S022	Skill in applying data dictionary concepts to implement mechanisms for transmitting processing permissions.	CT.DM-P7
Skill	S102	Skill in defining relevant permissions and data values for data processing.	CT.DM-P7
Skill	S108	Skill in designing systems.	CT.DM-P7
Skill	S191	Skill in implementing mechanisms to meet data processing requirements.	CT.DM-P7
Skill	S269	Skill in reviewing data processing permissions and data values for relevance.	CT.DM-P7
Skill	S296	Skill in translating privacy requirements into system design.	CT.DM-P7
Subcategory	**CT.DM-P8**	**Audit/log records are determined, documented, implemented, and reviewed in accordance with policy and incorporating the principle of data minimization.**	
Task	T013	Assess gaps between the organization's policy and audit/log records practices.	CT.DM-P8
Task	T095	Determine how to respond to gaps between the organization's policy and audit/log records practices in collaboration with [*organization-defined stakeholders*].	CT.DM-P8
Task	T247	Identify the systems that house the data elements that need to be logged.	CT.DM-P8
Task	T269	Maintain the organization's documents.	CT.DM-P8; CM.AW-P4
Task	T311	Verify that audit/log records incorporate the principle of data minimization.	CT.DM-P8
Knowledge	K115	Knowledge of organizational policies.	CT.DM-P8; CT.DM-P9
Knowledge	K109	Knowledge of organization's auditing and logging mechanisms.	CT.DM-P8
Knowledge	K194	Knowledge of systems that are currently being logged.	CT.DM-P8
Knowledge	K220	Knowledge of the data minimization principle.	CT.DM-P8
Knowledge	K257	Knowledge of the organization's data processing.	ID.IM-P1; ID.IM-P2; ID.IM-P3; ID.IM-P4; ID.IM-P5; ID.IM-P6; ID.IM-P7; ID.IM-P8; CT.PO-P1; CT.PO-P2; CT.PO-P3; CT.PO-P4; CT.DM-P1; CT.DM-P2; CT.DM-P3; CT.DM-P4; CT.DM-P5; CT.DM-P6; CT.DM-P7; CT.DM-P8; CT.DM-P9; CT.DM-P10; CM.AW-P1; CM.AW-P2; CM.AW-P3; CM.AW-P4; CM.AW-P5; CM.AW-P6; CM.AW-P7; CM.AW-P8
Skill	S012	Skill in aligning best practices for audit/log records with organizational policies.	CT.DM-P8
Skill	S033	Skill in applying the data minimization principle to audit/log records.	CT.DM-P8
Skill	S139	Skill in evaluating audit/log use cases based on system design.	CT.DM-P8

Statement Type	ID	Description	Subcategory Mapping
Skill	S161	Skill in facilitating changes to audit/log records practices in collaboration with [*organization-defined stakeholders*].	CT.DM-P8
Skill	S293	Skill in translating policy requirements into technical implementation.	CT.DM-P8
Subcategory	**CT.DM-P9**	**Technical measures implemented to manage data processing are tested and assessed.**	
Task	T007	Align tests for technical measures implemented to manage data processing with the latest industry standards and regulations.	CT.DM-P9
Task	T110	Determine tests for technical measures implemented to manage data processing.	CT.DM-P9
Task	T203	Evaluate the effectiveness of technical measures implemented to manage data processing.	CT.DM-P9
Task	T321	Verify that tests for technical measures implemented to manage data processing are in place.	CT.DM-P9
Knowledge	K115	Knowledge of organizational policies.	CT.DM-P8; CT.DM-P9
Knowledge	K191	Knowledge of system requirements.	CT.DM-P9
Knowledge	K197	Knowledge of technical measure testing best practices.	CT.DM-P9
Knowledge	K198	Knowledge of technical measures implemented to manage data processing.	CT.DM-P9
Knowledge	K257	Knowledge of the organization's data processing.	ID.IM-P1; ID.IM-P2; ID.IM-P3; ID.IM-P4; ID.IM-P5; ID.IM-P6; ID.IM-P7; ID.IM-P8; CT.PO-P1; CT.PO-P2; CT.PO-P3; CT.PO-P4; CT.DM-P1; CT.DM-P2; CT.DM-P3; CT.DM-P4; CT.DM-P5; CT.DM-P6; CT.DM-P7; CT.DM-P8; CT.DM-P9; CT.DM-P10; CM.AW-P1; CM.AW-P2; CM.AW-P3; CM.AW-P4; CM.AW-P5; CM.AW-P6; CM.AW-P7; CM.AW-P8
Knowledge	K304	Knowledge of the organization's technical environment.	CT.DM-P9
Skill	S250	Skill in performing analysis of technical measures to manage data processing for effectiveness.	CT.DM-P9
Skill	S036	Skill in applying updates to technical measures based on testing/assessment results.	CT.DM-P9
Skill	S198	Skill in interpreting diagnostic metrics.	CT.DM-P9
Skill	S304	Skill in writing tests for evaluating the effectiveness of technical measures.	CT.DM-P9
Subcategory	**CT.DM-P10**	**Stakeholder privacy preferences are included in algorithmic design objectives and outputs are evaluated against these preferences.**	
Task	T126	Determine the means through which stakeholder privacy preferences will be obtained.	CT.DM-P10
Task	T141	Determine whether algorithmic outputs align with identified stakeholder privacy preferences.	CT.DM-P10
Task	T151	Determine which stakeholder privacy preferences are in scope to include in algorithmic design objectives.	CT.DM-P10
Task	T272	Map stakeholder privacy preferences to defined algorithmic design objectives.	CT.DM-P10
Task	T279	Obtain [*organization-defined stakeholder*] privacy preferences for inclusion in algorithmic design objectives.	CT.DM-P10
Knowledge	K006	Knowledge of algorithmic design objectives with respect to business goals.	CT.DM-P10
Knowledge	K114	Knowledge of organizational policies and procedures that guide algorithmic design.	CT.DM-P10
Knowledge	K239	Knowledge of the organization's algorithmic design objectives.	CT.DM-P10
Knowledge	K257	Knowledge of the organization's data processing.	ID.IM-P1; ID.IM-P2; ID.IM-P3; ID.IM-P4; ID.IM-P5; ID.IM-P6; ID.IM-P7; ID.IM-P8; CT.PO-P1; CT.PO-P2; CT.PO-P3; CT.PO-P4; CT.DM-P1; CT.DM-P2; CT.DM-P3; CT.DM-P4; CT.DM-P5; CT.DM-P6; CT.DM-P7; CT.DM-P8; CT.DM-P9; CT.DM-P10; CM.AW-P1; CM.AW-P2; CM.AW-P3; CM.AW-P4; CM.AW-P5; CM.AW-P6; CM.AW-P7; CM.AW-P8

Statement Type	ID	Description	Subcategory Mapping
Skill	S116	Skill in determining the tradeoff between privacy and the utility of algorithmic outputs.	CT.DM-P10
Skill	S179	Skill in identifying stakeholders impacted by algorithmic design.	CT.DM-P10
Skill	S215	Skill in managing privacy/utility tradeoffs in a manner consistent with the organization's risk strategy/priorities.	CT.DM-P10
Skill	S222	Skill in mapping privacy requirements to algorithmic design objectives.	CT.DM-P10
Skill	S275	Skill in selecting means to obtain stakeholder privacy preferences based on organizational context.	CT.DM-P10
Subcategory	**CT.DP-P1**	**Data are processed to limit observability and linkability (e.g., data actions take place on local devices, privacy-preserving cryptography).**	
Task	T010	Apply, as needed, additional techniques that limit [*Select: observability and linkability; identification of individuals; formulation of inferences about individuals' behavior or activities*].	CT.DP-P1; CT.DP-P2; CT.DP-P3
Task	T021	Assess the purpose/use of each data action.	CT.DP-P1; CT.DP-P2; CT.DP-P3
Task	T083	Determine business objectives that require [*Select: linked or observable data; identification of individuals; formulation of inferences about individuals' behavior or activities*].	CT.DP-P1; CT.DP-P2; CT.DP-P3
Task	T089	Determine de-identification techniques the organization can utilize to address specific privacy risks.	CT.DP-P1; CT.DP-P2; CT.DP-P3
Task	T093	Determine how to apply technique(s) to data handled in each data action that limit [*Select: observability and linkability; identification of individuals; formulation of inferences about individuals' behavior or activities*].	CT.DP-P1; CT.DP-P2; CT.DP-P3
Task	T298	Select the technique(s) that apply to data handled in each data action that limit [*Select: observability and linkability; identification of individuals; formulation of inferences about individuals' behavior or activities*].	CT.DP-P1; CT.DP-P2; CT.DP-P3
Task	T320	Verify that techniques are applied to data handled in each data action that limit [*Select: observability and linkability; identification of individuals; formulation of inferences about individuals' behavior or activities*].	CT.DP-P1; CT.DP-P2; CT.DP-P3
Knowledge	K279	Knowledge of the organization's primary and secondary purposes/uses of data.	CT.DP-P1; CT.DP-P2; CT.DP-P3
Knowledge	K014	Knowledge of business needs and requirements associated with limiting [*Select: observability and linkability of data; identification of individuals; formulation of inferences about individuals' behavior or activities*].	CT.DP-P1; CT.DP-P2; CT.DP-P3
Knowledge	K060	Knowledge of de-identification techniques the organization is capable of implementing.	CT.DP-P1; CT.DP-P2; CT.DP-P3
Knowledge	K061	Knowledge of de-identification techniques, including resource requirements, technical capability, and applicable use cases.	CT.DP-P1; CT.DP-P2; CT.DP-P3
Knowledge	K112	Knowledge of organizational characteristics that can inhibit implementation of de-identification techniques.	CT.DP-P1; CT.DP-P2; CT.DP-P3
Knowledge	K151	Knowledge of re-identification techniques associated with limiting [*Select: observability and linkability of data; identification of individuals; formulation of inferences about individuals' behavior or activities*].	CT.DP-P1; CT.DP-P2; CT.DP-P3
Skill	S062	Skill in assessing the organization's data uses.	CT.DP-P1; CT.DP-P2; CT.DP-P3
Skill	S274	Skill in selecting de-identification techniques matched to risk classification.	CT.DP-P1; CT.DP-P2; CT.DP-P3
Skill	S112	Skill in determining de-identification techniques that are appropriate to address specific privacy risks in a given use case/context.	CT.DP-P1; CT.DP-P2; CT.DP-P3
Skill	S024	Skill in applying de-identification techniques that are appropriate to address specific privacy risks in a given use case/context.	CT.DP-P1; CT.DP-P2; CT.DP-P3
Skill	S117	Skill in determining whether the applied de-identification technique meets objectives.	CT.DP-P1; CT.DP-P2; CT.DP-P3
Skill	S156	Skill in executing re-identification techniques.	CT.DP-P1; CT.DP-P2; CT.DP-P3
Subcategory	**CT.DP-P2**	**Data are processed to limit the identification of individuals (e.g., de-identification privacy techniques, tokenization).**	
Task	T021	Assess the purpose/use of each data action.	CT.DP-P1; CT.DP-P2; CT.DP-P3
Task	T083	Determine business objectives that require [*Select: linked or observable data; identification of individuals; formulation of inferences about individuals' behavior or activities*].	CT.DP-P1; CT.DP-P2; CT.DP-P3
Task	T089	Determine de-identification techniques the organization can utilize to address specific privacy risks.	CT.DP-P1; CT.DP-P2; CT.DP-P3

Statement Type	ID	Description	Subcategory Mapping
Task	T298	Select the technique(s) that apply to data handled in each data action that limit [*Select: observability and linkability; identification of individuals; formulation of inferences about individuals' behavior or activities*].	CT.DP-P1; CT.DP-P2; CT.DP-P3
Task	T093	Determine how to apply technique(s) to data handled in each data action that limit [*Select: observability and linkability; identification of individuals; formulation of inferences about individuals' behavior or activities*].	CT.DP-P1; CT.DP-P2; CT.DP-P3
Task	T320	Verify that techniques are applied to data handled in each data action that limit [*Select: observability and linkability; identification of individuals; formulation of inferences about individuals' behavior or activities*].	CT.DP-P1; CT.DP-P2; CT.DP-P3
Task	T010	Apply, as needed, additional techniques that limit [*Select: observability and linkability; identification of individuals; formulation of inferences about individuals' behavior or activities*].	CT.DP-P1; CT.DP-P2; CT.DP-P3
Knowledge	K279	Knowledge of the organization's primary and secondary purposes/uses of data.	CT.DP-P1; CT.DP-P2; CT.DP-P3
Knowledge	K014	Knowledge of business needs and requirements associated with limiting [*Select: observability and linkability of data; identification of individuals; formulation of inferences about individuals' behavior or activities*].	CT.DP-P1; CT.DP-P2; CT.DP-P3
Knowledge	K060	Knowledge of de-identification techniques the organization is capable of implementing.	CT.DP-P1; CT.DP-P2; CT.DP-P3
Knowledge	K061	Knowledge of de-identification techniques, including resource requirements, technical capability, and applicable use cases.	CT.DP-P1; CT.DP-P2; CT.DP-P3
Knowledge	K112	Knowledge of organizational characteristics that can inhibit implementation of de-identification techniques.	CT.DP-P1; CT.DP-P2; CT.DP-P3
Knowledge	K151	Knowledge of re-identification techniques associated with limiting [*Select: observability and linkability of data; identification of individuals; formulation of inferences about individuals' behavior or activities*].	CT.DP-P1; CT.DP-P2; CT.DP-P3
Skill	S062	Skill in assessing the organization's data uses.	CT.DP-P1; CT.DP-P2; CT.DP-P3
Skill	S274	Skill in selecting de-identification techniques matched to risk classification.	CT.DP-P1; CT.DP-P2; CT.DP-P3
Skill	S112	Skill in determining de-identification techniques that are appropriate to address specific privacy risks in a given use case/context.	CT.DP-P1; CT.DP-P2; CT.DP-P3
Skill	S024	Skill in applying de-identification techniques that are appropriate to address specific privacy risks in a given use case/context.	CT.DP-P1; CT.DP-P2; CT.DP-P3
Skill	S117	Skill in determining whether the applied de-identification technique meets objectives.	CT.DP-P1; CT.DP-P2; CT.DP-P3
Skill	S156	Skill in executing re-identification techniques.	CT.DP-P1; CT.DP-P2; CT.DP-P3
Subcategory	**CT.DP-P3**	**Data are processed to limit the formulation of inferences about individuals’ behavior or activities (e.g., data processing is decentralized, distributed architectures).**	
Task	T021	Assess the purpose/use of each data action.	CT.DP-P1; CT.DP-P2; CT.DP-P3
Task	T083	Determine business objectives that require [*Select: linked or observable data; identification of individuals; formulation of inferences about individuals' behavior or activities*].	CT.DP-P1; CT.DP-P2; CT.DP-P3
Task	T089	Determine de-identification techniques the organization can utilize to address specific privacy risks.	CT.DP-P1; CT.DP-P2; CT.DP-P3
Task	T298	Select the technique(s) that apply to data handled in each data action that limit [*Select: observability and linkability; identification of individuals; formulation of inferences about individuals' behavior or activities*].	CT.DP-P1; CT.DP-P2; CT.DP-P3
Task	T093	Determine how to apply technique(s) to data handled in each data action that limit [*Select: observability and linkability; identification of individuals; formulation of inferences about individuals' behavior or activities*].	CT.DP-P1; CT.DP-P2; CT.DP-P3
Task	T320	Verify that techniques are applied to data handled in each data action that limit [*Select: observability and linkability; identification of individuals; formulation of inferences about individuals' behavior or activities*].	CT.DP-P1; CT.DP-P2; CT.DP-P3
Task	T010	Apply, as needed, additional techniques that limit [*Select: observability and linkability; identification of individuals; formulation of inferences about individuals' behavior or activities*].	CT.DP-P1; CT.DP-P2; CT.DP-P3
Knowledge	K279	Knowledge of the organization's primary and secondary purposes/uses of data.	CT.DP-P1; CT.DP-P2; CT.DP-P3
Knowledge	K014	Knowledge of business needs and requirements associated with limiting [*Select: observability and linkability of data; identification of individuals; formulation of inferences about individuals' behavior or activities*].	CT.DP-P1; CT.DP-P2; CT.DP-P3
Knowledge	K060	Knowledge of de-identification techniques the organization is capable of implementing.	CT.DP-P1; CT.DP-P2; CT.DP-P3

Statement Type	ID	Description	Subcategory Mapping
Knowledge	K061	Knowledge of de-identification techniques, including resource requirements, technical capability, and applicable use cases.	CT.DP-P1; CT.DP-P2; CT.DP-P3
Knowledge	K112	Knowledge of organizational characteristics that can inhibit implementation of de-identification techniques.	CT.DP-P1; CT.DP-P2; CT.DP-P3
Knowledge	K151	Knowledge of re-identification techniques associated with limiting [*Select: observability and linkability of data; identification of individuals; formulation of inferences about individuals' behavior or activities*].	CT.DP-P1; CT.DP-P2; CT.DP-P3
Skill	S062	Skill in assessing the organization's data uses.	CT.DP-P1; CT.DP-P2; CT.DP-P3
Skill	S274	Skill in selecting de-identification techniques matched to risk classification.	CT.DP-P1; CT.DP-P2; CT.DP-P3
Skill	S112	Skill in determining de-identification techniques that are appropriate to address specific privacy risks in a given use case/context.	CT.DP-P1; CT.DP-P2; CT.DP-P3
Skill	S024	Skill in applying de-identification techniques that are appropriate to address specific privacy risks in a given use case/context.	CT.DP-P1; CT.DP-P2; CT.DP-P3
Skill	S117	Skill in determining whether the applied de-identification technique meets objectives.	CT.DP-P1; CT.DP-P2; CT.DP-P3
Skill	S156	Skill in executing re-identification techniques.	CT.DP-P1; CT.DP-P2; CT.DP-P3
Subcategory	**CT.DP-P4**	**System or device configurations permit selective collection or disclosure of data elements.**	
Task	T132	Determine the organization's data collection and disclosure requirements.	CT.DP-P4
Task	T252	Implement configurations within system architecture and/or localized devices that allow for selective collection or disclosure of data.	CT.DP-P4
Task	T302	Test selective collection and disclosure configurability in system or device design.	CT.DP-P4
Task	T307	Update configuration settings as needed based on [*organization-defined factors*] for enabling selective collection or disclosure of data elements.	CT.DP-P4
Task	T312	Verify that configurations within system architecture and/or localized devices allow for selective collection or disclosure of data, consistent with organizational policy requirements.	CT.DP-P4
Knowledge	K020	Knowledge of categories of data elements that are candidates for data minimization.	CT.DP-P4
Knowledge	K043	Knowledge of data element functionality.	CT.DP-P4
Knowledge	K057	Knowledge of data use cases.	CT.DP-P4
Knowledge	K185	Knowledge of system design and configurations that minimize data collection or disclosure.	CT.DP-P4
Knowledge	K188	Knowledge of system or device constraints (i.e., what configurations are possible).	CT.DP-P4
Knowledge	K189	Knowledge of system or device data requirements.	CT.DP-P4
Knowledge	K190	Knowledge of system or device testing to verify selective collection and disclosure configurations are operable at all times.	CT.DP-P4
Skill	K319	Knowledge of the system development life cycle.	CT.DP-P4
Skill	S086	Skill in configuring a system or device to permit selective collection or disclosure of data elements.	CT.DP-P4
Skill	S105	Skill in designing selective collection and disclosure configurations.	CT.DP-P4
Skill	S106	Skill in designing system architecture and configuration baselines.	CT.DP-P4
Skill	S286	Skill in testing system configurations.	CT.DP-P4
Skill	S287	Skill in testing system designs.	CT.DP-P4
Subcategory	**CT.DP-P5**	**Attribute references are substituted for attribute values.**	
Task	T008	Apply additional techniques that substitute attribute references for attribute values.	CT.DP-P5
Task	T070	Define data utility requirements, outside of which the data no longer meets business use requirements.	CT.DP-P5
Task	T092	Determine how to apply data minimization techniques for substituting attribute values for attribute references.	CT.DP-P5

Statement Type	ID	Description	Subcategory Mapping
Task	T096	Determine if data can be minimized.	CT.DP-P5
Task	T297	Select the data minimization technique(s) for substituting attribute values for attribute references.	CT.DP-P5
Task	T301	Test data minimization against data utility and de-identification requirements.	CT.DP-P5
Task	T314	Verify that data minimization techniques are applied to substitute attribute values for attribute references.	CT.DP-P5
Knowledge	K013	Knowledge of boundaries outside of which a given data action fails to meet utility requirements.	CT.DP-P5
Knowledge	K058	Knowledge of data utility tradeoffs.	CT.DP-P5
Knowledge	K049	Knowledge of data minimization techniques.	CT.DP-P5
Knowledge	K098	Knowledge of metrics and measurements of data utility and data de-identification.	CT.DP-P5
Skill	S136	Skill in error rate calculation.	CT.DP-P5
Skill	S046	Skill in assessing error rate sensitivity.	CT.DP-P5
Skill	S044	Skill in assessing data utility tradeoffs.	CT.DP-P5
Skill	S023	Skill in applying data minimization techniques to achieve data utility and de-identification requirements.	CT.DP-P5
Subcategory	**CM.PO-P1**	**Transparency policies, processes, and procedures for communicating data processing purposes, practices, and associated privacy risks are established and in place.**	
Notes: Organizations may choose to evaluate existing policies/processes/procedures for gaps (e.g., incompleteness, outdated information) and determine necessary actions to address identified gaps.			
Task	T039	Create a policy/policies that addresses the purpose, scope, roles, responsibilities, and coordination required for communicating data processing purposes, practices, and associated privacy risks that is consistent with applicable laws, regulations, standards, and guidelines.	CM.PO-P1
Task	T058	Create a process(es)/procedure(s) that addresses audience, cadence, and mechanisms for communicating data processing purposes, practices, and associated privacy risks among [*organization-defined stakeholders*].	CM.PO-P1
Knowledge	K255	Knowledge of the organization's data processing goals.	ID.DE-P1; GV.PO-P6; GV.RM-P1; GV.RM-P2; GV.RM-P3; GV.MT-P3; GV.MT-P4; GV.MT-P5; GV.MT-P6; GV.MT-P7; CT.PO-P1; CT.PO-P2; CT.PO-P3; CM.PO-P1
Knowledge	K258	Knowledge of the organization's data strategy.	ID.DE-P1; GV.PO-P6; GV.RM-P1; GV.RM-P2; GV.RM-P3; GV.MT-P3; GV.MT-P4; GV.MT-P5; GV.MT-P6; GV.MT-P7; CT.PO-P1; CT.PO-P2; CT.PO-P3; CM.PO-P1
Knowledge	K292	Knowledge of the organization's privacy values.	GV.PO-P1; GV.MT-P3; GV.MT-P4; GV.MT-P5; GV.MT-P7; CT.PO-P1; CT.PO-P2; CT.PO-P3; CM.PO-P1
Skill	S126	Skill in drafting policies/processes/procedures that reflect the organization's privacy values.	CM.PO-P1
Skill	S127	Skill in drafting policies/processes/procedures.	ID.DE-P1; GV.MT-P3; GV.MT-P4; GV.MT-P5; GV.MT-P6; GV.MT-P7; CT.PO-P1; CT.PO-P2; CT.PO-P3; CM.PO-P1
Skill	S212	Skill in managing organizational policies.	GV.PO-P1; GV.MT-P3; GV.MT-P4; GV.MT-P5; GV.MT-P6; GV.MT-P7; CT.PO-P1; CT.PO-P2; CT.PO-P3; CM.PO-P1
Skill	S235	Skill in negotiating with [*organization-defined stakeholders*] to gain consensus on language requirements for policies/processes/procedures.	CM.PO-P1
Skill	S246	Skill in performing analysis of policies/processes/procedures and related documents for appropriate reflection of the organization’s privacy values.	CM.PO-P1

Statement Type	ID	Description	Subcategory Mapping
Subcategory	**CM.PO-P2**	**Roles and responsibilities (e.g., public relations) for communicating data processing purposes, practices, and associated privacy risks are established.**	
Task	T024	Assign privacy communications responsibilities to organizational roles.	CM.PO-P2
Task	T064	Create new roles that support privacy.	GV.PO-P3; CM.PO-P2
Task	T100	Determine organizational privacy communications responsibilities.	CM.PO-P2
Task	T226	Identify gaps in the organization's privacy communications responsibilities.	CM.PO-P2
Task	T271	Map privacy communications responsibilities to organizational roles.	CM.PO-P2
Knowledge	K029	Knowledge of communications vendors.	CM.PO-P2
Knowledge	K150	Knowledge of RACI Assignment Matrix (Responsible, Accountable, Consulted, Informed).	GV.PO-P3; GV.PO-P4; CM.PO-P2
Knowledge	K157	Knowledge of requirements for communicating privacy purposes, practices, and associated privacy risks internally and externally.	CM.PO-P2
Knowledge	K243	Knowledge of the organization's communications strategy.	CM.PO-P2
Knowledge	K242	Knowledge of the organization's communications policies and procedures.	CM.PO-P2
Knowledge	K278	Knowledge of the organization's preferred communications media.	CM.PO-P2
Knowledge	K307	Knowledge of the privacy team's operating model.	CM.PO-P2
Knowledge	K308	Knowledge of the privacy team's skillsets.	CM.PO-P2
Skill	S014	Skill in aligning organizational roles with data processing communication objectives.	CM.PO-P2
Skill	S090	Skill in crafting effective communications.	CM.PO-P2
Skill	S113	Skill in determining if existing talent can be used to fill skillset gap(s).	GV.PO-P3; CM.PO-P2
Skill	S129	Skill in drafting privacy role responsibilities.	GV.PO-P3; CM.PO-P2
Skill	S214	Skill in managing privacy requirements.	CM.PO-P2
Skill	S247	Skill in performing analysis of privacy requirements.	CM.PO-P2
Skill	S271	Skill in selecting communication mediums/channels for the intended audience(s) regarding data processing risks, practices, and purposes.	CM.PO-P2
Subcategory	**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.**	
Notes: Distinctions between mechanisms for transmitting processing permissions may depend on the organization. Some organizations may require separate activities to create and implement each one.[1]			
Task	T026	Assign responsibility for oversight of data processing awareness mechanisms.	CM.AW-P1
Task	T123	Determine the intended audience.	CM.AW-P1; CM.AW-P7
Task	T131	Determine the needs of the intended audience.	CM.AW-P1; CM.AW-P7
Task	T145	Determine whether the established needs of the intended audience for data processing awareness mechanisms are being met.	CM.AW-P1
Task	T191	Establish a project/execution plan for meeting the prioritized privacy risk management outcome(s).	CM.AW-P1
Task	T237	Identify required data processing awareness mechanisms.	CM.AW-P1
Task	T250	Implement a data processing awareness mechanism(s) that is appropriate for meeting intended audience needs.	CM.AW-P1; CM.AW-P2; CM.AW-P3
Knowledge	K024	Knowledge of characteristics of data processing awareness mechanisms.	CM.AW-P1
Knowledge	K027	Knowledge of communication mechanism design requirements that are derived from the needs of the intended audience.	CM.AW-P1
Knowledge	K234	Knowledge of the means of information delivery for data processing awareness mechanisms.	CM.AW-P1
Knowledge	K251	Knowledge of the organization's data processing activities.	CM.AW-P1

[1] Organizations may choose to evaluate existing mechanisms for gaps (e.g., incompleteness, outdated information) and determine necessary actions to address identified gaps.

Statement Type	ID	Description	Subcategory Mapping
Knowledge	K252	Knowledge of the organization's data processing awareness goals in consultation with [*organization-defined stakeholders*].	CM.AW-P1
Knowledge	K253	Knowledge of the organization's data processing awareness mechanisms.	CM.AW-P1
Knowledge	K254	Knowledge of the organization's data processing ecosystem.	ID.BE-P1; ID.DE-P1; ID.DE-P2; ID.DE-P3; ID.DE-P4; ID.DE-P5; CT.PO-P1; CT.PO-P2; CT.PO-P3; CT.PO-P4; CM.AW-P1; CM.AW-P2; CM.AW-P3; CM.AW-P4; CM.AW-P5; CM.AW-P6; CM.AW-P7; CM.AW-P8
Knowledge	K257	Knowledge of the organization's data processing.	ID.IM-P1; ID.IM-P2; ID.IM-P3; ID.IM-P4; ID.IM-P5; ID.IM-P6; ID.IM-P7; ID.IM-P8; CT.PO-P1; CT.PO-P2; CT.PO-P3; CT.PO-P4; CT.DM-P1; CT.DM-P2; CT.DM-P3; CT.DM-P4; CT.DM-P5; CT.DM-P6; CT.DM-P7; CT.DM-P8; CT.DM-P9; CT.DM-P10; CM.AW-P1; CM.AW-P2; CM.AW-P3; CM.AW-P4; CM.AW-P5; CM.AW-P6; CM.AW-P7; CM.AW-P8
Knowledge	K324	Knowledge of the user base for the organization's communications mechanisms.	CM.AW-P1
Subcategory	**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.**	
Notes: Distinctions between mechanisms for transmitting processing permissions may depend on the organization. Some organizations may require separate activities to create and implement each one.[2]			
Task	T114	Determine the categories of individuals whose feedback about the organization's data processing and associated privacy risks is needed.	CM.AW-P2
Task	T130	Determine the needs of the individuals providing (or who need to provide) feedback about the organization's data processing and associated privacy risks.	CM.AW-P2
Task	T209	Evaluate whether mechanisms for obtaining feedback about the organization's data processing practices and associated privacy risks meet audience needs.	CM.AW-P2
Task	T250	Implement a data processing awareness mechanism(s) that is appropriate for meeting intended audience needs.	CM.AW-P1; CM.AW-P2; CM.AW-P3
Task	T310	Validate that the mechanism(s) for obtaining feedback about the organization's data processing and associated privacy risks is operational/functional.	CM.AW-P2
Knowledge	K096	Knowledge of methods to communicate appropriately with the intended audience group.	CM.AW-P2
Knowledge	K235	Knowledge of the mechanism(s) through which individuals can provide feedback about the organization's data processing practices and associated privacy risks	CM.AW-P2
Knowledge	K236	Knowledge of the needs of the individuals providing (or who need to provide) feedback about the organization's data processing and associated privacy risks.	CM.AW-P2
Knowledge	K254	Knowledge of the organization's data processing ecosystem.	ID.BE-P1; ID.DE-P1; ID.DE-P2; ID.DE-P3; ID.DE-P4; ID.DE-P5; CT.PO-P1; CT.PO-P2; CT.PO-P3; CT.PO-P4; CM.AW-P1; CM.AW-P2; CM.AW-P3; CM.AW-P4; CM.AW-P5; CM.AW-P6; CM.AW-P7; CM.AW-P8

[2] Organizations may choose to evaluate existing mechanisms for gaps (e.g., incompleteness, outdated information) and determine necessary actions to address identified gaps.

Statement Type	ID	Description	Subcategory Mapping
Knowledge	K257	Knowledge of the organization's data processing.	ID.IM-P1; ID.IM-P2; ID.IM-P3; ID.IM-P4; ID.IM-P5; ID.IM-P6; ID.IM-P7; ID.IM-P8; CT.PO-P1; CT.PO-P2; CT.PO-P3; CT.PO-P4; CT.DM-P1; CT.DM-P2; CT.DM-P3; CT.DM-P4; CT.DM-P5; CT.DM-P6; CT.DM-P7; CT.DM-P8; CT.DM-P9; CT.DM-P10; CM.AW-P1; CM.AW-P2; CM.AW-P3; CM.AW-P4; CM.AW-P5; CM.AW-P6; CM.AW-P7; CM.AW-P8
Knowledge	K323	Knowledge of the types of individuals that can provide feedback on the organization's data processing and associated privacy risks.	CM.AW-P2
Skill	S042	Skill in assessing an audience's communication preferences.	CM.AW-P2
Skill	S063	Skill in assessing the quality and effectiveness of audience feedback mechanisms.	CM.AW-P2
Subcategory	**CM.AW-P3**	**System/product/service design enables data processing visibility.**	
Task	T017	Assess system/product/service design for data processing visibility.	CM.AW-P3
Task	T088	Determine data processing visibility design requirements for a system/product/service.	CM.AW-P3
Task	T216	Execute necessary activities based on system/product/service design that fails to enable data processing visibility.	CM.AW-P3
Task	T250	Implement a data processing awareness mechanism(s) that is appropriate for meeting intended audience needs.	CM.AW-P1; CM.AW-P2; CM.AW-P3
Knowledge	K125	Knowledge of privacy by design principles and related best practices.	CM.AW-P3
Knowledge	K128	Knowledge of privacy engineering principles as they pertain to data processing visibility.	CM.AW-P3
Knowledge	K254	Knowledge of the organization's data processing ecosystem.	ID.BE-P1; ID.DE-P1; ID.DE-P2; ID.DE-P3; ID.DE-P4; ID.DE-P5; CT.PO-P1; CT.PO-P2; CT.PO-P3; CT.PO-P4; CM.AW-P1; CM.AW-P2; CM.AW-P3; CM.AW-P4; CM.AW-P5; CM.AW-P6; CM.AW-P7; CM.AW-P8
Knowledge	K256	Knowledge of the organization's data processing visibility requirements.	CM.AW-P3
Knowledge	K257	Knowledge of the organization's data processing.	ID.IM-P1; ID.IM-P2; ID.IM-P3; ID.IM-P4; ID.IM-P5; ID.IM-P6; ID.IM-P7; ID.IM-P8; CT.PO-P1; CT.PO-P2; CT.PO-P3; CT.PO-P4; CT.DM-P1; CT.DM-P2; CT.DM-P3; CT.DM-P4; CT.DM-P5; CT.DM-P6; CT.DM-P7; CT.DM-P8; CT.DM-P9; CT.DM-P10; CM.AW-P1; CM.AW-P2; CM.AW-P3; CM.AW-P4; CM.AW-P5; CM.AW-P6; CM.AW-P7; CM.AW-P8
Skill	S257	Skill in privacy by design.	CM.AW-P3
Skill	S258	Skill in privacy engineering.	CT.DM-P5; CM.AW-P3
Skill	S284	Skill in system/product/service design.	CM.AW-P3
Subcategory	**CM.AW-P4**	**Records of data disclosures and sharing are maintained and can be accessed for review or transmission/disclosure.**	
Task	T071	Define regulatory, contractual, organizational record keeping requirements for data disclosure and sharing.	CM.AW-P4
Task	T273	Meet defined requirements for access to records of data disclosures and sharing via [*organization-determined actions*].	CM.AW-P4
Task	T274	Meet defined requirements for maintenance of records of data disclosures and sharing via [*organization-determined actions*].	CM.AW-P4

Statement Type	ID	Description	Subcategory Mapping
Task	T269	Maintain the organization's documents.	CT.DM-P8; CM.AW-P4
Task	T300	Store records for [*Select: data disclosure and sharing; data provenance and lineage*] in a format that can be accessed for review.	CM.AW-P4; CM.AW-P6
Task	T317	Verify that records of [*Select: data disclosure and sharing; data provenance and lineage*] are maintained.	CM.AW-P4; CM.AW-P6
Task	T318	Verify that records of [*Select: data disclosure and sharing; data provenance and lineage*] can be accessed for review.	CM.AW-P4; CM.AW-P6
Knowledge	K041	Knowledge of data classification and schema.	CM.AW-P4
Knowledge	K050	Knowledge of data modeling/mapping.	CT.DM-P1; CT.DM-P2; CT.DM-P3; CT.DM-P4; CT.DM-P5; CM.AW-P4
Knowledge	K064	Knowledge of document accessibility requirements.	ID.IM-P1; ID.IM-P2; ID.IM-P3; ID.IM-P4; ID.IM-P5; ID.IM-P6; ID.IM-P7; ID.IM-P8; CM.AW-P4
Knowledge	K336	Knowledge of ways data can be disclosed.	CM.AW-P4
Knowledge	K337	Knowledge of ways the organization can disclose or share data.	CM.AW-P4
Knowledge	K137	Knowledge of privacy requirements.	CT.DM-P1; CT.DM-P2; CT.DM-P3; CT.DM-P4; CT.DM-P5; CT.DM-P6; CT.DM-P7; CM.AW-P4
Knowledge	K187	Knowledge of system design.	CT.DM-P1; CT.DM-P2; CT.DM-P3; CT.DM-P4; CT.DM-P5; CT.DM-P6; CT.DM-P7; CM.AW-P4
Knowledge	K199	Knowledge of techniques to facilitate accessibility of data elements in systems.	CT.DM-P1; CT.DM-P2; CT.DM-P3; CT.DM-P4; CM.AW-P4
Knowledge	K254	Knowledge of the organization's data processing ecosystem.	ID.BE-P1; ID.DE-P1; ID.DE-P2; ID.DE-P3; ID.DE-P4; ID.DE-P5; CT.PO-P1; CT.PO-P2; CT.PO-P3; CT.PO-P4; CM.AW-P1; CM.AW-P2; CM.AW-P3; CM.AW-P4; CM.AW-P5; CM.AW-P6; CM.AW-P7; CM.AW-P8
Knowledge	K257	Knowledge of the organization's data processing.	ID.IM-P1; ID.IM-P2; ID.IM-P3; ID.IM-P4; ID.IM-P5; ID.IM-P6; ID.IM-P7; ID.IM-P8; CT.PO-P1; CT.PO-P2; CT.PO-P3; CT.PO-P4; CT.DM-P1; CT.DM-P2; CT.DM-P3; CT.DM-P4; CT.DM-P5; CT.DM-P6; CT.DM-P7; CT.DM-P8; CT.DM-P9; CT.DM-P10; CM.AW-P1; CM.AW-P2; CM.AW-P3; CM.AW-P4; CM.AW-P5; CM.AW-P6; CM.AW-P7; CM.AW-P8
Knowledge	K259	Knowledge of the organization's definitions for data disclosures and sharing.	CM.AW-P4
Knowledge	K272	Knowledge of the organization's mechanisms for data disclosures and sharing.	CM.AW-P4
Subcategory	**CM.AW-P5**	**Data corrections or deletions can be communicated to individuals or organizations (e.g., data sources) in the data processing ecosystem.**	
Task	T023	Assign an owner(s) for communicating about data corrections or deletions to the intended audience.	CM.AW-P5
Task	T086	Determine criteria that initiate communication about data corrections or deletions with the intended audience.	CM.AW-P5
Task	T113	Determine the categories of individuals and organizations that need information related to data corrections or deletions.	CM.AW-P5
Task	T125	Determine the means by which the organization will communicate information about data corrections or deletions with the intended audience.	CM.AW-P5
Task	T137	Determine what information about data corrections and deletions must be communicated to the intended audience.	CM.AW-P5

Statement Type	ID	Description	Subcategory Mapping
Knowledge	K123	Knowledge of pre-determined triggers to initiate communications related to data corrections or deletions.	CM.AW-P5
Knowledge	K089	Knowledge of means to effect data deletions and corrections in the data processing ecosystem.	CM.AW-P5
Knowledge	K248	Knowledge of the organization's contractual provisions regarding data processing operations.	CM.AW-P5
Knowledge	K254	Knowledge of the organization's data processing ecosystem.	ID.BE-P1; ID.DE-P1; ID.DE-P2; ID.DE-P3; ID.DE-P4; ID.DE-P5; CT.PO-P1; CT.PO-P2; CT.PO-P3; CT.PO-P4; CM.AW-P1; CM.AW-P2; CM.AW-P3; CM.AW-P4; CM.AW-P5; CM.AW-P6; CM.AW-P7; CM.AW-P8
Knowledge	K257	Knowledge of the organization's data processing.	ID.IM-P1; ID.IM-P2; ID.IM-P3; ID.IM-P4; ID.IM-P5; ID.IM-P6; ID.IM-P7; ID.IM-P8; CT.PO-P1; CT.PO-P2; CT.PO-P3; CT.PO-P4; CT.DM-P1; CT.DM-P2; CT.DM-P3; CT.DM-P4; CT.DM-P5; CT.DM-P6; CT.DM-P7; CT.DM-P8; CT.DM-P9; CT.DM-P10; CM.AW-P1; CM.AW-P2; CM.AW-P3; CM.AW-P4; CM.AW-P5; CM.AW-P6; CM.AW-P7; CM.AW-P8
Knowledge	K309	Knowledge of the process(es) by which communication content will be created, reviewed, and approved.	CM.AW-P5
Knowledge	K339	Knowledge of what data corrections or deletions are possible within the organization.	CM.AW-P5
Subcategory	**CM.AW-P6**	**Data provenance and lineage are maintained and can be accessed for review or transmission/disclosure.**	
Task	T018	Assess the accuracy and completeness of data provenance and lineage records.	CM.AW-P6
Task	T031	Communicate requirements for data provenance and lineage record keeping to [*organization-defined stakeholders*].	CM.AW-P6
Task	T287	Remediate identified gaps in the data provenance and lineage records consistent with pre-determined requirements.	CM.AW-P6
Task	T300	Store records for [*Select: data disclosure and sharing; data provenance and lineage*] in a format that can be accessed for review.	CM.AW-P4; CM.AW-P6
Task	T317	Verify that records of [*Select: data disclosure and sharing; data provenance and lineage*] are maintained.	CM.AW-P4; CM.AW-P6
Task	T318	Verify that records of [*Select: data disclosure and sharing; data provenance and lineage*] can be accessed for review.	CM.AW-P4; CM.AW-P6
Knowledge	K011	Knowledge of auditing standards for data provenance and lineage.	CM.AW-P6
Knowledge	K158	Knowledge of requirements in system design for accessing data provenance and lineage records for review or transmission/disclosure.	CM.AW-P6
Knowledge	K159	Knowledge of requirements in system design for maintaining data provenance and lineage records.	CM.AW-P6
Knowledge	K254	Knowledge of the organization's data processing ecosystem.	ID.BE-P1; ID.DE-P1; ID.DE-P2; ID.DE-P3; ID.DE-P4; ID.DE-P5; CT.PO-P1; CT.PO-P2; CT.PO-P3; CT.PO-P4; CM.AW-P1; CM.AW-P2; CM.AW-P3; CM.AW-P4; CM.AW-P5; CM.AW-P6; CM.AW-P7; CM.AW-P8
Knowledge	K257	Knowledge of the organization's data processing.	ID.IM-P1; ID.IM-P2; ID.IM-P3; ID.IM-P4; ID.IM-P5; ID.IM-P6; ID.IM-P7; ID.IM-P8; CT.PO-P1; CT.PO-P2; CT.PO-P3; CT.PO-P4; CT.DM-P1; CT.DM-P2; CT.DM-P3; CT.DM-P4; CT.DM-P5; CT.DM-P6; CT.DM-P7; CT.DM-P8; CT.DM-P9; CT.DM-P10; CM.AW-P1; CM.AW-P2; CM.AW-P3; CM.AW-P4; CM.AW-P5; CM.AW-P6; CM.AW-P7; CM.AW-P8

Statement Type	ID	Description	Subcategory Mapping
Knowledge	K305	Knowledge of the organization's tooling for maintaining data provenance and lineage.	CM.AW-P6
Skill	S061	Skill in assessing the organization's data provenance and lineage capabilities.	CM.AW-P6
Subcategory	**CM.AW-P7**	**Impacted individuals and organizations are notified about a privacy breach or event.**	
Task	T123	Determine the intended audience.	CM.AW-P1; CM.AW-P7
Task	T131	Determine the needs of the intended audience.	CM.AW-P1; CM.AW-P7
Task	T184	Draft privacy breach or event communications in consultation with [*organization-defined stakeholders*].	CM.AW-P7
Task	T276	Monitor for privacy breaches or events in collaboration with [*organization-defined stakeholders*].	CM.AW-P7
Task	T278	Notify the intended audience about a privacy breach or event.	CM.AW-P7
Task	T309	Validate operationality of mechanism(s) for delivering notifications to impacted individuals and organizations.	CM.AW-P7
Task	T316	Verify that privacy breach or event notification documentation is complete.	CM.AW-P7
Knowledge	K031	Knowledge of contact information for individuals or organizations that need to be notified of privacy breach or events.	CM.AW-P7
Knowledge	K039	Knowledge of contractual obligations for notifications to individuals and organizations about a privacy breach or event.	CM.AW-P7
Knowledge	K116	Knowledge of organizational privacy breaches or events that require notification to impacted individuals and organizations.	CM.AW-P7
Knowledge	K124	Knowledge of privacy breaches or events that require notification to impacted individuals and organizations.	CM.AW-P7
Knowledge	K155	Knowledge of reporting mechanisms that alert the organization to privacy breaches or events.	CM.AW-P7
Knowledge	K156	Knowledge of required breach notification templates, where applicable.	CM.AW-P7
Knowledge	K254	Knowledge of the organization's data processing ecosystem.	ID.BE-P1; ID.DE-P1; ID.DE-P2; ID.DE-P3; ID.DE-P4; ID.DE-P5; CT.PO-P1; CT.PO-P2; CT.PO-P3; CT.PO-P4; CM.AW-P1; CM.AW-P2; CM.AW-P3; CM.AW-P4; CM.AW-P5; CM.AW-P6; CM.AW-P7; CM.AW-P8
Knowledge	K257	Knowledge of the organization's data processing.	ID.IM-P1; ID.IM-P2; ID.IM-P3; ID.IM-P4; ID.IM-P5; ID.IM-P6; ID.IM-P7; ID.IM-P8; CT.PO-P1; CT.PO-P2; CT.PO-P3; CT.PO-P4; CT.DM-P1; CT.DM-P2; CT.DM-P3; CT.DM-P4; CT.DM-P5; CT.DM-P6; CT.DM-P7; CT.DM-P8; CT.DM-P9; CT.DM-P10; CM.AW-P1; CM.AW-P2; CM.AW-P3; CM.AW-P4; CM.AW-P5; CM.AW-P6; CM.AW-P7; CM.AW-P8
Knowledge	K267	Knowledge of the organization's incident response policies/processes/procedures.	CM.AW-P7; CM.AW-P8
Knowledge	K273	Knowledge of the organization's mechanisms for delivering internal and external communications.	CM.AW-P7
Knowledge	K281	Knowledge of the organization's privacy breach or event notification protocols.	CM.AW-P7
Skill	S048	Skill in assessing privacy events to determine whether a privacy breach has occurred.	CM.AW-P7
Skill	S114	Skill in determining the needs of the intended audience for privacy breach or event notifications.	CM.AW-P7
Skill	S128	Skill in drafting privacy breach or event communications for each relevant jurisdiction in consultation with [*organization-defined stakeholders*].	CM.AW-P7
Subcategory	**CM.AW-P8**	**Individuals are provided with mitigation mechanisms (e.g., credit monitoring, consent withdrawal, data alteration or deletion) to address impacts of problematic data actions.**	
Task	T078	Deploy communications related to the offer of mitigation mechanisms to categories of individuals that could be impacted by problematic data actions.	CM.AW-P8

Statement Type	ID	Description	Subcategory Mapping
Task	T098	Determine mitigation mechanisms to be offered to individuals impacted by problematic data actions.	CM.AW-P8
Task	T099	Determine necessary information to provide to categories of individuals that could be impacted by problematic data actions.	CM.AW-P8
Task	T112	Determine the categories of individual(s) that could be impacted by problematic data actions.	CM.AW-P8
Task	T127	Determine the means to communicate the offer of mitigation mechanisms to categories of individuals that could be impacted by problematic data actions.	CM.AW-P8
Knowledge	K099	Knowledge of mitigation mechanisms to address impacts of problematic data actions.	CM.AW-P8
Knowledge	K232	Knowledge of the impact of problematic data actions (i.e., on individuals and/or organizations).	GV.MT-P6; CM.AW-P8
Knowledge	K233	Knowledge of the impact of the organization's problematic data actions (i.e., on individuals and/or the organization).	GV.MT-P6; CM.AW-P8
Knowledge	K254	Knowledge of the organization's data processing ecosystem.	ID.BE-P1; ID.DE-P1; ID.DE-P2; ID.DE-P3; ID.DE-P4; ID.DE-P5; CT.PO-P1; CT.PO-P2; CT.PO-P3; CT.PO-P4; CM.AW-P1; CM.AW-P2; CM.AW-P3; CM.AW-P4; CM.AW-P5; CM.AW-P6; CM.AW-P7; CM.AW-P8
Knowledge	K257	Knowledge of the organization's data processing.	ID.IM-P1; ID.IM-P2; ID.IM-P3; ID.IM-P4; ID.IM-P5; ID.IM-P6; ID.IM-P7; ID.IM-P8; CT.PO-P1; CT.PO-P2; CT.PO-P3; CT.PO-P4; CT.DM-P1; CT.DM-P2; CT.DM-P3; CT.DM-P4; CT.DM-P5; CT.DM-P6; CT.DM-P7; CT.DM-P8; CT.DM-P9; CT.DM-P10; CM.AW-P1; CM.AW-P2; CM.AW-P3; CM.AW-P4; CM.AW-P5; CM.AW-P6; CM.AW-P7; CM.AW-P8
Knowledge	K267	Knowledge of the organization's incident response policies/processes/procedures.	CM.AW-P7; CM.AW-P8
Knowledge	K295	Knowledge of the organization's risk assessments.	CM.AW-P8
Knowledge	K296	Knowledge of the organization's risk management process(es).	GV.RM-P2; CM.AW-P8
Knowledge	K340	Knowledge of when to inform individuals about mitigation mechanisms in accordance with applicable law, policy, and contractual requirements.	CM.AW-P8
Skill	S016	Skill in aligning risk management processes to legal requirements.	CM.AW-P8
Skill	S180	Skill in identifying the appropriate mitigation mechanism to address impacts of problematic data actions.	CM.AW-P8

2. TKS Statements Inventory

This inventory lists the Privacy Workforce Taxonomy TKS Statements alphabetically and organized by Statement type. Organization-defined parameters in brackets provide flexibility for organizations to adapt and apply TKS Statements based on their unique context and needs. Note that some TKS Statements are mapped to multiple Subcategories, as indicated in the far-right column. Organizations can utilize the TKS Statements in accordance with their privacy workforce needs. TKS Statements can, for example, be used to build work roles or draft job descriptions.

Table 2. TKS Statements Inventory

Statement Type	ID	Description	Subcategory Mapping
Task	T001	Align data life cycle and system development life cycle target states.	CT.PO-P4
Task	T002	Align data processing activities with system/product/service development and operations procedures.	GV.PO-P2
Task	T003	Align governance and risk management policies/processes/procedures with privacy risk assessment results.	GV.PO-P6
Task	T004	Align mission/objectives/activities with [*organization-defined stakeholder*] priorities.	ID.BE-P2
Task	T005	Align priorities for mission/objectives/activities with privacy risk management decisions.	ID.BE-P2
Task	T006	Align priorities for mission/objectives/activities with privacy role(s) and responsibilities.	ID.BE-P2
Task	T007	Align tests for technical measures implemented to manage data processing with the latest industry standards and regulations.	CT.DM-P9
Task	T008	Apply additional techniques that substitute attribute references for attribute values.	CT.DP-P5
Task	T009	Apply the data map model to all data processing activities of systems/products/services.	ID.IM-P8
Task	T010	Apply, as needed, additional techniques that limit [*Select: observability and linkability; identification of individuals; formulation of inferences about individuals' behavior or activities*].	CT.DP-P1; CT.DP-P2; CT.DP-P3
Task	T011	Archive data elements access logs.	CT.DM-P1; CT.DM-P2; CT.DM-P3; CT.DM-P4
Task	T012	Assess [*Select: senior executive; privacy personnel; third party*] privacy-related duties and responsibilities at an [*organization-defined frequency*].	GV.AT-P2; GV.AT-P3; GV.AT-P4
Task	T013	Assess gaps between the organization's policy and audit/log records practices.	CT.DM-P8
Task	T014	Assess how the organization's role(s) in the data processing ecosystem affects its ability to manage risk.	GV.RM-P3
Task	T015	Assess internal and external stakeholder priorities.	ID.BE-P2
Task	T016	Assess problematic data actions for lessons learned.	GV.MT-P6
Task	T017	Assess system/product/service design for data processing visibility.	CM.AW-P3
Task	T018	Assess the accuracy and completeness of data provenance and lineage records.	AM.AW-P6
Task	T019	Assess the impact should identified problematic data actions of systems/products/services create problems.	ID.RA-P4
Task	T020	Assess the organization's risk tolerance for gaps between policies/processes/procedures and risks associated with current practices.	GV.RM-P2
Task	T021	Assess the purpose/use of each data action.	CT.DP-P1; CT.DP-P2; CT.DP-P3
Task	T022	Assess workforce learning needs at an [*organization-defined frequency*].	GV.AT-P1
Task	T023	Assign an owner(s) for communicating about data corrections or deletions to the intended audience.	CM.AW-P5
Task	T024	Assign privacy communications responsibilities to organizational roles.	CM.PO-P2
Task	T025	Assign privacy risk management responsibilities to organizational roles.	GV.PO-P3; GV.RM-P1
Task	T026	Assign responsibility for oversight of data processing awareness mechanisms.	CM.AW-P1
Task	T027	Attain [*organization-defined stakeholder*] feedback on the risk tolerance assessment.	GV.RM-P2
Task	T028	Categorize [*organization-defined third-party stakeholders*] based on common responsibilities.	GV.PO-P4
Task	T029	Classify data elements with their risk classification in context.	ID.IM-P6
Task	T030	Collect feedback on learning activities and materials from [*organization-defined stakeholders*].	GV.AT-P1
Task	T031	Communicate requirements for data provenance and lineage record keeping to [*organization-defined stakeholders*].	CM.AW-P6
Task	T032	Conduct fairness assessments of potential computational/statistical biases in the AI system.	ID.RA-P2
Task	T033	Create a data map model.	ID.IM-P8
Task	T034	Create an organizational privacy policy/policies for data processing that reflects the organization's privacy values and privacy risk management and is consistent with applicable laws, regulations, standards, and guidelines.	GV.PO-P1

Statement Type	ID	Description	Subcategory Mapping
Task	T035	Create a policy/policies that addresses the purpose, scope, roles, responsibilities, and coordination required for data management that is consistent with applicable laws, regulations, standards, and guidelines.	CT.PO-P2
Task	T036	Create a policy/policies that addresses the purpose, scope, roles, responsibilities, and coordination required for analysis and organizational information sharing related to problematic data actions that is consistent with applicable laws, regulations, standards, and guidelines.	GV.MT-P5
Task	T037	Create a policy/policies that addresses the purpose, scope, roles, responsibilities, and coordination required for assessing compliance with legal requirements that is consistent with applicable laws, regulations, standards, and guidelines.	GV.MT-P3
Task	T038	Create a policy/policies that addresses the purpose, scope, roles, responsibilities, and coordination required for assessing compliance with privacy policies that is consistent with applicable laws, regulations, standards, and guidelines.	GV.MT-P3
Task	T039	Create a policy/policies that addresses the purpose, scope, roles, responsibilities, and coordination required for communicating data processing purposes, practices, and associated privacy risks that is consistent with applicable laws, regulations, standards, and guidelines.	CM.PO-P1
Task	T040	Create a policy/policies that addresses the purpose, scope, roles, responsibilities, and coordination required for communicating progress on managing privacy risks that is consistent with applicable laws, regulations, standards, and guidelines.	GV.MT-P4
Task	T041	Create a policy/policies that addresses the purpose, scope, roles, responsibilities, and coordination required for data processing authorizations that is consistent with applicable laws, regulations, standards, and guidelines.	CT.PO-P1
Task	T042	Create a policy/policies that addresses the purpose, scope, roles, responsibilities, and coordination required for data processing ecosystem risk management that is consistent with applicable laws, regulations, standards, and guidelines.	ID.DE-P1
Task	T043	Create a policy/policies that addresses the purpose, scope, roles, responsibilities, and coordination required for enabling individuals' data processing preferences and requests that is consistent with applicable laws, regulations, standards, and guidelines.	CT.PO-P3
Task	T044	Create a policy/policies that addresses the purpose, scope, roles, responsibilities, and coordination required for managing feedback from individuals about organizational privacy practices that is consistent with applicable laws, regulations, standards, and guidelines.	GV.MT-P7
Task	T045	Create a process for communicating priorities for mission/objectives/activities.	ID.BE-P2
Task	T046	Create a process for communicating the organization’s priorities and key requirements for each system/product/service.	ID.BE-P3
Task	T047	Create a process for exchanging information relevant to the organization’s role(s) in the data processing ecosystem.	ID.BE-P1
Task	T048	Create a process for ongoing monitoring and review of data processing ecosystem party contract performance.	ID.BE-P3
Task	T049	Create a process for prioritizing mission/objectives/activities.	ID.BE-P2
Task	T050	Create a process for routinely assessing data processing ecosystem parties for conformance to their obligations.	ID.DE-P5
Task	T051	Create a process(es) to align [*organization-defined third-party stakeholder*] roles and responsibilities with privacy roles and responsibilities.	GV.PO-P4
Task	T052	Create a process(es)/procedure(s) for [*Select: receiving; responding to; tracking*] feedback from individuals about organizational privacy practices.	GV.MT-P7

Statement Type	ID	Description	Subcategory Mapping
Task	T053	Create a process(es)/procedure(s) for enabling individuals' data processing preferences and requests that includes relevant mechanisms to enable such preferences and requests.	CT.PO-P3
Task	T054	Create a process(es)/procedure(s) for facilitating analysis and information sharing about problematic data actions among [*organization-defined stakeholders*].	GV.MT-P5
Task	T055	Create a process(es)/procedure(s) for facilitating implementation of the data processing ecosystem risk management policy/policies and associated controls.	ID.DE-P1
Task	T056	Create a process(es)/procedure(s) for implementing policies for data processing authorizations related to [*Select: organizational decisions; individuals whose data are processed*].	CT.PO-P1
Task	T057	Create a process(es)/procedure(s) for tracking and managing data review, transfer, sharing, or disclosure, alteration, and deletion activities.	CT.PO-P2
Task	T058	Create a process(es)/procedure(s) that addresses audience, cadence, and mechanisms for communicating data processing purposes, practices, and associated privacy risks among [*organization-defined stakeholders*].	CM.PO-P1
Task	T059	Create a process(es)/procedure(s) that addresses audience, cadence, and mechanisms for communicating progress on organizational privacy risk management among [*organization-defined stakeholders*].	GV.MT-P4
Task	T060	Create a process(es)/procedure(s) that addresses audience, cadence, and mechanisms for communication about organizational privacy [*Select: policies; values]* among [*organization-defined stakeholders*].	GV.PO-P1
Task	T061	Create a process(es)/procedure(s) with objectives and associated methods and objects of assessment for assessing compliance with [*Select: legal requirements, privacy policies*].	GV.MT-P3
Task	T062	Create a risk management process(es) in collaboration with [*organization-defined stakeholders*].	GV.RM-P1
Task	T063	Create assessment categories of data processing ecosystem parties based on risk.	ID.DE-P5
Task	T064	Create new roles that support privacy.	GV.PO-P3; CM.PO-P2
Task	T065	Create processes to incorporate privacy best practices and values into system/product/service development and operations in collaboration with [*organization-defined stakeholders*].	GV.PO-P2
Task	T066	Define a set of problematic data actions and problems for assessing systems/products/services.	ID.RA-P3
Task	T067	Define acceptable levels of difference in AI system performance in accordance with established organizational governance policies, business requirements, regulatory compliance, legal frameworks, and ethical standards within the context of use.	ID.RA-P2
Task	T068	Define categories of data processing environments.	ID.IM-P7
Task	T069	Define categories of individuals whose data are being processed.	ID.IM-P3
Task	T070	Define data utility requirements, outside of which the data no longer meets business use requirements).	CT.DP-P5
Task	T071	Define regulatory, contractual, organizational record keeping requirements for data disclosure and sharing.	CM.AW-P4
Task	T072	Define the actions to be taken if disparity levels in AI system performance rise above acceptable levels.	ID.RA-P2
Task	T073	Define the AI system's goals/objectives in collaboration with human factors and socio-technical stakeholders.	ID.RA-P2
Task	T074	Define the AI system's learning tasks, including known assumptions and limitations.	ID.RA-P2
Task	T075	Define the processing permissions for data elements.	CT.DM-P7
Task	T076	Define the roles of data processing ecosystem parties.	ID.DE-P2
Task	T077	Define the scope of contextual factors for assessing the privacy risks of systems/products/services.	ID.RA-P1
Task	T078	Deploy communications related to the offer of mitigation mechanisms to categories of individuals that could be impacted by problematic data actions.	CM.AW-P8

Statement Type	ID	Description	Subcategory Mapping
Task	T079	Determine acceptable actions for responding to risks that exceed the organization's risk tolerance with input from [*organization-defined stakeholders*].	GV.RM-P3
Task	T080	Determine actions to update privacy policies based on the results of their evaluation and any related updates/revisions to privacy values.	GV.MT-P2
Task	T081	Determine actions to update privacy training based on the results of their evaluation and any related updates/revisions to privacy values and/or policies.	GV.MT-P2
Task	T082	Determine actions to update privacy values based on the results of their evaluation.	GV.MT-P2
Task	T083	Determine business objectives that require [*Select: linked or observable data; identification of individuals; formulation of inferences about individuals' behavior or activities*].	CT.DP-P1; CT.DP-P2; CT.DP-P3
Task	T084	Determine categories of data elements necessary to access for [*Select: review; transmission or disclosure; alteration; deletion*].	CT.DM-P1; CT.DM-P2; CT.DM-P3; CT.DM-P4
Task	T085	Determine changes to policies/processes/procedures based on lessons learned from problematic data actions in consultation with [*organization-defined stakeholders*].	GV.MT-P6
Task	T086	Determine criteria that initiate communication about data corrections or deletions with the intended audience.	CM.AW-P5
Task	T087	Determine data processing ecosystem parties on an [*organization-defined schedule*].	ID.DE-P2
Task	T088	Determine data processing visibility design requirements for a system/product/service.	CM.AW-P3
Task	T089	Determine de-identification techniques the organization can utilize to address specific privacy risks.	CT.DP-P1; CT.DP-P2; CT.DP-P3
Task	T090	Determine factors/events that trigger a review of privacy values/policies/training, including the scope of review associated with each triggering event.	GV.MT-P2
Task	T091	Determine how system performance varies across groups, within groups, or for intersecting groups, using context-specific fairness metrics.	ID.RA-P2
Task	T092	Determine how to apply data minimization techniques for substituting attribute values for attribute references.	CT.DP-P5
Task	T093	Determine how to apply technique(s) to data handled in each data action that limit [*Select: observability and linkability; identification of individuals; formulation of inferences about individuals' behavior or activities*].	CT.DP-P1; CT.DP-P2; CT.DP-P3
Task	T094	Determine how to meet privacy requirements for data destruction in systems that fail to do so.	CT.DM-P5
Task	T095	Determine how to respond to gaps between the organization's policy and audit/log records practices in collaboration with [*organization-defined stakeholders*].	CT.DM-P8
Task	T096	Determine if data can be minimized.	CT.DP-P5
Task	T097	Determine inventoried systems/products/services that support organizational priorities and key requirements.	CT.BE-P3
Task	T098	Determine mitigation mechanisms to be offered to individuals impacted by problematic data actions.	CM.AW-P8
Task	T099	Determine necessary information to provide to categories of individuals that could be impacted by problematic data actions.	CM.AW-P8
Task	T100	Determine organizational privacy communications responsibilities.	CM.PO-P2
Task	T101	Determine organizational privacy values in consultation with [*organization-defined stakeholders*].	GV.PO-P1
Task	T102	Determine remedial actions for systems that cannot implement [*Select: logging and monitoring data access requests; auditing data access logs; archiving data access logs*].	CT.DM-P1; CT.DM-P2; CT.DM-P3; CT.DM-P4
Task	T103	Determine remedial actions for systems that cannot support access requests to data elements for [*Select: review; transmission or disclosure; alteration; deletion*].	CT.DM-P1; CT.DM-P2; CT.DM-P3; CT.DM-P4
Task	T104	Determine remedial actions for systems that cannot support access to data elements for [*Select: review; transmission or disclosure; alteration; deletion*].	CT.DM-P1; CT.DM-P2; CT.DM-P3; CT.DM-P4

Statement Type	ID	Description	Subcategory Mapping
Task	T105	Determine remedial actions for systems that cannot transmit data using standardized formats, in consultation with [*organization-defined stakeholders*].	CT.DM-P6
Task	T106	Determine remedial actions for systems that cannot transmit processing permissions and related data values with data elements.	CT.DM-P7
Task	T107	Determine requirements for each system/product/service, based on organizational priorities and privacy laws and regulations.	CT.BE-P3
Task	T108	Determine resources to support the learning program.	GV.AT-P1
Task	T109	Determine sources of bias in test, evaluation, verification, and validation (TEVV) data.	ID.RA-P2
Task	T110	Determine tests for technical measures implemented to manage data processing.	CT.DM-P9
Task	T111	Determine the categories of entities that may request access to data elements for [*Select: review; transmission or disclosure; alteration; deletion*].	CT.DM-P1; CT.DM-P2; CT.DM-P3; CT.DM-P4
Task	T112	Determine the categories of individual(s) that could be impacted by problematic data actions.	CM.AW-P8
Task	T113	Determine the categories of individuals and organizations that need information related to data corrections or deletions.	CM.AW-P5
Task	T114	Determine the categories of individuals whose feedback about the organization's data processing and associated privacy risks is needed.	CM.AW-P2
Task	T115	Determine the current state of system processes in consultation with [*organization-defined stakeholders*] .	CT.PO-P4
Task	T116	Determine the data custodian responsible for data destruction.	CT.DM-P5
Task	T117	Determine the data destruction method(s).	CT.DM-P5
Task	T118	Determine the data to be destroyed in accordance with organizational policy.	CT.DM-P5
Task	T119	Determine the delivery methods for the learning program.	GV.AT-P1
Task	T120	Determine the extent to which governance and risk management policies/processes/procedures adequately address privacy risks.	GV.PO-P6
Task	T121	Determine the factors which will drive the re-evaluation of organizational privacy risk.	GV.MT-P1
Task	T122	Determine the feasibility for updating systems to meet privacy requirements for data destruction.	CT.DM-P5
Task	T123	Determine the intended audience.	CM.AW-P1; CM.AW-P7
Task	T124	Determine the level of granularity for illustrating or documenting data actions.	ID.IM-P4
Task	T125	Determine the means by which the organization will communicate information about data corrections or deletions with the intended audience.	CM.AW-P5
Task	T126	Determine the means through which stakeholder privacy preferences will be obtained.	CT.DM-P10
Task	T127	Determine the means to communicate the offer of mitigation mechanisms to categories of individuals that could be impacted by problematic data actions.	CM.AW-P8
Task	T128	Determine the methodology for data mapping, including level of granularity/detail.	ID.IM-P8
Task	T129	Determine the methodology for taking inventory of data.	ID.IM-P1; ID.IM-P2; ID.IM-P3; ID.IM-P4; ID.IM-P5; ID.IM-P6; ID.IM-P7
Task	T130	Determine the needs of the individuals providing (or who need to provide) feedback about the organization's data processing and associated privacy risks.	CM.AW-P2
Task	T131	Determine the needs of the intended audience.	CM.AW-P1; CM.AW-P7
Task	T132	Determine the organization's data collection and disclosure requirements.	CT.DP-P4
Task	T133	Determine the organization's non-regulation-defined role(s) in the data processing ecosystem.	GV.RM-P3
Task	T134	Determine the organization's regulation-defined role(s) in the data processing ecosystem.	GV.RM-P3
Task	T135	Determine the risks associated with each organizational role in the data processing ecosystem that exceed (or could exceed) the organization's risk tolerance.	GV.RM-P3

Statement Type	ID	Description	Subcategory Mapping
Task	T136	Determine the target state of system processes in consultation with [*organization-defined stakeholders*].	CT.PO-P4
Task	T137	Determine what information about data corrections and deletions must be communicated to the intended audience.	CM.AW-P5
Task	T138	Determine what system design artifacts should support the data mapping.	ID.IM-P8
Task	T139	Determine what the data inventory will be used for.	ID.IM-P1; ID.IM-P2; ID.IM-P3; ID.IM-P4; ID.IM-P5; ID.IM-P6; ID.IM-P7
Task	T140	Determine what the data map(s) will be used for.	ID.IM-P8
Task	T141	Determine whether algorithmic outputs align with identified stakeholder privacy preferences.	CT.DM-P10
Task	T142	Determine whether assessment of data processing ecosystem parties will be conducted by internal or external teams based on resources.	ID.DE-P5
Task	T143	Determine whether lessons learned from problematic data actions(s) require a change to policies/process/procedures.	GV.MT-P6
Task	T144	Determine whether privacy risk re-evaluation is merited based on analysis of internal and external events at an [*organization-defined cadence*].	GV.MT-P1
Task	T145	Determine whether the established needs of the intended audience for data processing awareness mechanisms are being met.	CM.AW-P1
Task	T146	Determine which components of privacy risk assessment should be re-evaluated based on changes to [*organization-defined key factors*].	GV.MT-P1
Task	T147	Determine which contextual factors apply to the data actions of a system/product/service.	ID.RA-P1
Task	T148	Determine which data is to be transmitted, in accordance with the organizational policy.	CT.DM-P6
Task	T149	Determine which interoperability framework(s) or similar multi-party approaches are applicable.	ID.DE-P4
Task	T150	Determine which problematic data actions and associated problems apply to the data actions of systems/products/services.	ID.RA-P3
Task	T151	Determine which stakeholder privacy preferences are in scope to include in algorithmic design objectives.	CT.DM-P10
Task	T152	Determine which standardized format to use for data transmission in accordance with the organizational policy.	CT.DM-P6
Task	T153	Develop a privacy risk response plan in consultation with [*organization-defined stakeholders*].	ID.RA-P5
Task	T154	Develop role-based learning materials for privacy personnel based on duties and responsibilities.	GV.AT-P3
Task	T155	Document a set of problematic data actions and problems associated with the data actions of systems/products/services.	ID.RA-P3
Task	T156	Document categories of data elements within the data actions of systems/products/services.	ID.IM-P6
Task	T157	Document categories of data processing environments.	ID.IM-P7
Task	T158	Document categories of individuals whose data are being processed, including their role within a system/product/service.	ID.IM-P3
Task	T159	Document categories of the purposes for the data actions of systems/products/services.	ID.IM-P5
Task	T160	Document data actions of systems/products/services.	ID.IM-P4
Task	T161	Document data elements that can be used to identify data subjects (i.e., direct and indirect identifiers).	ID.IM-P6
Task	T162	Document factors that may influence individuals affected by the data actions of a system/product/service.	ID.RA-P1
Task	T163	Document methods used for training data processing, including known limitations.	ID.RA-P2
Task	T164	Document owners and operators, including their roles with respect to the systems/products/services and components that process data.	ID.IM-P2
Task	T165	Document privacy risk assessments, including privacy risk prioritization.	ID.RA-P4

Statement Type	ID	Description	Subcategory Mapping
Task	T166	Document selected privacy controls.	ID.RA-P5
Task	T167	Document system/product/service development and operations processes.	GV.PO-P2
Task	T168	Document systems/products/services that process data.	ID.IM-P1
Task	T169	Document the AI system's goals/objectives in collaboration with human factors and socio-technical stakeholders.	ID.RA-P2
Task	T170	Document the AI system's learning tasks, including known assumptions and limitations.	ID.RA-P2
Task	T171	Document the degree to which the data actions of a system/product/service are visible to individuals.	ID.RA-P1
Task	T172	Document the degree to which the organization controls the processing of individuals' data.	ID.RA-P1
Task	T173	Document the evaluation of the risk level of privacy threat actors/threat actor communities associated with the data actions of a system/product/service.	ID.RA-P1
Task	T174	Document the extent of information technology experience (or understanding) of individuals affected by the data actions of a system/product/service.	ID.RA-P1
Task	T175	Document the mitigation strategy for privacy risk findings that require ongoing attention or remediation.	ID.RA-P5
Task	T176	Document the organization's set of problematic data actions and associated problems for assessing systems/products/services.	ID.RA-P3
Task	T177	Document the privacy interests of individuals affected by the data actions of a system/product/service.	ID.RA-P1
Task	T178	Document the privacy risk response decision(s) of the authorizing official or decision-maker.	ID.RA-P5
Task	T179	Document the risk management process(es) in collaboration with [*organization-defined stakeholders*].	GV.RM-P1
Task	T180	Document the scope of contextual factors for assessing the privacy risks of the organization's systems/products/services.	ID.RA-P1
Task	T181	Document the set(s) of contextual factors associated with the data actions of a system/product/service.	ID.RA-P1
Task	T182	Document the specific roles and responsibilities expected from each third party.	GV.AT-P4
Task	T183	Draft language within data processing ecosystem party contracts incorporating identified legal, technical, and organizational measures to meet privacy objectives.	ID.DE-P3; CT.DM-P1; CT.DM-P2; CT.DM-P3; CT.DM-P4
Task	T184	Draft privacy breach or event communications in consultation with [*organization-defined stakeholders*].	CM.AW-P7
Task	T185	Enumerate potential problems for identified problematic data actions.	ID.RA-P3
Task	T186	Establish a learning program plan.	GV.AT-P1
Task	T187	Establish a process for third parties to report potential biases in the AI system.	ID.RA-P2
Task	T188	Establish a process(es) for determining sources of bias in training data.	ID.RA-P2
Task	T189	Establish a process(es) for evaluating (i.e., monitor, test, and verify) the degree to which initial AI system conditions remain representative, accurate, and unbiased in the operational environment over time and under changing sociotechnical conditions.	ID.RA-P2
Task	T190	Establish a process(es) for monitoring AI system outputs for performance or bias issues that exceed established tolerance levels.	ID.RA-P2
Task	T191	Establish a project/execution plan for meeting the prioritized privacy risk management outcome(s).	CM.AW-P1
Task	T192	Establish mechanisms for regular communication and feedback among interdisciplinary AI actors and [*organization-defined stakeholders*].	ID.RA-P2
Task	T193	Establish principles that inform risk assessment and associated decision-making.	GV.RM-P2
Task	T194	Establish roles and responsibilities for identifying and managing information about data processing ecosystem parties on an [*organization-defined schedule*].	ID.DE-P2
Task	T195	Establish roles that support third-party stakeholder privacy risk management responsibilities.	GV.PO-P4
Task	T196	Evaluate AI systems in regards to disability inclusion, including consideration of disability status in bias testing, and discriminatory screen out processes that may arise from non-inclusive design or deployment decisions.	ID.RA-P2

Statement Type	ID	Description	Subcategory Mapping
Task	T197	Evaluate biases in the presentation of system output to end users, operators, and practitioners, in collaboration with human factors experts.	ID.RA-P2
Task	T198	Evaluate contractual terms for consistency with scope of work.	ID.DE-P3
Task	T199	Evaluate data processing ecosystem parties for conformance to their obligations.	ID.DE-P5
Task	T200	Evaluate privacy and security controls associated with the data processing ecosystem on an [*organization-defined schedule*].	ID.DE-P2
Task	T201	Evaluate privacy values/policies/training for gaps based on [*organization-defined triggering factors/events*].	GV.MT-P2
Task	T202	Evaluate systems/products/services for evidence of cognitive bias in design and development that could cause privacy problems to individuals.	ID.RA-P1
Task	T203	Evaluate the effectiveness of technical measures implemented to manage data processing.	CT.DM-P9
Task	T204	Evaluate the effectiveness of the applied privacy risk assessment approach (i.e., quantitative, qualitative, and semi-quantitative).	ID.RA-P4
Task	T205	Evaluate the learning program plan at an [*organization-defined frequency*] against the organization's training needs assessment.	GV.AT-P1
Task	T206	Evaluate the likelihood that identified problematic data actions of systems/products/services will create problems to individuals.	ID.RA-P4
Task	T207	Evaluate the organization's risk management process(es) for privacy gaps.	GV.RM-P1
Task	T208	Evaluate the risk level of privacy threat actors/threat actor communities associated with the data actions of a system/product/service.	ID.RA-P1
Task	T209	Evaluate whether mechanisms for obtaining feedback about the organization's data processing practices and associated privacy risks meet audience needs.	CM.AW-P2
Task	T210	Examine system design documentation/artifacts.	ID.IM-P4
Task	T211	Execute agreed-upon remedial actions for systems that cannot implement [*Select: logging and monitoring data access requests; auditing data access logs; archiving data access logs*].	CT.DM-P1; CT.DM-P2; CT.DM-P3; CT.DM-P4
Task	T212	Execute agreed-upon remedial actions for systems that cannot support access requests to data elements for [*Select: review; transmission or disclosure; alteration; deletion*].	CT.DM-P1; CT.DM-P2; CT.DM-P3; CT.DM-P4
Task	T213	Execute agreed-upon remedial actions for systems that cannot support access to data elements for [*Select: review; transmission or disclosure; alteration; deletion*].	CT.DM-P1; CT.DM-P2; CT.DM-P3; CT.DM-P4
Task	T214	Execute agreed-upon remedial actions for systems that cannot transmit data using standardized formats.	CT.DM-P6
Task	T215	Execute agreed-upon remedial actions for systems that cannot transmit processing permissions and related data values with data elements.	CT.DM-P7
Task	T216	Execute necessary activities based on system/product/service design that fails to enable data processing visibility.	CM.AW-P3
Task	T217	Identify any existing risk management policies/processes/procedures.	GV.RM-P1
Task	T218	Identify categories of data elements within the data actions of systems/products/services.	ID.IM-P6
Task	T219	Identify categories of purposes for the data actions of systems/products/services.	ID.IM-P5
Task	T220	Identify contractual privacy requirements.	GV.PO-P5
Task	T221	Identify data processing activities that fall outside the scope of existing development and operations procedures.	GV.PO-P2
Task	T222	Identify external training or certifications that support job performance.	ID.RA-P1
Task	T223	Identify factors that may influence individuals affected by the data actions of a system/product/service.	GV.AT-P3
Task	T224	Identify gaps in privacy requirements and responsibilities for all organizational roles.	GV.PO-P3
Task	T225	Identify gaps in the current learning program.	GV.AT-P1

Statement Type	ID	Description	Subcategory Mapping
Task	T226	Identify gaps in the organization's privacy communications responsibilities.	CM.PO-P2
Task	T227	Identify gaps in third-party stakeholder roles and responsibilities necessary to manage organizational privacy risk.	GV.PO-P4
Task	T228	Identify groups within the target population (i.e., user base and training data) that may require disaggregated analysis, in collaboration with impacted communities.	ID.RA-P2
Task	T229	Identify how the organization conveys risk tolerance.	GV.RM-P2
Task	T230	Identify legal, technical, and organizational measures data processing ecosystem parties can undertake to meet the organization's privacy objectives.	ID.DE-P3
Task	T231	Identify owners and operators of systems/products/services and components that process data.	ID.IM-P2
Task	T232	Identify owners' and operators' roles with respect to the systems/products/services and components that process data.	ID.IM-P2
Task	T233	Identify potential sources of human-cognitive bias across the AI system life cycle.	ID.RA-P2
Task	T234	Identify priorities for mission/objectives/activities.	ID.BE-P2
Task	T235	Identify privacy requirements in privacy laws and regulations as they apply to the organization's data processing activities.	GV.PO-P5
Task	T236	Identify privacy values implicated by the organization's inventoried data processing activities.	GV.PO-P2
Task	T237	Identify required data processing awareness mechanisms.	CM.AW-P1
Task	T238	Identify systems/products/services that process data.	ID.IM-P1
Task	T239	Identify the appropriate privacy risk assessment approach (i.e., quantitative, qualitative, and semi-quantitative) for evaluating the data actions of systems/products/services.	ID.RA-P4
Task	T240	Identify the categories of risk that inform existing organizational risk management process(es).	GV.RM-P1
Task	T241	Identify the data actions of the systems/products/services.	ID.IM-P4
Task	T242	Identify the degree to which the data actions of a system/product/service are visible to individuals.	ID.RA-P1
Task	T243	Identify the degree to which the organization controls the processing of individuals' data.	ID.RA-P1
Task	T244	Identify the extent of information technology experience (or understanding) of individuals affected by the data actions of a system/product/service.	ID.RA-P1
Task	T245	Identify the privacy interests of individuals affected by the data actions of a system/product/service.	ID.RA-P1
Task	T246	Identify the responsibilities necessary to support the organization's management of privacy risk.	GV.PO-P3
Task	T247	Identify the systems that house the data elements that need to be logged.	CT.DM-P8
Task	T248	Identify third parties with privacy roles and responsibilities.	GV.AT-P4
Task	T249	Identify third-party stakeholder roles and responsibilities to support privacy policies/processes/procedures.	GV.PO-P4
Task	T250	Implement a data processing awareness mechanism(s) that is appropriate for meeting intended audience needs.	CM.AW-P1; CM.AW-P2; CM.AW-P3
Task	T251	Implement applicable components of interoperability frameworks or similar multi-party approaches to the organization's data processing ecosystem risk management practices.	ID.DE-P4
Task	T252	Implement configurations within system architecture and/or localized devices that allow for selective collection or disclosure of data.	CT.DP-P4
Task	T253	Implement learning activities.	GV.AT-P1
Task	T254	Implement lessons learned from the evaluation of the learning plan into a revised learning plan at an [*organization-defined frequency*].	GV.AT-P1
Task	T255	Implement mechanisms for confirming/supporting AI system output and end user perspectives about that output.	ID.RA-P2
Task	T256	Implement risk responses in accordance with privacy risk response plan.	ID.RA-P5

Statement Type	ID	Description	Subcategory Mapping
Task	T257	Include data destruction requirements in system design.	CT.DM-P5
Task	T258	Include privacy requirements for [*Select: the transmission of data elements; transmitting processing permissions and related data values*] into system design.	CT.DM-P6; CT.DM-P7
Task	T259	Include privacy requirements for accessing data elements for [*Select: review; transmission or disclosure; alteration; deletion*] in system design.	CT.DM-P1; CT.DM-P2; CT.DM-P3; CT.DM-P4
Task	T260	Incorporate appropriate changes to policies/processes/procedures based on lessons learned from problematic data actions and with [*organization-defined stakeholder*] consensus.	GV.MT-P6
Task	T261	Incorporate privacy into the organization's risk management process(es).	GV.RM-P1
Task	T262	Incorporate stakeholder responses to the risk tolerance assessment into the organization's risk-related policies/processes/procedures.	GV.RM-P2
Task	T263	Inform [*organization-defined stakeholders*] of changes and new requirements to privacy values, policies, or trainings.	GV.MT-P2
Task	T264	Inform [*organization-defined stakeholders*] of priorities for organizational mission/objectives/activities, following the applicable process(es).	ID.BE-P2
Task	T265	Inform [*organization-defined stakeholders*] of the organization's role(s) in the data processing ecosystem following the applicable process(es).	ID.BE-P1
Task	T266	Inform applicable system/product/service owners and operators of key requirements and organizational priorities, according to established process(es).	ID.BE-P3
Task	T267	Interpret system design documentation/artifacts.	ID.IM-P8
Task	T268	Maintain a document repository for compliance with privacy laws and regulations.	GV.PO-P5
Task	T269	Maintain the organization's documents.	CT.DM-P8; CM.AW-P4
Task	T270	Map data life cycle activities to the system development life cycle, noting overlaps and impacted areas.	CT.PO-P4
Task	T271	Map privacy communications responsibilities to organizational roles.	CM.PO-P2
Task	T272	Map stakeholder privacy preferences to defined algorithmic design objectives.	CT.DM-P10
Task	T273	Meet defined requirements for access to records of data disclosures and sharing via [*organization-determined actions*].	CM.AW-P4
Task	T274	Meet defined requirements for maintenance of records of data disclosures and sharing via [*organization-determined actions*].	CM.AW-P4
Task	T275	Model results in close collaboration with impact assessors, socio-technical experts, and other AI actors with expertise in the context of use.	ID.RA-P2
Task	T276	Monitor for privacy breaches or events in collaboration with [*organization-defined stakeholders*].	CM.AW-P7
Task	T277	Negotiate privacy and security clauses in contracts.	ID.DE-P3; CT.DM-P1; CT.DM-P2; CT.DM-P3; CT.DM-P4
Task	T278	Notify the intended audience about a privacy breach or event.	CM.AW-P7
Task	T279	Obtain [*organization-defined stakeholder*] privacy preferences for inclusion in algorithmic design objectives.	CT.DM-P10
Task	T280	Prioritize data processing ecosystem risk management parties using privacy risk assessment results in accordance with established policies/processes/procedures.	ID.DE-P2
Task	T281	Prioritize risk responses to the problematic data actions of systems/products/services in consultation with [*organization-defined stakeholders*].	ID.RA-P5
Task	T282	Prioritize risks based on the likelihood and impact of the problematic data actions, accounting for organizational values, stakeholder expectations, and costs.	ID.RA-P4
Task	T283	Prioritize selected privacy controls in consultation with [*organization-defined stakeholders*].	ID.RA-P5
Task	T284	Provide [*organization-defined stakeholders*] with access to documentation of privacy risk assessments.	ID.RA-P3; ID.RA-P4

Statement Type	ID	Description	Subcategory Mapping
Task	T285	Provide [*organization-defined stakeholders*] with access to updated documentation of privacy risk assessments.	GV.MT-P1
Task	T286	Provide privacy learning materials to third parties.	GV.AT-P4
Task	T287	Remediate identified gaps in the data provenance and lineage records consistent with pre-determined requirements.	CM.AW-P6
Task	T288	Retain documentation associated with data destruction for regulatory purposes.	CT.DM-P5
Task	T289	Review industry-related standards and best practices related to the data life cycle and the system development life cycle for applicability.	CT.PO-P4
Task	T290	Select a method for visualizing and demonstrating privacy risk prioritization.	ID.RA-P4
Task	T291	Select a privacy risk assessment information repository tool.	ID.RA-P4
Task	T292	Select a system or data store for inventory information.	ID.IM-P1; ID.IM-P2; ID.IM-P3; ID.IM-P4; ID.IM-P5; ID.IM-P6; ID.IM-P7
Task	T293	Select a system or data store for mapping information.	ID.IM-P8
Task	T294	Select AI system performance and validation metrics that are interpretable and unambiguous for downstream decision-making tasks, taking socio-technical factors into consideration.	ID.RA-P2
Task	T295	Select an inventory tool option.	ID.IM-P1; ID.IM-P2; ID.IM-P3; ID.IM-P4; ID.IM-P5; ID.IM-P6; ID.IM-P7
Task	T296	Select privacy controls.	ID.RA-P5
Task	T297	Select the data minimization technique(s) for substituting attribute values for attribute references.	CT.DP-P5
Task	T298	Select the technique(s) that apply to data handled in each data action that limit [*Select: observability and linkability; identification of individuals; formulation of inferences about individuals' behavior or activities*].	CT.DP-P1; CT.DP-P2; CT.DP-P3
Task	T299	Select which components of interoperability frameworks or similar multi-party approaches to apply, based on a thorough assessment.	ID.DE-P4
Task	T300	Store records for [*Select: data disclosure and sharing; data provenance and lineage*] in a format that can be accessed for review.	CM.AW-P4; CM.AW-P6
Task	T301	Test data minimization against data utility and de-identification requirements.	CT.DP-P5
Task	T302	Test selective collection and disclosure configurability in system or device design.	CT.DP-P4
Task	T303	Test the effectiveness of privacy controls.	ID.RA-P5
Task	T304	Test the effectiveness of privacy risk responses.	ID.RA-P5
Task	T305	Train system/product/service owners and operators on key requirements and organizational priorities.	ID.BE-P3
Task	T306	Update all system/product/service development and operations processes with feedback and approval from leadership.	GV.PO-P2
Task	T307	Update configuration settings as needed based on [*organization-defined factors*] for enabling selective collection or disclosure of data elements.	CT.DP-P4
Task	T308	Update privacy roles and responsibilities in accordance with changes to third-party stakeholder relationships.	GV.PO-P4
Task	T309	Validate operationality of mechanism(s) for delivering notifications to impacted individuals and organizations.	CM.AW-P7
Task	T310	Validate that the mechanism(s) for obtaining feedback about the organization's data processing and associated privacy risks is operational/functional.	CM.AW-P2
Task	T311	Verify that audit/log records incorporate the principle of data minimization.	CT.DM-P8
Task	T312	Verify that configurations within system architecture and/or localized devices allow for selective collection or disclosure of data, consistent with organizational policy requirements.	CT.DP-P4

Statement Type	ID	Description	Subcategory Mapping
Task	T313	Verify that data is destroyed according to policy.	CT.DM-P5
Task	T314	Verify that data minimization techniques are applied to substitute attribute values for attribute references.	CT.DP-P5
Task	T315	Verify that organizational privacy values are established.	GV.PO-P1
Task	T316	Verify that privacy breach or event notification documentation is complete.	CM.AW-P7
Task	T317	Verify that records of [*Select: data disclosure and sharing; data provenance and lineage*] are maintained.	CM.AW-P4; CM.AW-P6
Task	T318	Verify that records of [*Select: data disclosure and sharing; data provenance and lineage*] can be accessed for review.	CM.AW-P4; CM.AW-P6
Task	T319	Verify that systems are designed in accordance with privacy requirements for data destruction.	CT.DM-P5
Task	T320	Verify that techniques are applied to data handled in each data action that limit [*Select: observability and linkability; identification of individuals; formulation of inferences about individuals' behavior or activities*].	CT.DP-P1; CT.DP-P2; CT.DP-P3
Task	T321	Verify that tests for technical measures implemented to manage data processing are in place.	CT.DM-P9
Task	T322	Verify that the system implements [*Select: authentication, logging, monitoring, data transformation to standardized formats*] for data transmission.	CT.DM-P6
Task	T323	Verify that the system implements [*Select: logging and monitoring data access requests; auditing data access logs; archiving data access logs*].	CT.DM-P1; CT.DM-P2; CT.DM-P3; CT.DM-P4
Task	T324	Verify that the system implements mechanisms for transmitting processing permissions and related data values with data elements.	CT.DM-P7
Task	T325	Verify that the system supports access requests to data elements for [*Select: review; transmission or disclosure; alteration; deletion*].	CT.DM-P1; CT.DM-P2; CT.DM-P3; CT.DM-P4
Task	T326	Verify that the system supports access to data elements for [*Select: review; transmission or disclosure; alteration; deletion*].	CT.DM-P1; CT.DM-P2; CT.DM-P3; CT.DM-P4
Knowledge	K001	Knowledge of [*organization-defined stakeholders*] impacted by privacy policies.	GV.PO-P1
Knowledge	K002	Knowledge of [*organization-defined stakeholders*] that need to understand the organization's role(s) in the data processing ecosystem.	ID.BE-P1
Knowledge	K003	Knowledge of [*organization-defined stakeholders*] to whom priorities for mission/objectives/activities must be communicated.	ID.BE-P2
Knowledge	K004	Knowledge of [*organization-selected, regulation-defined*] roles of system/product/service and component owners or operators.	ID.IM-P2
Knowledge	K005	Knowledge of access controls for reviewing data elements.	CT.DM-P1; CT.DM-P2; CT.DM-P3; CT.DM-P4
Knowledge	K006	Knowledge of algorithmic design objectives with respect to business goals.	CT.DM-P10
Knowledge	K007	Knowledge of applicable privacy controls, based on the organization's needs.	ID.RA-P5
Knowledge	K008	Knowledge of assessment methodologies.	ID.DE-P5
Knowledge	K009	Knowledge of assessment methods to evaluate data processing ecosystem parties for conformance to their obligations.	ID.DE-P5
Knowledge	K010	Knowledge of audit methodologies.	ID.DE-P5
Knowledge	K011	Knowledge of auditing standards for data provenance and lineage.	CM.AW-P6
Knowledge	K012	Knowledge of baseline privacy and security controls.	ID.DE-P2
Knowledge	K013	Knowledge of boundaries outside of which a given data action fails to meet utility requirements.	CT.DP-P5
Knowledge	K014	Knowledge of business needs and requirements associated with limiting [*Select: observability and linkability of data; identification of individuals; formulation of inferences about individuals' behavior or activities*].	CT.DP-P1; CT.DP-P2; CT.DP-P3
Knowledge	K015	Knowledge of business partners and the data they process for the organization.	GV.PO-P1; GV.PO-P2

Statement Type	ID	Description	Subcategory Mapping
Knowledge	K016	Knowledge of business practices, processes, and related activities that may pose privacy risk to the individuals affected by the data actions of a system/product/service.	ID.RA-P1
Knowledge	K017	Knowledge of business strategies and practices that implicate privacy.	GV.PO-P5
Knowledge	K018	Knowledge of business/sector-specific requirements for policies/processes/procedures.	ID.DE-P1
Knowledge	K019	Knowledge of categories of data elements in systems/products/services.	ID.DE-P2
Knowledge	K020	Knowledge of categories of data elements that are candidates for data minimization.	CT.DP-P4
Knowledge	K021	Knowledge of categories of individuals subject to heightened privacy risk.	ID.RA-P1
Knowledge	K022	Knowledge of categories of purposes for data actions.	ID.IM-P5
Knowledge	K023	Knowledge of changes to [*organization-defined key factors*] that determine risk re-evaluation.	GV.MT-P1
Knowledge	K024	Knowledge of characteristics of data processing awareness mechanisms.	CM.AW-P1
Knowledge	K025	Knowledge of clauses and legal terms necessary for agreements with data processing ecosystem parties.	ID.DE-P3
Knowledge	K026	Knowledge of codes of ethics, conduct, and practice associated with interoperability frameworks or similar multi-party approaches.	ID.DE-P4
Knowledge	K027	Knowledge of communication mechanism design requirements that are derived from the needs of the intended audience.	CM.AW-P1
Knowledge	K028	Knowledge of communications planning.	ID.BE-P3
Knowledge	K029	Knowledge of communications vendors.	CM.PO-P2
Knowledge	K030	Knowledge of considerations for transmission of data elements.	CT.DM-P6
Knowledge	K031	Knowledge of contact information for individuals or organizations that need to be notified of privacy breach or events.	CM.AW-P7
Knowledge	K032	Knowledge of contextual factors associated with implementation of data transmission mechanisms/ tools.	CT.DM-P6
Knowledge	K033	Knowledge of contextual factors associated with the AI system.	ID.RA-P2
Knowledge	K034	Knowledge of contextual factors that affect mitigation efforts.	ID.RA-P5
Knowledge	K035	Knowledge of contextual privacy risk factors that affect impact.	ID.RA-P4
Knowledge	K036	Knowledge of contextual privacy risk factors that affect likelihood.	ID.RA-P4
Knowledge	K037	Knowledge of contract enforcement mechanisms.	ID.DE-P3
Knowledge	K038	Knowledge of contractual obligations for data destruction.	CT.DM-P5
Knowledge	K039	Knowledge of contractual obligations for notifications to individuals and organizations about a privacy breach or event.	CM.AW-P7
Knowledge	K040	Knowledge of data actions of the systems/products/services.	ID.IM-P4
Knowledge	K041	Knowledge of data classification and schema.	CM.AW-P4
Knowledge	K042	Knowledge of data destruction method(s).	CT.DM-P5
Knowledge	K043	Knowledge of data element functionality.	CT.DP-P4
Knowledge	K044	Knowledge of data elements that are legally defined terms.	ID.IM-P1; ID.IM-P2; ID.IM-P3; ID.IM-P4; ID.IM-P5; ID.IM-P6; ID.IM-P7; ID.IM-P8
Knowledge	K045	Knowledge of data elements that are organization-defined terms or classifications.	ID.IM-P1; ID.IM-P2; ID.IM-P3; ID.IM-P4; ID.IM-P5; ID.IM-P6; ID.IM-P7; ID.IM-P8
Knowledge	K046	Knowledge of data flow mapping.	ID.IM-P8
Knowledge	K047	Knowledge of data life cycle.	CT.DM-P5
Knowledge	K048	Knowledge of data management practices.	ID.DE-P1
Knowledge	K049	Knowledge of data minimization techniques.	CT.DP-P5
Knowledge	K050	Knowledge of data modeling/mapping.	CT.DM-P1; CT.DM-P2; CT.DM-P3; CT.DM-P4; CT.DM-P5; CM.AW-P4

Statement Type	ID	Description	Subcategory Mapping
Knowledge	K051	Knowledge of data processing ecosystem parties, including their jurisdiction and role in relation to the organization's data processing activities.	GV.PO-P5
Knowledge	K052	Knowledge of data processing ecosystem party privacy standards of practice.	ID.DE-P3
Knowledge	K053	Knowledge of data processing ecosystem practices.	ID.DE-P1
Knowledge	K054	Knowledge of data processing environments.	ID.IM-P7; ID.DE-P2
Knowledge	K055	Knowledge of data processing requirements.	ID.DE-P1; GV.PO-P5
Knowledge	K056	Knowledge of data that must be retained.	CT.DM-P5
Knowledge	K057	Knowledge of data use cases.	CT.DP-P4
Knowledge	K058	Knowledge of data utility tradeoffs.	CT.DP-P5
Knowledge	K059	Knowledge of databases.	ID.IM-P6
Knowledge	K060	Knowledge of de-identification techniques the organization is capable of implementing.	CT.DP-P1; CT.DP-P2; CT.DP-P3
Knowledge	K061	Knowledge of de-identification techniques, including resource requirements, technical capability, and applicable use cases.	CT.DP-P1; CT.DP-P2; CT.DP-P3
Knowledge	K062	Knowledge of definitions of direct and indirect identifiers.	ID.IM-P6
Knowledge	K063	Knowledge of destruction evidence.	CT.DM-P5
Knowledge	K064	Knowledge of document accessibility requirements.	ID.IM-P1; ID.IM-P2; ID.IM-P3; ID.IM-P4; ID.IM-P5; ID.IM-P6; ID.IM-P7; ID.IM-P8; CM.AW-P4
Knowledge	K065	Knowledge of documentation related to the organization’s data processing environment.	ID.IM-P7
Knowledge	K066	Knowledge of effective strategies for communicating with [*organization-defined stakeholders*].	ID.BE-P1
Knowledge	K067	Knowledge of emerging technology.	GV.RM-P2
Knowledge	K068	Knowledge of enterprise risk management principles.	GV.RM-P1
Knowledge	K069	Knowledge of entity relationship diagramming.	ID.IM-P8
Knowledge	K070	Knowledge of existing learning materials.	GV.AT-P1
Knowledge	K071	Knowledge of existing policies/processes/procedures.	GV.PO-P1; GV.MT-P3; GV.MT-P4; GV.MT-P5; GV.MT-P7
Knowledge	K072	Knowledge of external party expectations regarding the organization's role(s).	ID.BE-P1
Knowledge	K073	Knowledge of factors that can create a need to update values/policies/training.	GV.MT-P2
Knowledge	K074	Knowledge of forms of systemic bias in images, text (or word embeddings), audio, or other complex or unstructured data.	ID.RA-P2
Knowledge	K075	Knowledge of gaps in privacy team skillsets.	GV.PO-P3
Knowledge	K076	Knowledge of general fairness metrics.	ID.RA-P2
Knowledge	K077	Knowledge of governance, risk, and compliance (GRC) tools used by the organization.	ID.RA-P5
Knowledge	K078	Knowledge of guidance and resources on identifiers.	ID.IM-P6
Knowledge	K079	Knowledge of implementation procedures associated with interoperability frameworks or similar multi-party approaches.	ID.DE-P4
Knowledge	K080	Knowledge of implementation rules and requirements associated with interoperability frameworks or similar multi-party approaches.	ID.DE-P4
Knowledge	K081	Knowledge of individual rights within privacy laws and regulations that govern the data actions of a system/product/service.	ID.RA-P1
Knowledge	K082	Knowledge of information or other evidence necessary for responding to regulators.	GV.PO-P5
Knowledge	K083	Knowledge of interoperability frameworks or similar multi-party approaches for managing data processing ecosystem privacy risk.	ID.DE-P4
Knowledge	K084	Knowledge of inventory (and other data management system) options and tools.	ID.IM-P1; ID.IM-P2; ID.IM-P3; ID.IM-P4; ID.IM-P5; ID.IM-P6; ID.IM-P7; ID.IM-P8
Knowledge	K085	Knowledge of key organizational roles related to data processing ecosystem risk management.	ID.DE-P1

Statement Type	ID	Description	Subcategory Mapping
Knowledge	K086	Knowledge of learning program delivery methods.	GV.AT-P1
Knowledge	K087	Knowledge of learning solutions.	GV.AT-P1
Knowledge	K088	Knowledge of legal, technical, and organizational measures to meet organizational privacy objectives.	ID.DE-P3
Knowledge	K089	Knowledge of means to effect data deletions and corrections in the data processing ecosystem.	CM.AW-P5
Knowledge	K090	Knowledge of mechanisms for transmitting processing permissions and related data values with data elements.	CT.DM-P7
Knowledge	K091	Knowledge of mechanisms/tools for archiving documentation associated with data destruction.	CT.DM-P5
Knowledge	K092	Knowledge of mechanisms/tools for archiving documentation associated with data elements access.	CT.DM-P1; CT.DM-P2; CT.DM-P3; CT.DM-P4
Knowledge	K093	Knowledge of mechanisms/tools for logging and monitoring access to data elements for review.	CT.DM-P1; CT.DM-P2; CT.DM-P3; CT.DM-P4
Knowledge	K094	Knowledge of mechanisms/tools for retaining logs associated with data destruction.	CT.DM-P5
Knowledge	K095	Knowledge of methods relating to system/product/service development and operations.	GV.PO-P2
Knowledge	K096	Knowledge of methods to communicate appropriately with the intended audience group.	CM.AW-P2
Knowledge	K097	Knowledge of methods to measure or estimate [*Select: the impact of problems for individuals from privacy events; the likelihood of privacy events; the likelihood of problems arising from privacy events; the likelihood of problems for individuals from privacy events; the severity of problems for individuals*].	ID.RA-P4
Knowledge	K098	Knowledge of metrics and measurements of data utility and data de-identification.	CT.DP-P5
Knowledge	K099	Knowledge of mitigation mechanisms to address impacts of problematic data actions.	CM.AW-P8
Knowledge	K100	Knowledge of mitigation strategies for applying privacy controls to address privacy risks.	ID.RA-P5
Knowledge	K101	Knowledge of mitigation strategies for applying privacy controls to systems/products/services.	ID.RA-P5
Knowledge	K102	Knowledge of modes of transmission of data elements in systems.	CT.DM-P7
Knowledge	K103	Knowledge of modes of transmission of data processing permissions.	CT.DM-P7
Knowledge	K104	Knowledge of mutual processes needed to engage with [*organization-defined third-party stakeholders*].	GV.PO-P4
Knowledge	K105	Knowledge of non-AI solutions to achieve system goals.	ID.RA-P2
Knowledge	K106	Knowledge of non-legal requirements.	ID.BE-P3
Knowledge	K107	Knowledge of obligations/commitments of data processing ecosystem parties.	ID.DE-P5
Knowledge	K108	Knowledge of organization's approach to information governance.	GV.RM-P2
Knowledge	K109	Knowledge of organization's auditing and logging mechanisms.	CT.DM-P8
Knowledge	K110	Knowledge of organization's internal and external policies.	GV.RM-P2
Knowledge	K111	Knowledge of organization's sector-specific risks.	GV.RM-P2
Knowledge	K112	Knowledge of organizational characteristics that can inhibit implementation of de-identification techniques.	CT.DP-P1; CT.DP-P2; CT.DP-P3
Knowledge	K113	Knowledge of organizational data governance.	CT.DM-P5; CT.DM-P6; CT.DM-P7
Knowledge	K114	Knowledge of organizational policies and procedures that guide algorithmic design.	CT.DM-P10
Knowledge	K115	Knowledge of organizational policies.	CT.DM-P8; CT.DM-P9
Knowledge	K116	Knowledge of organizational privacy breaches or events that require notification to impacted individuals and organizations.	CM.AW-P7
Knowledge	K117	Knowledge of organizational roles related to data destruction.	CT.DM-P5
Knowledge	K118	Knowledge of organizational stakeholders with expertise on systems/products/services.	ID.IM-P1
Knowledge	K119	Knowledge of owners and operators of systems/products/services.	ID.BE-P3
Knowledge	K120	Knowledge of policy governance procedures.	GV.PO-P1
Knowledge	K121	Knowledge of potential executive sponsors.	GV.RM-P1
Knowledge	K122	Knowledge of potential impacts of risks to the organization.	GV.RM-P2
Knowledge	K123	Knowledge of pre-determined triggers to initiate communications related to data corrections or deletions.	CM.AW-P5

Statement Type	ID	Description	Subcategory Mapping
Knowledge	K124	Knowledge of privacy breaches or events that require notification to impacted individuals and organizations.	CM.AW-P7
Knowledge	K125	Knowledge of privacy by design principles and related best practices.	CM.AW-P3
Knowledge	K126	Knowledge of privacy control baselines.	ID.RA-P5
Knowledge	K127	Knowledge of privacy control categorization practices (i.e., common/inherited, hybrid, and system-specific).	ID.RA-P5
Knowledge	K128	Knowledge of privacy engineering principles as they pertain to data processing visibility.	CM.AW-P3
Knowledge	K129	Knowledge of privacy guidelines and tools to aid with development of crosswalk(s) and/or compliance register(s).	GV.PO-P5
Knowledge	K130	Knowledge of privacy practices that may negatively impact the privacy of individuals.	ID.RA-P1
Knowledge	K131	Knowledge of privacy principles implicated by the data actions of a system/product/service.	ID.RA-P1
Knowledge	K132	Knowledge of privacy program objectives.	ID.DE-P3
Knowledge	K133	Knowledge of privacy program operating models.	GV.PO-P1
Knowledge	K134	Knowledge of privacy program operating principles.	GV.PO-P1
Knowledge	K135	Knowledge of privacy program priorities.	ID.DE-P3
Knowledge	K136	Knowledge of privacy requirements in systems/products/services.	ID.RA-P1
Knowledge	K137	Knowledge of privacy requirements.	CT.DM-P1; CT.DM-P2; CT.DM-P3; CT.DM-P4; CT.DM-P5; CT.DM-P6; CT.DM-P7; CM.AW-P4
Knowledge	K138	Knowledge of privacy risk assessment approaches (i.e., quantitative, qualitative, and semi-quantitative).	ID.RA-P1; ID.RA-P4
Knowledge	K139	Knowledge of privacy risk assessment methodologies.	ID.RA-P1; ID.RA-P4
Knowledge	K140	Knowledge of privacy risk mitigation controls.	ID.RA-P5
Knowledge	K141	Knowledge of privacy risks of greatest importance to the organization's senior executives.	GV.AT-P2
Knowledge	K142	Knowledge of privacy threat actor/threat actor community capabilities.	ID.RA-P1
Knowledge	K143	Knowledge of privacy threat actors associated with a given privacy threat category.	ID.RA-P1
Knowledge	K144	Knowledge of privacy tools for enabling data processing requests and preferences.	CT.PO-P3
Knowledge	K145	Knowledge of privacy values documentation practices.	GV.PO-P1
Knowledge	K146	Knowledge of privacy-related artifacts.	ID.BE-P3
Knowledge	K147	Knowledge of privacy-related social norms.	ID.RA-P3
Knowledge	K148	Knowledge of process documentation and flowcharts/diagrams related to the data life cycle and system development life cycle.	CT.PO-P4
Knowledge	K149	Knowledge of professional privacy training options.	GV.AT-P3
Knowledge	K150	Knowledge of RACI Assignment Matrix (Responsible, Accountable, Consulted, Informed).	GV.PO-P3; GV.PO-P4; CM.PO-P2
Knowledge	K151	Knowledge of re-identification techniques associated with limiting [*Select: observability and linkability of data; identification of individuals; formulation of inferences about individuals' behavior or activities*].	CT.DP-P1; CT.DP-P2; CT.DP-P3
Knowledge	K152	Knowledge of re-identification techniques research.	ID.IM-P6
Knowledge	K153	Knowledge of relationship dynamics with relevant external parties.	ID.BE-P1
Knowledge	K154	Knowledge of relevant criteria or factors as they apply to prioritizing data processing ecosystem parties.	ID.DE-P2
Knowledge	K155	Knowledge of reporting mechanisms that alert the organization to privacy breaches or events.	CM.AW-P7
Knowledge	K156	Knowledge of required breach notification templates, where applicable.	CM.AW-P7
Knowledge	K157	Knowledge of requirements for communicating privacy purposes, practices, and associated privacy risks internally and externally.	CM.PO-P2
Knowledge	K158	Knowledge of requirements in system design for accessing data provenance and lineage records for review or transmission/disclosure.	CM.AW-P6
Knowledge	K159	Knowledge of requirements in system design for maintaining data provenance and lineage records.	CM.AW-P6
Knowledge	K160	Knowledge of requirements related to data actions.	ID.IM-P4

Statement Type	ID	Description	Subcategory Mapping
Knowledge	K161	Knowledge of requirements related to purposes for data actions.	ID.IM-P5
Knowledge	K162	Knowledge of research related to information/power imbalances and their applicability to privacy risk.	ID.RA-P1
Knowledge	K163	Knowledge of resources required for risk management.	ID.BE-P1; ID.BE-P2; ID.BE-P3; GV.RM-P1; GV.RM-P2; GV.RM-P3
Knowledge	K164	Knowledge of resources to determine negotiation-specific priorities.	ID.DE-P3
Knowledge	K165	Knowledge of resources to support learning activities.	GV.AT-P1
Knowledge	K166	Knowledge of risk assessment and analysis systems.	ID.IM-P1; ID.IM-P2; ID.IM-P3; ID.IM-P4; ID.IM-P5; ID.IM-P6; ID.IM-P7; ID.IM-P8
Knowledge	K167	Knowledge of risk assessment criteria.	GV.RM-P2
Knowledge	K168	Knowledge of risk management processes.	ID.DE-P1; ID.DE-P2; ID.DE-P3; ID.DE-P4; ID.DE-P5; GV.RM-P1; GV.RM-P2; GV.RM-P3
Knowledge	K169	Knowledge of risk management system options.	ID.RA-P3; ID.RA-P4
Knowledge	K170	Knowledge of risk response measurement techniques.	ID.RA-P5
Knowledge	K171	Knowledge of risk response prioritization.	ID.RA-P5
Knowledge	K172	Knowledge of risk responses.	ID.RA-P5
Knowledge	K173	Knowledge of risk scoring based on industry and organizational processes.	ID.RA-P4
Knowledge	K174	Knowledge of roles and responsibilities assigned to the participants in the values/policies/training review process.	GV.MT-P2
Knowledge	K175	Knowledge of roles and responsibilities assigned to the privacy risk re-evaluation process.	GV.MT-P1
Knowledge	K176	Knowledge of safeguards in place for human use of the AI system's output.	ID.RA-P2
Knowledge	K177	Knowledge of software development methodologies.	CT.PO-P4
Knowledge	K178	Knowledge of stakeholder management practices.	ID.BE-P3
Knowledge	K179	Knowledge of stakeholders from whom to gather contextual factors related to the data actions of a system/product/service.	ID.RA-P1
Knowledge	K180	Knowledge of stakeholders responsible for the systems that store individuals' data processing preferences and requests.	CT.PO-P3
Knowledge	K181	Knowledge of stakeholders who need to be informed of privacy risk assessments.	GV.MT-P1
Knowledge	K182	Knowledge of standardized formats for data transmission.	CT.DM-P6
Knowledge	K183	Knowledge of statistical methods for data cleaning, transformation, and balancing.	ID.RA-P2
Knowledge	K184	Knowledge of statistical techniques for mitigating underrepresentation in data.	ID.RA-P2
Knowledge	K185	Knowledge of system design and configurations that minimize data collection or disclosure.	CT.DP-P4
Knowledge	K186	Knowledge of system design documentation/artifacts.	ID.IM-P4; ID.IM-P8
Knowledge	K187	Knowledge of system design.	CT.DM-P1; CT.DM-P2; CT.DM-P3; CT.DM-P4; CT.DM-P5; CT.DM-P6; CT.DM-P7; CM.AW-P4
Knowledge	K188	Knowledge of system or device constraints (i.e., what configurations are possible).	CT.DP-P4
Knowledge	K189	Knowledge of system or device data requirements.	CT.DP-P4
Knowledge	K190	Knowledge of system or device testing to verify selective collection and disclosure configurations are operable at all times.	CT.DP-P4
Knowledge	K191	Knowledge of system requirements.	CT.DM-P9
Knowledge	K192	Knowledge of system/product/service data life cycle operations.	ID.IM-P4
Knowledge	K193	Knowledge of system/product/service inventories.	ID.BE-P3
Knowledge	K194	Knowledge of systems that are currently being logged.	CT.DM-P8
Knowledge	K195	Knowledge of systems/products/services within scope of risk management.	GV.RM-P1
Knowledge	K196	Knowledge of teams responsible for systems that store individuals' data processing preferences and requests.	CT.PO-P3

Statement Type	ID	Description	Subcategory Mapping
Knowledge	K197	Knowledge of technical measure testing best practices.	CT.DM-P9
Knowledge	K198	Knowledge of technical measures implemented to manage data processing.	CT.DM-P9
Knowledge	K199	Knowledge of techniques to facilitate accessibility of data elements in systems.	CT.DM-P1; CT.DM-P2; CT.DM-P3; CT.DM-P4; CM.AW-P4
Knowledge	K200	Knowledge of testing modules that can be incorporated throughout the AI life cycle and corroborated by independent evaluators.	ID.RA-P2
Knowledge	K201	Knowledge of the AI system's data collection.	ID.RA-P2
Knowledge	K202	Knowledge of the AI system's minimum functionality.	ID.RA-P2
Knowledge	K203	Knowledge of the AI system's potential benefits.	ID.RA-P2
Knowledge	K204	Knowledge of the AI systems' technical specifications and requirements.	ID.RA-P2
Knowledge	K205	Knowledge of the applied privacy risk assessment methodology.	ID.RA-P4
Knowledge	K206	Knowledge of the applied privacy risk model's requirements.	ID.RA-P4
Knowledge	K207	Knowledge of the audit common body of knowledge (CBK).	ID.DE-P2
Knowledge	K208	Knowledge of the capabilities of [*organization-defined third-party stakeholders*].	GV.PO-P4
Knowledge	K209	Knowledge of the categories of entities that may request access to an organization's data elements.	CT.DM-P1; CT.DM-P2; CT.DM-P3; CT.DM-P4
Knowledge	K210	Knowledge of the categories of entities that may request data transmission.	CT.DM-P6
Knowledge	K211	Knowledge of the completeness, representativeness, and balance of data sources for the AI system.	ID.RA-P2
Knowledge	K212	Knowledge of the components of conformance evaluation processes built around categories of risk.	ID.DE-P5
Knowledge	K213	Knowledge of the components of the organization's privacy risk assessments.	GV.MT-P1
Knowledge	K214	Knowledge of the contextual nature of privacy regarding how the data actions of a system/product/service impact individuals.	ID.RA-P1
Knowledge	K215	Knowledge of the contractual obligations for processing data elements.	CT.DM-P7
Knowledge	K216	Knowledge of the correlation between the organization's data actions and potential problems to individuals.	ID.RA-P3
Knowledge	K217	Knowledge of the costs of implementing privacy controls.	ID.RA-P5
Knowledge	K218	Knowledge of the data assets.	ID.BE-P1
Knowledge	K219	Knowledge of the data life cycle stages.	ID.RA-P5
Knowledge	K220	Knowledge of the data minimization principle.	CT.DM-P8
Knowledge	K221	Knowledge of the difference between a risk mitigation strategy and a privacy risk control.	ID.RA-P5
Knowledge	K222	Knowledge of the difference between structured and unstructured data.	ID.IM-P6
Knowledge	K223	Knowledge of the different roles privacy threat actors may play in a system/product/service.	ID.RA-P1
Knowledge	K224	Knowledge of the different types of problematic data actions.	GV.MT-P6
Knowledge	K225	Knowledge of the distinction between data management practices and policies/processes/procedures.	ID.DE-P1
Knowledge	K226	Knowledge of the effect of preventative policies/processes/procedures on problematic data action(s).	GV.MT-P6
Knowledge	K227	Knowledge of the enterprise methodology used to test and evaluate privacy controls.	ID.RA-P5
Knowledge	K228	Knowledge of the extent to which privacy controls can be implemented within the organization.	ID.RA-P5
Knowledge	K229	Knowledge of the extent to which privacy is considered/addressed as a risk within the organization.	GV.RM-P1
Knowledge	K230	Knowledge of the extent to which, for a given task, humans can utilize and oversee the AI system's outputs.	ID.RA-P2
Knowledge	K231	Knowledge of the factors that inform the organization's risk tolerance determination.	GV.RM-P3
Knowledge	K232	Knowledge of the impact of problematic data actions (i.e., on individuals and/or organizations).	GV.MT-P6; CM.AW-P8
Knowledge	K233	Knowledge of the impact of the organization's problematic data actions (i.e., on individuals and/or the organization).	GV.MT-P6; CM.AW-P8
Knowledge	K234	Knowledge of the means of information delivery for data processing awareness mechanisms.	CM.AW-P1

Statement Type	ID	Description	Subcategory Mapping
Knowledge	K235	Knowledge of the mechanism(s) through which individuals can provide feedback about the organization's data processing practices and associated privacy risks	CM.AW-P2
Knowledge	K236	Knowledge of the needs of the individuals providing (or who need to provide) feedback about the organization's data processing and associated privacy risks.	CM.AW-P2
Knowledge	K237	Knowledge of the organization's ability to mitigate privacy risk.	ID.DE-P3
Knowledge	K238	Knowledge of the organization's activities that impact privacy.	GV.PO-P6
Knowledge	K239	Knowledge of the organization's algorithmic design objectives.	CT.DM-P10
Knowledge	K240	Knowledge of the organization's and other data processing ecosystem parties' relative bargaining positions/powers.	ID.DE-P3
Knowledge	K241	Knowledge of the organization's budget approval process.	ID.BE-P2
Knowledge	K242	Knowledge of the organization's communications policies and procedures.	CM.PO-P2
Knowledge	K243	Knowledge of the organization's communications strategy.	CM.PO-P2
Knowledge	K244	Knowledge of the organization's components.	ID.IM-P2; ID.IM-P7; ID.IM-P8; ID.BE-P1; ID.BE-P2; ID.BE-P3
Knowledge	K245	Knowledge of the organization's contract management practices.	ID.DE-P3
Knowledge	K246	Knowledge of the organization's contracting process.	ID.DE-P3
Knowledge	K247	Knowledge of the organization's contractual commitments.	GV.RM-P3
Knowledge	K248	Knowledge of the organization's contractual provisions regarding data processing operations.	CM.AW-P5
Knowledge	K249	Knowledge of the organization's data disposition instructions.	CT.DM-P5
Knowledge	K250	Knowledge of the organization's data elements, including associated data values and processing permissions.	CT.DM-P7
Knowledge	K251	Knowledge of the organization's data processing activities.	CM.AW-P1
Knowledge	K252	Knowledge of the organization's data processing awareness goals in consultation with [*organization-defined stakeholders*].	CM.AW-P1
Knowledge	K253	Knowledge of the organization's data processing awareness mechanisms.	CM.AW-P1
Knowledge	K254	Knowledge of the organization's data processing ecosystem.	ID.BE-P1; ID.DE-P1; ID.DE-P2; ID.DE-P3; ID.DE-P4; ID.DE-P5; CT.PO-P1; CT.PO-P2; CT.PO-P3; CT.PO-P4; CM.AW-P1; CM.AW-P2; CM.AW-P3; CM.AW-P4; CM.AW-P5; CM.AW-P6; CM.AW-P7; CM.AW-P8
Knowledge	K255	Knowledge of the organization's data processing goals.	ID.DE-P1; GV.PO-P6; GV.RM-P1; GV.RM-P2; GV.RM-P3; GV.MT-P3; GV.MT-P4; GV.MT-P5; GV.MT-P6; GV.MT-P7; CT.PO-P1; CT.PO-P2; CT.PO-P3; CM.PO-P1
Knowledge	K256	Knowledge of the organization's data processing visibility requirements.	CM.AW-P3
Knowledge	K257	Knowledge of the organization's data processing.	ID.IM-P1; ID.IM-P2; ID.IM-P3; ID.IM-P4; ID.IM-P5; ID.IM-P6; ID.IM-P7; ID.IM-P8; CT.PO-P1; CT.PO-P2; CT.PO-P3; CT.PO-P4; CT.DM-P1; CT.DM-P2; CT.DM-P3; CT.DM-P4; CT.DM-P5; CT.DM-P6; CT.DM-P7; CT.DM-P8; CT.DM-P9; CT.DM-P10; CM.AW-P1; CM.AW-P2; CM.AW-P3; CM.AW-P4; CM.AW-P5; CM.AW-P6; CM.AW-P7; CM.AW-P8

Statement Type	ID	Description	Subcategory Mapping
Knowledge	K258	Knowledge of the organization's data strategy.	ID.DE-P1; GV.PO-P6; GV.RM-P1; GV.RM-P2; GV.RM-P3; GV.MT-P3; GV.MT-P4; GV.MT-P5; GV.MT-P6; GV.MT-P7; CT.PO-P1; CT.PO-P2; CT.PO-P3; CM.PO-P1
Knowledge	K259	Knowledge of the organization's definitions for data disclosures and sharing.	CM.AW-P4
Knowledge	K260	Knowledge of the organization's documentation related to data processing ecosystem parties.	ID.DE-P2
Knowledge	K261	Knowledge of the organization's expansion or consolidation plans.	ID.BE-P2; GV.RM-P1; GV.RM-P2; GV.RM-P3
Knowledge	K262	Knowledge of the organization's external products and services that use personal data.	ID.BE-P1
Knowledge	K263	Knowledge of the organization's functional areas.	GV.AT-P1
Knowledge	K264	Knowledge of the organization's future roadmap.	ID.BE-P2; GV.RM-P1; GV.RM-P2; GV.RM-P3
Knowledge	K265	Knowledge of the organization's governance processes.	GV.PO-P1
Knowledge	K266	Knowledge of the organization's governance structure.	GV.PO-P6; GV.RM-P1
Knowledge	K267	Knowledge of the organization's incident response policies/processes/procedures.	CM.AW-P7; CM.AW-P8
Knowledge	K268	Knowledge of the organization's internal stakeholder strategy and objectives related to data management.	CT.PO-P4
Knowledge	K269	Knowledge of the organization's internal stakeholder strategy and objectives related to system development.	CT.PO-P4
Knowledge	K270	Knowledge of the organization's leadership structure.	GV.AT-P2
Knowledge	K271	Knowledge of the organization's legal requirements related to policies/processes/procedures.	GV.MT-P3; GV.MT-P4; GV.MT-P5; GV.MT-P7
Knowledge	K272	Knowledge of the organization's mechanisms for data disclosures and sharing.	CM.AW-P4
Knowledge	K273	Knowledge of the organization's mechanisms for delivering internal and external communications.	CM.AW-P7
Knowledge	K274	Knowledge of the organization's mission/objectives/activities.	ID.BE-P2
Knowledge	K275	Knowledge of the organization's needs for information that can be provided from inventory and mapping.	ID.IM-P1; ID.IM-P2; ID.IM-P3; ID.IM-P4; ID.IM-P5; ID.IM-P6; ID.IM-P7; ID.IM-P8
Knowledge	K276	Knowledge of the organization's operations, including associated revenue streams if applicable.	ID.BE-P1
Knowledge	K277	Knowledge of the organization's policy management infrastructure.	GV.MT-P2
Knowledge	K278	Knowledge of the organization's preferred communications media.	CM.PO-P2
Knowledge	K279	Knowledge of the organization's primary and secondary purposes/uses of data.	CT.DP-P1; CT.DP-P2; CT.DP-P3
Knowledge	K280	Knowledge of the organization's prioritized privacy outcomes.	ID.RA-P5; GV.PO-P1; GV.PO-P3; GV.RM-P1; GV.MT-P1; GV.MT-P2
Knowledge	K281	Knowledge of the organization's privacy breach or event notification protocols.	CM.AW-P7
Knowledge	K282	Knowledge of the organization's privacy control baseline.	GV.MT-P1
Knowledge	K283	Knowledge of the organization's privacy needs related to each [*organization-defined third-party stakeholder*].	GV.PO-P4
Knowledge	K284	Knowledge of the organization's privacy operating model.	GV.PO-P3
Knowledge	K285	Knowledge of the organization's privacy requirements.	CT.DM-P5
Knowledge	K286	Knowledge of the organization's privacy risk management decisions.	ID.BE-P2
Knowledge	K287	Knowledge of the organization's privacy risk management strategy.	GV.MT-P3; GV.MT-P4; GV.MT-P5; GV.MT-P7
Knowledge	K288	Knowledge of the organization's privacy risks.	ID.BE-P2; ID.BE-P3
Knowledge	K289	Knowledge of the organization's privacy roadmap.	GV.PO-P3
Knowledge	K290	Knowledge of the organization's privacy roles and responsibilities.	ID.BE-P2
Knowledge	K291	Knowledge of the organization's privacy strategy.	GV.PO-P4
Knowledge	K292	Knowledge of the organization's privacy values.	GV.PO-P1; GV.MT-P3; GV.MT-P4; GV.MT-P5; GV.MT-P7; CT.PO-P1; CT.PO-P2; CT.PO-P3; CM.PO-P1

Statement Type	ID	Description	Subcategory Mapping
Knowledge	K293	Knowledge of the organization's process for management and approval of policies/processes/procedures.	GV.MT-P3; GV.MT-P4; GV.MT-P5; GV.MT-P6; GV.MT-P7
Knowledge	K294	Knowledge of the organization's required formats for data transmission.	CT.DM-P6
Knowledge	K295	Knowledge of the organization's risk assessments.	CM.AW-P8
Knowledge	K296	Knowledge of the organization's risk management process(es).	GV.RM-P2; CM.AW-P8
Knowledge	K297	Knowledge of the organization's risk tolerance.	ID.BE-P3; ID.RA-P5; ID.DE-P3; GV.RM-P3; GV.MT-P1
Knowledge	K298	Knowledge of the organization's role(s) in the data processing ecosystem.	ID.DE-P2
Knowledge	K299	Knowledge of the organization's structure.	ID.BE-P1
Knowledge	K300	Knowledge of the organization's systems that store data.	CT.PO-P2
Knowledge	K301	Knowledge of the organization's systems that store individuals' data processing preferences and requests.	CT.PO-P3
Knowledge	K302	Knowledge of the organization's systems that store/log authorizations.	CT.PO-P1
Knowledge	K303	Knowledge of the organization's systems/products/services.	GV.MT-P1; ID.IM-P1; ID.IM-P2; ID.IM-P3; ID.IM-P4; ID.IM-P5; ID.IM-P6; ID.IM-P7; ID.IM-P8; ID.BE-P3; ID.RA-P1
Knowledge	K304	Knowledge of the organization's technical environment.	CT.DM-P9
Knowledge	K305	Knowledge of the organization's tooling for maintaining data provenance and lineage.	CM.AW-P6
Knowledge	K306	Knowledge of the privacy expectations of individuals interacting with or affected by the organization's systems/products/services.	CT.PO-P3
Knowledge	K307	Knowledge of the privacy team's operating model.	CM.PO-P2
Knowledge	K308	Knowledge of the privacy team's skillsets.	CM.PO-P2
Knowledge	K309	Knowledge of the process(es) by which communication content will be created, reviewed, and approved.	CM.AW-P5
Knowledge	K310	Knowledge of the relationship among data inventory elements (i.e., ID.IM-P1 - P7) and how they apply to the creation of data maps.	ID.IM-P8
Knowledge	K311	Knowledge of the relationship between privacy controls and risk factors.	ID.RA-P5
Knowledge	K312	Knowledge of the relationships and dependencies among policies, processes, and procedures.	GV.MT-P3; GV.MT-P4; GV.MT-P5; GV.MT-P6; GV.MT-P7
Knowledge	K313	Knowledge of the relationships between privacy risk mitigating controls and privacy risks.	ID.RA-P5
Knowledge	K314	Knowledge of the results of privacy risk assessments conducted or sanctioned by the organization.	GV.PO-P6
Knowledge	K315	Knowledge of the set of organizational roles.	ID.IM-P2
Knowledge	K316	Knowledge of the set of problematic data actions and problems for assessing an organization’s systems/products/services.	ID.RA-P3
Knowledge	K317	Knowledge of the skills matrix within the organization.	ID.DE-P2
Knowledge	K318	Knowledge of the structure of your organization's technology-related functions.	ID.IM-P1; ID.IM-P2; ID.IM-P3; ID.IM-P4; ID.IM-P5; ID.IM-P6; ID.IM-P7; ID.IM-P8
Knowledge	K319	Knowledge of the system development life cycle.	CT.DP-P4
Knowledge	K320	Knowledge of the technical aspects of system development.	CT.PO-P4
Knowledge	K321	Knowledge of the technical aspects of the system development life cycle.	CT.PO-P4
Knowledge	K322	Knowledge of the third parties' data processing activities	GV.AT-P4
Knowledge	K323	Knowledge of the types of individuals that can provide feedback on the organization's data processing and associated privacy risks.	CM.AW-P2
Knowledge	K324	Knowledge of the user base for the organization's communications mechanisms.	CM.AW-P1
Knowledge	K325	Knowledge of the ways in which the organization's role(s) in the data processing ecosystem affects its ability to manage risk.	GV.RM-P3
Knowledge	K326	Knowledge of the workforce population.	GV.AT-P1

Statement Type	ID	Description	Subcategory Mapping
Knowledge	K327	Knowledge of third parties associated with the AI system(s).	ID.RA-P2
Knowledge	K328	Knowledge of third parties.	ID.IM-P2
Knowledge	K329	Knowledge of third-party data processing activities.	GV.PO-P4
Knowledge	K330	Knowledge of third-party stakeholder risk types.	GV.PO-P4
Knowledge	K331	Knowledge of types of cognitive biases that could cause privacy problems to individuals during the design and development of systems/products/services.	ID.RA-P1
Knowledge	K332	Knowledge of types of data elements.	ID.IM-P6
Knowledge	K333	Knowledge of types of privacy threat actors.	ID.RA-P1
Knowledge	K334	Knowledge of types of privacy threat categories.	ID.RA-P1
Knowledge	K335	Knowledge of vendor management concepts.	GV.PO-P4
Knowledge	K336	Knowledge of ways data can be disclosed.	CM.AW-P4
Knowledge	K337	Knowledge of ways the organization can disclose or share data.	CM.AW-P4
Knowledge	K338	Knowledge of ways the organization stores/keeps privacy risk assessments.	GV.MT-P1
Knowledge	K339	Knowledge of what data corrections or deletions are possible within the organization.	CM.AW-P5
Knowledge	K340	Knowledge of when to inform individuals about mitigation mechanisms in accordance with applicable law, policy, and contractual requirements.	CM.AW-P8
Knowledge	K341	Knowledge of where information on ecosystem parties is located.	GV.PO-P5
Knowledge	K342	Knowledge of where organizational governance and risk management policies/processes/procedures are documented.	GV.PO-P6
Knowledge	K343	Knowledge of where organizational privacy values are documented.	GV.PO-P1
Knowledge	K344	Knowledge of where the organization keeps inventories of systems/products/services.	ID.BE-P3
Knowledge	K345	Knowledge of where the organization's data is located.	CT.DM-P5
Knowledge	K346	Knowledge of where your organization keeps formal documentation on its current state of privacy compliance.	GV.PO-P5; GV.MT-P3; GV.MT-P4; GV.MT-P5; GV.MT-P7
Knowledge	K347	Knowledge of whether [*organization-defined stakeholders*] process privacy-related information in conflict with the organization's privacy values.	GV.PO-P2
Knowledge	K348	Knowledge of why information/power imbalances related to the data processing of a system/product/service exist.	ID.RA-P1
Knowledge	K349	Knowledge of workforce learning preferences.	GV.AT-P1
Skill	S001	Skill in adapting learning activities and materials to meet evolving needs.	GV.AT-P1
Skill	S002	Skill in adapting training to audience knowledge level.	GV.AT-P2
Skill	S003	Skill in addressing gaps between current practices and policy requirements.	ID.DE-P1; GV.MT-P2
Skill	S004	Skill in adjusting controls to privacy risks based on risk responses.	ID.RA-P5
Skill	S005	Skill in advising [*organization-defined stakeholders*] on appropriate outcomes based on gaps between legal requirements and organizational objectives.	GV.MT-P2; CT.PO-P4
Skill	S006	Skill in advocating for an enterprise risk management strategy.	GV.RM-P1
Skill	S007	Skill in advocating for data processing ecosystem risk management policies/processes/procedures to [*organization-defined stakeholders*].	ID.DE-P1
Skill	S008	Skill in advocating for privacy equities with [*organization-defined stakeholders*], including securing executive sponsorship where necessary.	GV.RM-P1
Skill	S009	Skill in advocating for privacy program resources and prioritization.	ID.BE-P2
Skill	S010	Skill in advocating for privacy risk management priorities.	GV.RM-P3
Skill	S011	Skill in advocating for stakeholder action.	ID.BE-P3
Skill	S012	Skill in aligning best practices for audit/log records with organizational policies.	CT.DM-P8
Skill	S013	Skill in aligning executive roles and responsibilities to their specific business function.	GV.AT-P2

Statement Type	ID	Description	Subcategory Mapping
Skill	S014	Skill in aligning organizational roles with data processing communication objectives.	CM.PO-P2
Skill	S015	Skill in aligning organizational roles with organizational privacy objectives.	GV.PO-P3
Skill	S016	Skill in aligning risk management processes to legal requirements.	CM.AW-P8
Skill	S017	Skill in applying an appropriate privacy control baseline to the data actions of systems/products/services.	ID.RA-P5
Skill	S018	Skill in applying audit methodologies.	ID.DE-P2
Skill	S019	Skill in applying codes of ethics, conduct, and practice associated with interoperability frameworks or similar multi-party approaches to external processes within the data processing ecosystem.	ID.DE-P4
Skill	S020	Skill in applying criteria for a privacy risk re-evaluation.	GV.MT-P1
Skill	S021	Skill in applying data destruction methods.	CT.DM-P5
Skill	S022	Skill in applying data dictionary concepts to implement mechanisms for transmitting processing permissions.	CT.DM-P7
Skill	S023	Skill in applying data minimization techniques to achieve data utility and de-identification requirements.	CT.DP-P5
Skill	S024	Skill in applying de-identification techniques that are appropriate to address specific privacy risks in a given use case/context.	CT.DP-P1; CT.DP-P2; CT.DP-P3
Skill	S025	Skill in applying mathematical/computational techniques (i.e., pre-, in-, and post-processing) to balance model performance quality with bias considerations based on data characteristics, model performance, and sociotechnical context.	ID.RA-P2
Skill	S026	Skill in applying methodologies for assigning stakeholder roles and responsibilities.	ID.DE-P1
Skill	S027	Skill in applying privacy requirements to prioritize organizational mission/objectives/activities.	ID.BE-P2
Skill	S028	Skill in applying privacy threat modeling methods.	ID.RA-P3
Skill	S029	Skill in applying privacy tools to policy/process/procedure creation.	CT.PO-P3
Skill	S030	Skill in applying templates for privacy-related system/product/service development and operations procedures.	GV.PO-P2
Skill	S031	Skill in applying templates to manage [*organization-defined third-party stakeholder*] responsibilities.	GV.PO-P4
Skill	S032	Skill in applying test, evaluation, verification, and validation (TEVV) protocols for models, systems and their subcomponents, deployment, and operation.	ID.RA-P2
Skill	S033	Skill in applying the data minimization principle to audit/log records.	CT.DM-P8
Skill	S034	Skill in applying the organization's privacy policies to match its role(s) in the data processing ecosystem with its data processing.	ID.BE-P1
Skill	S035	Skill in applying the results of training need assessments to the evaluation of learning programs.	GV.AT-P1
Skill	S036	Skill in applying updates to technical measures based on testing/assessment results.	CT.DM-P9
Skill	S037	Skill in applying vendor risk management (VRM) methodologies to understand where and how data processing ecosystem partners process data the organization is responsible for.	GV.PO-P5
Skill	S038	Skill in articulating how privacy incorporates into the organization's risks.	GV.RM-P2
Skill	S039	Skill in articulating recommended privacy priorities.	ID.RA-P5
Skill	S040	Skill in articulating the relationship between privacy risk mitigating controls and privacy risk.	ID.RA-P5; GV.MT-P1
Skill	S041	Skill in assessing a learner's demonstrated privacy knowledge.	GV.AT-P1
Skill	S042	Skill in assessing an audience's communication preferences.	CM.AW-P2
Skill	S043	Skill in assessing data labels for evidence of bias.	ID.RA-P2
Skill	S044	Skill in assessing data utility tradeoffs.	CT.DP-P5
Skill	S045	Skill in assessing differences in distributions of AI system outcomes across and within groups, including intersecting groups.	ID.RA-P2
Skill	S046	Skill in assessing error rate sensitivity.	CT.DP-P5
Skill	S047	Skill in assessing policies/processes/procedures for efficacy.	ID.DE-P1
Skill	S048	Skill in assessing privacy events to determine whether a privacy breach has occurred.	CM.AW-P7

Statement Type	ID	Description	Subcategory Mapping
Skill	S049	Skill in assessing privacy gaps in the organization's implementation of interoperability framework or similar multi-party approaches.	ID.DE-P4
Skill	S050	Skill in assessing privacy threat actor/threat actor community capabilities.	ID.RA-P1
Skill	S051	Skill in assessing risk based on the changes to the scope of work.	ID.DE-P3
Skill	S052	Skill in assessing system/product/service support for organizational priorities.	ID.BE-P3
Skill	S053	Skill in assessing the AI system's technical specifications and requirements for alignment with its goals/objectives.	ID.RA-P2
Skill	S054	Skill in assessing the impact of changes to organizational operations on its role(s) in the data processing ecosystem.	ID.BE-P1
Skill	S055	Skill in assessing the impact of information/power imbalances on the severity of privacy problems.	ID.RA-P1
Skill	S056	Skill in assessing the impact of new laws and regulations on contract negotiation.	GV.PO-P5
Skill	S057	Skill in assessing the impact of new laws and regulations on privacy requirements.	GV.PO-P5; GV.MT-P1
Skill	S058	Skill in assessing the impact of privacy threat categories on a system/product/service.	ID.RA-P1
Skill	S059	Skill in assessing the impact of the privacy risk mitigation strategy on individuals.	ID.RA-P5
Skill	S060	Skill in assessing the impact of the privacy risk mitigation strategy on operations.	ID.RA-P5
Skill	S061	Skill in assessing the organization's data provenance and lineage capabilities.	CM.AW-P6
Skill	S062	Skill in assessing the organization's data uses.	CT.DP-P1; CT.DP-P2; CT.DP-P3
Skill	S063	Skill in assessing the quality and effectiveness of audience feedback mechanisms.	CM.AW-P2
Skill	S064	Skill in assessing the tradeoff between utility and privacy associated with implementing mechanisms/tools.	CT.DM-P1; CT.DM-P2; CT.DM-P3; CT.DM-P4
Skill	S065	Skill in assessing what factors should influence changes to the organization's values/policies/training.	GV.MT-P2
Skill	S066	Skill in assessing whether knowledge is transformed into behavior.	GV.AT-P1
Skill	S067	Skill in assigning priority to privacy risk mitigation controls.	ID.RA-P5
Skill	S068	Skill in assigning risk based upon likelihood of it being realized.	ID.RA-P4
Skill	S069	Skill in assigning risk using industry standard tools and techniques.	ID.RA-P4
Skill	S070	Skill in attaining approval from organizational decision-makers.	ID.DE-P1
Skill	S071	Skill in auditing technical and organizational privacy measures.	ID.DE-P5
Skill	S072	Skill in automating legal and regulatory requirements involving privacy operations.	GV.PO-P5
Skill	S073	Skill in building system architecture.	CT.DM-P1; CT.DM-P2; CT.DM-P3; CT.DM-P4; CT.DM-P5; CT.DM-P6
Skill	S074	Skill in calculating risk prioritization.	ID.RA-P5; GV.MT-P1
Skill	S075	Skill in classifying data.	ID.IM-P6
Skill	S076	Skill in communicating [*organization-defined stakeholder*] expectations.	ID.BE-P1
Skill	S077	Skill in communicating metrics (and related insights) to ensure [*organization-defined stakeholder*] support.	ID.DE-P2
Skill	S078	Skill in communicating privacy benefits and risks to the organization's mission/objectives/activities.	ID.BE-P2
Skill	S079	Skill in communicating privacy legal requirements/principles to [*organization-defined stakeholders*] and decision-makers.	ID.BE-P1; GV.MT-P2; GV.MT-P3; GV.MT-P4; GV.MT-P5; GV.MT-P7
Skill	S080	Skill in comparing/contrasting the data life cycle with the system development life cycle within the organization, applying insights from relevant documentation.	CT.PO-P4
Skill	S081	Skill in conducting a privacy risk assessment.	ID.RA-P4; GV.MT-P1
Skill	S082	Skill in conducting assessments of technical and organizational privacy measures.	ID.DE-P5
Skill	S083	Skill in conducting exploratory or investigative activities.	ID.BE-P1
Skill	S084	Skill in conducting root cause analysis.	GV.MT-P6
Skill	S085	Skill in conducting training needs assessment(s).	GV.AT-P1

Statement Type	ID	Description	Subcategory Mapping
Skill	S086	Skill in configuring a system or device to permit selective collection or disclosure of data elements.	CT.DP-P4
Skill	S087	Skill in coordinating with [*organization-defined stakeholders*] on activities related to policies/processes/procedures.	ID.DE-P1
Skill	S088	Skill in correlating problematic data actions with potential problems.	ID.RA-P4; GV.MT-P6
Skill	S089	Skill in crafting effective communications plans.	ID.BE-P3
Skill	S090	Skill in crafting effective communications.	CM.PO-P2
Skill	S091	Skill in creating activities that incorporate privacy values into systems/products/service development and operations.	GV.PO-P2
Skill	S092	Skill in creating conformity assessment processes in collaboration with [*organization-defined stakeholders*].	ID.DE-P5
Skill	S093	Skill in creating consistent processes across the organization for the design, delivery, and evaluation of programs.	CT.PO-P4
Skill	S094	Skill in creating custom, context-specific fairness metrics, in collaboration with affected communities.	ID.RA-P2
Skill	S095	Skill in creating organizational policies.	GV.PO-P1
Skill	S096	Skill in creating policy governance procedures.	GV.PO-P1
Skill	S097	Skill in creating process flows that promote clarity of privacy values and best practices.	GV.PO-P2
Skill	S098	Skill in creating tests to measure the mitigation effectiveness of privacy controls.	ID.RA-P5
Skill	S099	Skill in customizing fairness metrics to specific context of use.	ID.RA-P2
Skill	S100	Skill in data cleaning and balancing.	ID.RA-P2
Skill	S101	Skill in defining criteria for ongoing monitoring and review of contract performance.	ID.DE-P3
Skill	S102	Skill in defining relevant permissions and data values for data processing.	CT.DM-P7
Skill	S103	Skill in designing a privacy roadmap.	GV.PO-P3
Skill	S104	Skill in designing feedback mechanisms to provide insight into learning activities and materials.	GV.AT-P1
Skill	S105	Skill in designing selective collection and disclosure configurations.	CT.DP-P4
Skill	S106	Skill in designing system architecture and configuration baselines.	CT.DP-P4
Skill	S107	Skill in designing system architecture.	CT.DM-P1; CT.DM-P2; CT.DM-P3; CT.DM-P4; CT.DM-P5; CT.DM-P6
Skill	S108	Skill in designing systems.	CT.DM-P7
Skill	S109	Skill in determining appropriate changes to governance, risk, and privacy policies/processes/procedures.	GV.PO-P6; GV.MT-P1; GV.MT-P2
Skill	S110	Skill in determining appropriate changes to policies/processes/procedures to mitigate past issues from problematic data actions.	GV.MT-P6
Skill	S111	Skill in determining contractual obligations that arise from the organization's role in the data processing ecosystem.	GV.RM-P3
Skill	S112	Skill in determining de-identification techniques that are appropriate to address specific privacy risks in a given use case/context.	CT.DP-P1; CT.DP-P2; CT.DP-P3
Skill	S113	Skill in determining if existing talent can be used to fill skillset gap(s).	GV.PO-P3; CM.PO-P2
Skill	S114	Skill in determining the needs of the intended audience for privacy breach or event notifications.	CM.AW-P7
Skill	S115	Skill in determining the organization's privacy maturity level.	GV.PO-P3
Skill	S116	Skill in determining the tradeoff between privacy and the utility of algorithmic outputs.	CT.DM-P10
Skill	S117	Skill in determining whether the applied de-identification technique meets objectives.	CT.DP-P1; CT.DP-P2; CT.DP-P3
Skill	S118	Skill in determining which privacy laws and regulations apply to the data actions of a system/product/service.	ID.RA-P1
Skill	S119	Skill in determining which privacy principles are implicated by the data actions of a system/product/service.	ID.RA-P1

Statement Type	ID	Description	Subcategory Mapping
Skill	S120	Skill in developing relationships with [*organization-defined stakeholders*] to instill privacy values within system/product/service development and operations.	GV.PO-P2
Skill	S121	Skill in developing taxonomies.	ID.IM-P3; ID.IM-P4; ID.IM-P5
Skill	S122	Skill in differentiating between causal/inferential relationships and correlated relationships, as well as selection of proxies used in measurement models.	ID.RA-P2
Skill	S123	Skill in differentiating user roles within the system/product/service.	ID.RA-P1
Skill	S124	Skill in documenting where information on ecosystem parties is located.	GV.PO-P5
Skill	S125	Skill in drafting contracts.	ID.DE-P3
Skill	S126	Skill in drafting policies/processes/procedures that reflect the organization's privacy values.	CM.PO-P1
Skill	S127	Skill in drafting policies/processes/procedures.	ID.DE-P1; GV.MT-P3; GV.MT-P4; GV.MT-P5; GV.MT-P6; GV.MT-P7; CT.PO-P1; CT.PO-P2; CT.PO-P3; CM.PO-P1
Skill	S128	Skill in drafting privacy breach or event communications for each relevant jurisdiction in consultation with [*organization-defined stakeholders*].	CM.AW-P7
Skill	S129	Skill in drafting privacy role responsibilities.	GV.PO-P3; CM.PO-P2
Skill	S130	Skill in drafting privacy roles and responsibilities that relate to third-party stakeholder relationships.	GV.PO-P4
Skill	S131	Skill in drafting requirements from priorities, using the organization's collaboration/communication tools if necessary.	ID.BE-P3
Skill	S132	Skill in drafting standard contractual language designed to meet an organization’s privacy program objectives.	ID.DE-P3
Skill	S133	Skill in educating *[organization-defined stakeholders]* on privacy risk.	GV.RM-P1
Skill	S134	Skill in effectively leading group discussions involving the relationship between privacy values and data processing activities.	GV.PO-P2
Skill	S135	Skill in engaging with development teams to identify privacy requirements of systems/products/services.	ID.RA-P1
Skill	S136	Skill in error rate calculation.	CT.DP-P5
Skill	S137	Skill in establishing risk prioritization.	ID.RA-P5
Skill	S138	Skill in evaluating (i.e., quantitatively, qualitatively) the impact of risk responses on privacy risk.	ID.RA-P5
Skill	S139	Skill in evaluating audit/log use cases based on system design.	CT.DM-P8
Skill	S140	Skill in evaluating contextual factors to implement data transmission mechanisms.	CT.DM-P6
Skill	S141	Skill in evaluating contracts based on [*organization-defined criteria*].	ID.DE-P3
Skill	S142	Skill in evaluating how privacy laws and regulations apply to the organization's data processing goals.	ID.BE-P1
Skill	S143	Skill in evaluating how privacy requirements affect the risk/benefit calculus within privacy risk assessment.	ID.RA-P1
Skill	S144	Skill in evaluating how privacy standards and best practices apply to the organization's data processing goals.	ID.BE-P1
Skill	S145	Skill in evaluating mechanisms/tools for compatibility with existing system architecture.	CT.DM-P1; CT.DM-P2; CT.DM-P3; CT.DM-P4
Skill	S146	Skill in evaluating mechanisms/tools for effectiveness in meeting privacy requirements.	CT.DM-P1; CT.DM-P2; CT.DM-P3; CT.DM-P4
Skill	S147	Skill in evaluating privacy requirements documentation for a system/product/service.	ID.RA-P1
Skill	S148	Skill in evaluating privacy risk models.	ID.RA-P4
Skill	S149	Skill in evaluating privacy values within relevant systems/products/services and operations.	GV.PO-P2
Skill	S150	Skill in evaluating the effectiveness of interoperability frameworks or similar multi-party approaches to address privacy risks across the organization's data processing ecosystem.	ID.DE-P4
Skill	S151	Skill in evaluating the effectiveness of risk responses.	ID.RA-P5

Statement Type	ID	Description	Subcategory Mapping
Skill	S152	Skill in evaluating the quality of information received.	ID.IM-P1; ID.IM-P2; ID.IM-P3; ID.IM-P4; ID.IM-P5; ID.IM-P6; ID.IM-P7; ID.IM-P8
Skill	S153	Skill in evaluating the risk tolerance of individuals affected by the data actions of a system/product/service.	ID.RA-P1
Skill	S154	Skill in evaluating whether privacy values are aligned with operations.	GV.MT-P2
Skill	S155	Skill in executing a communications plan.	ID.BE-P3; GV.MT-P2
Skill	S156	Skill in executing re-identification techniques.	CT.DP-P1; CT.DP-P2; CT.DP-P3
Skill	S157	Skill in explaining complex topics/ideas.	ID.BE-P3; GV.MT-P2
Skill	S158	Skill in explaining contractual privacy responsibilities.	ID.DE-P3
Skill	S159	Skill in explaining recent documented exploits or attacks to technical and non-technical staff, to facilitate classification of data elements as direct or indirect identifiers.	ID.IM-P6
Skill	S160	Skill in explaining risk response strategies to stakeholders.	ID.RA-P5
Skill	S161	Skill in facilitating changes to audit/log records practices in collaboration with [*organization-defined stakeholders*].	CT.DM-P8
Skill	S162	Skill in facilitating communication among [*organization-defined stakeholders*] about the learning program plan, including how it supports organizational and learning goals and impacts personnel.	GV.AT-P1
Skill	S163	Skill in facilitating productive privacy values discussions.	GV.PO-P1
Skill	S164	Skill in fostering changes necessary to reduce risk and strengthen the organization's privacy posture.	GV.PO-P6
Skill	S165	Skill in gathering correct, accurate, and relevant information.	ID.RA-P1; GV.PO-P5
Skill	S166	Skill in harmonizing the design, delivery, and evaluation methodologies within system development.	CT.PO-P4
Skill	S167	Skill in identifying assumptions and decisions made for data and metadata selection.	ID.RA-P2
Skill	S168	Skill in identifying data elements that are legally defined terms.	ID.IM-P1; ID.IM-P2; ID.IM-P3; ID.IM-P4; ID.IM-P5; ID.IM-P6; ID.IM-P7; ID.IM-P8
Skill	S169	Skill in identifying data elements that are organization-defined terms or classifications.	ID.IM-P1; ID.IM-P2; ID.IM-P3; ID.IM-P4; ID.IM-P5; ID.IM-P6; ID.IM-P7; ID.IM-P8
Skill	S170	Skill in identifying data processing requirements applicable to the organization.	ID.DE-P1
Skill	S171	Skill in identifying effective mitigation strategies for applying privacy controls to address privacy risks.	ID.RA-P5
Skill	S172	Skill in identifying input data features that may serve as proxies for demographic group membership or otherwise give rise to emergent bias within AI systems.	ID.RA-P2
Skill	S173	Skill in identifying objective data points or information to measure or estimate privacy risk factors.	ID.RA-P4
Skill	S174	Skill in identifying owners and operators with respect to the systems/products/services and components that process data.	ID.IM-P2
Skill	S175	Skill in identifying privacy practices that negatively impact the privacy of an individual.	ID.RA-P1
Skill	S176	Skill in identifying privacy roles and responsibilities related to new data processing activities.	GV.PO-P4
Skill	S177	Skill in identifying requirements in privacy laws and regulations.	ID.BE-P2
Skill	S178	Skill in identifying roles and decision-makers to collaborate for consensus-building.	GV.PO-P1; ID.DE-P1
Skill	S179	Skill in identifying stakeholders impacted by algorithmic design.	CT.DM-P10
Skill	S180	Skill in identifying the appropriate mitigation mechanism to address impacts of problematic data actions.	CM.AW-P8
Skill	S181	Skill in identifying the most appropriate internal or external individuals involved in [*organization-defined third-party stakeholder*] engagement.	GV.PO-P4
Skill	S182	Skill in identifying the organization's role in the data processing ecosystem.	GV.RM-P3
Skill	S183	Skill in identifying the organization’s systems/products/services that process data.	ID.IM-P1
Skill	S184	Skill in identifying training needs related to privacy risk measurement or estimation.	ID.RA-P4
Skill	S185	Skill in identifying types of harms from computational/statistical bias.	ID.RA-P2
Skill	S186	Skill in identifying undocumented/implicit risk tolerance policies/processes/procedures.	GV.RM-P2

Statement Type	ID	Description	Subcategory Mapping
Skill	S187	Skill in identifying whether previously performed privacy risk assessments are still relevant to the organization.	GV.PO-P6
Skill	S188	Skill in implementing controls.	ID.DE-P2
Skill	S189	Skill in implementing inventory (and other data management system) options and tools.	ID.IM-P1; ID.IM-P2; ID.IM-P3; ID.IM-P4; ID.IM-P5; ID.IM-P6; ID.IM-P7; ID.IM-P8
Skill	S190	Skill in implementing leadership mandates.	GV.PO-P2
Skill	S191	Skill in implementing mechanisms to meet data processing requirements.	CT.DM-P7
Skill	S192	Skill in implementing new methods within system management and data management based on gap analysis results.	CT.PO-P4
Skill	S193	Skill in implementing privacy risk response plans tailored to organizational needs.	ID.RA-P5
Skill	S194	Skill in implementing privacy risk responses in collaboration with [*organization-defined stakeholders*].	ID.RA-P5
Skill	S195	Skill in implementing risk responses based on context.	ID.RA-P5
Skill	S196	Skill in incorporating organizational privacy priorities into governance and risk management policies/processes/procedures.	GV.PO-P6
Skill	S197	Skill in informing stakeholders of privacy risks.	ID.RA-P5
Skill	S198	Skill in interpreting diagnostic metrics.	CT.DM-P9
Skill	S199	Skill in interpreting leadership mandates.	GV.PO-P2
Skill	S200	Skill in interpreting privacy risk assessment results.	ID.DE-P2; GV.PO-P6
Skill	S201	Skill in interpreting system design documentation/artifacts.	ID.IM-P8
Skill	S202	Skill in interpreting training data/feedback.	GV.AT-P1
Skill	S203	Skill in leading discovery activities to align privacy values with system/product/service development and operations.	GV.PO-P2
Skill	S204	Skill in leveraging methodologies for assigning stakeholder roles and responsibilities.	GV.PO-P1
Skill	S205	Skill in maintaining taxonomies.	ID.IM-P3; ID.IM-P4; ID.IM-P5
Skill	S206	Skill in making privacy-related recommendations for actions.	ID.DE-P1
Skill	S207	Skill in making risk response decisions in consultation with [*organization-defined stakeholders*].	ID.RA-P5
Skill	S208	Skill in managing appropriate response-related actions to inquiries that involve privacy concerns.	GV.PO-P2
Skill	S209	Skill in managing interoperability frameworks or similar multi-party approaches to address privacy risks across the organization's data processing ecosystem.	ID.DE-P4
Skill	S210	Skill in managing multi-stakeholder processes.	GV.RM-P1
Skill	S211	Skill in managing mutual privacy expectations with third-party stakeholders.	GV.PO-P4
Skill	S212	Skill in managing organizational policies.	GV.PO-P1; GV.MT-P3; GV.MT-P4; GV.MT-P5; GV.MT-P6; GV.MT-P7; CT.PO-P1; CT.PO-P2; CT.PO-P3; CM.PO-P1
Skill	S213	Skill in managing privacy compliance efforts.	GV.PO-P5
Skill	S214	Skill in managing privacy requirements.	CM.PO-P2
Skill	S215	Skill in managing privacy/utility tradeoffs in a manner consistent with the organization's risk strategy/priorities.	CT.DM-P10
Skill	S216	Skill in managing relationships with data processing ecosystem parties.	ID.DE-P2
Skill	S217	Skill in managing stakeholder expectations.	ID.BE-P1
Skill	S218	Skill in mapping data flows.	ID.IM-P8
Skill	S219	Skill in mapping entity relationships.	ID.IM-P8
Skill	S220	Skill in mapping governance, risk, and privacy policies/processes/procedures.	GV.PO-P6
Skill	S221	Skill in mapping policies/processes/procedures to identified problems.	GV.MT-P6
Skill	S222	Skill in mapping privacy requirements to algorithmic design objectives.	CT.DM-P10

Statement Type	ID	Description	Subcategory Mapping
Skill	S223	Skill in mapping processes.	ID.IM-P8
Skill	S224	Skill in marking outputs to clearly show they came from an AI.	ID.RA-P2
Skill	S225	Skill in matching mitigation controls to privacy risk factors.	ID.RA-P5
Skill	S226	Skill in measuring or estimating the impact of privacy events on individuals.	ID.RA-P4
Skill	S227	Skill in measuring or estimating the impact of problems for individuals from privacy events.	ID.RA-P4
Skill	S228	Skill in measuring or estimating the likelihood of privacy events.	ID.RA-P4
Skill	S229	Skill in measuring or estimating the likelihood of problems for individuals arising from privacy events.	ID.RA-P4
Skill	S230	Skill in measuring or estimating the likelihood of problems for individuals from privacy events.	ID.RA-P4
Skill	S231	Skill in measuring privacy values within relevant systems/products/services and operations.	GV.PO-P2
Skill	S232	Skill in modeling privacy threats.	ID.RA-P3
Skill	S233	Skill in negotiating third-party agreements to align with organizational privacy roles and responsibilities.	GV.PO-P4
Skill	S234	Skill in negotiating to reach agreements about organizational values and policies.	GV.PO-P1
Skill	S235	Skill in negotiating with [*organization-defined stakeholders*] to gain consensus on language requirements for policies/processes/procedures.	CM.PO-P1
Skill	S236	Skill in negotiating with [*organization-defined stakeholders*] to meet privacy risk assessment goals.	ID.RA-P1
Skill	S237	Skill in negotiating with external parties.	ID.DE-P3
Skill	S238	Skill in negotiating with internal stakeholders.	ID.DE-P3
Skill	S239	Skill in obtaining stakeholder engagement.	GV.RM-P1
Skill	S240	Skill in organizing a team capable of understanding the relevance and effectiveness of policies/processes/procedures.	ID.DE-P1
Skill	S241	Skill in organizing stakeholder priorities.	ID.BE-P2
Skill	S242	Skill in performing a data discovery exercise manually or via tool(s) for digital and non-digital data.	ID.BE-P1
Skill	S243	Skill in performing a gap analysis.	GV.PO-P6
Skill	S244	Skill in performing analysis of contract language for adherence to data processing and privacy requirements.	ID.DE-P3
Skill	S245	Skill in performing analysis of data used by [*organization-defined stakeholders*] to ensure privacy values are followed.	GV.PO-P2
Skill	S246	Skill in performing analysis of policies/processes/procedures and related documents for appropriate reflection of the organization’s privacy values.	CM.PO-P1
Skill	S247	Skill in performing analysis of privacy requirements.	CM.PO-P2
Skill	S248	Skill in performing analysis of quantified harms from computational/statistical bias for contextually significant differences across groups, within groups, and among intersecting groups.	ID.RA-P2
Skill	S249	Skill in performing analysis of risk in a defined risk management process.	GV.RM-P2
Skill	S250	Skill in performing analysis of technical measures to manage data processing for effectiveness.	CT.DM-P9
Skill	S251	Skill in performing analysis of the organization's role(s) under applicable privacy laws and regulations.	ID.BE-P1
Skill	S252	Skill in performing contract negotiations and reviews that are effective for achieving privacy objectives.	GV.PO-P5
Skill	S253	Skill in performing gap analysis related to privacy risk measurement or estimation.	ID.RA-P4
Skill	S254	Skill in performing gap analysis to determine if privacy values are missing from system/product/service development and operations processes.	GV.PO-P2
Skill	S255	Skill in performing system analysis.	CT.DM-P1; CT.DM-P2; CT.DM-P3; CT.DM-P4; CT.DM-P5; CT.DM-P6
Skill	S256	Skill in prioritizing organizational mission/objectives/activities.	ID.BE-P2
Skill	S257	Skill in privacy by design.	CM.AW-P3
Skill	S258	Skill in privacy engineering.	CT.DM-P5; CM.AW-P3
Skill	S259	Skill in process mapping.	ID.RA-P2

Statement Type	ID	Description	Subcategory Mapping
Skill	S260	Skill in providing alternative means of using data in accord with the organization's privacy values.	GV.PO-P2
Skill	S261	Skill in querying inventory management systems.	ID.IM-P1; ID.IM-P2; ID.IM-P3; ID.IM-P4; ID.IM-P5; ID.IM-P6; ID.IM-P7; ID.IM-P8
Skill	S262	Skill in recognizing cognitive biases related to the system/product/service life cycle.	ID.RA-P1
Skill	S263	Skill in recognizing information/power imbalances related to data processing.	ID.RA-P1
Skill	S264	Skill in reporting from inventory management systems.	ID.IM-P1; ID.IM-P2; ID.IM-P3; ID.IM-P4; ID.IM-P5; ID.IM-P6; ID.IM-P7; ID.IM-P8
Skill	S265	Skill in researching legal opinions and related best practices in accord with laws and regulations.	GV.PO-P5
Skill	S266	Skill in researching trends involving individual data processing preferences and request types.	CT.PO-P3
Skill	S267	Skill in retrieving information on data elements from databases, unstructured data stores, and other stores of data.	ID.IM-P6
Skill	S268	Skill in reviewing and interpreting system design documentation/artifacts to identify data actions.	ID.IM-P4
Skill	S269	Skill in reviewing data processing permissions and data values for relevance.	CT.DM-P7
Skill	S270	Skill in selecting an effective approach to gather contextual information from [*organization-defined stakeholders*].	ID.RA-P1
Skill	S271	Skill in selecting communication mediums/channels for the intended audience(s) regarding data processing risks, practices, and purposes.	CM.PO-P2
Skill	S272	Skill in selecting controls.	ID.DE-P2
Skill	S273	Skill in selecting data transmission formats based on context and consistent with organizational requirements.	CT.DM-P6
Skill	S274	Skill in selecting de-identification techniques matched to risk classification.	CT.DP-P1; CT.DP-P2; CT.DP-P3
Skill	S275	Skill in selecting means to obtain stakeholder privacy preferences based on organizational context.	CT.DM-P10
Skill	S276	Skill in selecting methods to include in documentation related to system/product/service development and operations.	GV.PO-P2
Skill	S277	Skill in selecting policy and/or technical controls in the context of stakeholder values, mission, and objectives.	CT.PO-P4
Skill	S278	Skill in selecting privacy control(s) to address an identified privacy risk.	ID.RA-P5
Skill	S279	Skill in selecting privacy control(s) to mitigate an identified privacy risk.	ID.RA-P5
Skill	S280	Skill in selecting privacy controls in the absence of a privacy control baseline.	ID.RA-P5
Skill	S281	Skill in selecting risk responses to address identified privacy risks.	ID.RA-P5
Skill	S282	Skill in soliciting information from organizational stakeholders using a variety of communication methods.	ID.BE-P2
Skill	S283	Skill in surveying or interviewing [*organization-defined stakeholders*].	ID.RA-P3
Skill	S284	Skill in system/product/service design.	CM.AW-P3
Skill	S285	Skill in tailoring conformity assessment processes for relevance and applicability to the organization.	ID.DE-P5
Skill	S286	Skill in testing system configurations.	CT.DP-P4
Skill	S287	Skill in testing system designs.	CT.DP-P4
Skill	S288	Skill in tracing data lineage.	ID.RA-P2
Skill	S289	Skill in translating between technical and non-technical privacy requirements.	CT.DM-P5
Skill	S290	Skill in translating individual data processing requests and preferences into viable organizational policies/processes/procedures.	CT.PO-P3
Skill	S291	Skill in translating legal and regulatory requirements to plain language/widely understandable terminology.	CT.PO-P4
Skill	S292	Skill in translating legal/business privacy requirements to technical privacy requirements.	CT.DM-P6

Statement Type	ID	Description	Subcategory Mapping
Skill	S293	Skill in translating policy requirements into technical implementation.	CT.DM-P8
Skill	S294	Skill in translating privacy benefits and risks to the organization's mission/objectives/activities.	ID.BE-P2
Skill	S295	Skill in translating privacy objectives to legal/contractual language.	ID.DE-P3
Skill	S296	Skill in translating privacy requirements into system design.	CT.DM-P7
Skill	S297	Skill in translating relevant concepts of privacy policies to the organization's practices and activities.	GV.MT-P3; GV.MT-P4; GV.MT-P5; GV.MT-P7
Skill	S298	Skill in translating relevant legal and regulatory requirements to the organization's needs.	GV.PO-P5; GV.MT-P2; GV.MT-P3; GV.MT-P4; GV.MT-P5; GV.MT-P7; CT.PO-P1; CT.PO-P2; CT.PO-P3
Skill	S299	Skill in using governance, risk, and compliance (GRC) tools.	ID.RA-P5
Skill	S300	Skill in using risk management systems or document repositories to create documentation of privacy risk assessments.	ID.RA-P3; ID.RA-P4
Skill	S301	Skill in using tools to assess privacy risk.	ID.RA-P4
Skill	S302	Skill in utilizing legal and regulatory analysis tools.	GV.PO-P5
Skill	S303	Skill in writing technical content for risk management processes.	GV.RM-P1
Skill	S304	Skill in writing tests for evaluating the effectiveness of technical measures.	CT.DM-P9

References

[1] Grassi PA, Garcia ME, Fenton JL (2017) Digital Identity Guidelines. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-63-3, Includes updates as of March 02, 2020. https://doi.org/10.6028/NIST.SP.800-63-3

[2] "Definitions," Title 44 U.S. Code, Sec. 3542. 2013 ed. https://www.govinfo.gov/app/details/USCODE-2013-title44/USCODE-2013-title44-chap35-subchapIII-sec3542

[3] 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), NIST Cybersecurity White Paper (CSWP) NIST CSWP 10. https://doi.org/10.6028/NIST.CSWP.10

[4] Brooks SW, Garcia ME, Lefkovitz NB, Lightman S, Nadeau EM (2017) An Introduction to Privacy Engineering and Risk Management in Federal Systems. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8062. https://doi.org/10.6028/NIST.IR.8062

[5] Joint Task Force (2020) Security and Privacy Controls for Information Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-53, Rev. 5. Includes updates as of December 10, 2020.

[6] Office of Management and Budget (2017) Preparing for and Responding to a Breach of Personally Identifiable Information. (The White House, Washington, DC), OMB Memorandum M-17-12, January 3, 2017. Available at https://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2017/m-17-12_0.pdf

[7] Joint Task Force (2018) Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-37, Rev. 2. https://doi.org/10.6028/NIST.SP.800-37r2

[8] Grassi PA, Lefkovitz NB, Nadeau EM, Galluzzo RJ, Dinh AT (2018) Attribute Metadata: A Proposed Schema for Evaluating Federated Attributes. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8112. https://doi.org/10.6028/NIST.IR.8112

[9] Joint Task Force Transformation Initiative (2012) Guide for Conducting Risk Assessments. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-30, Rev. 1. https://doi.org/10.6028/NIST.SP.800-30r1

[10] Joint Task Force Transformation Initiative (2011) Managing Information Security Risk: Organization, Mission, and Information System View. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-39. https://doi.org/10.6028/NIST.SP.800-39

[11] National Institute of Standards and Technology (2018) Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Cybersecurity White Paper (CSWP) NIST CSWP 6. https://doi.org/10.6028/NIST.CSWP.6

Appendix A. Task, Knowledge, and Skill Statements Cheat Sheet

The table below compiles the definitions, general principles, and rules for drafting TKS Statements. For more information on TKS Statements, please review the TKS Statements Authoring Guide for Workforce Frameworks available at: https://www.nist.gov/system/files/documents/2021/07/30/TKS_Authoring_Guide13apr2021-508Compliant.pdf.

TKS Statements "Cheat Sheet"
General Principles
• **Flexible:** The statements can be applied or combined in various ways to address different local circumstances and needs.
• **Consistent:** The statements are drafted following common rules to ensure that they align with other statements in the building block category and can be used in a uniform manner.
• **Clear:** The statements are easy to read and understand, and not overly complex or lacking clarity.
• **Affirmative:** The statements are structured in an affirmative (i.e., grammatically positive) form in contrast to grammatically negative statements that use language such as "do not" or "avoid".
• **Discrete:** The statements should not include more than one (compound) idea.
Rules
Task Statements
• Begin with the activity being executed • Are directed toward the achievement of organizational objectives • Include only one task in a single statement
Knowledge Statements
• Begin with "Knowledge of" followed by a concept • Are limited to one concept in a single statement
Skill Statements
• Begin with "Skill in" followed by a verb • Represent observable actions • Include only one skill in a single statement
Definitions
Task: An activity that is directed toward the achievement of organizational objectives. **Knowledge:** A retrievable set of concepts within memory. **Skill:** The capacity to perform an observable action.

Appendix B. NIST Privacy Framework Glossary

This glossary, reproduced from NIST Privacy Framework, Version 1.0, defines key terms used for the purposes of the NIST Privacy Framework and NIST Privacy Workforce Taxonomy IPD.

attribute reference
A statement asserting a property of a subscriber without necessarily containing identity information, independent of format. For example, for the attribute "birthday," a reference could be "older than 18" or "born in December." [1]

attribute value
A complete statement asserting a property of a subscriber, independent of format. For example, for the attribute "birthday," a value could be "12/1/1980" or "December 1, 1980." [1]

availability
Ensuring timely and reliable access to and use of information. [2]

category
The subdivision of a Function into groups of privacy outcomes closely tied to programmatic needs and particular activities.

communicate-p (Function)
Develop and implement appropriate activities to enable organizations and individuals to have a reliable understanding and engage in a dialogue about how data are processed and associated privacy risks. [3]

confidentiality
Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [2]

control-p (Function)
Develop and implement appropriate activities to enable organizations or individuals to manage data with sufficient granularity to manage privacy risks. [3]

core
A set of privacy protection activities and outcomes. The Framework Core comprises three elements: Functions, Categories, and Subcategories.[3]

cybersecurity incident
A cybersecurity event that has been determined to have an impact on the organization prompting the need for response and recovery. [11]

An occurrence that (1) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or (2) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies. [6]

data
A representation of information, including digital and non-digital formats.

data Action
A system/product/service data life cycle operation, including, but not limited to collection, retention, logging, generation, transformation, use, disclosure, sharing, transmission, and disposal. [4, adapted]

data element
The smallest named item of data that conveys meaningful information.

data processing
The collective set of data actions (i.e., the complete data life cycle, including, but not limited to collection, retention, logging, generation, transformation, use, disclosure, sharing, transmission, and disposal). [4, adapted]

disassociability
Enabling the processing of data or events without association to individuals or devices beyond the operational requirements of the system. [4, adapted]

function
A component of the Core that provides the highest level of structure for organizing basic privacy activities into Categories and Subcategories.

Govern-P (Function)
Develop and implement the organizational governance structure to enable an ongoing understanding of the organization's risk management priorities that are informed by privacy risk. [3]

Identify-P (Function)
Develop the organizational understanding to manage privacy risk for individuals arising from data processing. [3]

implementation tier
Provides a point of reference on how an organization views privacy risk and whether it has sufficient processes and resources in place to manage that risk. [3]

individual
A single person or a group of persons, including at a societal level.

integrity
Guarding against improper information modification or destruction and includes ensuring information non- repudiation and authenticity. [2]

lineage

The history of processing of a data element, which may include point-to-point data flows, and the data actions performed upon the data element.

manageability
Providing the capability for granular administration of data, including alteration, deletion, and selective disclosure. [4, adapted]

metadata
Information describing the characteristics of data.

This may include, for example, structural metadata describing data structures (i.e., data format, syntax, semantics) and descriptive metadata describing data contents. [5, adapted]

predictability
Enabling reliable assumptions by individuals, owners, and operators about data and their processing by a system, product, or service. [4, adapted]

privacy breach
The loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where (1) a person other than an authorized user accesses or potentially accesses data or (2) an authorized user accesses data for an other than authorized purpose. [6, adapted]

privacy control
The administrative, technical, and physical safeguards employed within an organization to satisfy privacy requirements. [7, adapted]

privacy event
The occurrence or potential occurrence of problematic data actions.

privacy requirement
A specification for system/product/service functionality to meet stakeholders' desired privacy outcomes.

privacy risk management
A specification for system/product/service functionality to meet stakeholders' desired privacy outcomes.

problematic data action
A data action that could cause an adverse effect for individuals. [4, adapted]

processing
See Data Processing.

profile
A selection of specific Functions, Categories, and Subcategories from the Core that an organization has prioritized to help it manage privacy risk.

protect-p (Function)
Develop and implement appropriate data processing safeguards. [3]

provenance
Metadata pertaining to the origination or source of specified data. [8, adapted]

risk
A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence. [9]

risk management
The process of identifying, assessing, and responding to risk.

risk tolerance
The level of risk or degree of uncertainty that is acceptable to organizations. [10]

subcategory
The further divisions of a Category into specific outcomes of technical and/or management activities. [3]