NIST IR 8477-Based Set Theory Relationship Mapping (STRM)
Reference document: Secure Controls Framework (SCF) version 2026.1
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: NIST Privacy Framework v1.0
Focal Document URL: https://www.nist.gov/privacy-framework
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-general-nist-privacy-framework-1-0.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
ID-P	IDENTIFY-P	Develop the organizational understanding to manage privacy risk for individuals arising from data processing.	Functional	Subset Of	Security, Compliance & Resilience Program (SCRP)	GOV-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls.	10	
ID.IM-P	Inventory and Mapping	Data processing by systems, products, or services is understood and informs the management of privacy risk.	Functional	Intersects With	Asset Governance	AST-01	Mechanisms exist to facilitate an IT Asset Management (ITAM) program to implement and manage asset management controls.	8	
ID.IM-P	Inventory and Mapping	Data processing by systems, products, or services is understood and informs the management of privacy risk.	Functional	Intersects With	Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.	8	
ID.IM-P1	N/A	Systems/products/services that process data are inventoried.	Functional	Intersects With	Asset Inventories	AST-02	Mechanisms exist to perform inventories of Technology Assets, Applications, Services and/or Data (TAASD) that:(1) Accurately reflects the current TAASD in use;(2) Identifies authorized software products, including business justification details;(3) Is at the level of granularity deemed necessary for tracking and reporting;(4) Includes organization-defined information deemed necessary to achieve effective property accountability; and(5) Is available for review and audit by designated organizational personnel.	8	
ID.IM-P1	N/A	Systems/products/services that process data are inventoried.	Functional	Intersects With	Third-Party Inventories	TPM-01.1	Mechanisms exist to maintain a current, accurate and complete list of External Service Providers (ESPs) that can potentially impact the Confidentiality, Integrity, Availability and/or Safety (CIAS) of the organization's Technology Assets, Applications, Services and/or Data (TAASD).	8	
ID.IM-P2	N/A	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.	Functional	Intersects With	Asset Ownership Assignment	AST-03	Mechanisms exist to ensure asset ownership responsibilities are assigned, tracked and managed at a team, individual, or responsible organization level to establish a common understanding of requirements for asset protection.	8	
ID.IM-P2	N/A	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.	Functional	Intersects With	Accountability Information	AST-03.1	Mechanisms exist to include capturing the name, position and/or role of individuals responsible/accountable for administering assets as part of the technology asset inventory process.	8	
ID.IM-P2	N/A	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.	Functional	Intersects With	Responsible, Accountable, Supportive, Consulted & Informed (RASCI) Matrix	TPM-05.4	Mechanisms exist to document and maintain a Responsible, Accountable, Supportive, Consulted & Informed (RASCI) matrix, or similar documentation, to delineate assignment for security, compliance and resilience controls between internal stakeholders and External Service Providers (ESPs).	8	
ID.IM-P3	N/A	Categories of individuals (e.g., customers, employees or prospective employees, consumers) whose data are being processed are inventoried.	Functional	Intersects With	Sensitive Data Inventories	DCH-06.2	Mechanisms exist to maintain inventory logs of all sensitive media and conduct sensitive media inventories at least annually.	8	
ID.IM-P3	N/A	Categories of individuals (e.g., customers, employees or prospective employees, consumers) whose data are being processed are inventoried.	Functional	Intersects With	Inventory of Personal Data (PD)	PRI-05.5	Mechanisms exist to establish and maintain a current inventory of all Technology Assets, Applications and/or Services (TAAS) that collect, receive, process, store, transmit, share, update and/or dispose Personal Data (PD).	8	
ID.IM-P3	N/A	Categories of individuals (e.g., customers, employees or prospective employees, consumers) whose data are being processed are inventoried.	Functional	Intersects With	Personal Data (PD) Inventory Automation Support	PRI-05.6	Automated mechanisms exist to determine if Personal Data (PD) is maintained in electronic form.	3	
ID.IM-P3	N/A	Categories of individuals (e.g., customers, employees or prospective employees, consumers) whose data are being processed are inventoried.	Functional	Intersects With	Personal Data (PD) Categories	PRI-05.7	Mechanisms exist to define and implement data handling and protection requirements for specific categories of sensitive Personal Data (PD).	8	
ID.IM-P4	N/A	Data actions of the systems/products/services are inventoried.	Functional	Intersects With	Data Action Mapping	AST-02.8	Mechanisms exist to create and maintain a map of Technology Assets, Applications and/or Services (TAAS) where sensitive/regulated data is stored, transmitted or processed.	5	
ID.IM-P5	N/A	The purposes for the data actions are inventoried.	Functional	Intersects With	Defining Business Context & Mission	GOV-08	Mechanisms exist to define the context of its business model and document the organization's mission.	5	
ID.IM-P5	N/A	The purposes for the data actions are inventoried.	Functional	Intersects With	Data Action Mapping	AST-02.8	Mechanisms exist to create and maintain a map of Technology Assets, Applications and/or Services (TAAS) where sensitive/regulated data is stored, transmitted or processed.	5	
ID.IM-P5	N/A	The purposes for the data actions are inventoried.	Functional	Intersects With	Business Process Definition	PRM-06	Mechanisms exist to define business processes with consideration for security, compliance and resilience that determines:(1) The resulting risk to organizational operations, assets, individuals and other organizations; and(2) Information protection needs arising from the defined business processes and revises the processes as necessary, until an achievable set of protection needs is obtained.	5	
ID.IM-P5	N/A	The purposes for the data actions are inventoried.	Functional	Intersects With	Service Delivery (Business Process Support)	OPS-03	Mechanisms exist to define supporting business processes and implement appropriate governance and service management to ensure appropriate planning, delivery and support of the organization's technology capabilities supporting business functions, workforce, and/or customers based on industry-recognized standards to achieve the specific goals of the process area.	5	
ID.IM-P6	N/A	Data elements within the data actions are inventoried.	Functional	Subset Of	Data Action Mapping	AST-02.8	Mechanisms exist to create and maintain a map of Technology Assets, Applications and/or Services (TAAS) where sensitive/regulated data is stored, transmitted or processed.	10	
ID.IM-P6	N/A	Data elements within the data actions are inventoried.	Functional	Intersects With	Inventory of Personal Data (PD)	PRI-05.5	Mechanisms exist to establish and maintain a current inventory of all Technology Assets, Applications and/or Services (TAAS) that collect, receive, process, store, transmit, share, update and/or dispose Personal Data (PD).	5	
ID.IM-P6	N/A	Data elements within the data actions are inventoried.	Functional	Intersects With	Personal Data (PD) Inventory Automation Support	PRI-05.6	Automated mechanisms exist to determine if Personal Data (PD) is maintained in electronic form.	5	
ID.IM-P7	N/A	The data processing environment is identified (e.g., geographic location, internal, cloud, third parties).	Functional	Intersects With	Network Diagrams & Data Flow Diagrams (DFDs)	AST-04	Mechanisms exist to maintain network architecture diagrams that:(1) Contain sufficient detail to assess the security of the network's architecture;(2) Reflect the current architecture of the network environment; and(3) Document all sensitive/regulated data flows.	8	
ID.IM-P7	N/A	The data processing environment is identified (e.g., geographic location, internal, cloud, third parties).	Functional	Intersects With	Geographic Location of Data	DCH-19	Mechanisms exist to inventory, document and maintain data flows for data that is resident (permanently or temporarily) within a service's geographically distributed applications (physical and virtual), infrastructure, systems components and/or shared with other third-parties.	8	
ID.IM-P7	N/A	The data processing environment is identified (e.g., geographic location, internal, cloud, third parties).	Functional	Intersects With	Applied Security, Compliance and Resilience Controls Documentation	IAO-03	Mechanisms exist to generate authoritative documentation (e.g., System Security Plan (SSP)) that:(1) Identifies key architectural and implementation information on in-scope Technology Assets, Applications and/or Services (TAAS);(2) Reflects the current state of applied security, compliance and resilience controls on applicable People, Processes, Technologies, Data and/or Facilities (PPTDF) that are contained within the system boundary; and(3) Provides a historical record of applied security controls, including changes	3	
ID.IM-P7	N/A	The data processing environment is identified (e.g., geographic location, internal, cloud, third parties).	Functional	Intersects With	Data Protection Impact Assessment (DPIA)	RSK-10	Mechanisms exist to conduct a Data Protection Impact Assessment (DPIA) on Technology Assets, Applications and/or Services (TAAS) that store, process and/or transmit Personal Data (PD) to identify and remediate reasonably-expected risks.	8	
ID.IM-P8	N/A	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.	Functional	Intersects With	Asset-Service Dependencies	AST-01.1	Mechanisms exist to identify and assess the security of Technology Assets, Applications and/or Services (TAAS) that support more than one critical business function.	5	
ID.IM-P8	N/A	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.	Functional	Intersects With	Stakeholder Identification & Involvement	AST-01.2	Mechanisms exist to identify and involve pertinent stakeholders of critical Technology Assets, Applications, Services and/or Data (TAASD) to support the ongoing secure management of those assets.	5	
ID.IM-P8	N/A	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.	Functional	Intersects With	Data Action Mapping	AST-02.8	Mechanisms exist to create and maintain a map of Technology Assets, Applications and/or Services (TAAS) where sensitive/regulated data is stored, transmitted or processed.	5	
ID.IM-P8	N/A	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.	Functional	Intersects With	Network Diagrams & Data Flow Diagrams (DFDs)	AST-04	Mechanisms exist to maintain network architecture diagrams that:(1) Contain sufficient detail to assess the security of the network's architecture;(2) Reflect the current architecture of the network environment; and(3) Document all sensitive/regulated data flows.	5	
ID.IM-P8	N/A	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.	Functional	Intersects With	Geographic Location of Data	DCH-19	Mechanisms exist to inventory, document and maintain data flows for data that is resident (permanently or temporarily) within a service's geographically distributed applications (physical and virtual), infrastructure, systems components and/or shared with other third-parties.	5	
ID.BE-P	Business Environment	The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform privacy roles, responsibilities, and risk management decisions.	Functional	Subset Of	Security, Compliance & Resilience Program (SCRP)	GOV-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls.	10	
ID.BE-P1	N/A	The organization's role(s) in the data processing ecosystem are identified and communicated.	Functional	Intersects With	Defining Business Context & Mission	GOV-08	Mechanisms exist to define the context of its business model and document the organization's mission.	8	
ID.BE-P1	N/A	The organization's role(s) in the data processing ecosystem are identified and communicated.	Functional	Intersects With	Joint Processing of Personal Data (PD)	PRI-07.2	Mechanisms exist to clearly define and communicate the organization's role in processing Personal Data (PD) in the data processing ecosystem.	3	
ID.BE-P1	N/A	The organization's role(s) in the data processing ecosystem are identified and communicated.	Functional	Intersects With	Business Process Definition	PRM-06	Mechanisms exist to define business processes with consideration for security, compliance and resilience that determines:(1) The resulting risk to organizational operations, assets, individuals and other organizations; and(2) Information protection needs arising from the defined business processes and revises the processes as necessary, until an achievable set of protection needs is obtained.	8	
ID.BE-P2	N/A	Priorities for organizational mission, objectives, and activities are established and communicated.	Functional	Intersects With	Defining Business Context & Mission	GOV-08	Mechanisms exist to define the context of its business model and document the organization's mission.	8	
ID.BE-P3	N/A	Systems/products/services that support organizational priorities are identified and key requirements communicated.	Functional	Intersects With	Identify Critical Assets	BCD-02	Mechanisms exist to identify and document the critical Technology Assets, Applications, Services and/or Data (TAASD) that support essential missions and business functions.	8	
ID.BE-P3	N/A	Systems/products/services that support organizational priorities are identified and key requirements communicated.	Functional	Intersects With	Use of Critical Technologies	HRS-05.4	Mechanisms exist to govern usage policies for critical technologies.	5	
ID.BE-P3	N/A	Systems/products/services that support organizational priorities are identified and key requirements communicated.	Functional	Intersects With	Applied Security, Compliance and Resilience Controls Documentation	IAO-03	Mechanisms exist to generate authoritative documentation (e.g., System Security Plan (SSP)) that:(1) Identifies key architectural and implementation information on in-scope Technology Assets, Applications and/or Services (TAAS);(2) Reflects the current state of applied security, compliance and resilience controls on applicable People, Processes, Technologies, Data and/or Facilities (PPTDF) that are contained within the system boundary; and(3) Provides a historical record of applied security controls, including changes	5	
ID.BE-P3	N/A	Systems/products/services that support organizational priorities are identified and key requirements communicated.	Functional	Intersects With	Security Concept Of Operations (CONOPS)	OPS-02	Mechanisms exist to develop a security Concept of Operations (CONOPS), or a similarly-defined plan for achieving cybersecurity objectives, that documents management, operational and technical measures implemented to apply defense-in-depth techniques that is communicated to all appropriate stakeholders.	5	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
ID.BE-P3	N/A	Systems/products/services that support organizational priorities are identified and key requirements communicated.	Functional	Intersects With	Business Process Definition	PRM-06	Mechanisms exist to define business processes with consideration for security, compliance and resilience that determines:(1) The resulting risk to organizational operations, assets, individuals and other organizations; and(2) Information protection needs arising from the defined business processes and revises the processes as necessary, until an achievable set of protection needs is obtained.	8	
ID.BE-P3	N/A	Systems/products/services that support organizational priorities are identified and key requirements communicated.	Functional	Intersects With	Criticality Analysis During Development	TDA-06.1	Mechanisms exist to require the developer of the Technology Asset, Application and/or Service (TAAS) to perform a criticality analysis at organization-defined decision points in the Secure Development Life Cycle (SDLC).	8	
ID.BE-P3	N/A	Systems/products/services that support organizational priorities are identified and key requirements communicated.	Functional	Intersects With	Third-Party Criticality Assessments	TPM-02	Mechanisms exist to identify, prioritize and assess suppliers and partners of critical Technology Assets, Applications and/or Services (TAAS) using a supply chain risk assessment process relative to their importance in supporting the delivery of high-value services.	8	
ID.RA-P	Risk Assessment	The organization understands the privacy risks to individuals and how such privacy risks may create follow-on impacts on organizational operations, including mission, functions, other risk management priorities (e.g., compliance, financial), reputation, workforce, and culture.	Functional	Subset Of	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	10	
ID.RA-P1	N/A	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).	Functional	Subset Of	Data Protection Impact Assessment (DPIA)	RSK-10	Mechanisms exist to conduct a Data Protection Impact Assessment (DPIA) on Technology Assets, Applications and/or Services (TAAS) that store, process and/or transmit Personal Data (PD) to identify and remediate reasonably-expected risks.	10	
ID.RA-P2	N/A	Data analytic inputs and outputs are identified and evaluated for bias.	Functional	Subset Of	Data Protection Impact Assessment (DPIA)	RSK-10	Mechanisms exist to conduct a Data Protection Impact Assessment (DPIA) on Technology Assets, Applications and/or Services (TAAS) that store, process and/or transmit Personal Data (PD) to identify and remediate reasonably-expected risks.	10	
ID.RA-P3	N/A	Potential problematic data actions and associated problems are identified.	Functional	Subset Of	Data Protection Impact Assessment (DPIA)	RSK-10	Mechanisms exist to conduct a Data Protection Impact Assessment (DPIA) on Technology Assets, Applications and/or Services (TAAS) that store, process and/or transmit Personal Data (PD) to identify and remediate reasonably-expected risks.	10	
ID.RA-P4	N/A	Problematic data actions, likelihoods, and impacts are used to determine and prioritize risk.	Functional	Subset Of	Data Protection Impact Assessment (DPIA)	RSK-10	Mechanisms exist to conduct a Data Protection Impact Assessment (DPIA) on Technology Assets, Applications and/or Services (TAAS) that store, process and/or transmit Personal Data (PD) to identify and remediate reasonably-expected risks.	10	
ID.RA-P5	N/A	Risk responses are identified, prioritized, and implemented.	Functional	Subset Of	Data Protection Impact Assessment (DPIA)	RSK-10	Mechanisms exist to conduct a Data Protection Impact Assessment (DPIA) on Technology Assets, Applications and/or Services (TAAS) that store, process and/or transmit Personal Data (PD) to identify and remediate reasonably-expected risks.	10	
ID.DE-P	Data Processing Ecosystem Risk Management	The organization's priorities, constraints, risk tolerance, and assumptions are established and used to support risk decisions associated with managing privacy risk and third parties within the data processing ecosystem. The organization has established and implemented the processes to identify, assess, and manage privacy risks within the data processing ecosystem.	Functional	Subset Of	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	10	
ID.DE-P1	N/A	Data processing ecosystem risk management policies, processes, and procedures are identified, established, assessed, managed, and agreed to by organizational stakeholders.	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	8	
ID.DE-P1	N/A	Data processing ecosystem risk management policies, processes, and procedures are identified, established, assessed, managed, and agreed to by organizational stakeholders.	Functional	Intersects With	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	8	
ID.DE-P2	N/A	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.	Functional	Intersects With	Supply Chain Risk Management (SCRM) Plan	RSK-09	Mechanisms exist to develop a plan for Supply Chain Risk Management (SCRM) associated with the development, acquisition, maintenance and disposal of Technology Assets, Applications and/or Services (TAAS), including documenting selected mitigating actions and monitoring performance against those plans.	8	
ID.DE-P2	N/A	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.	Functional	Intersects With	Data Protection Impact Assessment (DPIA)	RSK-10	Mechanisms exist to conduct a Data Protection Impact Assessment (DPIA) on Technology Assets, Applications and/or Services (TAAS) that store, process and/or transmit Personal Data (PD) to identify and remediate reasonably-expected risks.	8	
ID.DE-P3	N/A	Contracts with data processing ecosystem parties are used to implement appropriate measures designed to meet the objectives of an organization's privacy program.	Functional	Intersects With	Adequate Security for Sensitive / Regulated Data In Support of Contracts	IAO-03.2	Mechanisms exist to protect sensitive/regulated data that is collected, developed, received, transmitted, used or stored in support of the performance of a contract.	5	
ID.DE-P3	N/A	Contracts with data processing ecosystem parties are used to implement appropriate measures designed to meet the objectives of an organization's privacy program.	Functional	Intersects With	Data Privacy Requirements for Contractors & Service Providers	PRI-07.1	Mechanisms exist to include data privacy requirements in contracts and other acquisition-related documents that establish data privacy roles and responsibilities for contractors and service providers.	5	
ID.DE-P3	N/A	Contracts with data processing ecosystem parties are used to implement appropriate measures designed to meet the objectives of an organization's privacy program.	Functional	Intersects With	Supply Chain Risk Management (SCRM) Plan	RSK-09	Mechanisms exist to develop a plan for Supply Chain Risk Management (SCRM) associated with the development, acquisition, maintenance and disposal of Technology Assets, Applications and/or Services (TAAS), including documenting selected mitigating actions and monitoring performance against those plans.	5	
ID.DE-P3	N/A	Contracts with data processing ecosystem parties are used to implement appropriate measures designed to meet the objectives of an organization's privacy program.	Functional	Intersects With	Data Protection Impact Assessment (DPIA)	RSK-10	Mechanisms exist to conduct a Data Protection Impact Assessment (DPIA) on Technology Assets, Applications and/or Services (TAAS) that store, process and/or transmit Personal Data (PD) to identify and remediate reasonably-expected risks.	5	
ID.DE-P3	N/A	Contracts with data processing ecosystem parties are used to implement appropriate measures designed to meet the objectives of an organization's privacy program.	Functional	Intersects With	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or Data (TAASD).	5	
ID.DE-P4	N/A	Interoperability frameworks or similar multi-party approaches are used to manage data processing ecosystem privacy risks.	Functional	Intersects With	Data Portability	PRI-06.6	Mechanisms exist to format exports of Personal Data (PD) in a structured, machine-readable format that allows data subjects to transfer their PD to another controller without hindrance.	3	
ID.DE-P4	N/A	Interoperability frameworks or similar multi-party approaches are used to manage data processing ecosystem privacy risks.	Functional	Intersects With	Secure Engineering Principles	SEA-01	Mechanisms exist to facilitate the implementation of industry-recognized security, compliance and resilience practices in the specification, design, development, implementation and modification of Technology Assets, Applications and/or Services (TAAS).	8	
ID.DE-P5	N/A	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.	Functional	Intersects With	Security, Compliance & Resilience Assessments	CPL-03	Mechanisms exist to regularly review processes and documented procedures to ensure conformity with the organization's security, compliance and/or resilience policies, standards and other applicable requirements.	8	
ID.DE-P5	N/A	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.	Functional	Intersects With	Risk Assessment	RSK-04	Mechanisms exist to conduct recurring assessments of risk that includes the likelihood and magnitude of harm, from unauthorized access, use, disclosure, disruption, modification or destruction of the organization's Technology Assets, Applications, Services and/or Data (TAASD).	5	
ID.DE-P5	N/A	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.	Functional	Intersects With	Risk Assessment Update	RSK-07	Mechanisms exist to routinely update risk assessments and react accordingly upon identifying new security vulnerabilities, including using outside sources for security vulnerability information.	5	
ID.DE-P5	N/A	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.	Functional	Intersects With	Supply Chain Risk Assessment	RSK-09.1	Mechanisms exist to periodically assess supply chain risks associated with Technology Assets, Applications and/or Services (TAAS).	5	
ID.DE-P5	N/A	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.	Functional	Intersects With	Third-Party Risk Assessments & Approvals	TPM-04.1	Mechanisms exist to conduct a risk assessment prior to the acquisition or outsourcing of technology-related Technology Assets, Applications and/or Services (TAAS).	5	
ID.DE-P5	N/A	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.	Functional	Intersects With	Review of Third-Party Services	TPM-08	Mechanisms exist to monitor, regularly review and assess External Service Providers (ESPs) for compliance with established contractual requirements for security, compliance and resilience controls.	8	
GV-P	GOVERN-P	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.	Functional	Subset Of	Security, Compliance & Resilience Program (SCRP)	GOV-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls.	10	
GV.PO-P	Governance Policies, Processes, and Procedures	The policies, processes, and procedures to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of privacy risk.	Functional	Subset Of	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	10	
GV.PO-P1	N/A	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.	Functional	Intersects With	Security, Compliance & Resilience Program (SCRP)	GOV-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls.	8	
GV.PO-P1	N/A	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.	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	8	
GV.PO-P1	N/A	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.	Functional	Intersects With	Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.	8	
GV.PO-P1	N/A	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.	Functional	Intersects With	Data Privacy Program	PRI-01	Mechanisms exist to facilitate the implementation and operation of data protection controls throughout the data lifecycle to ensure all forms of Personal Data (PD) are processed lawfully, fairly and transparently.	8	
GV.PO-P1	N/A	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.	Functional	Intersects With	Dissemination of Data Privacy Program Information	PRI-01.3	Mechanisms exist to:(1) Ensure that the public has access to information about organizational data privacy activities and can communicate with its Chief Privacy Officer (CPO) or similar role;(2) Ensure that organizational data privacy practices are publicly available through organizational websites or document repositories;(3) Utilize publicly facing email addresses and/or phone lines to enable the public to provide feedback and/or direct questions to data privacy office(s) regarding data privacy practices; and(4) Inform data subjects when changes are made to the privacy notice and the nature of such changes.	5	
GV.PO-P2	N/A	Processes to instill organizational privacy values within system/product/service development and operations are established and in place.	Functional	Intersects With	Business As Usual (BAU) Security, Compliance & Resilience Practices	GOV-14	Mechanisms exist to incorporate security, compliance and resilience principles into Business As Usual (BAU) practices through executive leadership involvement.	8	
GV.PO-P2	N/A	Processes to instill organizational privacy values within system/product/service development and operations are established and in place.	Functional	Intersects With	Operationalizing Security, Compliance & Resilience Capabilities	GOV-15	Mechanisms exist to compel data and/or process owners to operationalize security, compliance and resilience practices for each Technology Asset, Application and/or Service (TAAS) under their control.	8	
GV.PO-P2	N/A	Processes to instill organizational privacy values within system/product/service development and operations are established and in place.	Functional	Intersects With	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	5	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
GV.PO-P2	N/A	Processes to instill organizational privacy values within system/product/service development and operations are established and in place.	Functional	Intersects With	User Awareness	HRS-03.1	Mechanisms exist to communicate with users about their roles and responsibilities to maintain a safe and secure working environment.	5	
GV.PO-P2	N/A	Processes to instill organizational privacy values within system/product/service development and operations are established and in place.	Functional	Intersects With	Secure Engineering Principles	SEA-01	Mechanisms exist to facilitate the implementation of industry-recognized security, compliance and resilience practices in the specification, design, development, implementation and modification of Technology Assets, Applications and/or Services (TAAS).	5	
GV.PO-P2	N/A	Processes to instill organizational privacy values within system/product/service development and operations are established and in place.	Functional	Intersects With	Centralized Management of Security, Compliance & Resilience Controls	SEA-01.1	Mechanisms exist to centrally-manage the organization-wide management and implementation of security, compliance and resilience controls and related processes.	5	
GV.PO-P2	N/A	Processes to instill organizational privacy values within system/product/service development and operations are established and in place.	Functional	Intersects With	Alignment With Enterprise Architecture	SEA-02	Mechanisms exist to develop an enterprise architecture, aligned with industry-recognized leading practices, with consideration for security, compliance and resilience principles that addresses risk to organizational operations, assets, individuals and other organizations.	5	
GV.PO-P2	N/A	Processes to instill organizational privacy values within system/product/service development and operations are established and in place.	Functional	Intersects With	Standardized Terminology	SEA-02.1	Mechanisms exist to standardize technology and process terminology to reduce confusion amongst groups and departments.	5	
GV.PO-P3	N/A	Roles and responsibilities for the workforce are established with respect to privacy.	Functional	Intersects With	Assigned Security, Compliance & Resilience Responsibilities	GOV-04	Mechanisms exist to assign one or more qualified individuals with the mission and resources to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide Security, Compliance & Resilience Program (SCRP).	5	
GV.PO-P3	N/A	Roles and responsibilities for the workforce are established with respect to privacy.	Functional	Intersects With	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	8	
GV.PO-P3	N/A	Roles and responsibilities for the workforce are established with respect to privacy.	Functional	Intersects With	Chief Privacy Officer (CPO)	PRI-01.1	Mechanisms exist to appoints a Chief Privacy Officer (CPO) or similar role, with the authority, mission, accountability and resources to coordinate, develop and implement, applicable data privacy requirements and manage data privacy risks through the organization-wide data privacy program.	5	
GV.PO-P3	N/A	Roles and responsibilities for the workforce are established with respect to privacy.	Functional	Intersects With	Data Protection Officer (DPO)	PRI-01.4	Mechanisms exist to appoint a Data Protection Officer (DPO):(1) Based on professional qualifications; and(2) To be involved in all issues related to how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and/or disposed.	5	
GV.PO-P3	N/A	Roles and responsibilities for the workforce are established with respect to privacy.	Functional	Intersects With	Data Fiduciary	PRI-01.8	Mechanisms exist to appoint an individual to determine the following criteria about Personal Data (PD):(1) The purpose why PD is necessary;(2) Authorized methods to collect, receive, process, store, transmit, share, update and/or dispose PD; and(3) Authorized parties PD may be shared with.	5	
GV.PO-P3	N/A	Roles and responsibilities for the workforce are established with respect to privacy.	Functional	Intersects With	Responsible, Accountable, Supportive, Consulted & Informed (RASCI) Matrix	TPM-05.4	Mechanisms exist to document and maintain a Responsible, Accountable, Supportive, Consulted & Informed (RASCI) matrix, or similar documentation, to delineate assignment for security, compliance and resilience controls between internal stakeholders and External Service Providers (ESPs).	5	
GV.PO-P3	N/A	Roles and responsibilities for the workforce are established with respect to privacy.	Functional	Intersects With	Third-Party Personnel Security	TPM-06	Mechanisms exist to control personnel security requirements including security roles and responsibilities for third-party providers.	5	
GV.PO-P4	N/A	Privacy roles and responsibilities are coordinated and aligned with third-party stakeholders (e.g., service providers, customers, partners).	Functional	Intersects With	Third-Party Management	TPM-01	Mechanisms exist to facilitate the implementation of third-party management controls.	5	
GV.PO-P4	N/A	Privacy roles and responsibilities are coordinated and aligned with third-party stakeholders (e.g., service providers, customers, partners).	Functional	Intersects With	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or Data (TAASD).	5	
GV.PO-P4	N/A	Privacy roles and responsibilities are coordinated and aligned with third-party stakeholders (e.g., service providers, customers, partners).	Functional	Intersects With	Responsible, Accountable, Supportive, Consulted & Informed (RASCI) Matrix	TPM-05.4	Mechanisms exist to document and maintain a Responsible, Accountable, Supportive, Consulted & Informed (RASCI) matrix, or similar documentation, to delineate assignment for security, compliance and resilience controls between internal stakeholders and External Service Providers (ESPs).	8	
GV.PO-P4	N/A	Privacy roles and responsibilities are coordinated and aligned with third-party stakeholders (e.g., service providers, customers, partners).	Functional	Intersects With	Third-Party Personnel Security	TPM-06	Mechanisms exist to control personnel security requirements including security roles and responsibilities for third-party providers.	8	
GV.PO-P5	N/A	Legal, regulatory, and contractual requirements regarding privacy are understood and managed.	Functional	Intersects With	Statutory, Regulatory & Contractual Compliance	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	8	
GV.PO-P5	N/A	Legal, regulatory, and contractual requirements regarding privacy are understood and managed.	Functional	Intersects With	Data Privacy Program	PRI-01	Mechanisms exist to facilitate the implementation and operation of data protection controls throughout the data lifecycle to ensure all forms of Personal Data (PD) are processed lawfully, fairly and transparently.	5	
GV.PO-P5	N/A	Legal, regulatory, and contractual requirements regarding privacy are understood and managed.	Functional	Intersects With	Reasonable Data Privacy Practices	PRI-01.11	Mechanisms exist to limit the collection, receiving, processing, storage, transmission, sharing, updating and/or disposal of Personal Data (PD) according to reasonable consumer expectations for what is necessary and proportionate.	8	
GV.PO-P6	N/A	Governance and risk management policies, processes, and procedures address privacy risks.	Functional	Subset Of	Security, Compliance & Resilience Program (SCRP)	GOV-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls.	10	
GV.PO-P6	N/A	Governance and risk management policies, processes, and procedures address privacy risks.	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	8	
GV.PO-P6	N/A	Governance and risk management policies, processes, and procedures address privacy risks.	Functional	Intersects With	Data Privacy Program	PRI-01	Mechanisms exist to facilitate the implementation and operation of data protection controls throughout the data lifecycle to ensure all forms of Personal Data (PD) are processed lawfully, fairly and transparently.	8	
GV.PO-P6	N/A	Governance and risk management policies, processes, and procedures address privacy risks.	Functional	Intersects With	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	8	
GV.RM-P	Risk Management Strategy	The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	Functional	Subset Of	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	10	
GV.RM-P1	N/A	Risk management processes are established, managed, and agreed to by organizational stakeholders.	Functional	Subset Of	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	10	
GV.RM-P2	N/A	Organizational risk tolerance is determined and clearly expressed.	Functional	Equal	Risk Tolerance	RSK-01.3	Mechanisms exist to define organizational risk tolerance, the specified range of acceptable results.	10	
GV.RM-P3	N/A	The organization's determination of risk tolerance is informed by its role(s) in the data processing ecosystem.	Functional	Intersects With	Defining Business Context & Mission	GOV-08	Mechanisms exist to define the context of its business model and document the organization's mission.	8	
GV.RM-P3	N/A	The organization's determination of risk tolerance is informed by its role(s) in the data processing ecosystem.	Functional	Intersects With	Business Process Definition	PRM-06	Mechanisms exist to define business processes with consideration for security, compliance and resilience that determines:(1) The resulting risk to organizational operations, assets, individuals and other organizations; and(2) Information protection needs arising from the defined business processes and revises the processes as necessary, until an achievable set of protection needs is obtained.	8	
GV.RM-P3	N/A	The organization's determination of risk tolerance is informed by its role(s) in the data processing ecosystem.	Functional	Intersects With	Risk Framing	RSK-01.1	Mechanisms exist to identify:(1) Assumptions affecting risk assessments, risk response and risk monitoring;(2) Constraints affecting risk assessments, risk response and risk monitoring;(3) The organizational risk tolerance; and(4) Priorities, benefits and trade-offs considered by the organization for managing risk.	8	
GV.RM-P3	N/A	The organization's determination of risk tolerance is informed by its role(s) in the data processing ecosystem.	Functional	Intersects With	Risk Appetite	RSK-01.5	Mechanisms exist to define organizational risk appetite, the degree of uncertainty the organization is willing to accept in anticipation of a reward.	8	
GV.AT-P	Awareness and Training	The organization's workforce and third parties engaged in data processing are provided privacy awareness education and are trained to perform their privacy-related duties and responsibilities consistent with related policies, processes, procedures, and agreements and organizational privacy values.	Functional	Subset Of	Security, Compliance & Resilience-Minded Workforce	SAT-01	Mechanisms exist to facilitate the implementation of security workforce development and awareness controls.	10	
GV.AT-P1	N/A	The workforce is informed and trained on its roles and responsibilities.	Functional	Subset Of	Security, Compliance & Resilience-Minded Workforce	SAT-01	Mechanisms exist to facilitate the implementation of security workforce development and awareness controls.	10	
GV.AT-P1	N/A	The workforce is informed and trained on its roles and responsibilities.	Functional	Intersects With	Security, Compliance & Resilience Awareness Training	SAT-02	Mechanisms exist to provide all employees and contractors appropriate security, compliance and resilience awareness education and training that is relevant for their job function.	5	
GV.AT-P1	N/A	The workforce is informed and trained on its roles and responsibilities.	Functional	Intersects With	Role-Based Security, Compliance & Resilience Training	SAT-03	Mechanisms exist to provide role-based security, compliance and resilience-related training:(1) Before authorizing access to the system or performing assigned duties;(2) When required by system changes; and(3) Annually thereafter.	5	
GV.AT-P2	N/A	Senior executives understand their roles and responsibilities.	Functional	Subset Of	Security, Compliance & Resilience-Minded Workforce	SAT-01	Mechanisms exist to facilitate the implementation of security workforce development and awareness controls.	10	
GV.AT-P2	N/A	Senior executives understand their roles and responsibilities.	Functional	Intersects With	Security, Compliance & Resilience Awareness Training	SAT-02	Mechanisms exist to provide all employees and contractors appropriate security, compliance and resilience awareness education and training that is relevant for their job function.	5	
GV.AT-P2	N/A	Senior executives understand their roles and responsibilities.	Functional	Intersects With	Role-Based Security, Compliance & Resilience Training	SAT-03	Mechanisms exist to provide role-based security, compliance and resilience-related training:(1) Before authorizing access to the system or performing assigned duties;(2) When required by system changes; and(3) Annually thereafter.	5	
GV.AT-P3	N/A	Privacy personnel understand their roles and responsibilities.	Functional	Subset Of	Security, Compliance & Resilience-Minded Workforce	SAT-01	Mechanisms exist to facilitate the implementation of security workforce development and awareness controls.	10	
GV.AT-P3	N/A	Privacy personnel understand their roles and responsibilities.	Functional	Intersects With	Security, Compliance & Resilience Awareness Training	SAT-02	Mechanisms exist to provide all employees and contractors appropriate security, compliance and resilience awareness education and training that is relevant for their job function.	5	
GV.AT-P3	N/A	Privacy personnel understand their roles and responsibilities.	Functional	Intersects With	Role-Based Security, Compliance & Resilience Training	SAT-03	Mechanisms exist to provide role-based security, compliance and resilience-related training:(1) Before authorizing access to the system or performing assigned duties;(2) When required by system changes; and(3) Annually thereafter.	5	
GV.AT-P4	N/A	Third parties (e.g., service providers, customers, partners) understand their roles and responsibilities.	Functional	Subset Of	Security, Compliance & Resilience-Minded Workforce	SAT-01	Mechanisms exist to facilitate the implementation of security workforce development and awareness controls.	10	
GV.AT-P4	N/A	Third parties (e.g., service providers, customers, partners) understand their roles and responsibilities.	Functional	Intersects With	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or Data (TAASD).	8	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
GV.AT-P4	N/A	Third parties (e.g., service providers, customers, partners) understand their roles and responsibilities.	Functional	Intersects With	Responsible, Accountable, Supportive, Consulted & Informed (RASCI) Matrix	TPM-05.4	Mechanisms exist to document and maintain a Responsible, Accountable, Supportive, Consulted & Informed (RASCI) matrix, or similar documentation, to delineate assignment for security, compliance and resilience controls between internal stakeholders and External Service Providers (ESPs).	8	
GV.AT-P4	N/A	Third parties (e.g., service providers, customers, partners) understand their roles and responsibilities.	Functional	Intersects With	Third-Party Personnel Security	TPM-06	Mechanisms exist to control personnel security requirements including security roles and responsibilities for third-party providers.	8	
GV.MT-P	Monitoring and Review	The policies, processes, and procedures for ongoing review of the organization's privacy posture are understood and inform the management of privacy risk.	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	8	
GV.MT-P	Monitoring and Review	The policies, processes, and procedures for ongoing review of the organization's privacy posture are understood and inform the management of privacy risk.	Functional	Intersects With	Data Privacy Program	PRI-01	Mechanisms exist to facilitate the implementation and operation of data protection controls throughout the data lifecycle to ensure all forms of Personal Data (PD) are processed lawfully, fairly and transparently.	8	
GV.MT-P1	N/A	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.	Functional	Intersects With	Risk Assessment	RSK-04	Mechanisms exist to conduct recurring assessments of risk that includes the likelihood and magnitude of harm, from unauthorized access, use, disclosure, disruption, modification or destruction of the organization's Technology Assets, Applications, Services and/or Data (TAASD).	8	
GV.MT-P1	N/A	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.	Functional	Intersects With	Risk Assessment Update	RSK-07	Mechanisms exist to routinely update risk assessments and react accordingly upon identifying new security vulnerabilities, including using outside sources for security vulnerability information.	8	
GV.MT-P1	N/A	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.	Functional	Intersects With	Supply Chain Risk Assessment	RSK-09.1	Mechanisms exist to periodically assess supply chain risks associated with Technology Assets, Applications and/or Services (TAAS).	5	
GV.MT-P1	N/A	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.	Functional	Intersects With	Data Protection Impact Assessment (DPIA)	RSK-10	Mechanisms exist to conduct a Data Protection Impact Assessment (DPIA) on Technology Assets, Applications and/or Services (TAAS) that store, process and/or transmit Personal Data (PD) to identify and remediate reasonably-expected risks.	5	
GV.MT-P2	N/A	Privacy values, policies, and training are reviewed and any updates are communicated.	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCRP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	8	
GV.MT-P3	N/A	Policies, processes, and procedures for assessing compliance with legal requirements and privacy policies are established and in place.	Functional	Intersects With	Reasonable Data Privacy Practices	PRI-01.11	Mechanisms exist to limit the collection, receiving, processing, storage, transmission, sharing, updating and/or disposal of Personal Data (PD) according to reasonable consumer expectations for what is necessary and proportionate.	8	
GV.MT-P4	N/A	Policies, processes, and procedures for communicating progress on managing privacy risks are established and in place.	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	8	
GV.MT-P4	N/A	Policies, processes, and procedures for communicating progress on managing privacy risks are established and in place.	Functional	Intersects With	Measures of Performance	GOV-05	Mechanisms exist to develop, report and monitor Security, Compliance & Resilience Program (SCRP) measures of performance.	8	
GV.MT-P4	N/A	Policies, processes, and procedures for communicating progress on managing privacy risks are established and in place.	Functional	Intersects With	Security, Compliance & Resilience Controls Oversight	CPL-02	Mechanisms exist to provide a security, compliance and resilience controls oversight function that reports to the organization's executive leadership.	8	
GV.MT-P4	N/A	Policies, processes, and procedures for communicating progress on managing privacy risks are established and in place.	Functional	Intersects With	Security, Compliance & Resilience Controls Oversight	CPL-02	Mechanisms exist to provide a security, compliance and resilience controls oversight function that reports to the organization's executive leadership.	8	
GV.MT-P4	N/A	Policies, processes, and procedures for communicating progress on managing privacy risks are established and in place.	Functional	Intersects With	Capabilities Deficiency Tracking	IAO-05	minimum:(1) Deficiency tracking number;(2) Applicable security, compliance and/or resilience control;(3) Description of the deficiency(ies);(4) Risk associated with the deficiency(ies);(5) Source deficiency identification/detection;(6) Temporary compensating controls, if applicable; (7) Point of Contact (POC) (e.g., asset/process owner);(8) Resources required to conduct remediation actions;(9) Planned remedial actions to the	8	
GV.MT-P5	N/A	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).	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	8	
GV.MT-P5	N/A	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).	Functional	Intersects With	Incident Handling	IRO-02	Mechanisms exist to cover:(1) Preparation;(2) Automated event detection or manual incident report intake;(3) Analysis;(4) Containment;(5) Eradication; and(6) Recovery.	3	
GV.MT-P5	N/A	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).	Functional	Intersects With	Reasonable Data Privacy Practices	PRI-01.11	Mechanisms exist to limit the collection, receiving, processing, storage, transmission, sharing, updating and/or disposal of Personal Data (PD) according to reasonable consumer expectations for what is necessary and proportionate.	8	
GV.MT-P6	N/A	Policies, processes, and procedures incorporate lessons learned from problematic data actions.	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	8	
GV.MT-P6	N/A	Policies, processes, and procedures incorporate lessons learned from problematic data actions.	Functional	Intersects With	Root Cause Analysis (RCA) & Lessons Learned	IRO-13	Mechanisms exist to incorporate lessons learned from analyzing and resolving cybersecurity and data protection incidents to reduce the likelihood or impact of future incidents.	8	
GV.MT-P7	N/A	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.	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	8	
GV.MT-P7	N/A	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.	Functional	Intersects With	User Feedback Management	PRI-06.4	Mechanisms exist to maintain a process to efficiently and effectively respond to requests, complaints, concerns or questions from authenticated data subjects about Personal Data (PD) the organization collects, receives, processes, stores, transmits, shares, updates and/or disposes.	8	
CT-P	CONTROL-P	Develop and implement appropriate activities to enable organizations or individuals to manage data with sufficient granularity to manage privacy risks.	Functional	Subset Of	Data Privacy Program	PRI-01	Mechanisms exist to facilitate the implementation and operation of data protection controls throughout the data lifecycle to ensure all forms of Personal Data (PD) are processed lawfully, fairly and transparently.	10	
CT.PO-P	Data Processing Policies, Processes, and Procedures	Policies, processes, and procedures are maintained and used to manage data processing (e.g., purpose, scope, roles and responsibilities in the data processing ecosystem, and management commitment) consistent with the organization's risk strategy to protect individuals' privacy.	Functional	Subset Of	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	10	