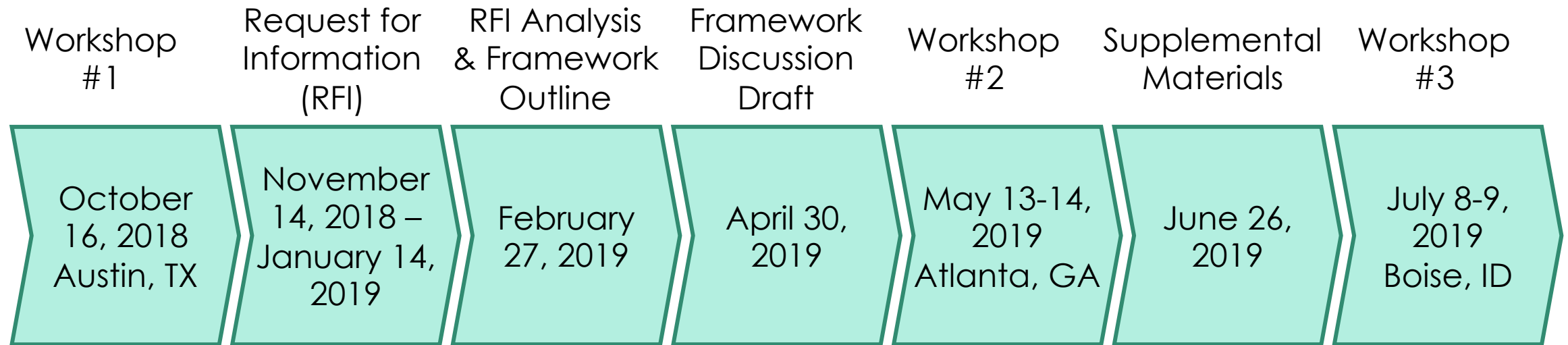


**Getting to V1.0 of the  
NIST Privacy Framework:  
Workshop #3  
July 8, 2019**

# Process to Date



Feedback encouraged and promoted throughout the process

# Materials for Working Sessions

Sessions 1-3 and 6

Draft  
Executive  
Summary

Updated  
Cores

Integrated  
version

Separated  
version

Sessions 4-5

Roadmap  
Topics

Hypothetical  
Profiles

# WORKSHOP OBJECTIVE #1

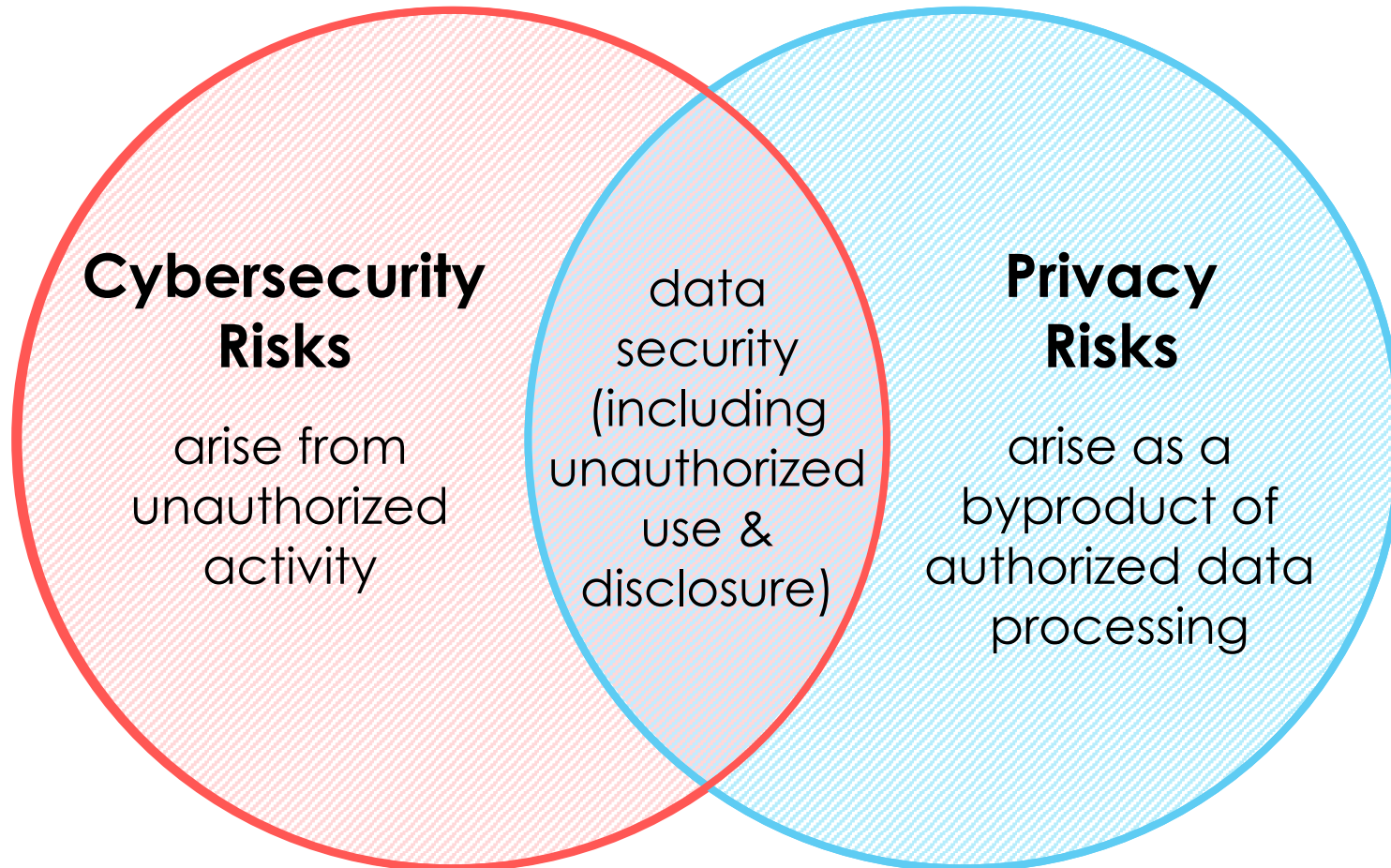
Material: Draft Executive Summary

**Purpose, value, & scope**

# Value

The Privacy Framework provides a **shared lexicon** and is a practical tool that can assist organizations—even those fully compliant with relevant laws or regulations—in making **ethical decisions** when designing or deploying their products and services and **avoiding losses of trust** that damage their reputations and can slow adoption or cause abandonment of these products and services.

# Relationship Between Cybersecurity and Privacy Risk



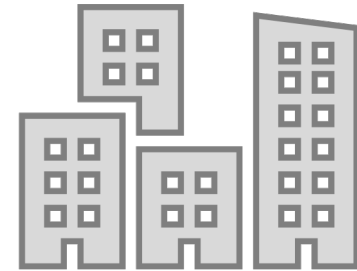
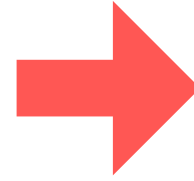
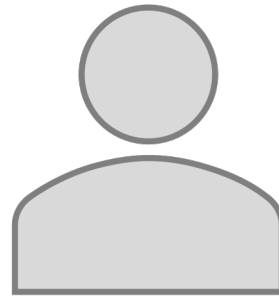
**Data:** A representation of information, including digital and non-digital formats, with the potential for adverse consequences for individuals when processed

**Data Action:** A system/product/service operation that processes data

**Data Processing:** An operation or set of operations performed upon data across the full 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

# Privacy Risk and Organizational Risk



## Problem

arises from data processing

## Individual

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

## Organization

experiences secondary impact  
(e.g., customer abandonment, noncompliance costs, harm to reputation)

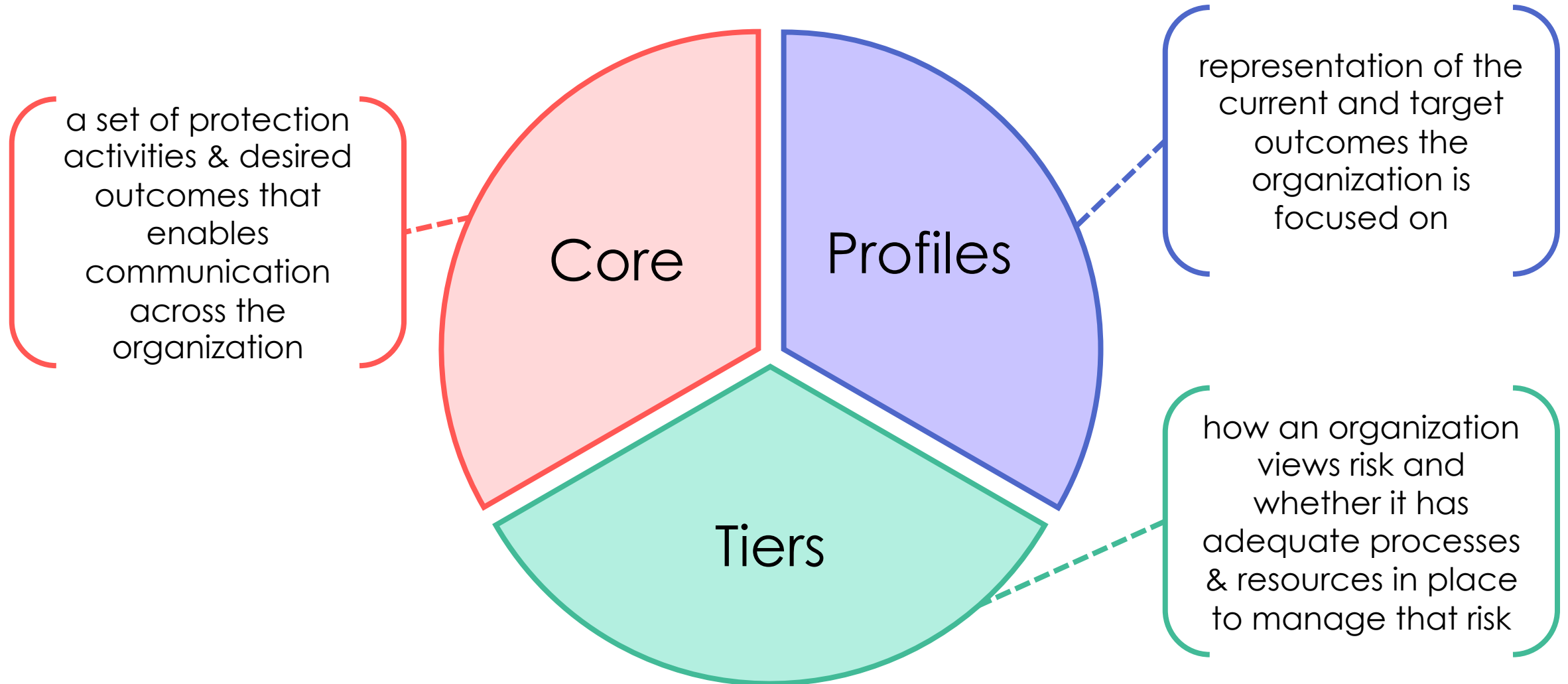
# WORKSHOP OBJECTIVE #2

Material: Updated Cores

**Risk-based & flexible**

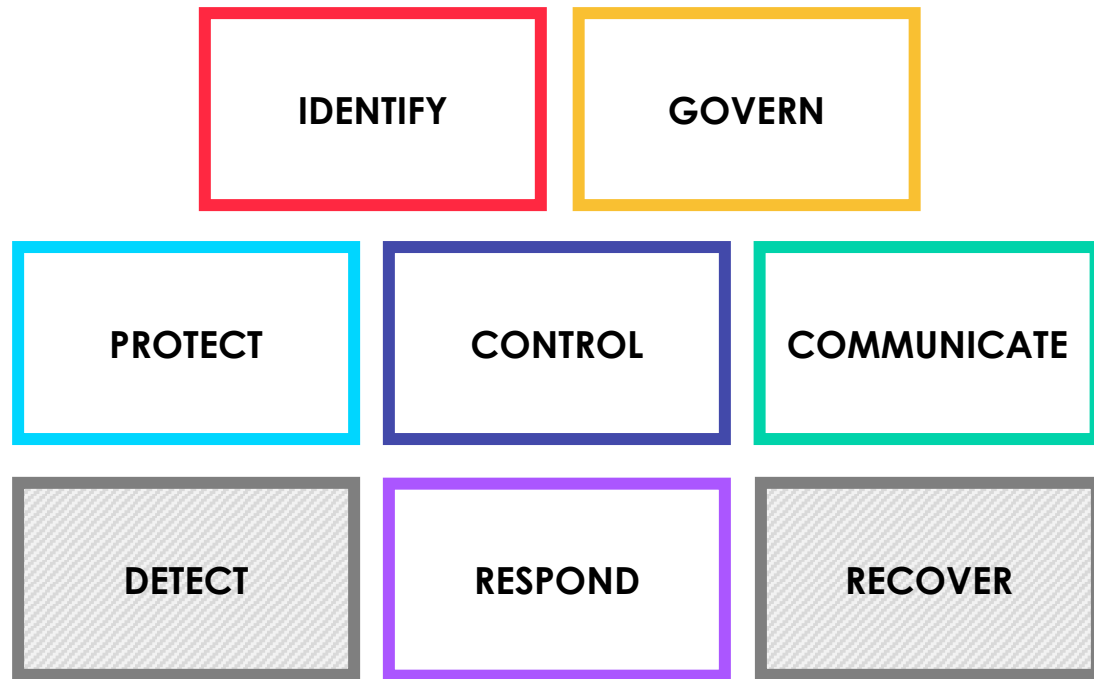


# Privacy & Cybersecurity Framework Alignment

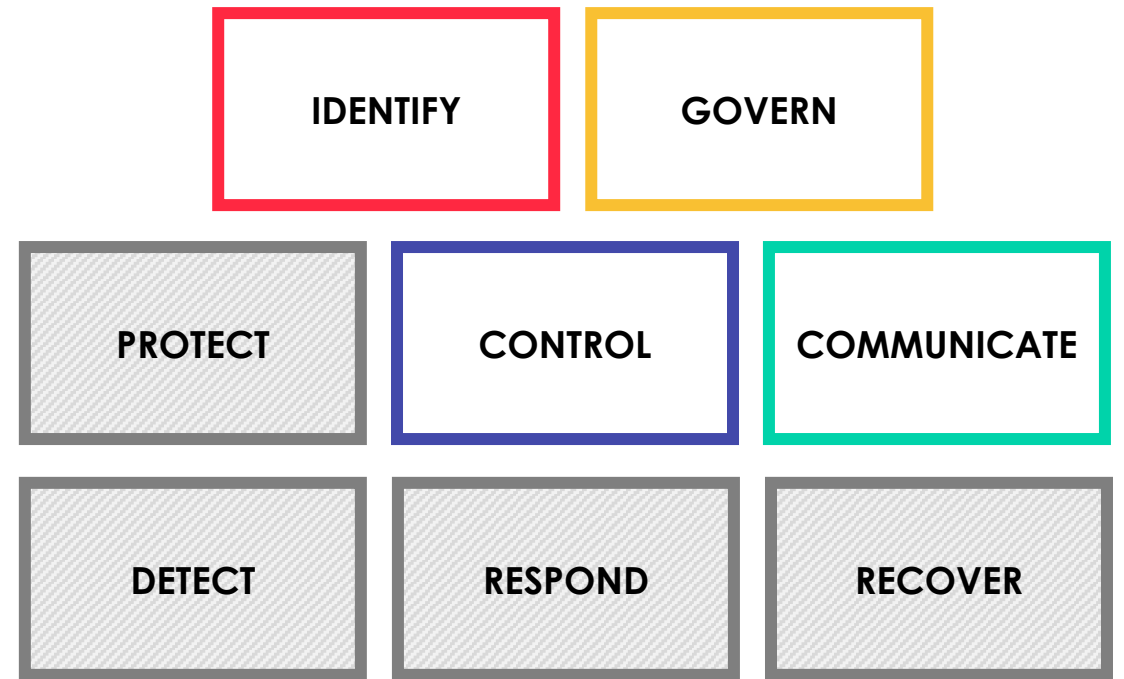


# Two Proposed Cores

## Integrated Core



## Separated Core



# Flexible Implementation

**Not a checklist:** organizations may not need to achieve every outcome or activity reflected in the Core

**Partial achievement:** organizations are not obligated to achieve an outcome in its entirety

**Bundling:** organizations may need to consider multiple outcomes in combination to appropriately manage privacy risk

**Order:** table format of Core is not intended to suggest an implementation order or degree of importance

# WORKSHOP OBJECTIVE #3

Material: Hypothetical Profiles

**Accessibility & efficacy for  
bridging communication  
gaps**

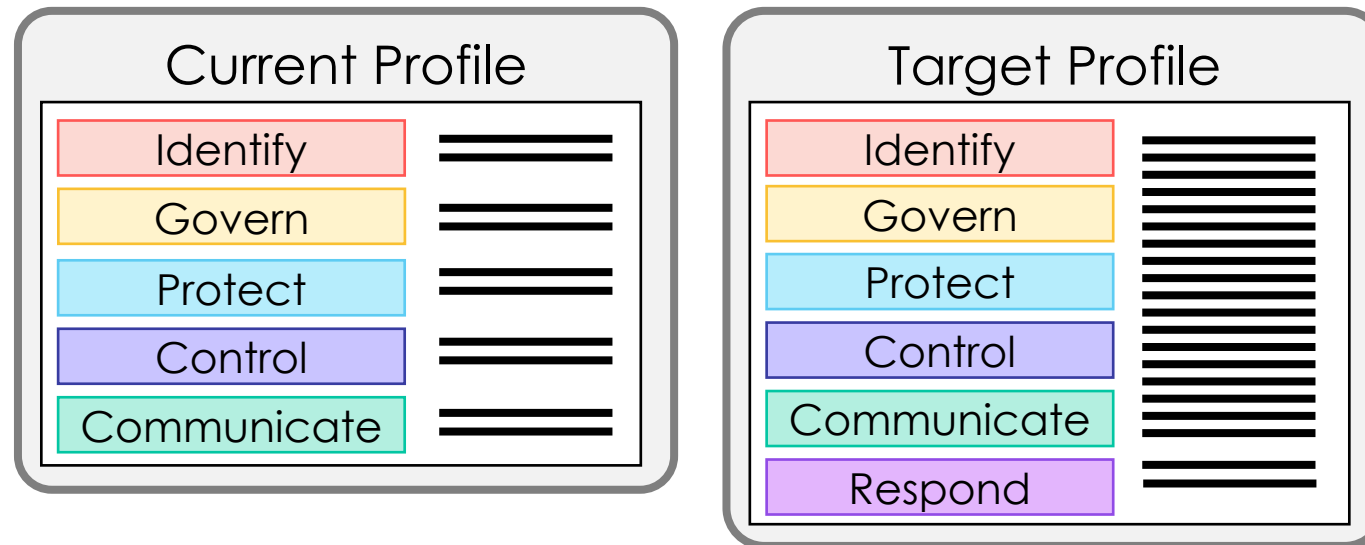
# Finding Yourself in the Core



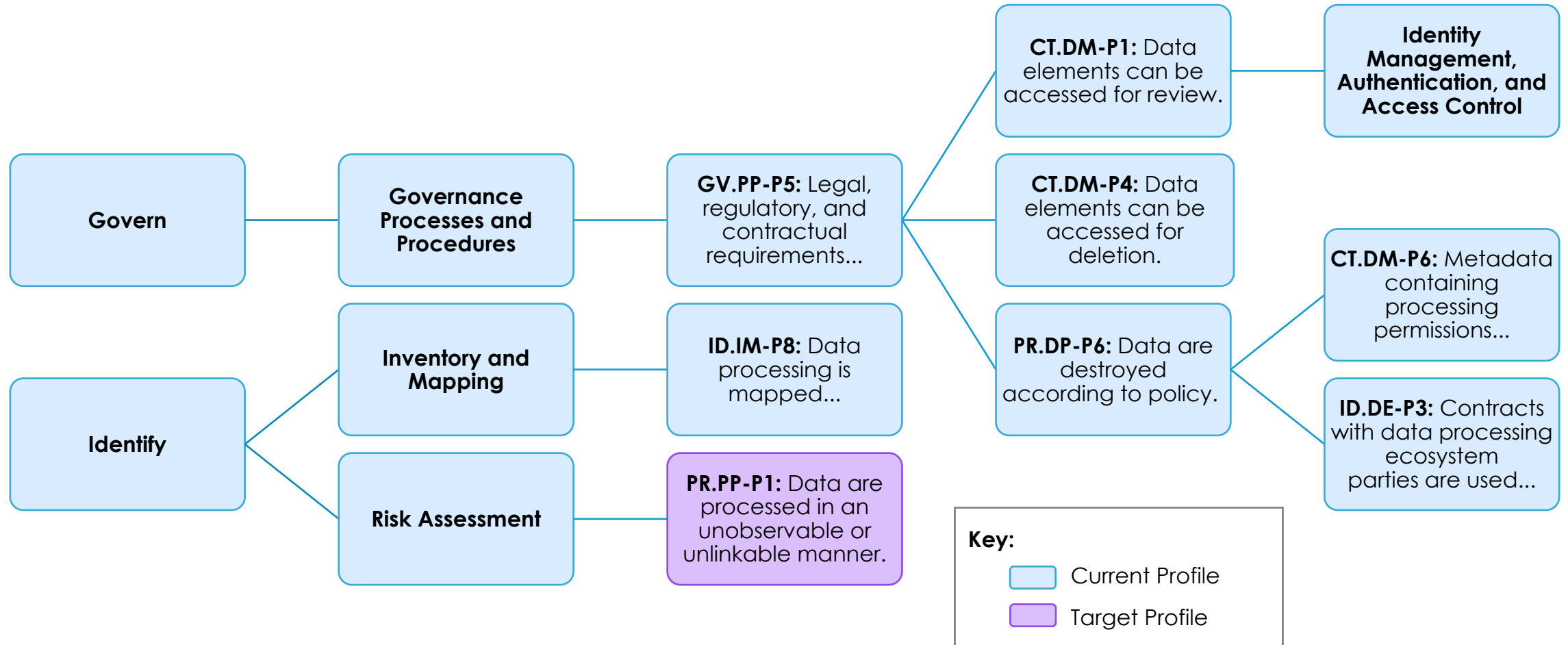
# Collaboration & Profile Development

cross-functional  
collaboration

- organizational or industry sector goals
- legal/regulatory requirements & industry best practices
- organization's risk management priorities
  - the privacy needs of individuals



# Hypothetical Partial Profile



# WORKSHOP OBJECTIVE #4

Material: Roadmap Topics

**Gap areas & needs**



# 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



# Resources



## Website

<https://nist.gov/privacyframework>



## Mailing List

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



## Contact Us

[PrivacyFramework@nist.gov](mailto:PrivacyFramework@nist.gov)

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