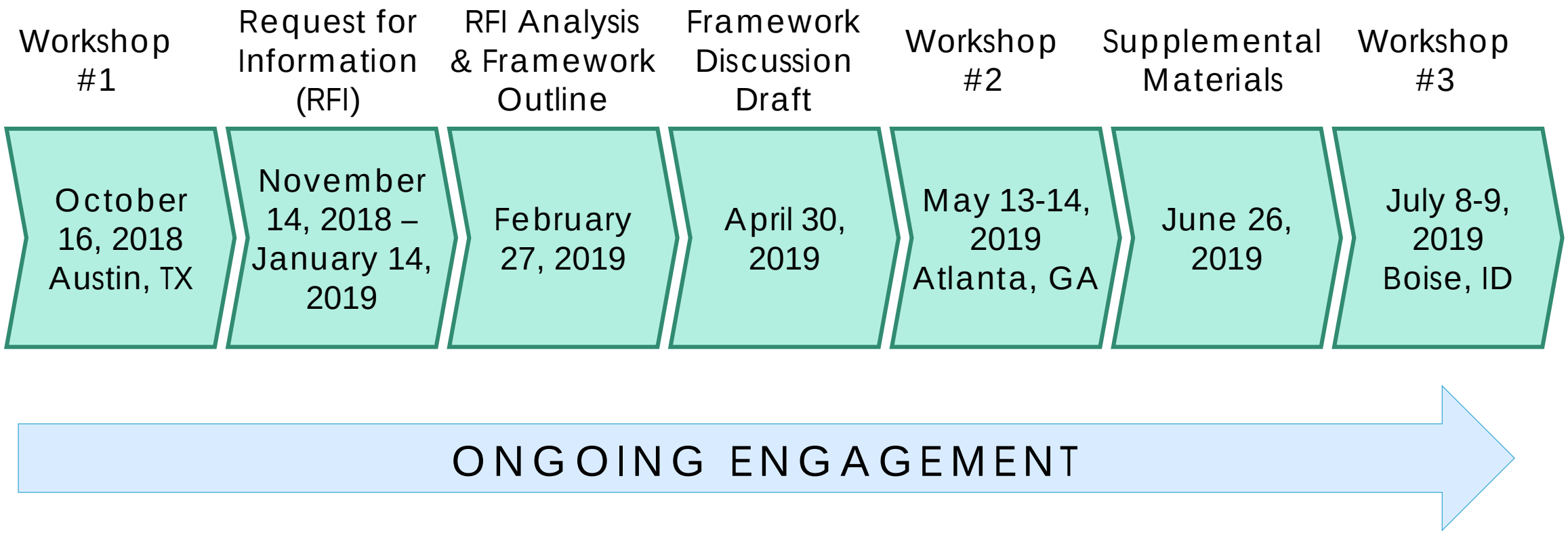
NIST Privacy Framework

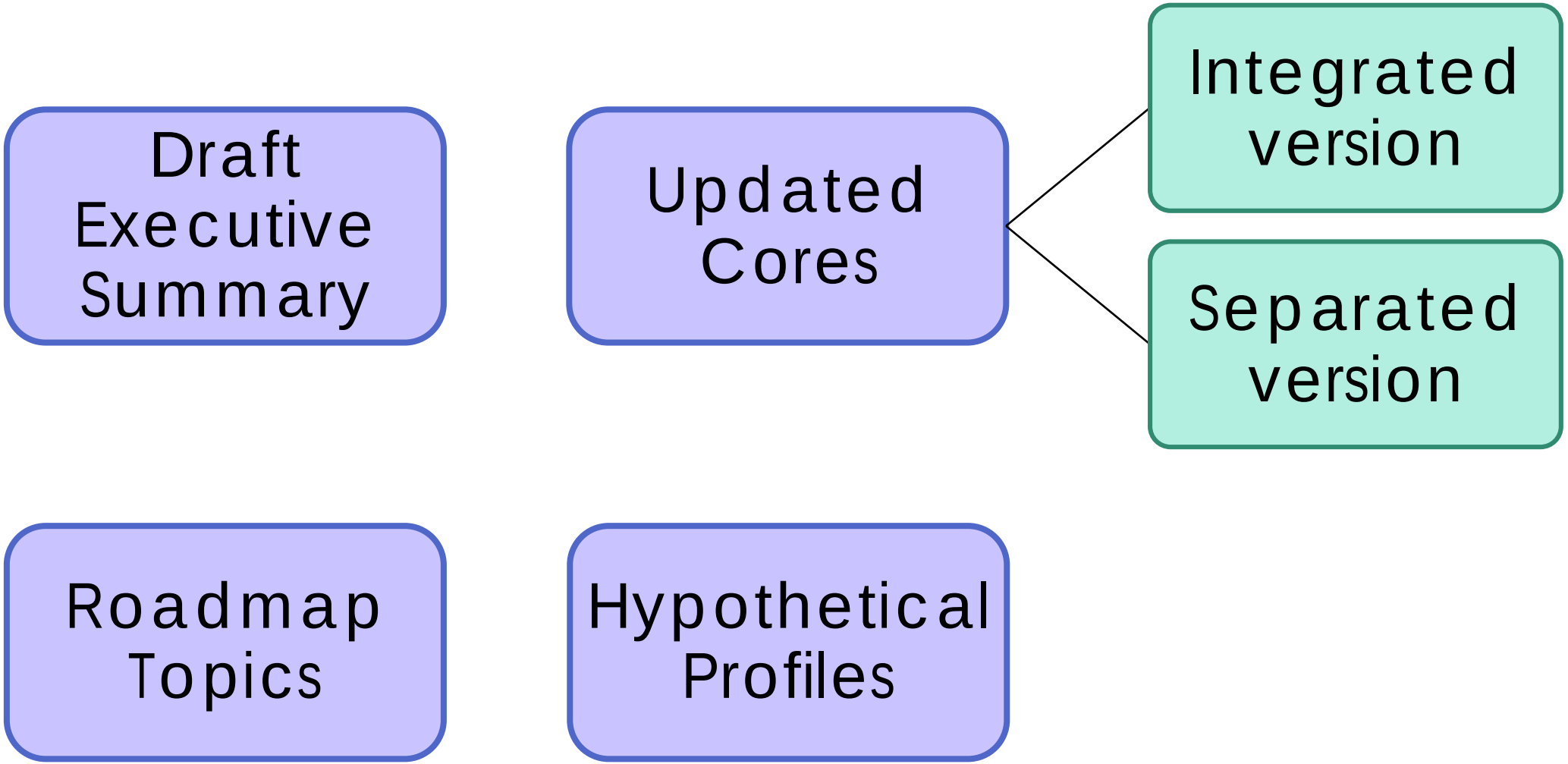
August 2019

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

Process to Date



Supplemental Materials (June 2019)

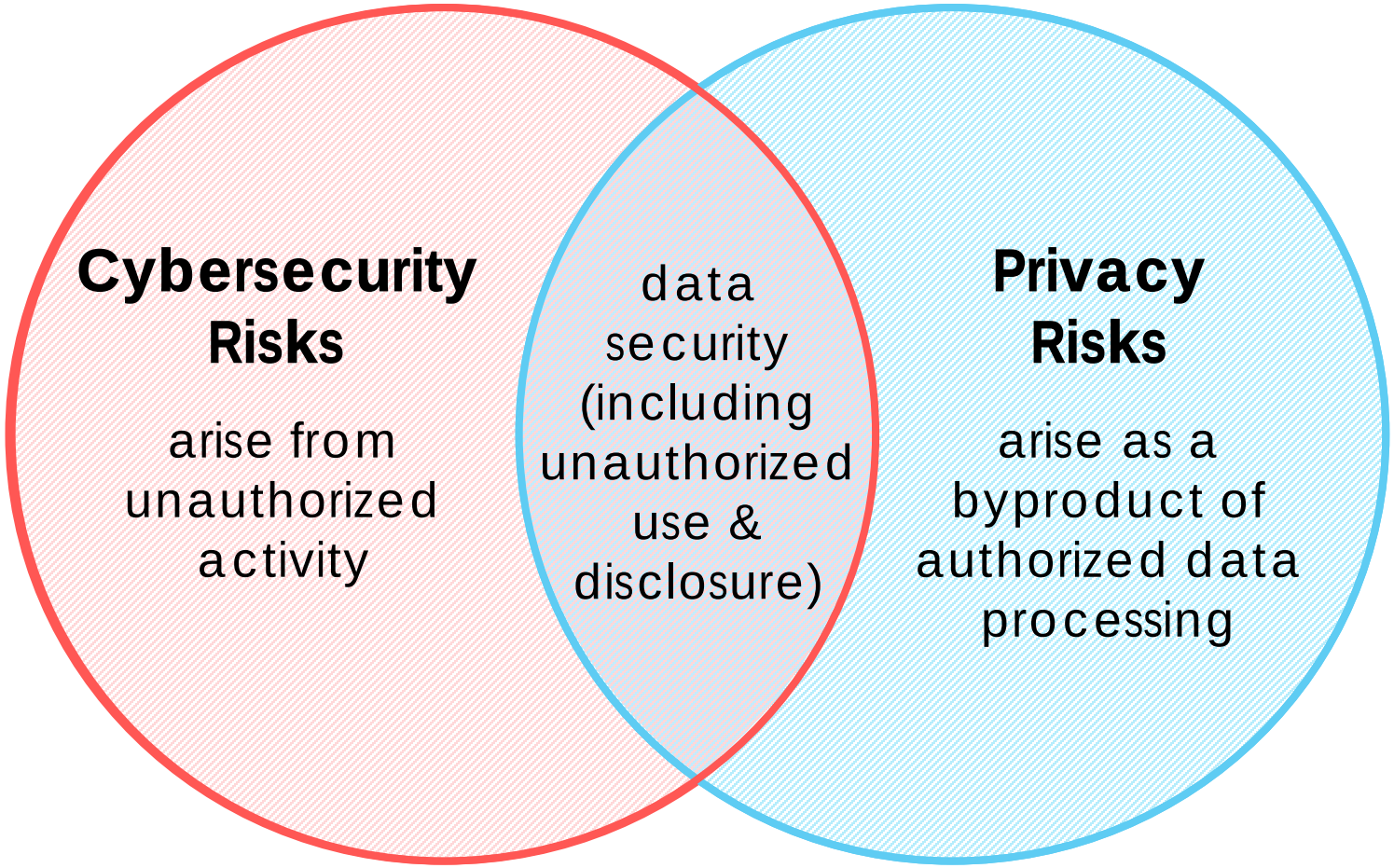


Purpose, value, & scope

Privacy Framework Value

- Shared lexicon
- Making ethical decisions when designing or deploying products and services
- Avoiding losses of trust that damage reputations and can slow adoption or cause abandonment of products and services.

Relationship Between Cybersecurity and Privacy Risk



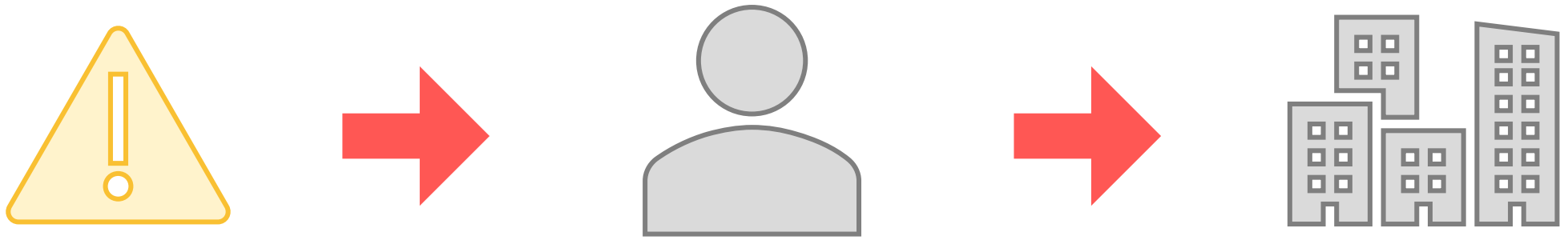
Data: A representation of information, including digital and non-digital formats, with the potential for adverse consequences for individuals when processed

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)

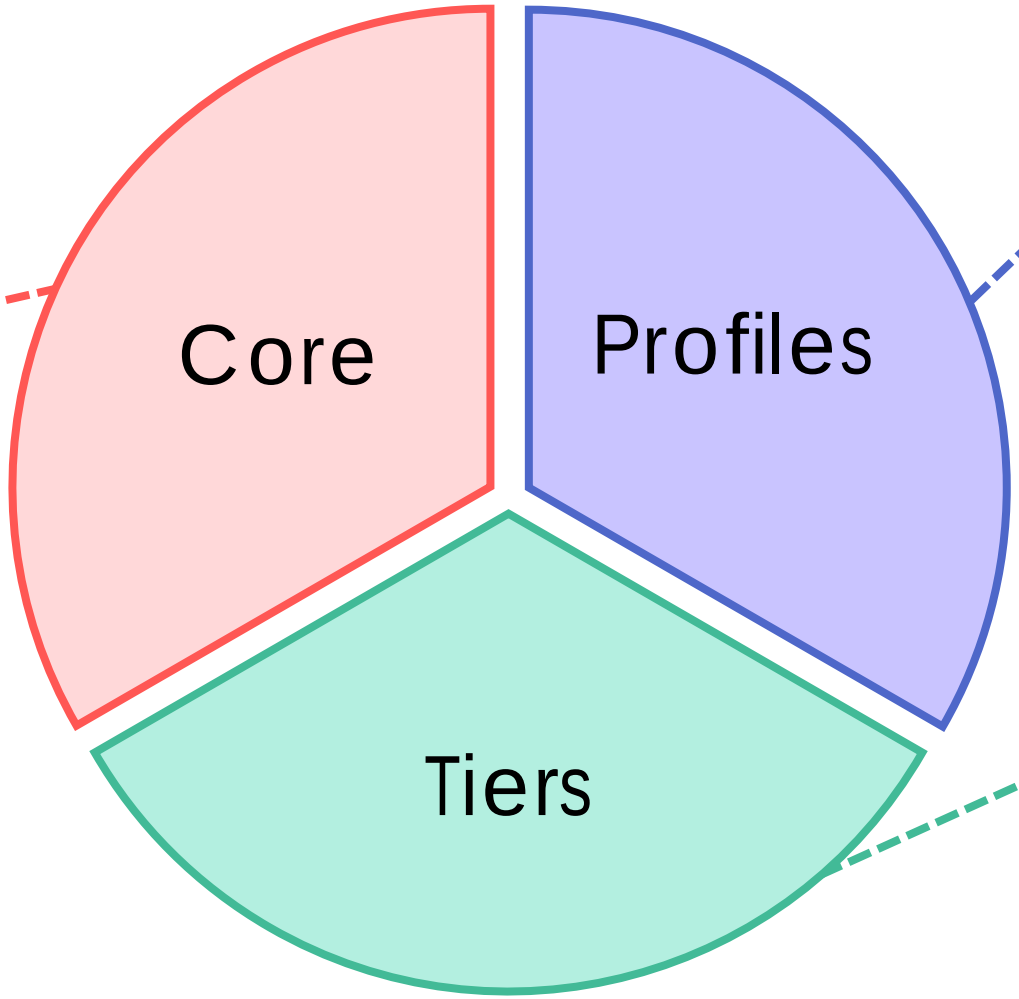
Organization

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

Risk-based & flexible

Privacy & Cybersecurity Framework Alignment

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

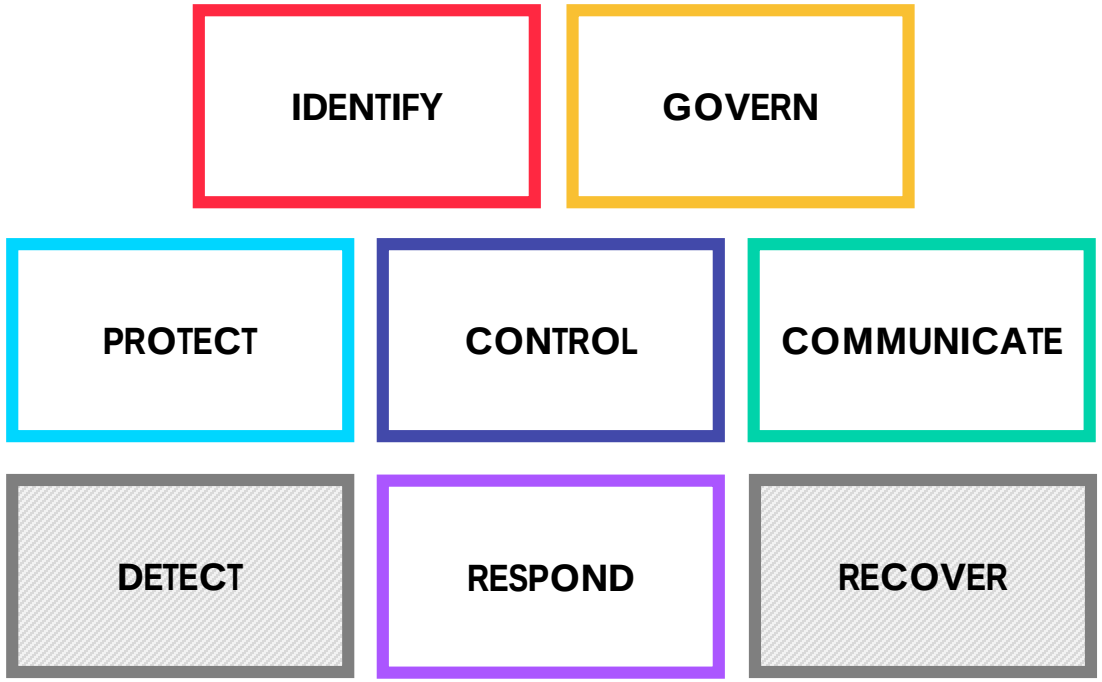


representation of the current and target outcomes the organization is focused on

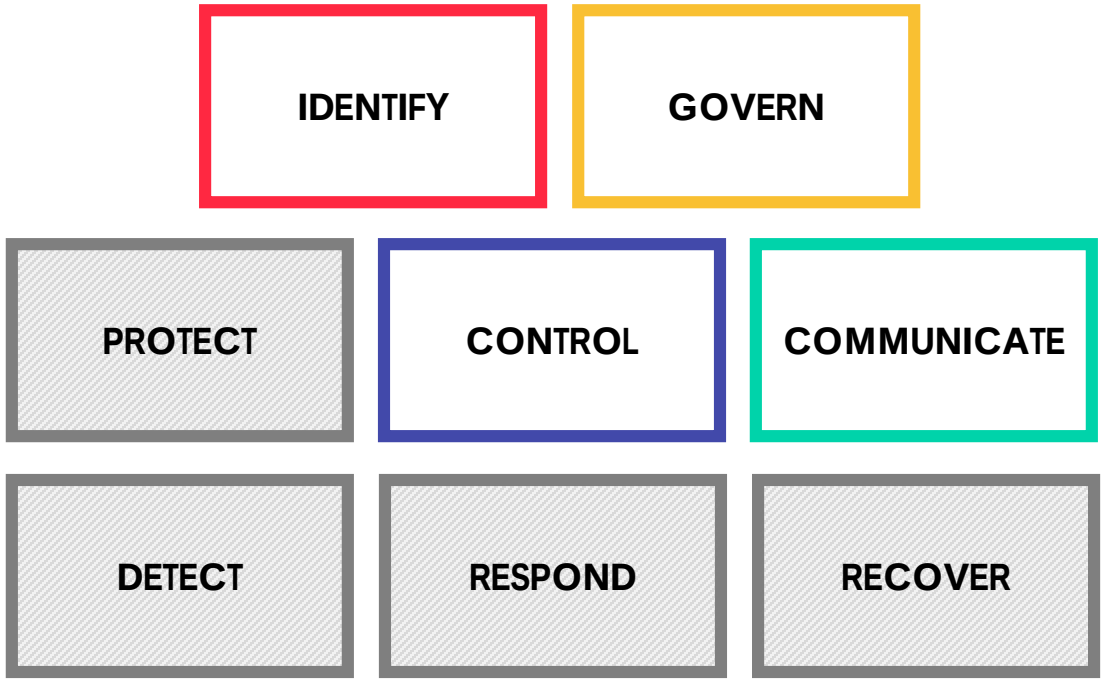
how an organization views risk and whether it has adequate processes & resources in place to manage that risk

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

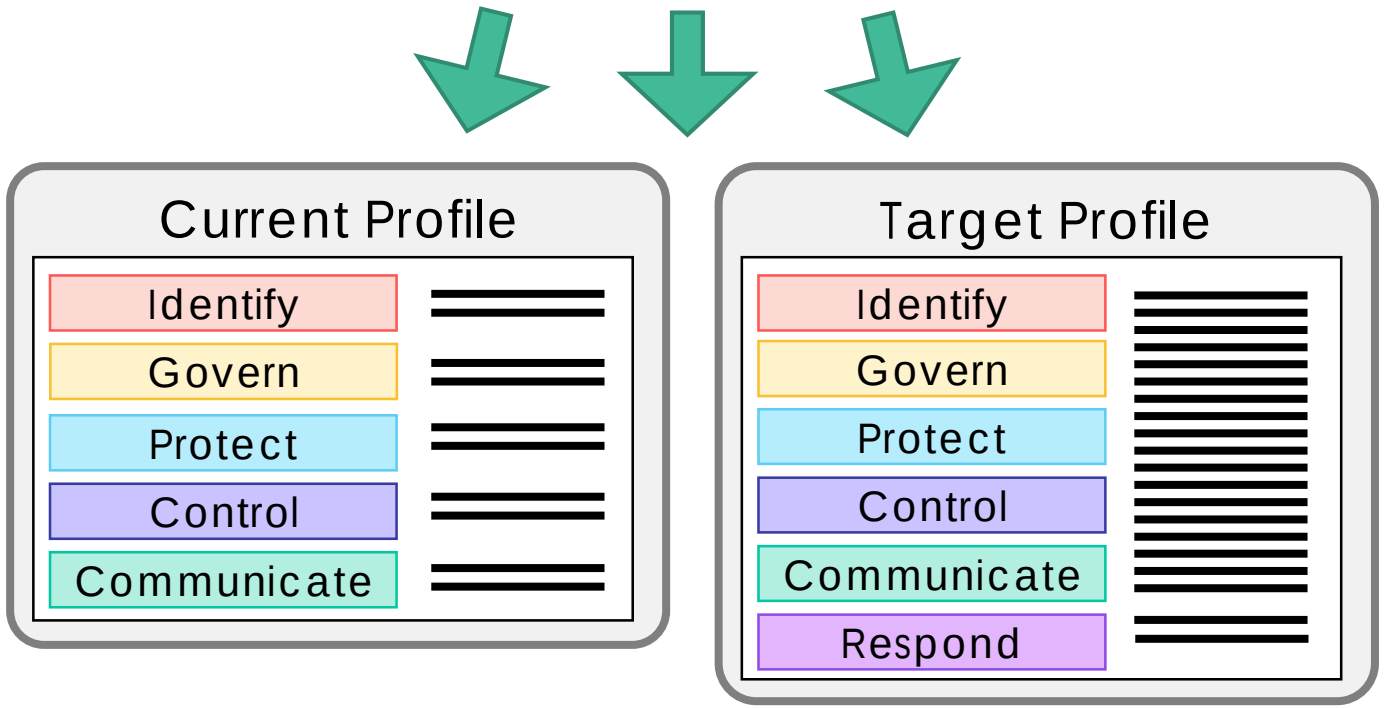
Accessibility & efficacy for bridging communication gaps

Finding Yourself in the Core

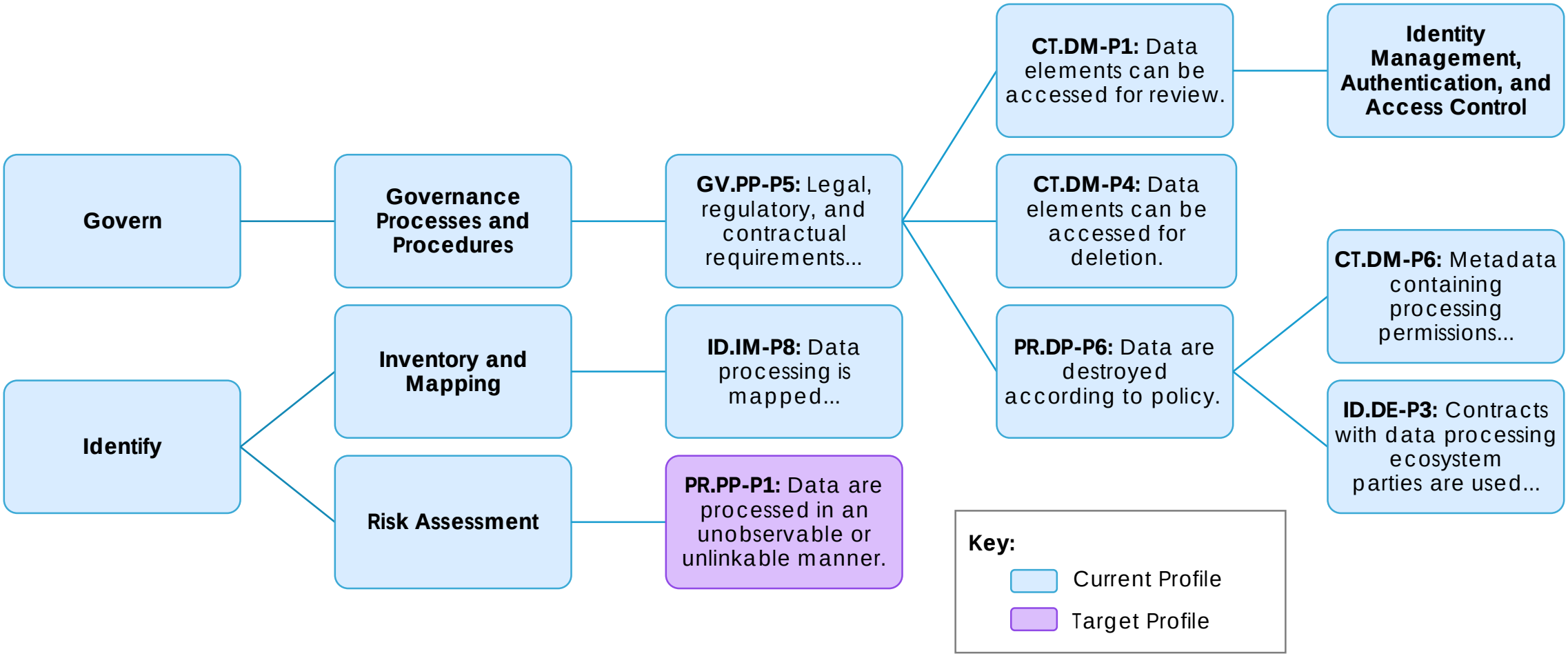
Collaboration & Profile Development

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



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

NIST Privacy Engineering Collaboration Space

August 2019

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

Why a collaboration space?

- Need for more tools, solutions, and processes supporting privacy engineering
- Greater awareness of those that already exist
- Better understanding of benefits and integration into systems or enterprise risk management processes
- Construct that helps organizations match the appropriate tools, solutions, or processes to their needs

About +
Collaboration Space −
Introduction
Operating Rules
Moderators
Contribute +
Browse +
Resources
Events
Get Involved

CONNECT WITH US

Collaboration Space

Welcome

This space has just launched! To kick off, we are focusing on **de-identification** and **privacy risk assessment**, and welcome feedback on future topics of interest.

Contact Us

NIST's Privacy Engineering Collaboration Space is an online venue open to the public where practitioners can discover, share, discuss, and improve upon open source tools, solutions, and processes that support privacy engineering and risk management.

Contribute

Created a privacy tool? Have a use case to share? Post it or collaborate on other contributions in the space.

Contribute

Browse

Interested in tools or use cases for de-identification and privacy risk assessment? Browse the contributions.

Browse

usnistgov / PrivacyEngCollabSpace

Unwatch 11 | Unstar 12 | Fork 9

Code | Issues 0 | Pull requests 2 | Projects 0 | Wiki | Insights | Settings

Privacy Engineering Collaboration Space https://www.nist.gov/itl/applied-cybe... Edit

de-identification differential-privacy risk-management Manage topics

154 commits | 1 branch | 0 releases | 5 contributors

Branch: master | New pull request | Create new file | Upload files | Find File | Clone or download

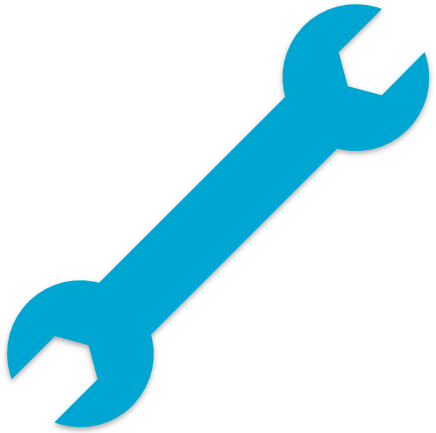
kboeckl fixes analysis typographical error — Latest commit 40ceb7d on Apr 2

.github	Update ISSUE_TEMPLATE.md	3 months ago
assets	resize img k	3 months ago
templates	Change management to assessment	a month ago
tools	fixes analysis typographical error	a month ago
use-cases	change management to assessment	a month ago
CONTRIBUTING.md	change management to assessment	a month ago
README.md	Update README.md	a month ago

README.md

Privacy Engineering Collaboration Space

What to Contribute



Tools

Use Cases

Feedback

Initial Focus Areas

De-identification

Privacy Risk Assessment

De-Identification Tools

Approximate Minima Perturbation (AMP) Carnegie Mellon University; Boston University; University of California, Berkeley; University of California, Santa Cruz; Peking University

ARX Data Anonymization Tool TUM - Technical University of Munich

Differential Privacy Synthetic Data Challenge Algorithms Various Challenge Participants

Differentially Private Stochastic Gradient Descent (DP-SGD) Google

De-Identification Tools (continued)

Ektelo UMass Amherst, Duke University, Colgate University

GUPT: Privacy preserving data analysis made easy University of California, Berkeley; University of California, Santa Cruz; Cornell University

PixelDP Columbia University

Privacy Protection Application (PPA) US Department of Transportation

Private Aggregation of Teacher Ensembles (PATE) Google

Privacy Risk Assessment Tools & Use Cases

City of Seattle Open Data Risk Assessment

Future of Privacy Forum (FPF) | *Use Case*

FAIR Privacy

Enterprivacy Consulting Group | *Tool*

NIST PRAM

NIST | *Tool*

Engage!

- **Explore** the space
- **Contribute** your tools and use cases
- **Spread the word** about the space

Resources

Privacy Framework

Website

https://www.nist.gov/privacyframework

Contact Us

PrivacyFramework@nist.gov

@NISTcyber #PrivacyFramework

Mailing List

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

Collaboration Space

www.nist.gov/itl/applied-cybersecurity/privacy-engineering/collaboration-space

collabspace@nist.gov