

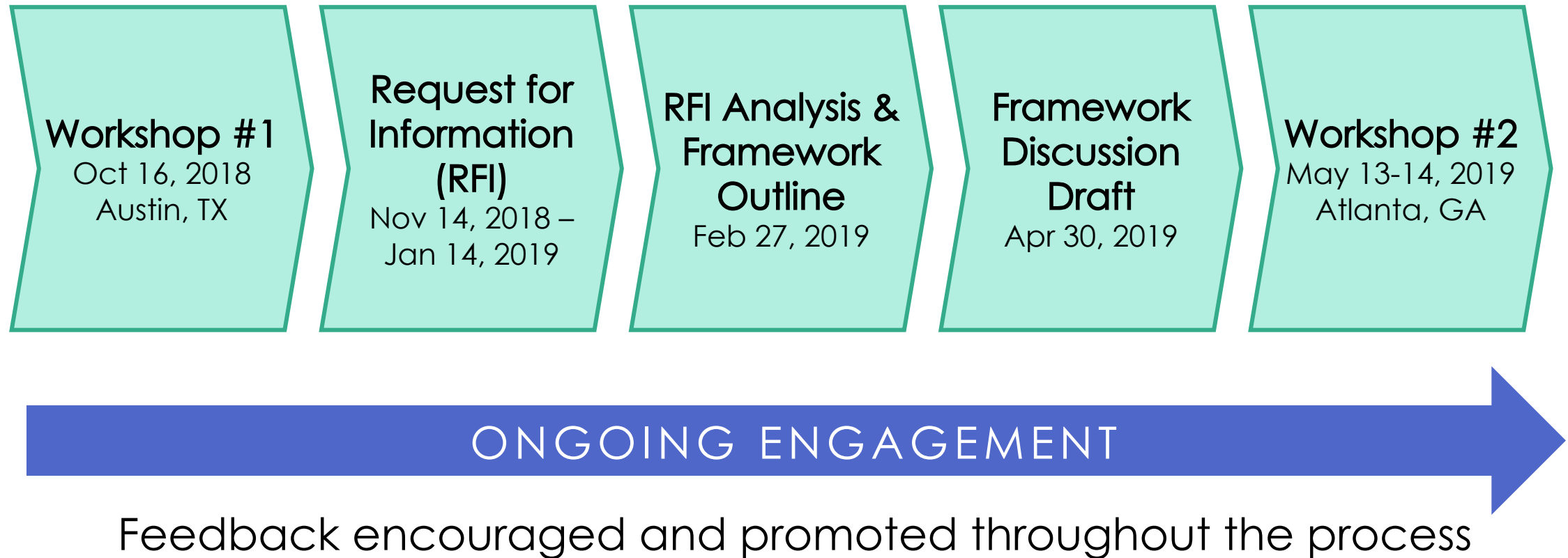
WEBINAR
NIST Privacy Framework
Discussion Draft
May 28, 2019

Why NIST?

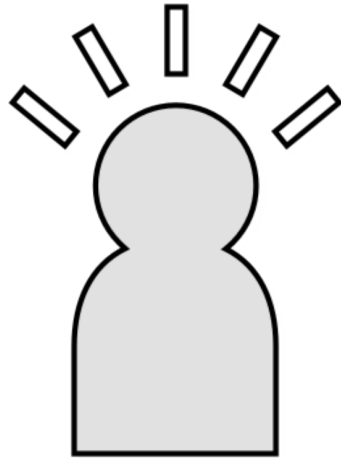
- Long track record of successfully, collaboratively working with public and private sectors
- Experience developing the Cybersecurity Framework
- Extensive privacy expertise



Process to Date

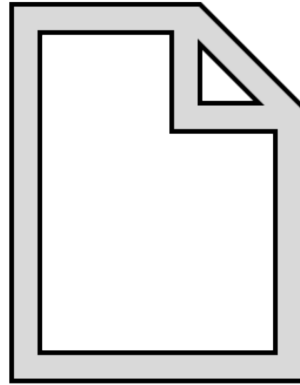
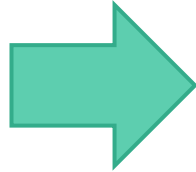


NIST Privacy Framework: What is it?

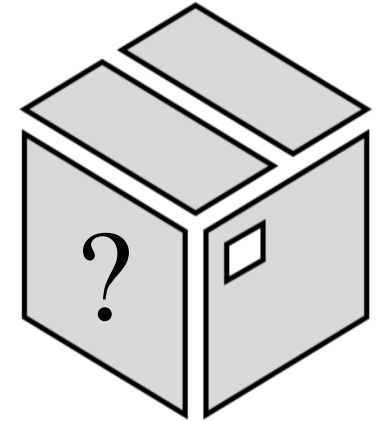
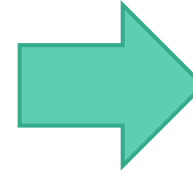


Attributes:

- 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?"

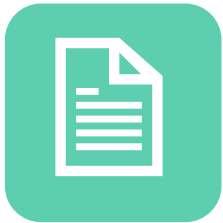
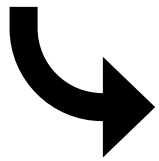


future state:
NIST Privacy
Framework version
1.0

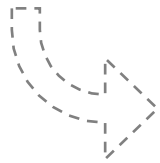
Framework Development Stages



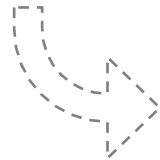
Working Outline – February 2019



Discussion Draft – April 2019



Preliminary Draft – Anticipated
July/August 2019



Version 1.0 – Anticipated
October 2019

Upcoming Opportunities to Engage

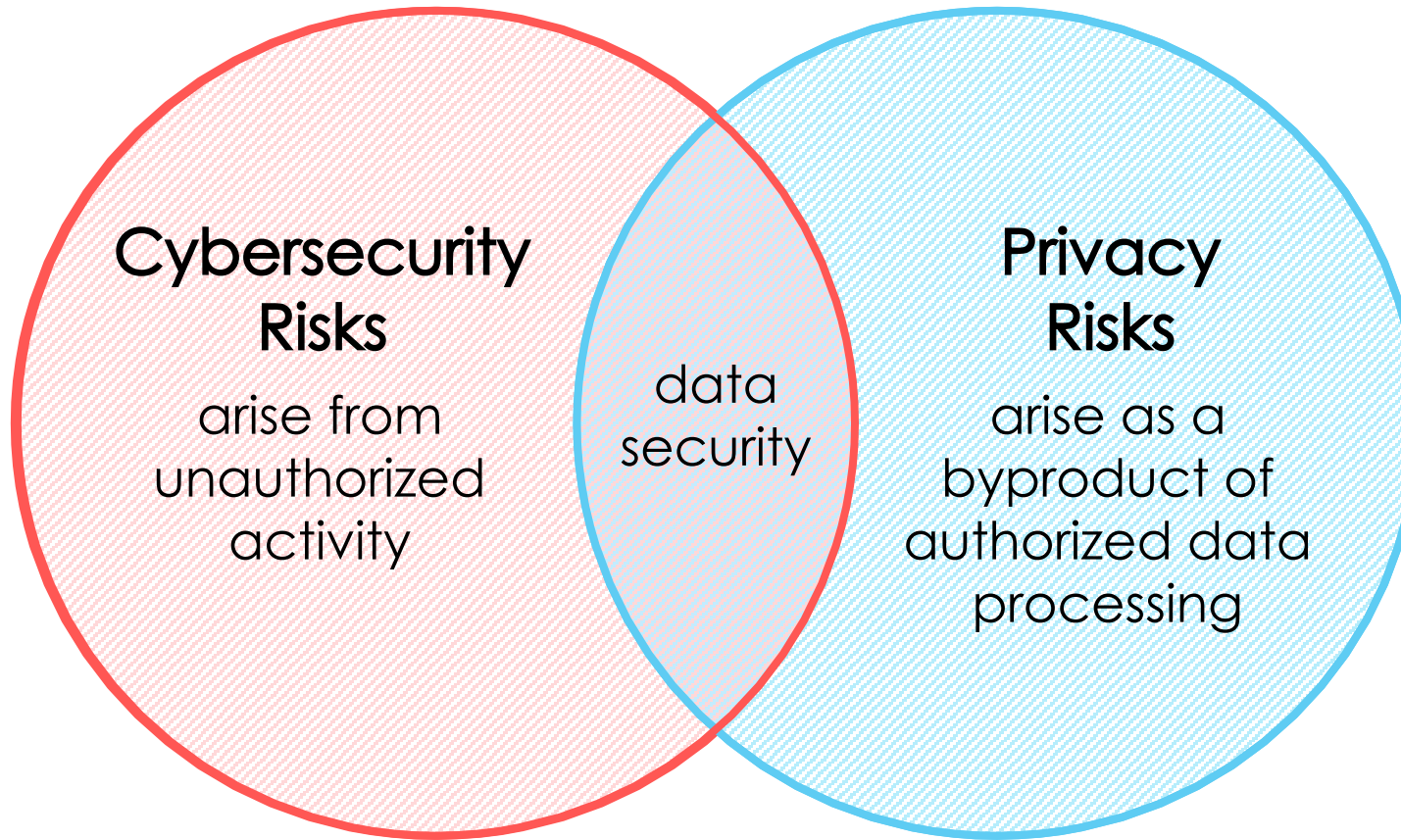


Getting to V1.0 of the NIST Privacy Framework: Workshop #3

July 8-9, 2019 | Boise, Idaho

Review of NIST Privacy Framework Discussion Draft

Relationship Between Cybersecurity and Privacy Risk



- 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

Relationship between 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



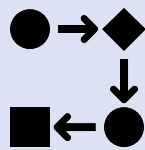
Determining Privacy
Capabilities



Defining Privacy
Requirements



Conducting Privacy
Risk Assessments

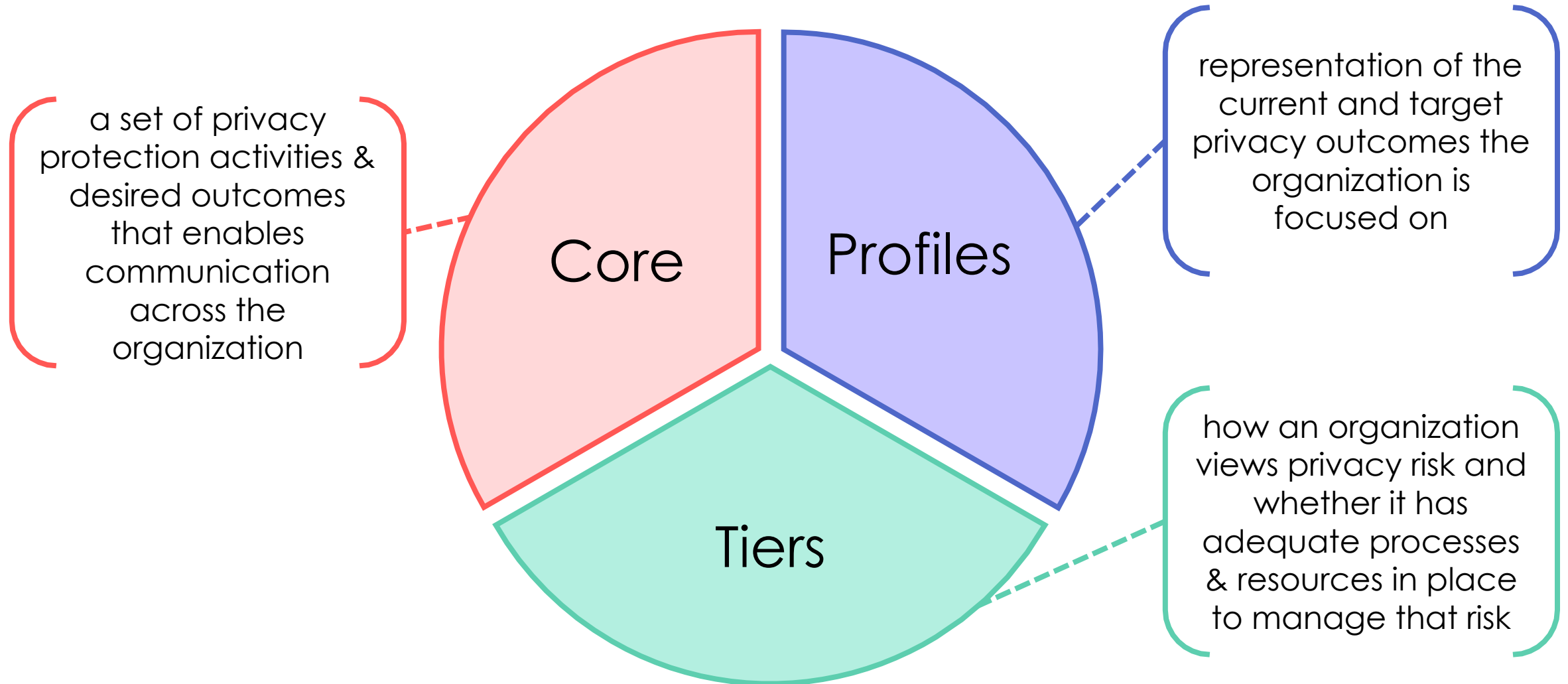


Creating Privacy
Requirements
Traceability



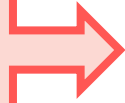
Monitoring Changing
Privacy Risks

Privacy Framework Structure



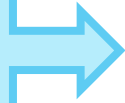
Core Functions

Identify (ID)



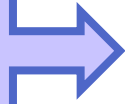
Develop the organizational understanding to manage privacy risk for individuals arising from data processing or their interactions with systems, products, or services.

Protect (PR)



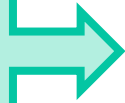
Develop and implement appropriate data processing safeguards.

Control (CT)



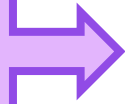
Develop and implement appropriate activities to enable organizations or individuals to manage data with sufficient granularity to manage privacy risks.

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.

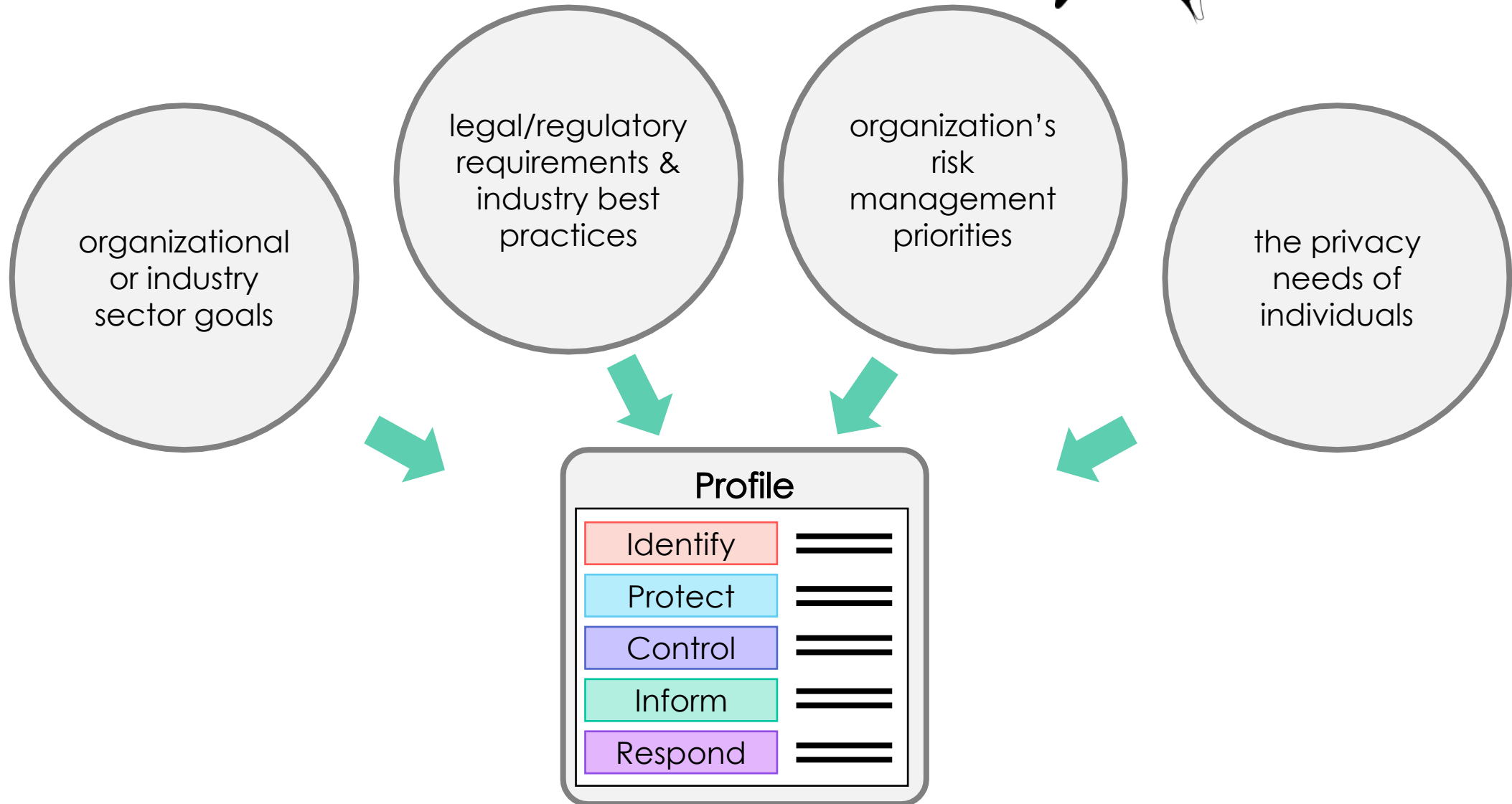
Example Core Categories

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.

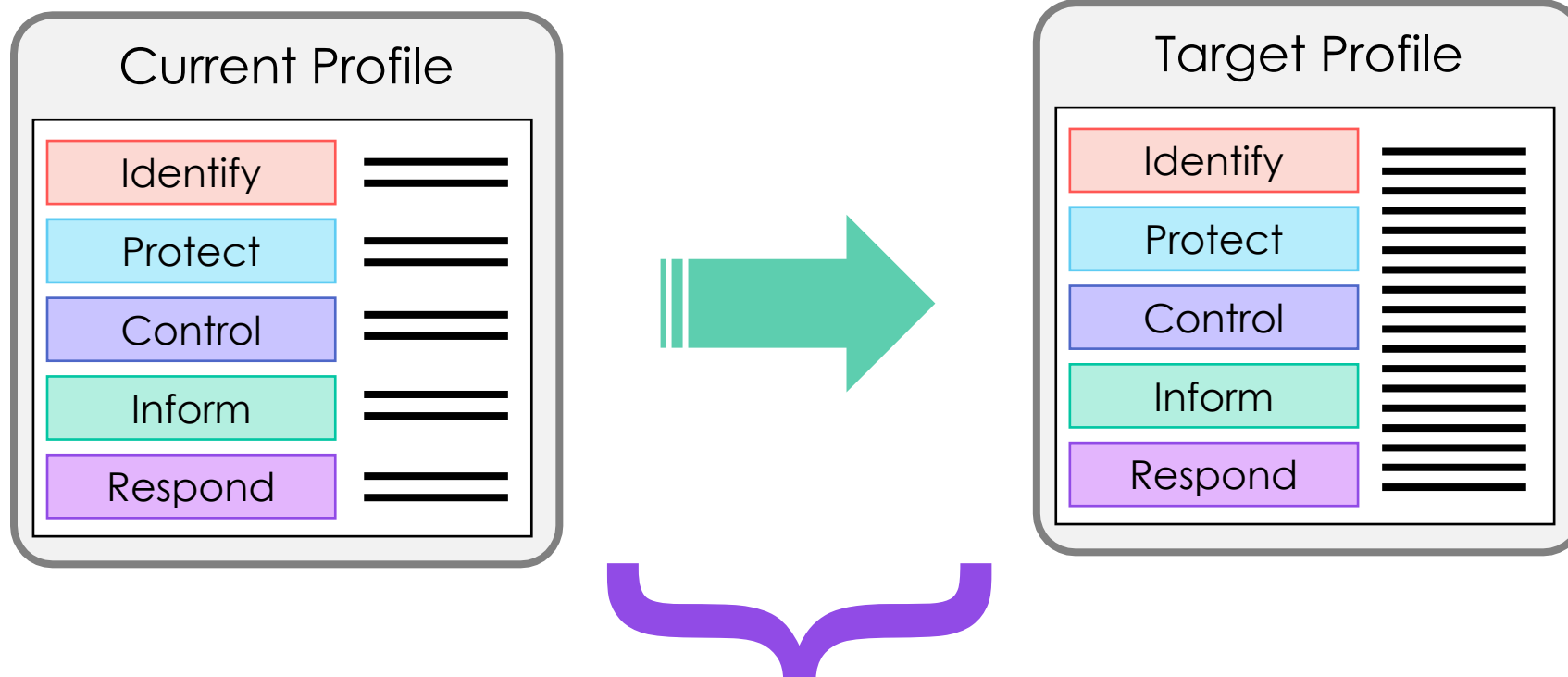
Example Core Subcategories

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.

Privacy Framework Profiles

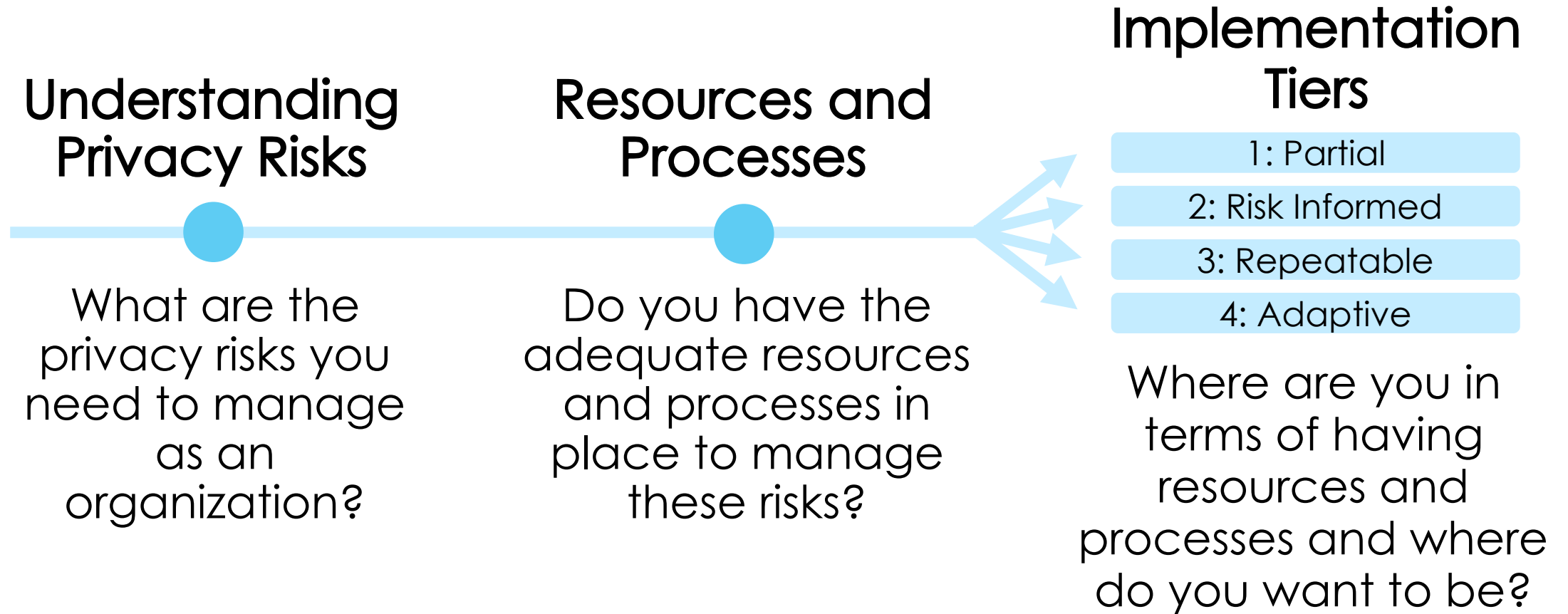


Current and Target Profiles



- 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



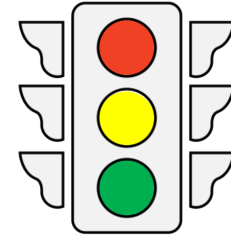
How to Use the Privacy Framework



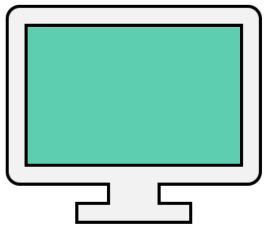
Strengthening
Accountability



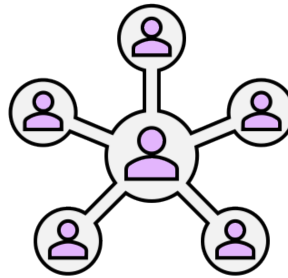
Basic Review of
Privacy Practices



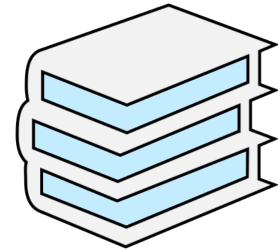
Establishing or Improving
a Privacy Program



Application in the
System Development
Life Cycle

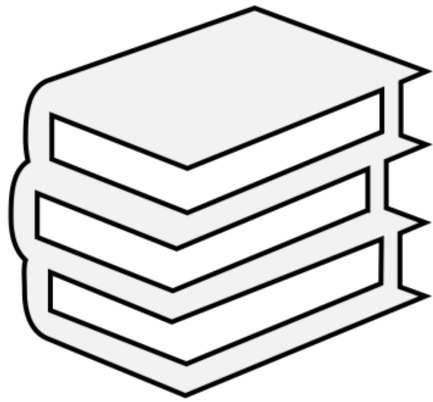


Communicating Privacy
Requirements with
Stakeholders



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

Roadmap



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](#)