NIST Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management

CYBR 4400/5400: Principles of Internet Policy, Lecture 5-4

Dr. David Reed, Technology, Cybersecurity, and Policy Program, CU Boulder

Today's Lecture

- Project Presentations on 4/27 (CYBR 4400, CYBR 5400), & 4/29 (CYBR 5400)
  - 10 minute presentations (due 4/27 for 4400, 4/29 for 5400)
  - Distance students - possible to present live on Zoom? Please let me know
  - Paper due Sunday, 4/26 at midnight
- Current Events
  - China's Social Credit System
  - Impact of GDPR
- Lecture on NIST Privacy Framework

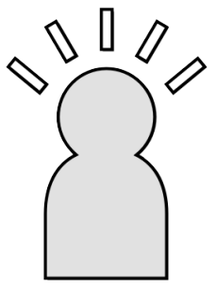
NIST Privacy Framework Webinar: Ready, Set, Adopt Version 1.0

National Institute of Standards and Technology
U.S. Department of Commerce

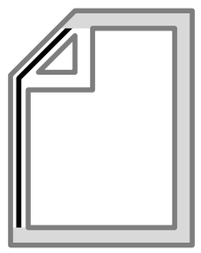
Source: Slides accessed on April 2, 2020 at https://www.nist.gov/news-events/events/2020/01/nist-privacy-framework-webinar-ready-set-adopt-version-10

Collaborative Development

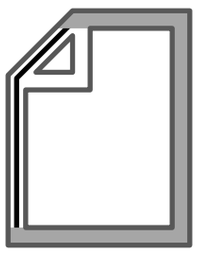
Starting Point
Attributes



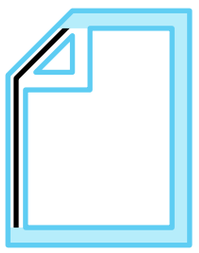
Outline

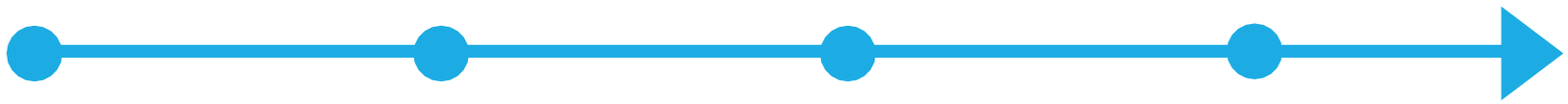


Discussion Draft



Preliminary Draft





2
public comment periods

3
public workshops

5
webinars

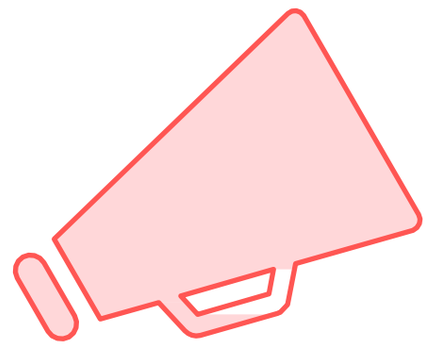
Version 1.0

Value Proposition

Privacy Framework supports:

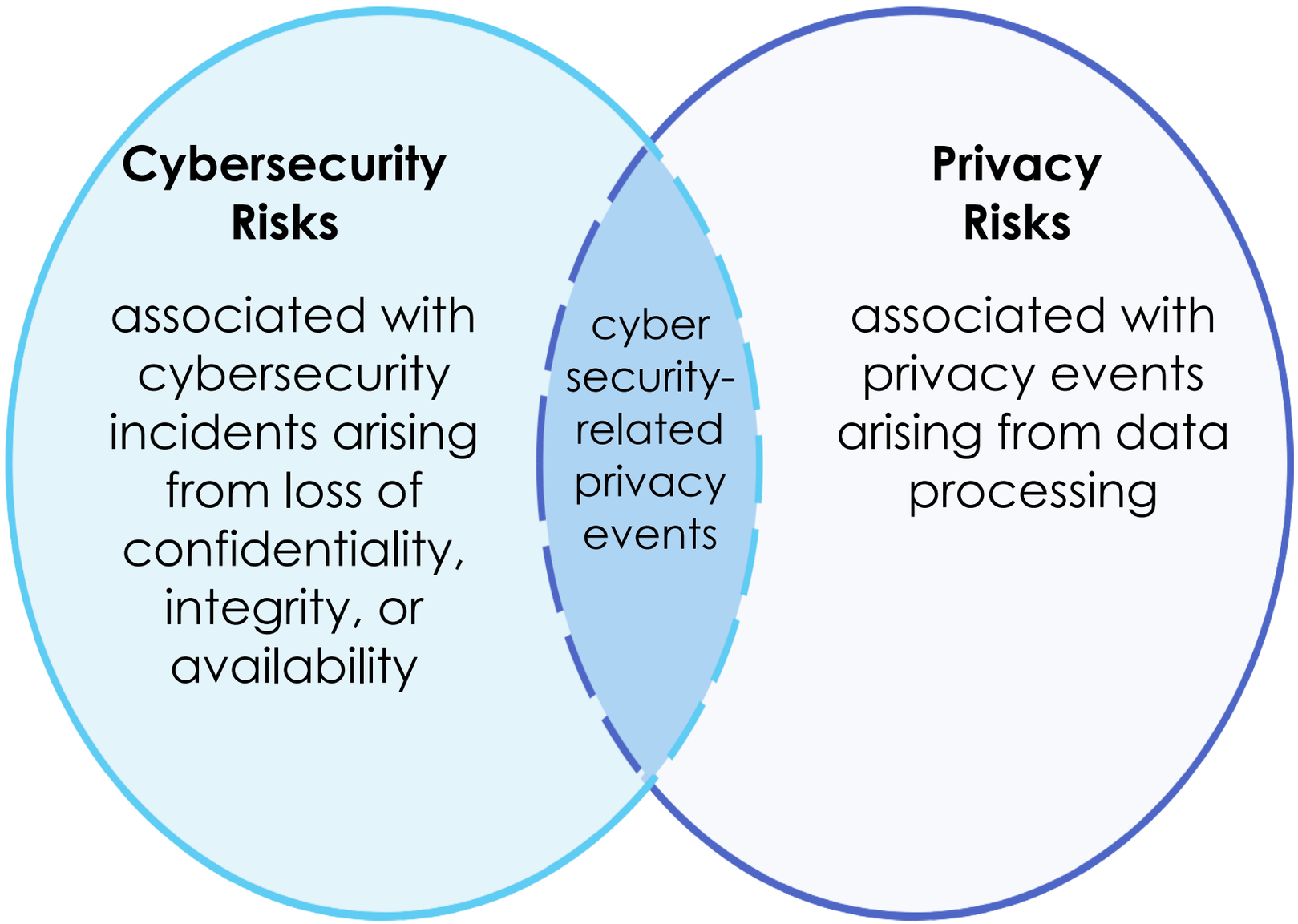
Building customer trust

Fulfilling current compliance obligations



Facilitating communication

Relationship Between Cybersecurity and Privacy Risk



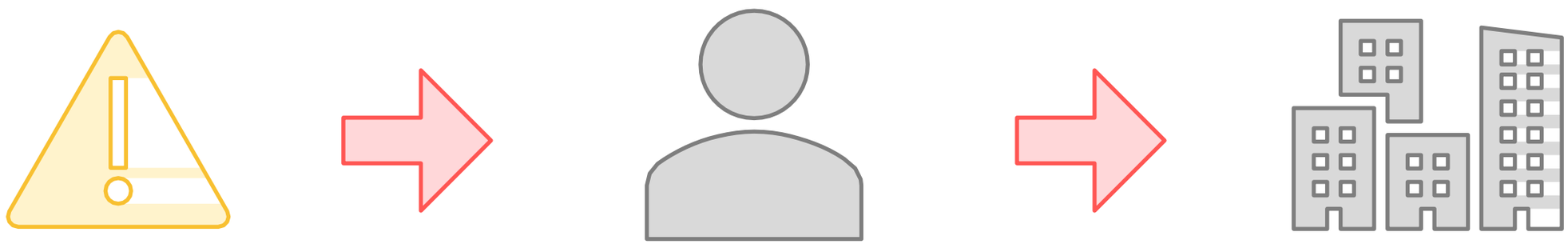
Data: A representation of information, including digital and non-digital formats

Privacy Event: The potential occurrence of problematic data action

Data Processing: The collective set of data actions (i.e., complete data life cycle including collection, retention, logging, generation, transformation, use, disclosure, sharing, transmission, and disposal)

Privacy Risk: The likelihood that individuals will experience problems resulting from data processing, and the impact should they occur

Privacy Risk and Organizational Risk



Problem

arises from data processing

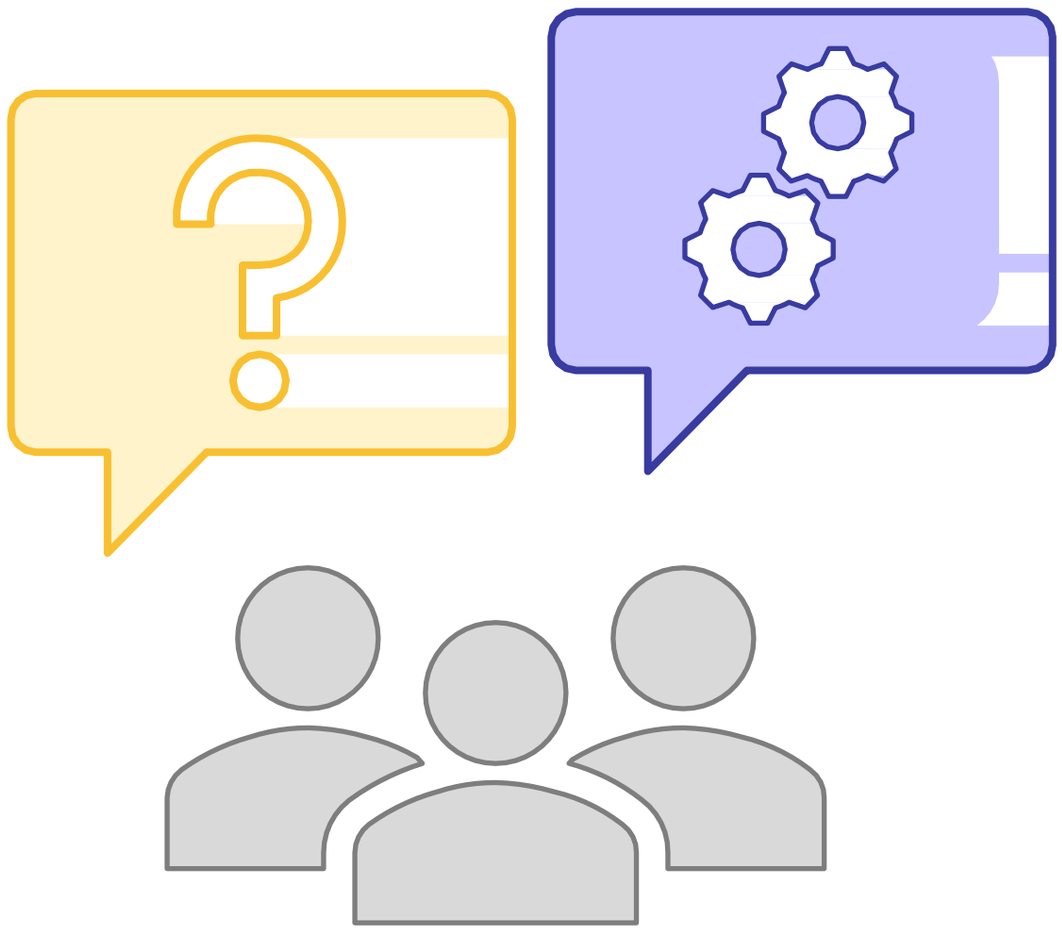
Individual

experiences direct impact (e.g., embarrassment, discrimination, economic loss)

Organization

resulting impact (e.g., customer abandonment, noncompliance costs, harm to reputation or internal culture)

Role of Privacy Risk Assessment

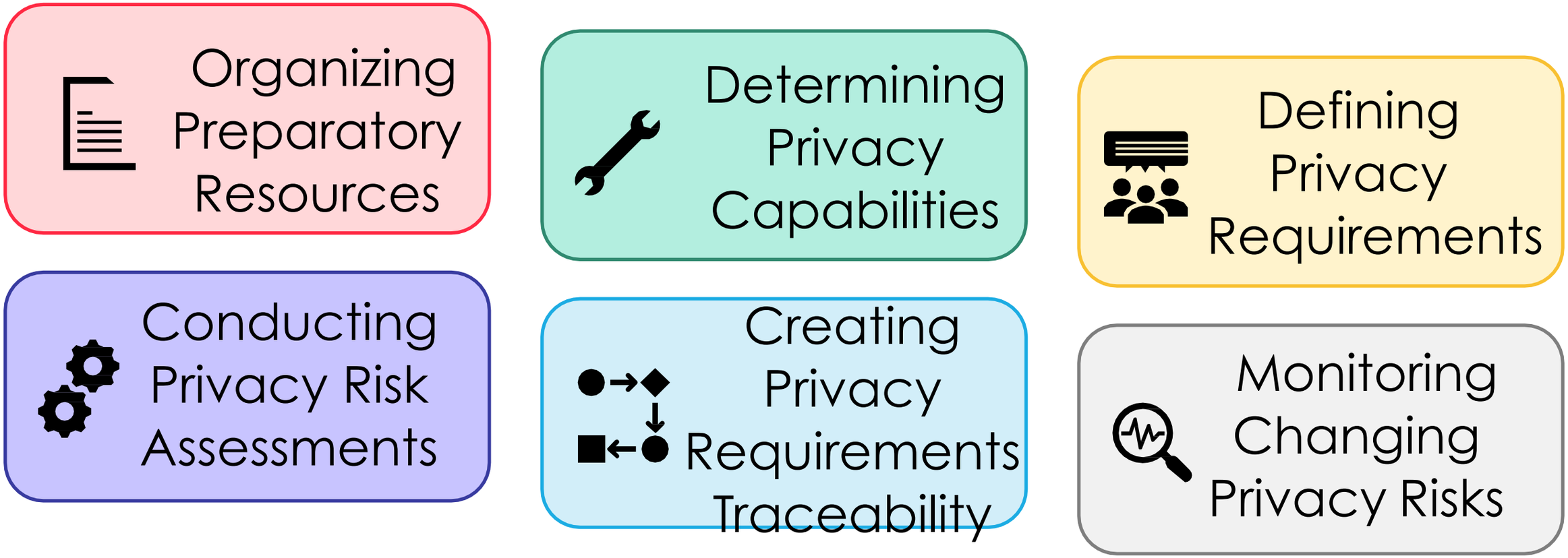


Cross-organizational set of processes that help organizations understand how their systems and services may create problems for individuals, and how to develop effective solutions to manage such risks

Privacy Risk Assessments

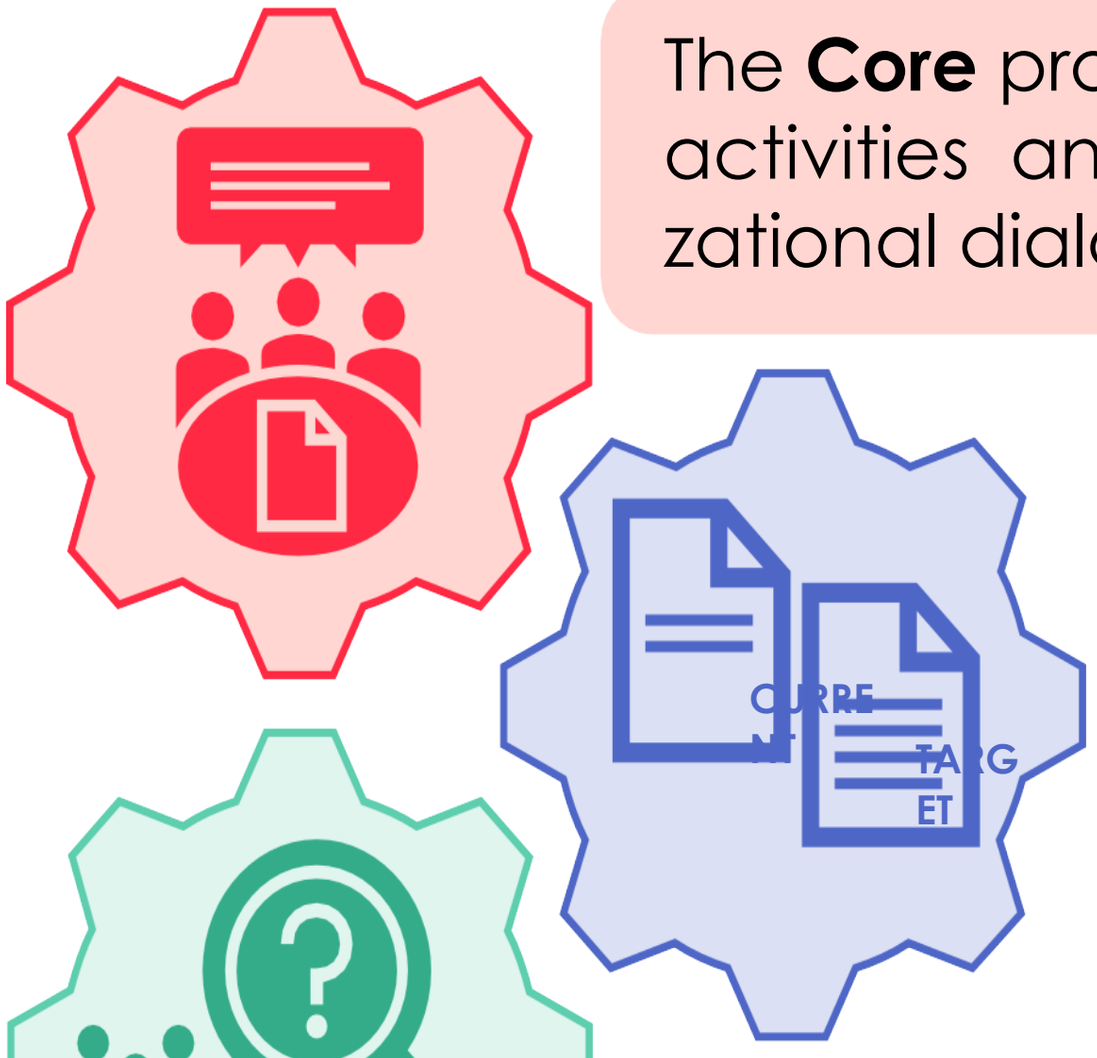
- Information to weigh benefits of data processing against risks and determine appropriate response (proportionality)
- Outcomes:
  - Mitigating the risk (e.g., technical and/or policy measures that minimize the risk to acceptable degree)
  - Transferring or sharing the risk (e.g., contracts can share or transfer risk to other organizations, privacy notices/ consent mechanisms means of sharing risk with individuals)
  - Avoiding the risk (e.g., organizations may determine risks outweigh benefits, forego data processing)
  - Accepting the risk (e.g., organizations may determine problems are minimal/unlikely, therefore benefits outweigh risks)

Appendix D: Key Privacy Risk Management Practices



FRAMEWORK STRUCTURE

Privacy Framework Structure

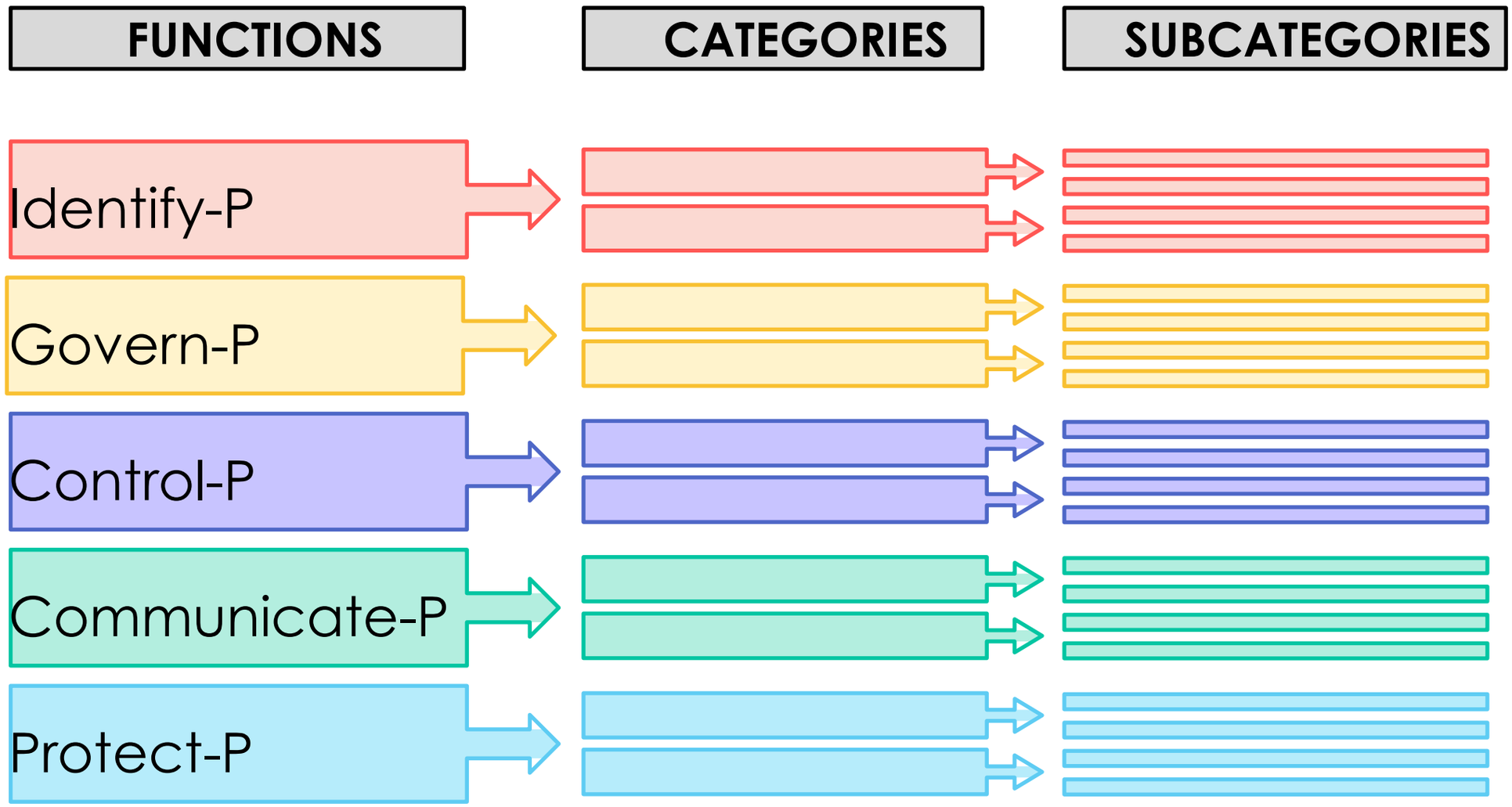


The **Core** provides an increasingly granular set of activities and outcomes that enable an organizational dialogue about managing privacy risk

Profiles are a selection of specific Functions, Categories, and Subcategories from the Core that the organization has prioritized to help it manage privacy risk

Implementation Tiers help an organization communicate about whether it has sufficient processes and resources in place to manage privacy risk and achieve its Target Profile

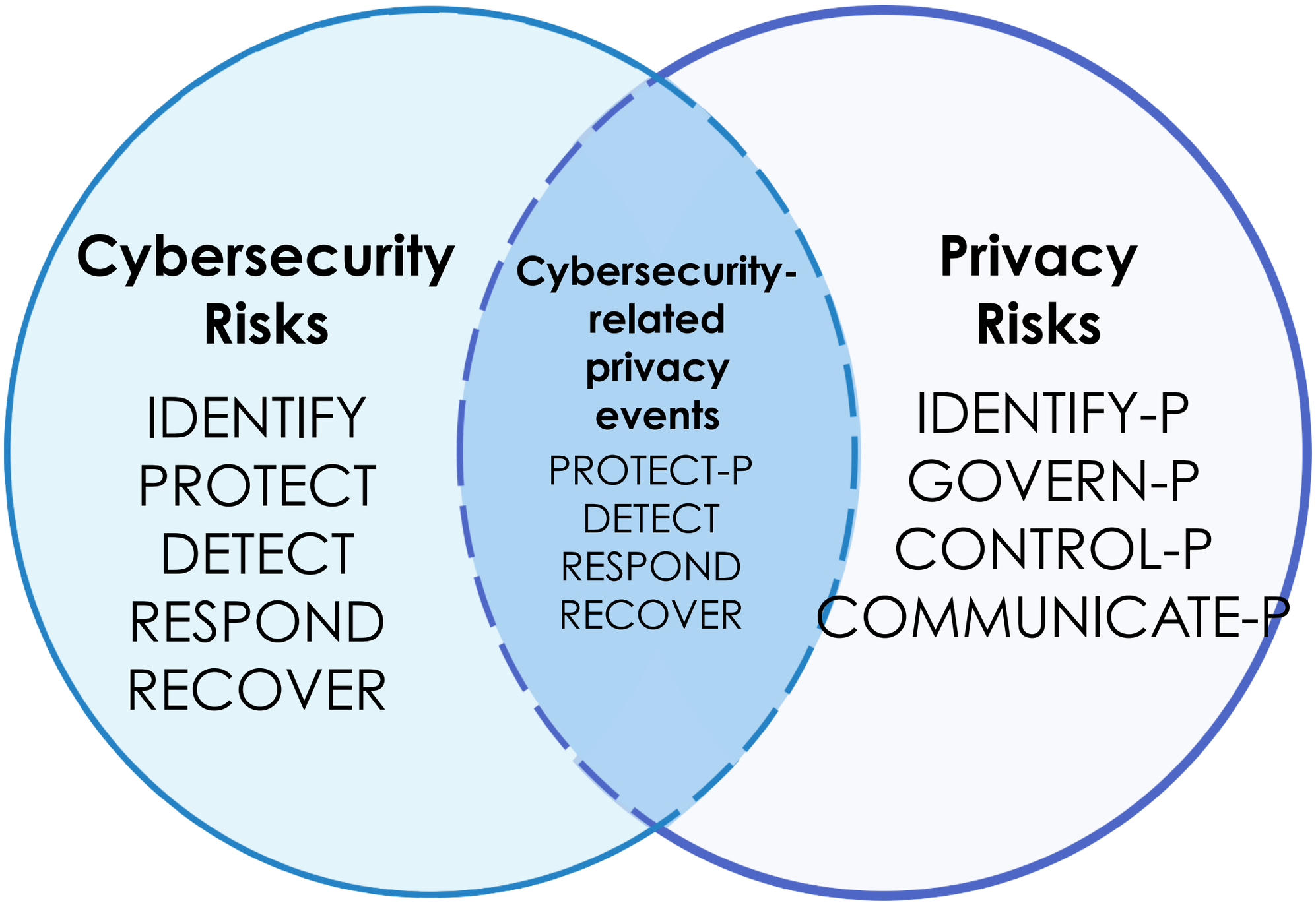
Privacy Framework Core



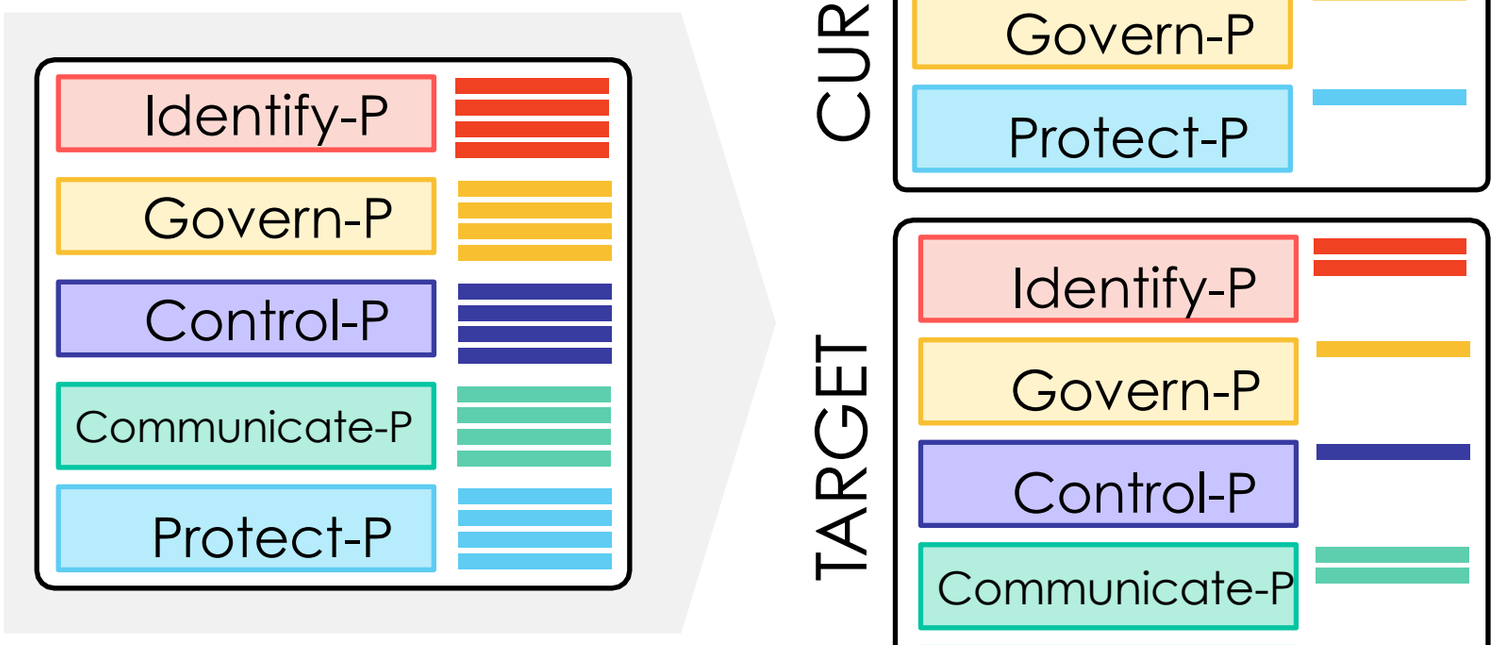
Privacy Framework Core

FUNCTIONS	CATEGORIES	SUBCATEGORIES
Identify-P	Develop the organizational understanding to manage privacy risk for individuals	
Govern-P	Organizational governance to enable ongoing understanding of organization's risk management priorities	
Control-P	Enable organizations or individuals to manage data with sufficient granularity to manage privacy risks	
Communicate-P	Enable reliable understanding and engage in a dialogue about how data are processed and associated privacy risks	
Protect-P	Develop and implement appropriate data processing safeguards	

Cybersecurity Framework Alignment



Profiles



Consider:

- Organizational goals
- Role(s) in the data processing ecosystem or industry sector
- Legal/regulatory requirements and industry best practices
- Organization's risk management priorities
- Privacy needs of individuals

Implementation Tiers

Understanding Privacy Risks

What are the privacy risks you need to manage as an organization?

Resources and Processes

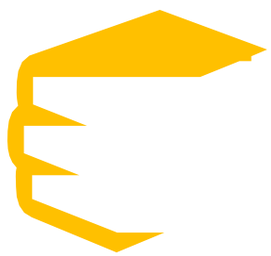
Do you have sufficient resources and processes in place to manage these risks?

Implementation Tiers

1: Partial
2: Risk Informed
3: Repeatable
4: Adaptive

Where are you in terms of having resources and processes and where do you want to be?

How to Use the Privacy Framework



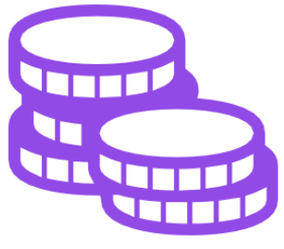
Informative References

Strengthening Accountability

Establishing or Improving a Privacy Program

Applying to the System Development Life Cycle

Using within the Data Processing Ecosystem



Informing Buying Decisions

APPENDIX A: THE CORE

Identify-P

Function	Category	Subcategory
IDENTIFY-P (ID-P): Develop the organizational understanding to manage privacy risk for individuals arising from data processing.	**Inventory and Mapping (ID.IM-P):** Data processing by systems, products, or services is understood and informs the management of privacy risk.	**ID.IM-P1:** Systems/products/services that process data are inventoried.
		ID.IM-P2: Owners or operators (e.g., the organization or third parties such as service providers, partners, customers, and developers) and their roles with respect to the systems/products/services and components (e.g., internal or external) that process data are inventoried.
		ID.IM-P3: Categories of individuals (e.g., customers, employees or prospective employees, consumers) whose data are being processed are inventoried.
		ID.IM-P4: Data actions of the systems/products/services are inventoried.
		ID.IM-P5: The purposes for the data actions are inventoried.
		ID.IM-P6: Data elements within the data actions are inventoried.
		ID.IM-P7: The data processing environment is identified (e.g., geographic location, internal, cloud, third parties).
		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.
	Business Environment (ID.BE-P): The organization's	**ID.BE-P1:** The organization's role(s) in the data processing ecosystem are identified

Identify-P (continued)

Function	Category	Subcategory
	Risk Assessment (ID.RA-P): 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.	**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).
		ID.RA-P2: Data analytic inputs and outputs are identified and evaluated for bias.
		ID.RA-P3: Potential problematic data actions and associated problems are identified.
		ID.RA-P4: Problematic data actions, likelihoods, and impacts are used to determine and prioritize risk.
		ID.RA-P5: Risk responses are identified, prioritized, and implemented.
	Data Processing Ecosystem Risk Management (ID.DE-P): The organization's priorities, constraints, risk 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	**ID.DE-P1:** Data processing ecosystem risk management policies, processes, and procedures are identified, established, assessed, managed, and agreed to by organizational stakeholders.
		ID.DE-P2: Data processing ecosystem parties (e.g., service providers, customers, partners, product manufacturers, application developers) are identified, prioritized, and assessed using a privacy risk assessment

Govern-P

Function	Category	Subcategory
GOVERN-P (GV-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.	**Governance Policies, Processes, and Procedures (GV.PO-P):** The policies, processes, and procedures to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of privacy risk.	**GV.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.
		GV.PO-P2: Processes to instill organizational privacy values within system/product/service development and operations are established and in place.
		GV.PO-P3: Roles and responsibilities for the workforce are established with respect to privacy.
		GV.PO-P4: Privacy roles and responsibilities are coordinated and aligned with third-party stakeholders (e.g., service providers, customers, partners).
		GV.PO-P5: Legal, regulatory, and contractual requirements regarding privacy are understood and managed.
		GV.PO-P6: Governance and risk management policies, processes, and procedures address privacy risks.

Govern-P (continued)

	Function	Category	Subcategory
		Monitoring and Review (GV.MT-P): The policies, processes, and procedures for ongoing review of the organization's privacy posture are understood and inform the management of privacy risk.	**GV.MT-P1:** Privacy risk is re-evaluated on an ongoing basis and as key factors, including the organization's business environment (e.g., introduction of new technologies), governance (e.g., legal obligations, risk tolerance), data processing, and systems/products/services change.
			GV.MT-P2: Privacy values, policies, and training are reviewed and any updates are communicated.
			GV.MT-P3: Policies, processes, and procedures for assessing compliance with legal requirements and privacy policies are established and in place.
			GV.MT-P4: Policies, processes, and procedures for communicating progress on managing privacy risks are established and in place.
			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).
			GV.MT-P6: Policies, processes, and procedures incorporate lessons learned from problematic data actions.
			GV.MT-P7: Policies, processes, and procedures for receiving, tracking

Control-P

Function	Category	Subcategory
CONTROL-P (CT-P): Develop and implement appropriate activities to enable organizations or individuals to manage data with sufficient granularity to manage privacy risks.	**Data Processing Policies, Processes, and Procedures (CT.PO-P):** 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.	**CT.PO-P1:** Policies, processes, and procedures for authorizing data processing (e.g., organizational decisions, individual consent), revoking authorizations, and maintaining authorizations are established and in place.
		CT.PO-P2: Policies, processes, and procedures for enabling data review, transfer, sharing or disclosure, alteration, and deletion are established and in place (e.g., to maintain data quality, manage data retention).
		CT.PO-P3: Policies, processes, and procedures for enabling individuals' data processing preferences and requests are established and in place.
		CT.PO-P4: A data life cycle to manage data is aligned and implemented with the system development life cycle to manage systems.
	Data Processing Management (CT.DM-P): Data are managed consistent with the organization's risk strategy to protect individuals' privacy, increase manageability, and enable the implementation of privacy principles (e.g., individual participation, data quality, data minimization).	**CT.DM-P1:** Data elements can be accessed for review.
		CT.DM-P2: Data elements can be accessed for transmission or disclosure.
		CT.DM-P3: Data elements can be accessed for alteration.
		CT.DM-P4: Data elements can be accessed for deletion.

Control-P (continued)

	Function	Category	Subcategory
		Disassociated Processing (CT.DP-P): Data processing solutions increase disassociability consistent with the organization's risk strategy to protect individuals' privacy and enable implementation of privacy principles (e.g., data minimization).	**CT.DP-P1:** Data are processed to limit observability and linkability (e.g., data actions take place on local devices, privacy-preserving cryptography).
			CT.DP-P2: Data are processed to limit the identification of individuals (e.g., de-identification privacy techniques, tokenization).
			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).
			CT.DP-P4: System or device configurations permit selective collection or disclosure of data elements.
			CT.DP-P5: Attribute references are substituted for attribute values.

Communicate-P

Function	Category	Subcategory
COMMUNICATE-P (CM-P): 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.	**Communication Policies, Processes, and Procedures (CM.PO-P):** Policies, processes, and procedures are maintained and used to increase transparency of the organization's data processing practices (e.g., purpose, scope, roles and responsibilities in the data processing ecosystem, and management commitment) and associated privacy risks.	**CM.PO-P1:** Transparency policies, processes, and procedures for communicating data processing purposes, practices, and associated privacy risks are established and in place.
		CM.PO-P2: Roles and responsibilities (e.g., public relations) for communicating data processing purposes, practices, and associated privacy risks are established.
	Data Processing Awareness (CM.AW-P): Individuals and organizations have reliable knowledge about data processing practices and associated privacy risks, and effective mechanisms are used and maintained to increase predictability consistent with the organization's risk strategy to protect individuals' privacy.	**CM.AW-P1:** Mechanisms (e.g., notices, internal or public reports) for communicating data processing purposes, practices, associated privacy risks, and options for enabling individuals' data processing preferences and requests are established and in place.
		CM.AW-P2: Mechanisms for obtaining feedback from individuals (e.g., surveys or focus groups) about data processing and associated privacy risks are established and in place.
		CM.AW-P3: System/product/service design enables data processing visibility.
		CM.AW-P4: Records of data disclosures and sharing are maintained and can be accessed for review or transmission/disclosure.

Protect-P

Function	Category	Subcategory
PROTECT-P (PR-P): Develop and implement appropriate data processing safeguards.	**Data Protection Policies, Processes, and Procedures (PR.PO-P):** Security and privacy policies (e.g., purpose, scope, roles and responsibilities in the data processing ecosystem, and management commitment), processes, and procedures are maintained and used to manage the protection of data.	**PR.PO-P1:** A baseline configuration of information technology is created and maintained incorporating security principles (e.g., concept of least functionality).
		PR.PO-P2: Configuration change control processes are established and in place.
		PR.PO-P3: Backups of information are conducted, maintained, and tested.
		PR.PO-P4: Policy and regulations regarding the physical operating environment for organizational assets are met.
		PR.PO-P5: Protection processes are improved.
		PR.PO-P6: Effectiveness of protection technologies is shared.
		PR.PO-P7: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are established, in place, and managed.
		PR.PO-P8: Response and recovery plans are tested.
		PR.PO-P9: Privacy procedures are included in human resources practices (e.g., deprovisioning, personnel screening).
		PR.PO-P10: A vulnerability management plan is developed and implemented.
	Identity Management, Authentication	**PR.AC-P1:** Identities and credentials are issued, managed, verified

Protect-P (continued)

Function	Category	Subcategory
	Data Security (PR.DS-P): Data are managed consistent with the organization's risk strategy to protect individuals' privacy and maintain data confidentiality, integrity, and availability.	**PR.DS-P1:** Data-at-rest are protected.
		PR.DS-P2: Data-in-transit are protected.
		PR.DS-P3: Systems/products/services and associated data are formally managed throughout removal, transfers, and disposition.
		PR.DS-P4: Adequate capacity to ensure availability is maintained.
		PR.DS-P5: Protections against data leaks are implemented.
		PR.DS-P6: Integrity checking mechanisms are used to verify software, firmware, and information integrity.
		PR.DS-P7: The development and testing environment(s) are separate from the production environment.
		PR.DS-P8: Integrity checking mechanisms are used to verify hardware integrity.
	Maintenance (PR.MA-P): System maintenance and repairs are performed consistent with policies, processes, and procedures.	**PR.MA-P1:** Maintenance and repair of organizational assets are performed and logged, with approved and controlled tools.
		PR.MA-P2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access.
	Protective Technology (PR.PT-P): Technical security solutions are managed to ensure the security and resilience of	**PR.PT-P1:** Removable media is protected and its use restricted according to policy.
		PR.PT-P2: The principle of least functionality is incorporated by