WEBINAR
NIST Privacy Framework 101
Preparing for Workshop #3

June 27, 2019

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

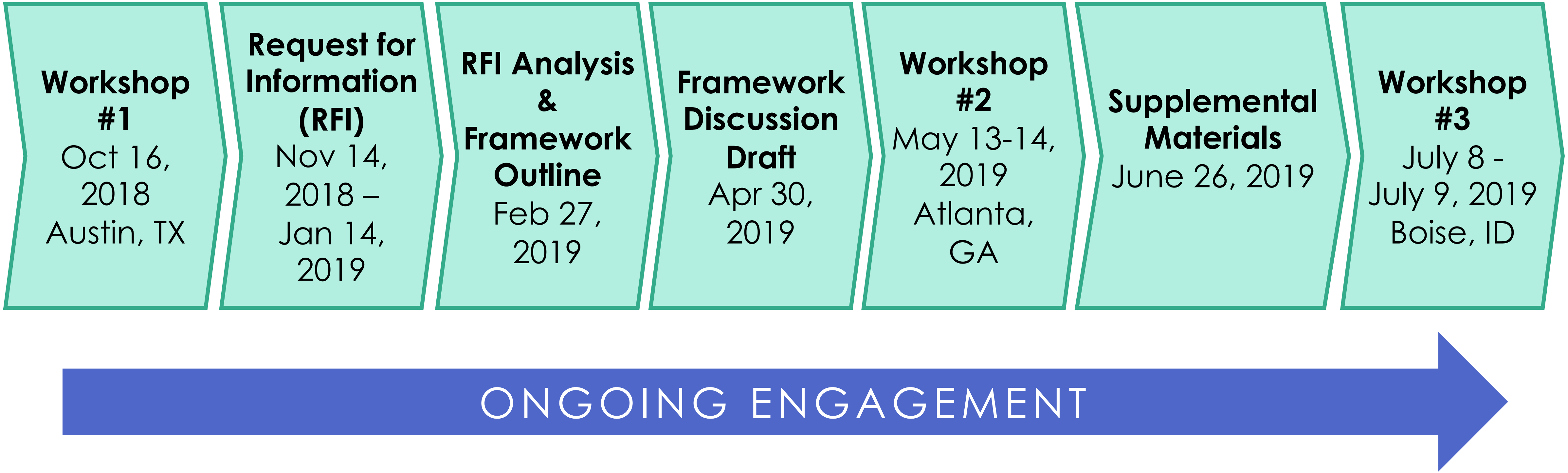
Getting to V1.0 of the NIST Privacy Framework: Workshop #3

July 8-9, 2019 | Boise, Idaho

Why NIST?

- Long track record of successfully, collaboratively working with public and private sectors
- Experience developing the Cybersecurity Framework
- Extensive privacy expertise

Process to Date



Workshop #1
Oct 16, 2018
Austin, TX

Request for Information (RFI)
Nov 14, 2018 – Jan 14, 2019

RFI Analysis & Framework Outline
Feb 27, 2019

Framework Discussion Draft
Apr 30, 2019

Workshop #2
May 13-14, 2019
Atlanta, GA

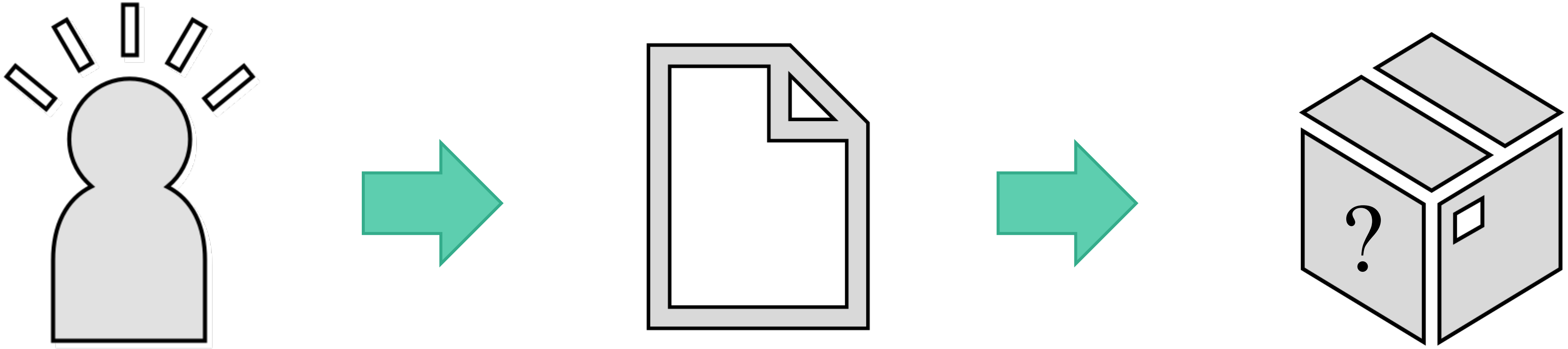
Supplemental Materials
June 26, 2019

Workshop #3
July 8 - July 9, 2019
Boise, ID

ONGOING ENGAGEMENT

Feedback encouraged and promoted throughout the process

NIST Privacy Framework: What is it?



Attributes:

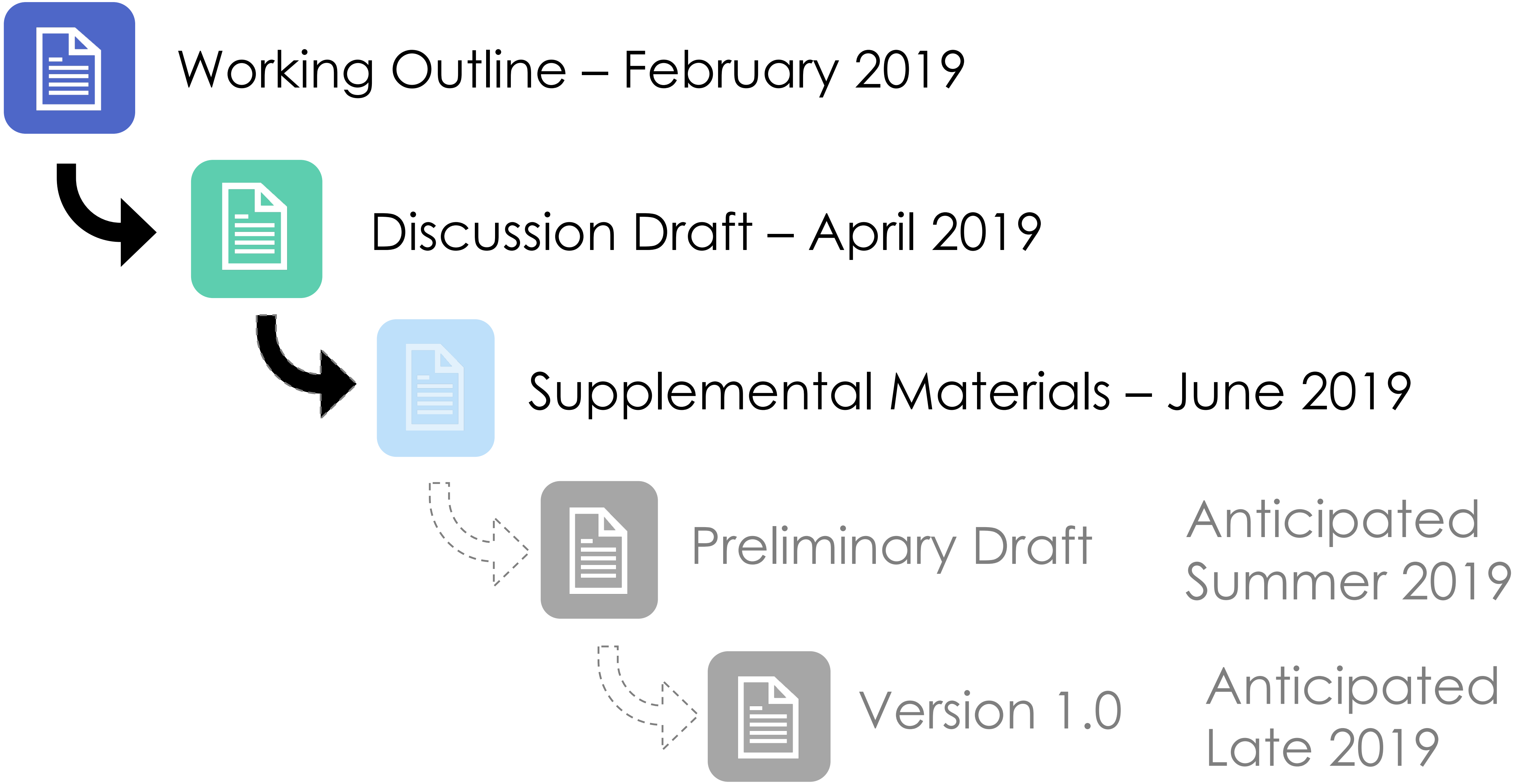
- voluntary
- risk- & outcome-based
- non-prescriptive
- accessible language
- adaptable
- compatible with legal regimes

Enterprise risk management tool to help organizations answer the fundamental question: "How are we considering the privacy impacts to individuals as we develop our systems, products, and services?"

future state:

NIST Privacy Framework version 1.0

Framework Development Stages



Working Outline – February 2019

Discussion Draft – April 2019

Supplemental Materials – June 2019

Preliminary Draft

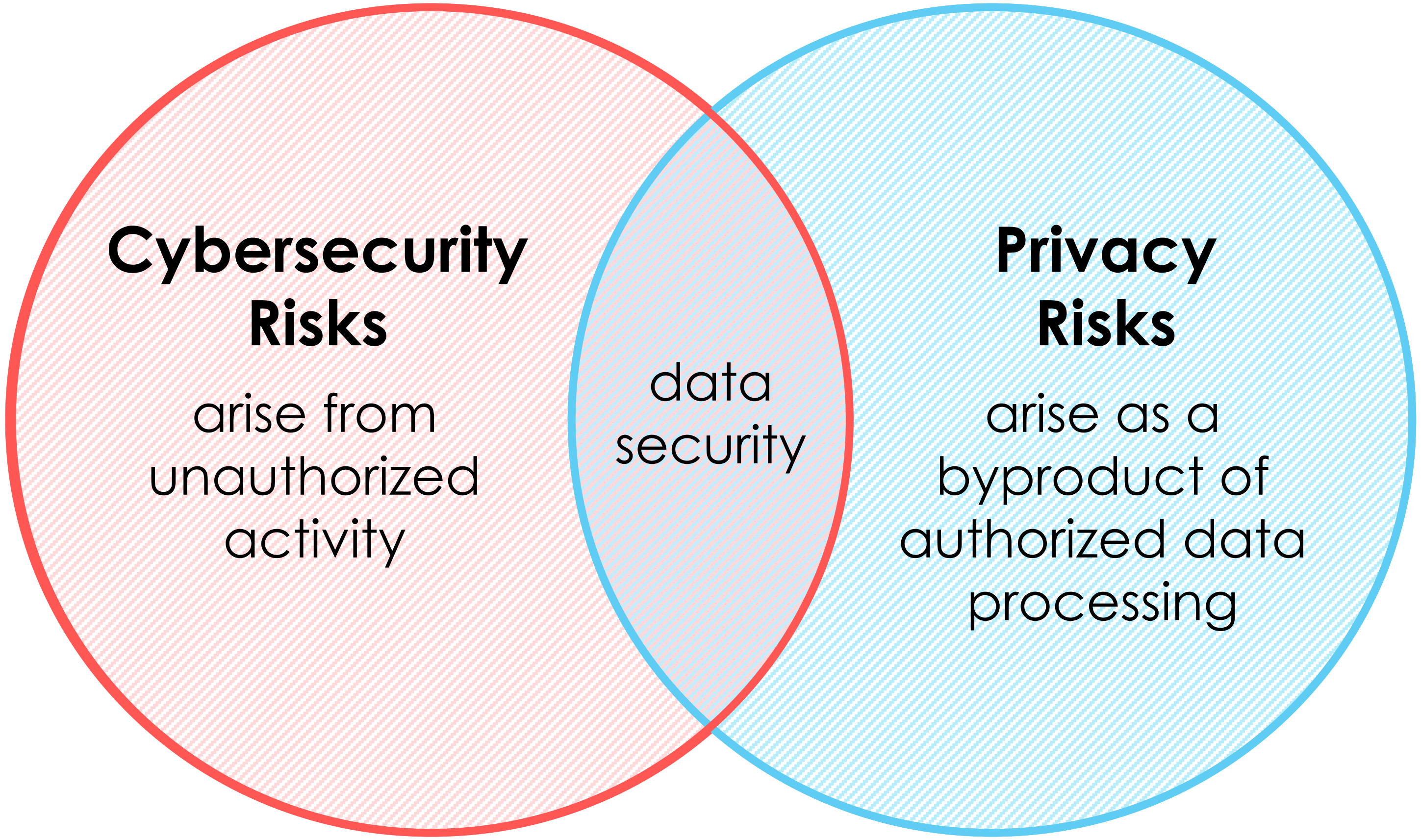
Anticipated
Summer 2019

Version 1.0

Anticipated
Late 2019

In-Depth Review of NIST Privacy Framework Discussion Draft

Relationship Between Cybersecurity and Privacy Risk



Cybersecurity Risks

arise from unauthorized activity

data security

Privacy Risks

arise as a byproduct of authorized data processing

- There is a clear recognition that security of data plays an important role in the protection of privacy
- Individual privacy cannot be achieved solely by securing data
- Authorized processing: system operations that handle data (collection – disposal) to enable the system to achieve mission/business objectives

Key Definitions

For the purposes of the Privacy Framework:

Data

A representation of information with the potential for adverse consequences for individuals when processed

Data Processing

Complete data life cycle, including but not limited to: collection, retention, logging, generation, transformation, use, disclosure, transfer, and disposal

Privacy Risk

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

Importance of Privacy Risk Management and Risk Assessment

Privacy risk assessments:

> "…can help organizations make ethical decisions and avoid losses of trust that damage their reputations or slow adoption or cause abandonment of products and services."

Appendix D: Key Privacy Risk Management Practices

Organizing Preparatory Resources

Determining Privacy Capabilities

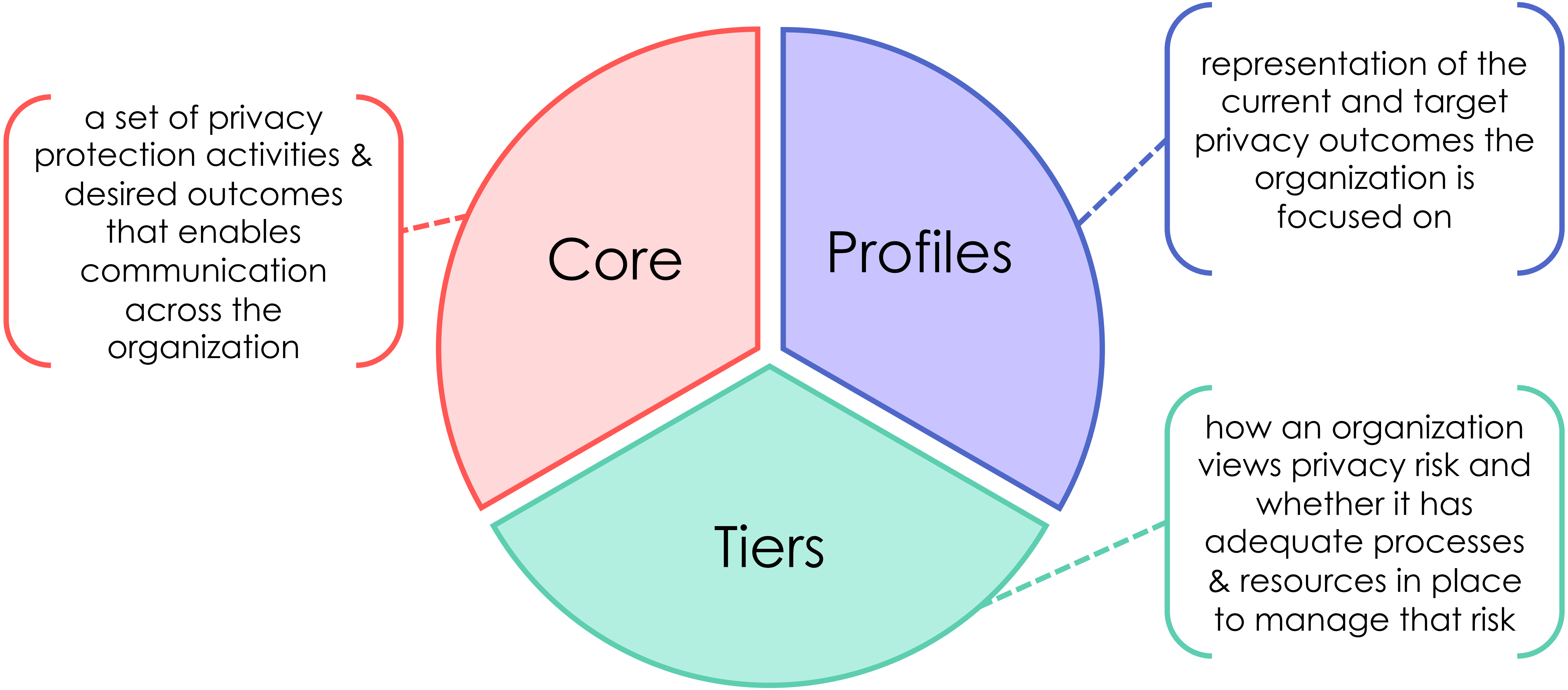
Defining Privacy Requirements

Conducting Privacy Risk Assessments

Creating Privacy Requirements Traceability

Monitoring Changing Privacy Risks

Privacy Framework Structure



a set of privacy protection activities & desired outcomes that enables communication across the organization

representation of the current and target privacy outcomes the organization is focused on

how an organization views privacy risk and whether it has adequate processes & resources in place to manage that risk

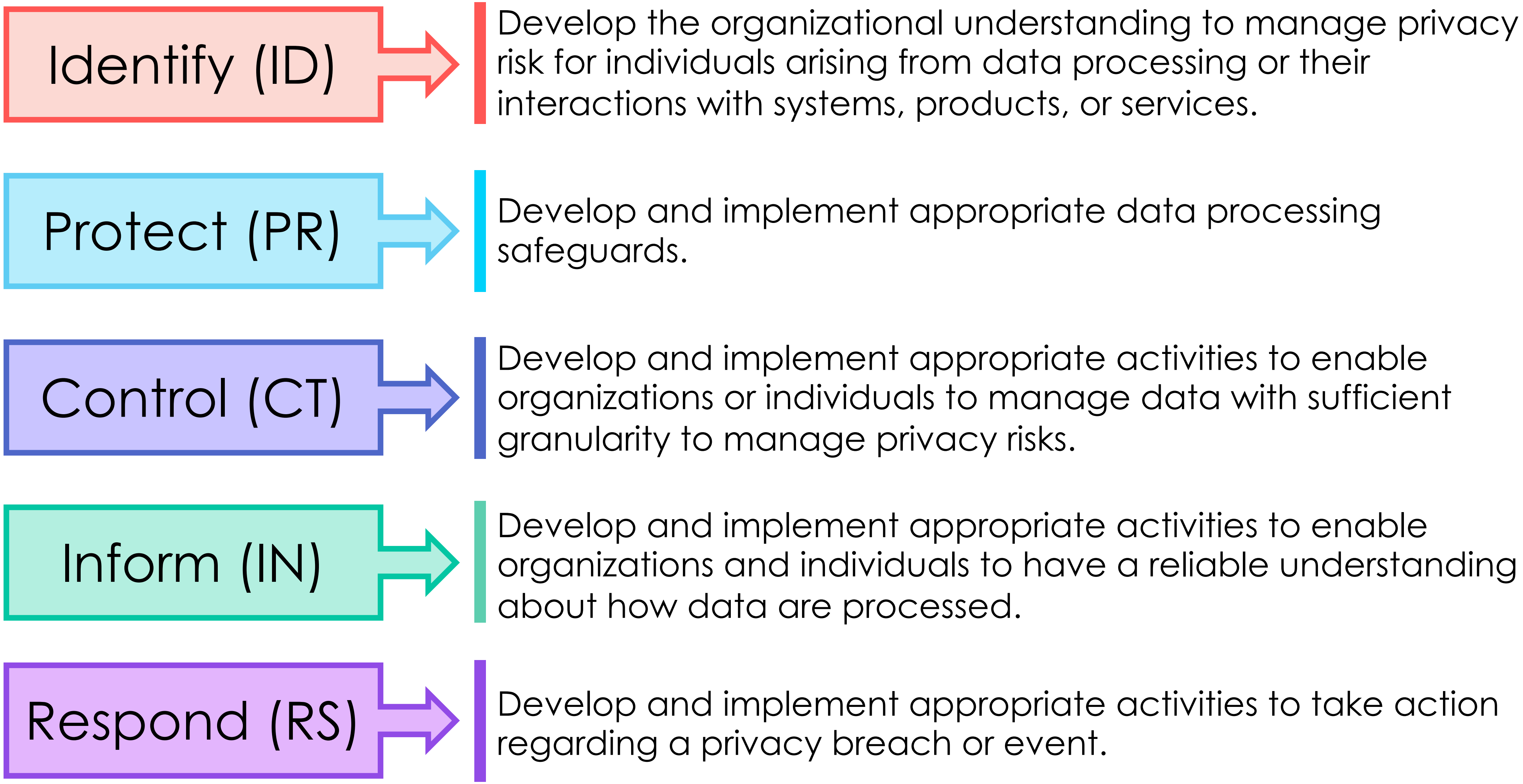
Example Core Subcategories

ID	ID.IM-P	ID.IM-P6	Data processing is mapped, illustrating the processing of data elements by system components and their owner/operators, and interactions of individuals and organizations with the systems/products/services.
PR	PR.PP-P	PR.PP-P2	Data are processed to limit the identification of individuals.
CT	CT.DM-P	CT.DM-P6	Data elements can be accessed for deletion.
IN	IN.AW-P	IN.AW-P7	Data analytic inputs and outputs are understood and evaluated for bias.
RS	RS.RE-P	RS.RE-P1	Processes for receiving and responding to complaints, concerns, and questions from individuals about organizational privacy practices are in place.

Example Core Categories

ID	Inventory and Mapping (ID.IM-P)	Data processing and individuals' interactions with systems, products, or services are understood and inform the management of privacy risk.
PR	Protected Processing (PR.PP-P)	Technical data processing solutions increase disassociability consistent with related policies, procedures, and agreements and the organization's risk strategy to protect individuals' privacy.
CT	Data Management (CT.DM-P)	Data are managed consistent with the organization's risk strategy to protect individuals' privacy and increase manageability.
IN	Data Processing Awareness (IN.AW-P)	Individuals and organizations have an awareness of data processing practices, and processes and procedures are used and maintained to increase predictability consistent with the organization's risk strategy to protect individuals' privacy.
RS	Redress (RS.RE-P)	Organizational response activities include processes or mechanisms to address impacts to individuals that arise from data processing.

Core Functions



Identify (ID): Develop the organizational understanding to manage privacy risk for individuals arising from data processing or their interactions with systems, products, or services.

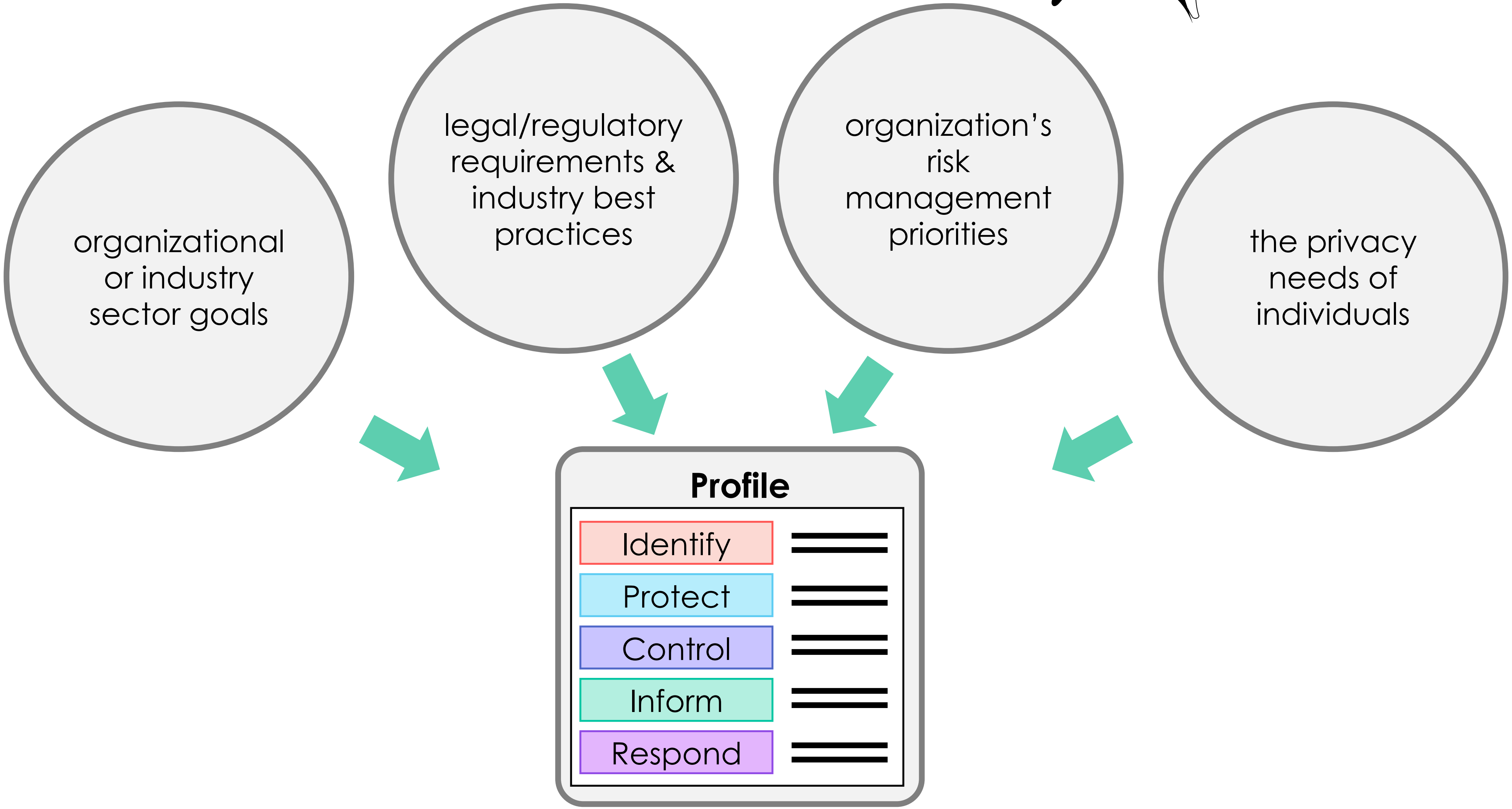
Protect (PR): Develop and implement appropriate data processing safeguards.

Control (CT): Develop and implement appropriate activities to enable organizations or individuals to manage data with sufficient granularity to manage privacy risks.

Inform (IN): Develop and implement appropriate activities to enable organizations and individuals to have a reliable understanding about how data are processed.

Respond (RS): Develop and implement appropriate activities to take action regarding a privacy breach or event.

Privacy Framework Profiles



organizational or industry sector goals

legal/regulatory requirements & industry best practices

organization’s risk management priorities

the privacy needs of individuals

Profile

Identify

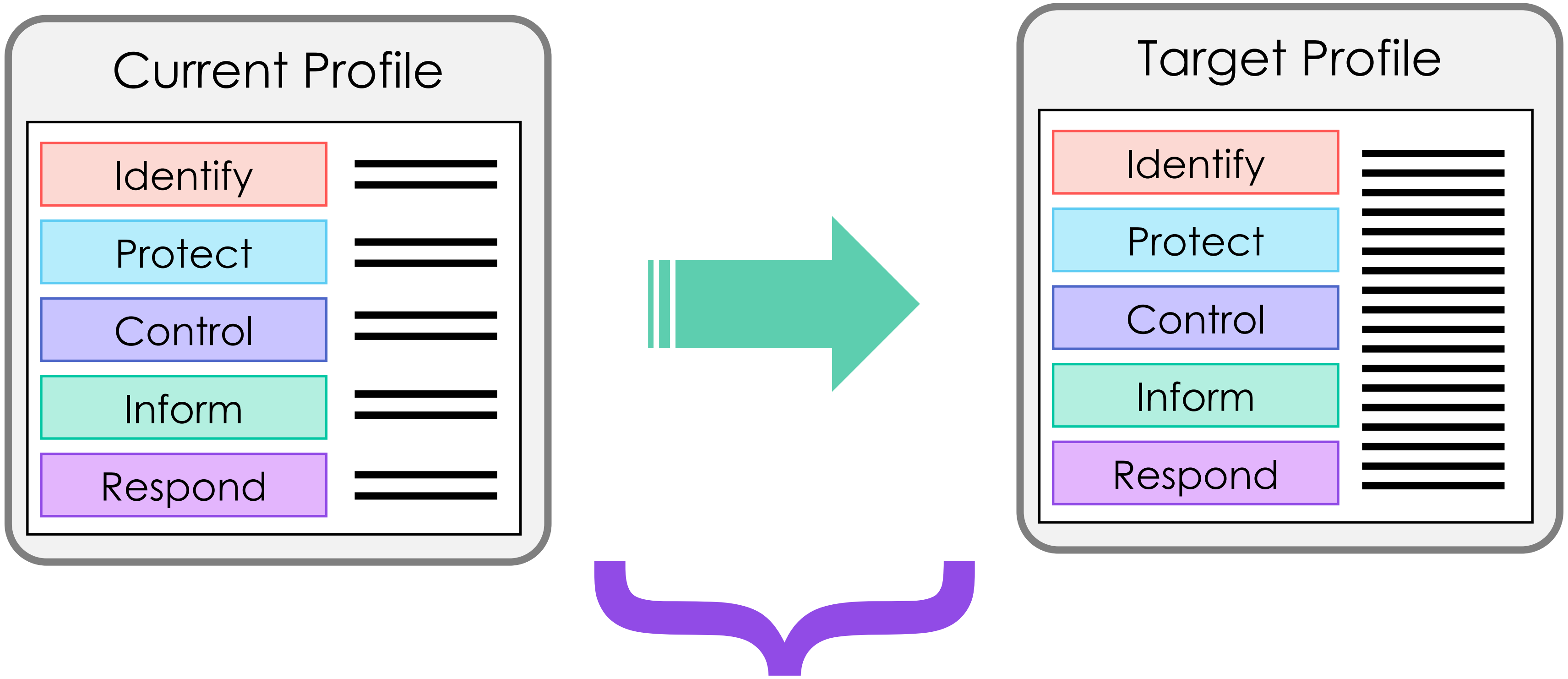
Protect

Control

Inform

Respond

Current and Target Profiles



Current Profile

Identify

Protect

Control

Inform

Respond

Target Profile

Identify

Protect

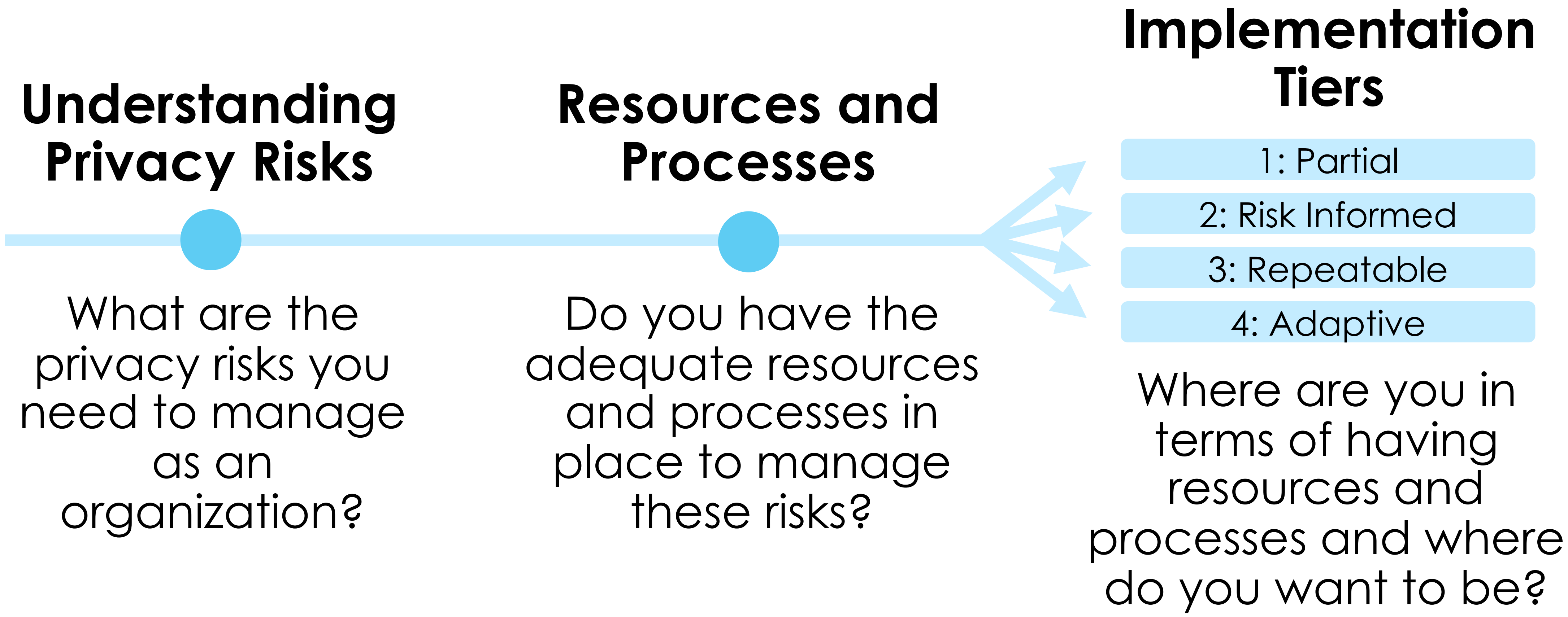
Control

Inform

Respond

- identify gaps
- develop an action plan for improvement
- gauge the resources that would be needed (e.g., staffing, funding) to achieve privacy outcomes

Implementation Tiers



Understanding Privacy Risks

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

Resources and Processes

Do you have the adequate 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

Strengthening Accountability

Basic Review of Privacy Practices

Establishing or Improving a Privacy Program

Application in the System Development Life Cycle

Communicating Privacy Requirements with Stakeholders

Informative References

Informative References

- Specific sections of standards, guidelines, and practices that can be mapped to the Core subcategories and support achievement of the subcategory outcomes
- NIST has provided a mapping of the Core subcategories to relevant NIST guidance
- NIST will develop a process for accepting external informative references

Categories and Subcategories: Identify

IDENTIFY-P (ID)	**Inventory and Mapping (ID.IM-P):** Data processing and individuals’ interactions with systems, products, or services are understood and inform the management of privacy risk.	**ID.IM-P1:** Systems/products/services that process data, or with which individuals are interacting, are inventoried.
		ID.IM-P2: The owners or operators of systems/products/services that process data, or with which individuals are interacting, are identified.
		ID-IM-P3: Data elements that systems/products/services are processing are inventoried.
		ID.IM-P4: Data actions are identified.
		ID.IM-P5: The data processing environment is identified (e.g., internal, cloud).
		ID.IM-P6: Data processing is mapped, illustrating the processing of data elements by system components and their owner/operators, and interactions of individuals and organizations with the systems/products/services.
	Business Environment (ID.BE-P): The organization’s mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform privacy roles, responsibilities, and risk management decisions.	**ID.BE-P1:** The organization’s role in the supply chain is identified and communicated.
		ID.BE-P2: Priorities for organizational mission, objectives, and activities are established and communicated.
		ID.BE-P3: Systems/products/services that support organizational priorities are identified and key functional requirements communicated.

Categories and Subcategories: Identify

	IDENTIFY-P (ID)	**Governance (ID.GV-P):** The policies, procedures, and processes to manage and monitor the organization’s regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of privacy risk.	**ID.GV-P1:** Organizational privacy policies are established and communicated.
			ID.GV-P2: Processes to instill organizational privacy values within system/product/service development operations are in place.
			ID.GV-P3: Privacy roles and responsibilities for the entire workforce are established.
			ID.GV-P4: Privacy roles and responsibilities are coordinated and aligned with third-party stakeholders (e.g., suppliers, customers, partners).
			ID.GV-P5: Legal, regulatory, and contractual requirements regarding privacy are understood and managed.
			ID.GV-P6: Governance and risk management processes address privacy risks.

Categories and Subcategories: Identify

IDENTIFY-P (ID)	**Risk Assessment (ID.RA-P):** The organization understands the privacy risks to individuals and how such privacy risks may create secondary impacts on organizational operations (including mission, functions, reputation, or workforce culture).	**ID.RA-P1:** The purposes for the data actions are identified.
		ID.RA-P2: Contextual factors related to the systems/products/services and the data actions are identified (e.g., individuals' privacy interests and perceptions, demographics, data sensitivity).
		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 and prioritized.
		ID.RA-P6: Risk is re-evaluated as data processing or individuals' interactions with systems/products/services change.
	Risk Management Strategy (ID.RM-P): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	**ID.RM-P1:** Risk management processes are established, managed, and agreed to by organizational stakeholders.
		ID.RM-P2: Organizational risk tolerance is determined and clearly expressed.
		ID.RM-P3: The organization's determination of risk tolerance is informed by its role in the ecosystem.

Categories and Subcategories: Identify

IDENTIFY-P (ID)	**Supply Chain Risk Management (ID.SC-P):** The organization’s priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing privacy supply chain risk. The organization has established and implemented the processes to identify, assess, and manage privacy supply chain risks.	**ID.SC-P1:** Supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders.
		ID.SC-P2: Service providers/suppliers/third-party partners of data processing systems, products, and services are identified, prioritized, and assessed using a supply chain risk assessment process.
		ID.SC-P3: Contracts with service providers/suppliers/third-party partners are used to implement appropriate measures designed to meet the objectives of an organization’s privacy program and supply chain risk management plan.
		ID.SC-P4: Service providers/suppliers/third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations.
		ID.SC-P5: Response planning and testing are conducted with service providers/suppliers/third-party providers.

Categories and Subcategories: Protect

PROTECT-P (PR)	**Identity Management, Authentication, and Access Control (PR.AC-P):** Access to data and devices is limited to authorized individuals, processes, and devices, and is managed consistent with the assessed risk of unauthorized access.	**PR.AC-P1:** Identities and credentials are issued, managed, verified, revoked, and audited for authorized individuals, processes, and devices.
		PR.AC-P2: Physical access to data and devices is managed.
		PR.AC-P3: Remote access is managed.
		PR.AC-P4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties.
		PR.AC-P5: Network integrity is protected (e.g., network segregation, network segmentation).
		PR.AC-P6: Individuals and devices are proofed and bound to credentials, and authenticated commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks).
		PR.AC-P7: Attribute references are used instead of attribute values.
		PR.AT-P1: All users are informed and trained.
	Awareness and Training (PR.AT-P): The organization's personnel and partners are provided privacy awareness education and are trained to perform their privacy-related duties and responsibilities consistent with related policies, procedures, and agreements.	**PR.AT-P2:** Privileged users understand their roles and responsibilities.
		PR.AT-P3: Third-party stakeholders (e.g., service providers, customers, partners) understand their roles and responsibilities.
		PR.AT-P4: Senior executives understand their roles and responsibilities.
		PR.AT-P5: Privacy personnel understand their roles and responsibilities.

Categories and Subcategories: Protect

PROTECT-P (PR)	**Data Security (PR.DS-P):** Data are managed consistent with the organization’s risk strategy to protect individuals’ privacy and maintain data confidentiality, integrity, and availability.	**PR.DS-P1:** Data-at-rest is protected.
		PR.DS-P2: Data-in-transit is 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.

Categories and Subcategories: Protect

	PROTECT-P (PR)	**Data Protection Processes and Procedures (PR.DP-P):** Security and privacy policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage the protection of data.	**PR.DP-P1:** A baseline configuration of security and privacy controls is created and maintained.
			PR.DP-P2: A system development life cycle to manage systems and an information life cycle to manage data are aligned and implemented.
			PR.DP-P3: Configuration change control processes are in place.
			PR.DP-P4: Backups of information are conducted, maintained, and tested.
			PR.DP-P5: Policy and regulations regarding the physical operating environment for organizational assets are met.
			PR.DP-P6: Data are destroyed according to policy.
			PR.DP-P7: Protection processes are improved.
			PR.DP-P8: Effectiveness of protection technologies is shared.
			PR.DP-P9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed.
			PR.DP-P10: Response and recovery plans are tested.
			PR.DP-P11: Privacy procedures are included in human resources practices (e.g., deprovisioning, personnel screening).
			PR.DP-P12: A vulnerability management plan is developed and implemented.

Categories and Subcategories: Protect

PROTECT-P (PR)	**Maintenance (PR.MA-P):** System maintenance and repairs are performed consistent with policies and procedures.	**PR.MA-P1:** Maintenance and repair of organizational assets are performed and logged, with approved and controlled tools.
		PR.MA-P2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access.
	Protective Technology (PR.PT-P): Technical security solutions are managed to ensure the security and resilience of systems/products/services and associated data, consistent with related policies, procedures, and agreements.	**PR.PT-P1:** Audit/log records are determined, documented, implemented, and reviewed in accordance with policy and incorporating the principle of data minimization.
		PR.PT-P2: Removable media is protected and its use restricted according to policy.
		PR.PT-P3: The principle of least functionality is incorporated by configuring systems to provide only essential capabilities.
		PR.PT-P4: Communications and control networks are protected.
		PR.PT-P5: Mechanisms (e.g., failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations.

Categories and Subcategories: Protect

	PROTECT-P (PR)	**Protected Processing (PR.PP-P):** Technical data processing solutions increase disassociability consistent with related policies, procedures,	**PR.PP-P1:** Data are processed in an unobservable or unlinkable manner.
			PR.PP-P2: Data are processed to limit the identification of individuals.
			PR.PP-P3: Data are processed to restrict the formulation of inferences about individuals' behavior or activities.
			PR.PP-P4: Data are processed through a distributed system architecture.
			PR.PP-P5: Data are processed on local devices.

Categories and Subcategories: Control

CONTROL-P (CT)	**Data Management Processes and Procedures (CT.PO-P):** Policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage data consistent with the organization's risk strategy to protect individuals' privacy.	**CT.PO-P1:** Policies and procedures for authorizing data processing and maintaining authorizations are in place.
		CT.PO-P2: Processes for enabling data review, transmission/disclosure, alteration, or deletion are in place.
		CT.PO-P3: Processes and procedures for enabling individuals' data processing preferences and requests (e.g., individual participation) are in place.
	Data Management (CT.DM-P): Data are managed consistent with the organization's risk strategy to protect individuals' privacy and increase manageability.	**CT.DM-P1:** System or device configurations permit selective collection or disclosure of data elements to allow for implementation of privacy principles (e.g., data minimization).
		CT.DM-P2: Individuals' authorization for the data action is obtained.
		CT.DM-P3: Data elements can be accessed for review.
		CT.DM-P4: Data elements can be accessed for transmission or disclosure.
		CT.DM-P5: Data elements can be accessed for alteration.
		CT.DM-P6: Data elements can be accessed for deletion.
		CT.DM-P7: Metadata containing processing permissions and related data values are transmitted with data elements.
		CT.DM-P8: Processing permissions are transmitted using standardized formats.

Categories and Subcategories: Inform

INFORM-P (IN)	**Transparency Processes and Procedures (IN.TP-P):** Policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to increase transparency of the organization's data processing practices.	**IN.TP-P1:** Transparency procedures and mechanisms (e.g., internal or public reports) for data processing practices are in place.
		IN.TP-P2: Processes for communicating data processing purposes are in place.
	Data Processing Awareness (IN.AW-P): Individuals and organizations have an awareness of data processing practices, and processes and procedures are used and maintained to increase predictability consistent with the organization's risk strategy to protect individuals' privacy.	**IN.AW-P1:** Records of data disclosures are maintained and can be shared.
		IN.AW-P2: Individuals are informed about data processing practices.
		IN.AW-P3: System/product/service design enhances data processing visibility.
		IN.AW-P4: Data sources are informed of data deletion and correction.
		IN.AW-P5: Individuals are informed when data are corrected or deleted.
		IN.AW-P6: Data provenance is maintained and can be shared.
		IN.AW-P7: Data analytic inputs and outputs are understood and evaluated for bias.

Categories and Subcategories: Respond

	RESPOND-P (RS)	**Response Planning (RS.RP-P):** Response processes and procedures are executed and maintained to ensure response to privacy breaches and events.	**RS.RP-P1:** Response plan is executed during or after a privacy breach or event.
		Communications (RS.CO-P): Response activities are coordinated with internal and external stakeholders (e.g., external support from law enforcement agencies).	**RS.CO-P1:** Personnel know their roles and order of operations when a response is needed.
			RS.CO-P2: Privacy breaches and events are reported consistent with established criteria.
			RS.CO-P3: Information is shared consistent with response plans.
			RS.CO-P4: Coordination with stakeholders occurs consistent with response plans.
			RS.CO-P5: Data for voluntary information sharing is restricted to what is necessary for understanding the privacy breach or event.
			RS.CO-P6: Impacted individuals are notified about a privacy breach or event.

Categories and Subcategories: Respond

RESPOND-P (RS)	**Mitigation (RS.MI-P):** Activities are performed to prevent expansion of, mitigate, and resolve privacy breaches and events.	**RS.MI-P1:** Privacy breaches and events are contained.
		RS.MI-P2: Privacy breaches and events are mitigated.
		RS.MI-P3: Newly identified problematic data actions are mitigated or documented as accepted risks.
	Improvements (RS.IM-P): Organizational privacy practices are improved by incorporating lessons learned from privacy breaches and events.	**RS.IM-P1:** Policies and processes incorporate lessons learned.
	Redress (RS.RE-P): Organizational response activities include processes or mechanisms to address impacts to individuals that arise from data processing.	**RS.RE-P1:** Processes for receiving and responding to complaints, concerns, and questions from individuals about organizational privacy practices are in place.
		RS.RE-P2: Individuals are provided with mitigation mechanisms.

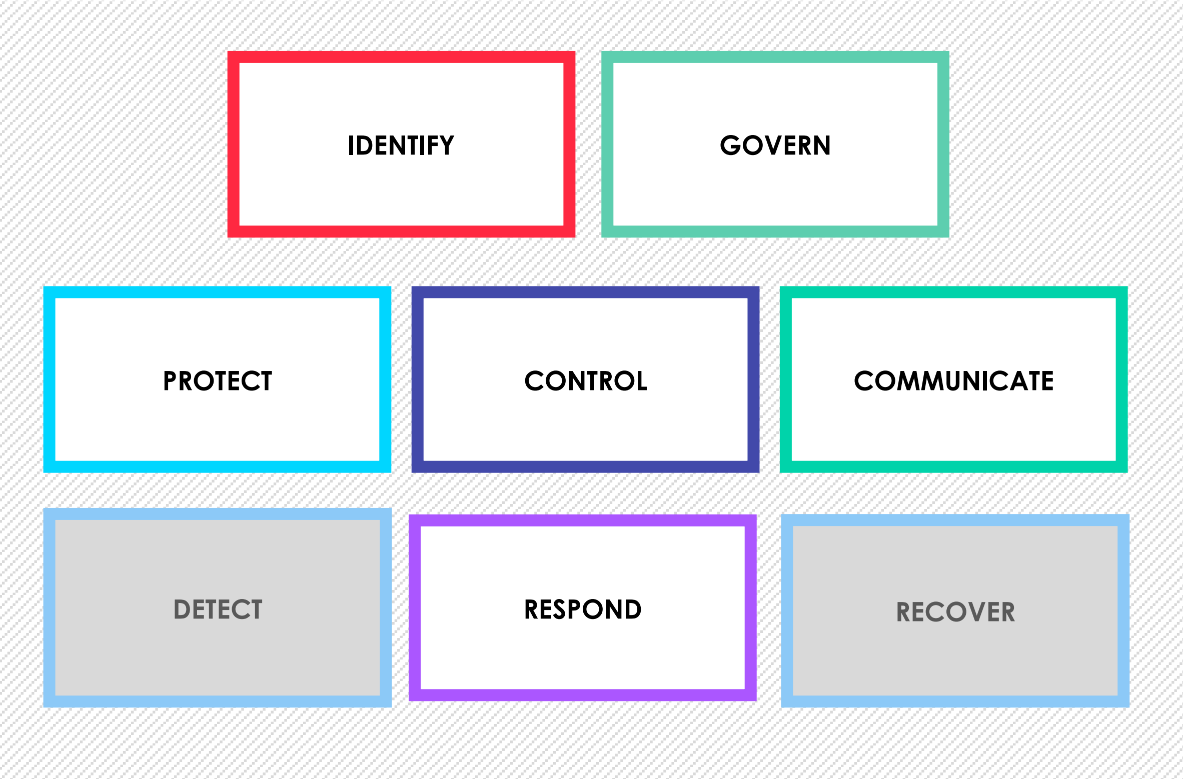
Preview of Supplemental Materials to the Privacy Framework Discussion Draft

Supplemental Materials

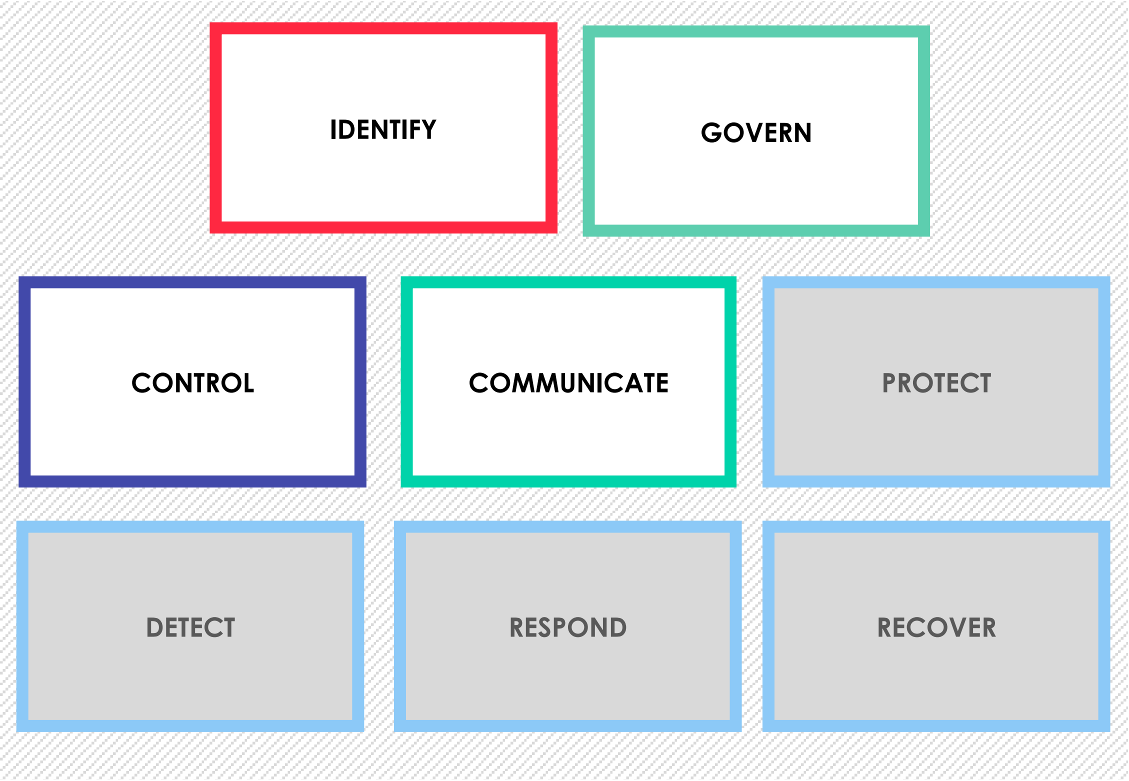
- Draft Executive Summary
- Hypothetical Use Case Profiles
- Proposed Roadmap Topic Areas
- Two Proposed Cores: Integrated and Separated Versions

Two Proposed Cores

Integrated Core



Separated Core



Resources

Website

https://nist.gov/privacyframework

Mailing List

https://groups.google.com/a/list.nist.gov/forum/#!forum/privacyframework

Contact Us

PrivacyFramework@nist.gov

@NISTcyber #PrivacyFramework