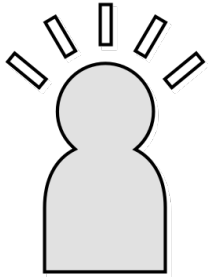


NIST Privacy Framework Preliminary Draft October 2019

Collaborative Development

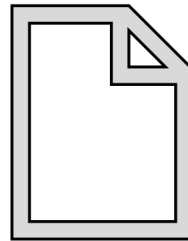
Starting Point

Attributes



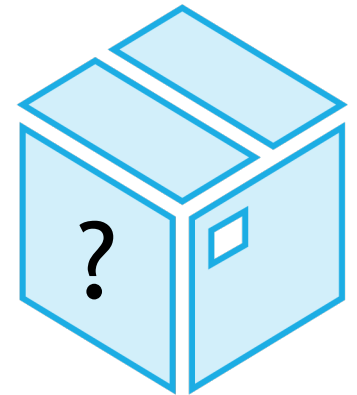
Current State

Preliminary Draft



Version

1.0



2

public
comment
periods

3

public
workshops

5

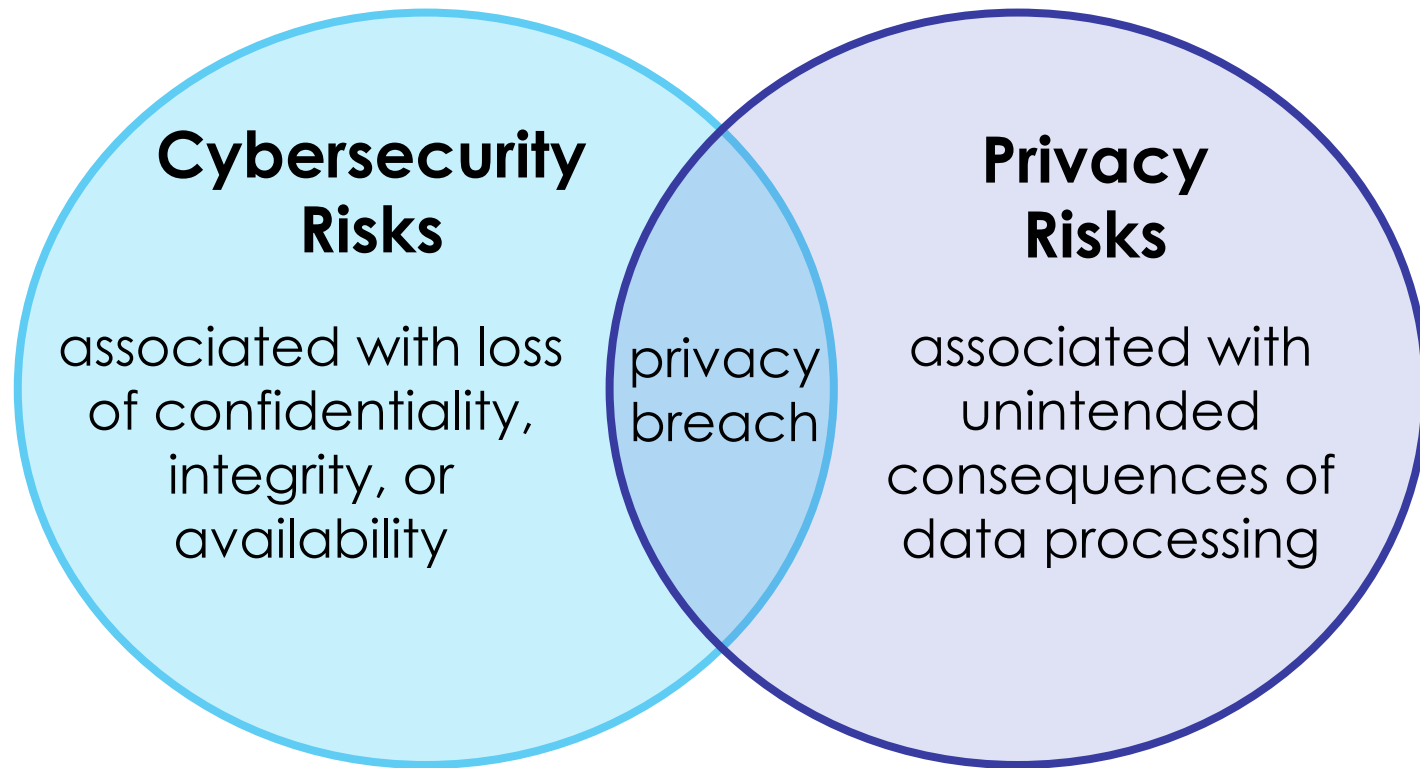
webinars

ongoing

stakeholder
engagement

Privacy Risk Management

Relationship Between Cybersecurity and Privacy Risk



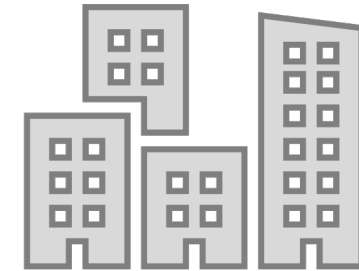
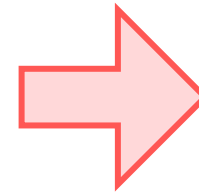
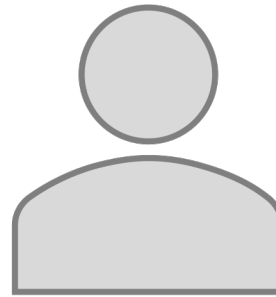
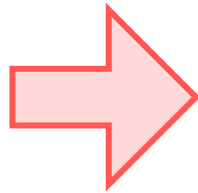
Data: A representation of information, including digital and non-digital formats

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

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

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

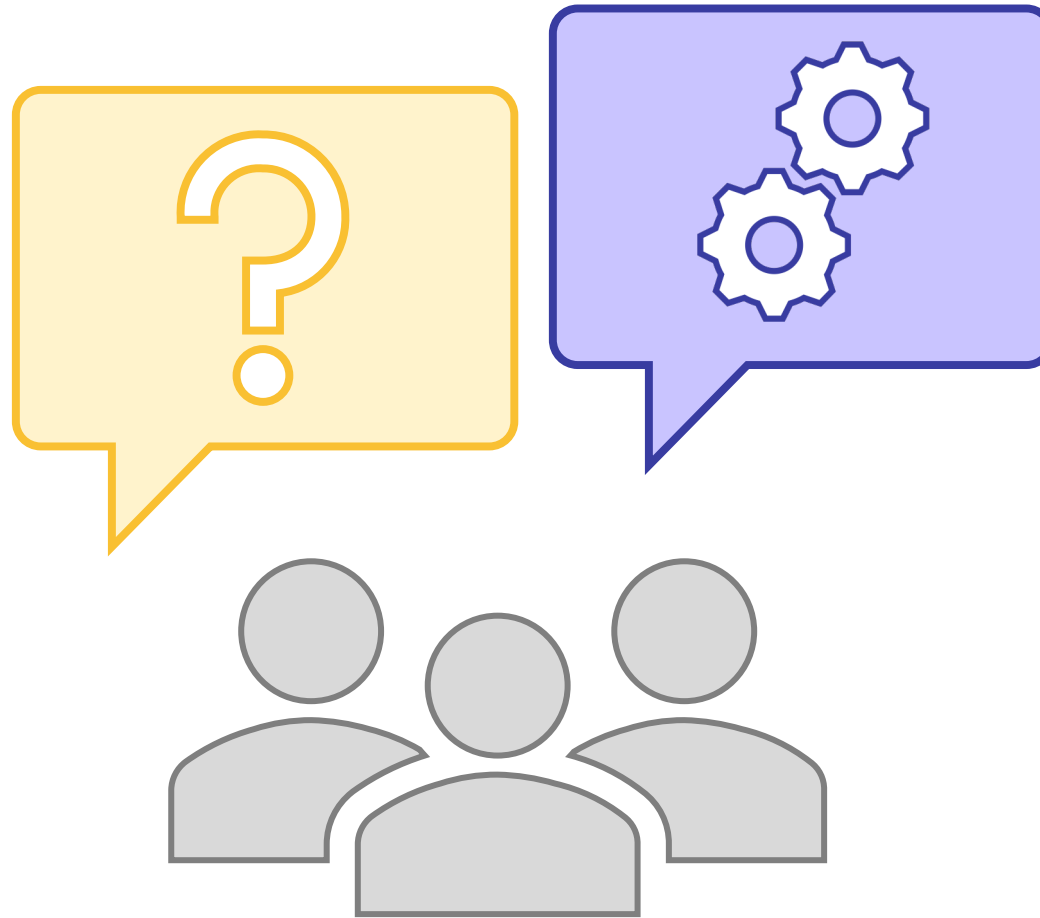
Individual

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



Appendix D: Key Privacy Risk Management Practices



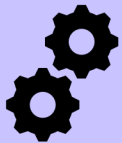
Organizing
Preparatory
Resources



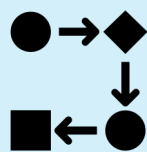
Determining Privacy
Capabilities



Defining Privacy
Requirements



Conducting Privacy
Risk Assessments



Creating Privacy
Requirements
Traceability



Monitoring Changing
Privacy Risks

Privacy Framework Components

Privacy Framework Structure



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



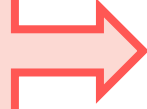
Profiles are a selection of specific Functions, Categories, and Subcategories from the Core that the organization has prioritized to help it manage privacy risk



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

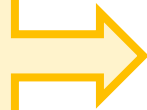
Core: Functions

Identify-P



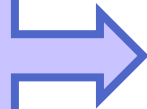
Develop the organizational understanding to manage privacy risk for individuals arising from data processing.

Govern-P



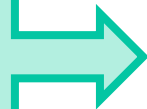
Develop and implement the organizational governance structure to enable an ongoing understanding of the organization's risk management priorities that are informed by privacy risk.

Control-P



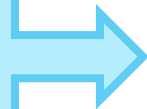
Develop and implement appropriate activities to enable organizations or individuals to manage data with sufficient granularity to manage privacy risks.

Communicate-P



Develop and implement appropriate activities to enable organizations and individuals to have a reliable understanding about how data are processed and associated privacy risks.

Protect-P



Develop and implement appropriate data processing safeguards.

Example Categories

ID-P

Inventory and Mapping (ID.IM-P)

Data processing by systems, products, or services is understood and informs the management of privacy risk.

GV-P

Governance Policies, Processes, and Procedures (GV.PP-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.

CT-P

Data 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).

CM-P

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.

PR-P

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.

Example Subcategories

ID-P	ID.IM-P	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.

GV-P	GV.PP-P	GV.PP-P5
------	---------	-----------------

Legal, regulatory, and contractual requirements regarding privacy are understood and managed.

CT-P	CT.DM-P	CT.DM-P4
------	---------	-----------------

Data elements can be accessed for deletion.

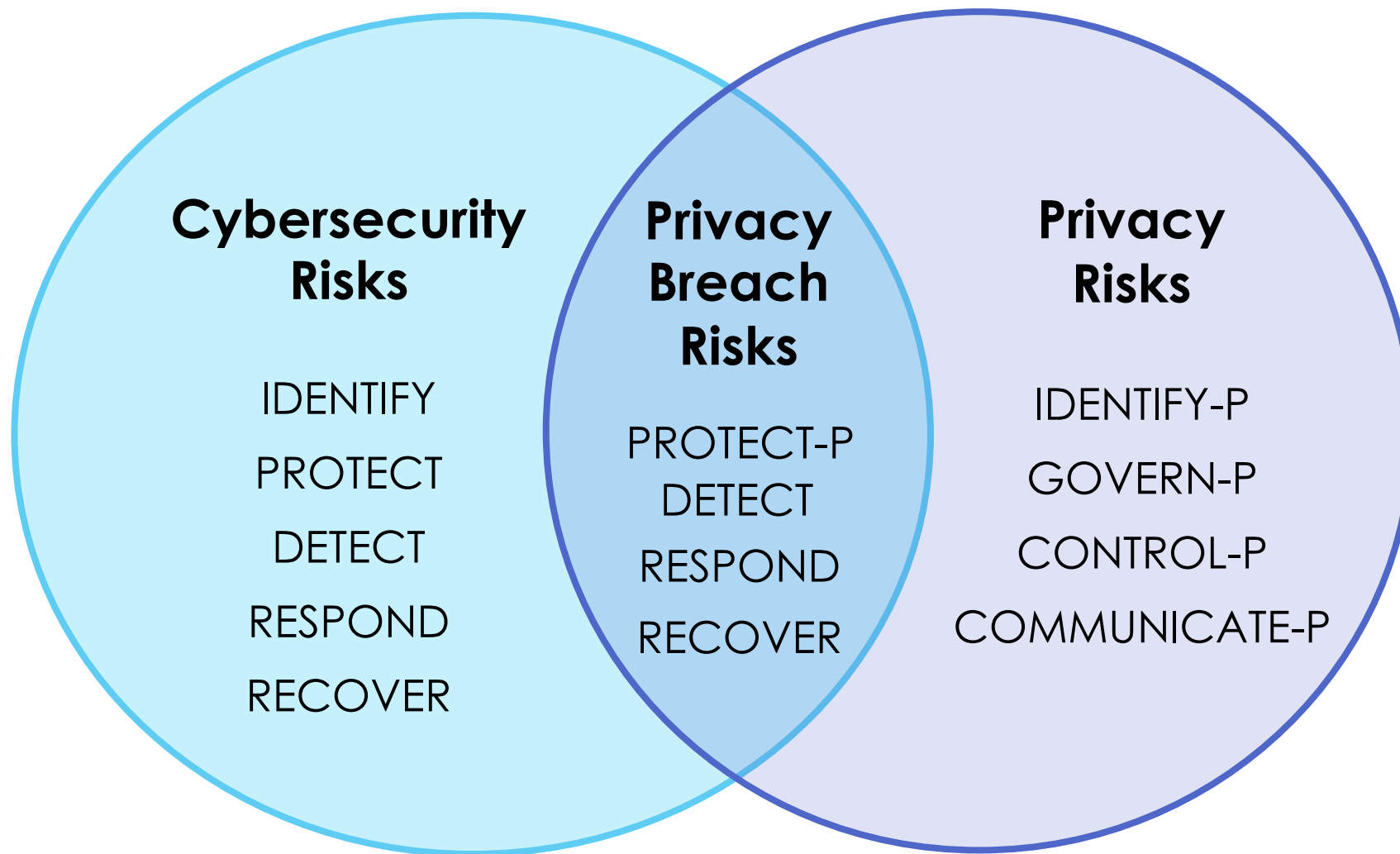
CM-P	CM.AW-P	CM.AW-P1
------	---------	-----------------

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.

PR-P	PR.DS-P	PR.DS-P1
------	---------	-----------------

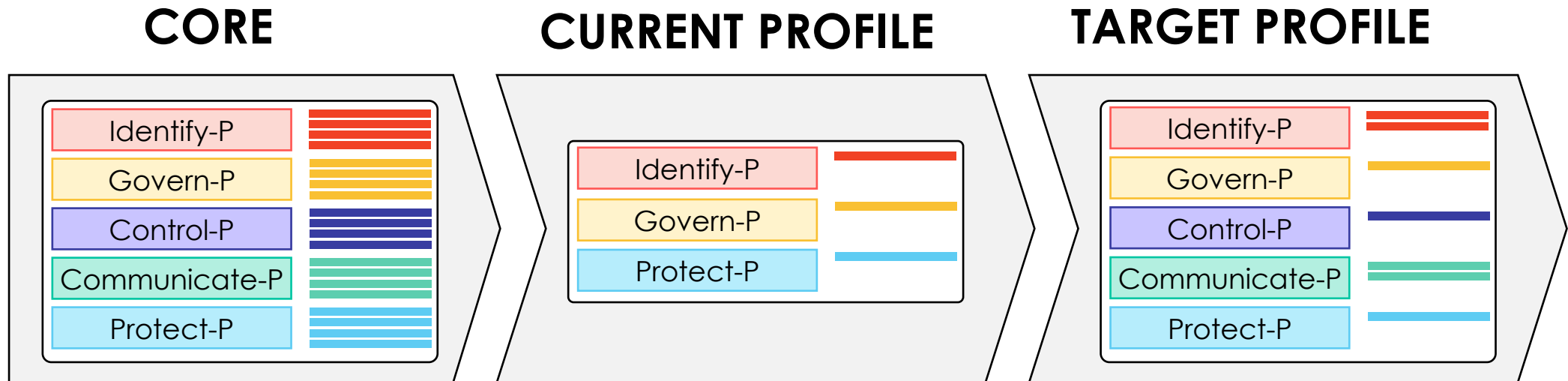
Data-at-rest are protected.

Cybersecurity Framework Alignment

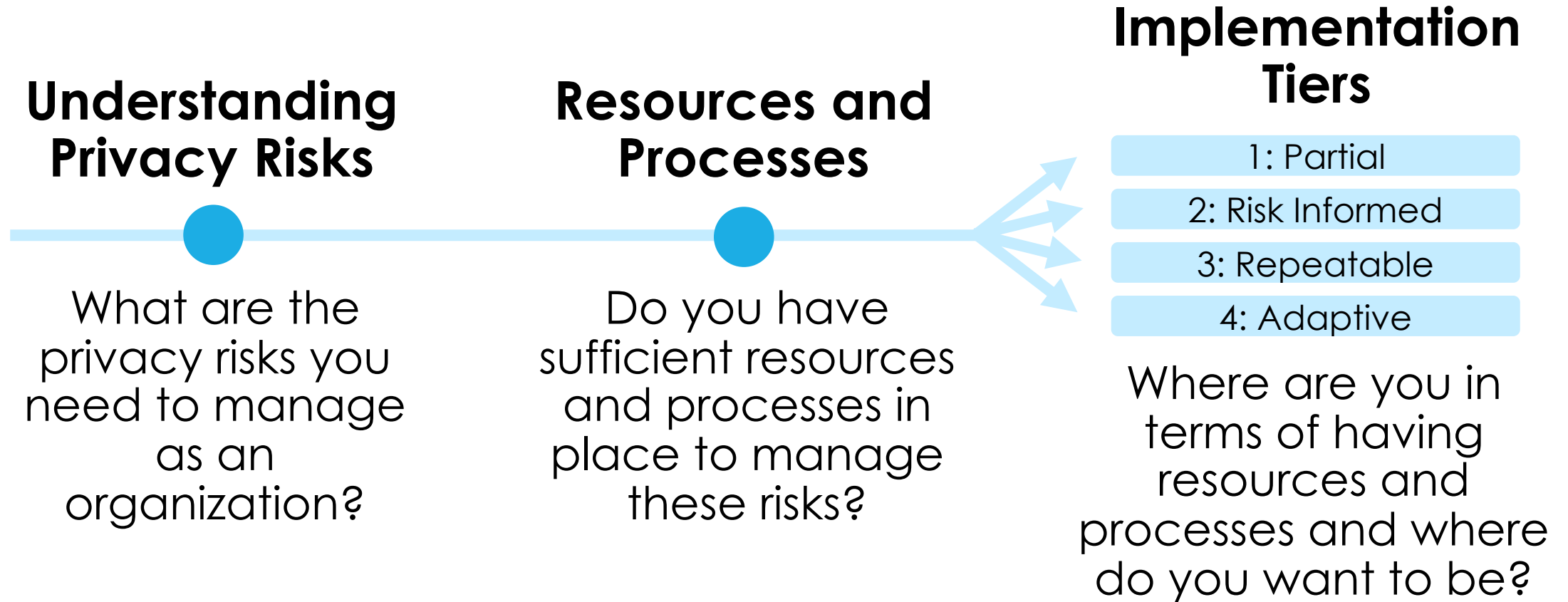


Profiles

- Organizational or industry sector goals
- Legal/regulatory requirements & industry best practices
- Organization's risk management priorities
- Privacy needs of individuals



Implementation Tiers



Value Proposition

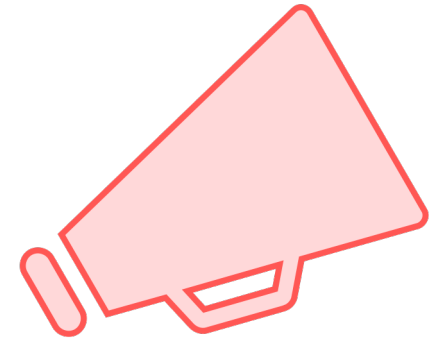
Privacy Framework supports:



Building
customer
trust

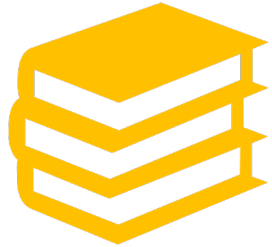


Fulfilling current
compliance
obligations



Facilitating
communication

How to Use the Privacy Framework



Informative
References



Strengthening
Accountability



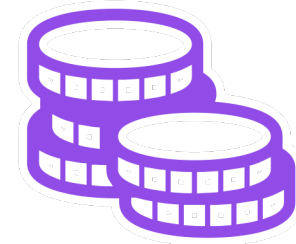
Establishing or Improving
a Privacy Program



Applying to the
System Development
Life Cycle

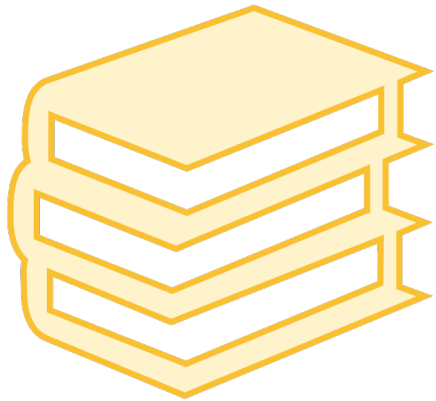


Using within the Data
Processing Ecosystem



Informing Buying
Decisions

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 Subcategories to relevant NIST guidance
- NIST will develop a process for accepting external informative references

Next Steps

Laying the Groundwork for the Future

Seeking to improve and overcome challenges around:

- Mechanisms to provide confidence
- Emerging technologies
- Privacy risk assessment
- Privacy workforce
- Re-identification risk
- Technical standards



Adopt me!

- **Trial run** – share insights as feedback
- **V1 use pledge** – lead on privacy
- **NIST repository** – provide use cases and informative references



Submit Comments

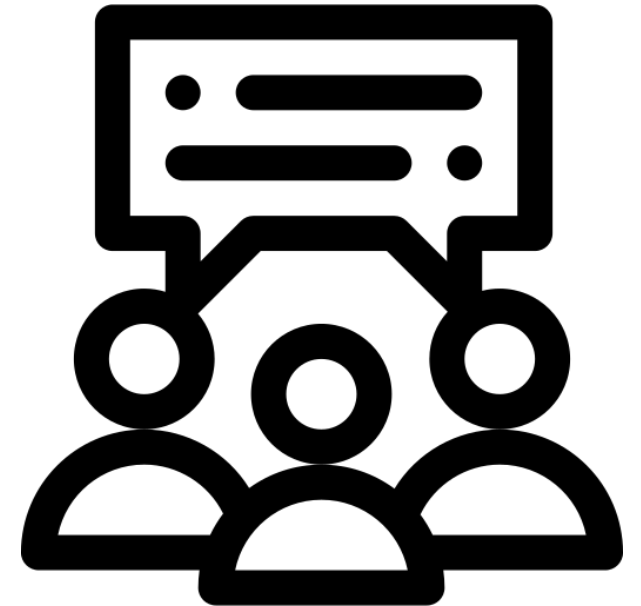
Comment period closes **October 24, 2019 at 5:00 PM ET**

Comments will be posted publicly on Privacy Framework website

Key areas for feedback

Do the outcomes:

- cover existing practices;
- strengthen individuals' privacy protection;
- enable effective organizational use;
- support enterprise mission/business objectives; and
- facilitate compliance with applicable laws or regulations?



Resources



Website

<https://www.nist.gov/privacyframework>



Mailing List

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



Contact Us

PrivacyFramework@nist.gov

[@NISTcyber](#) [#PrivacyFramework](#)