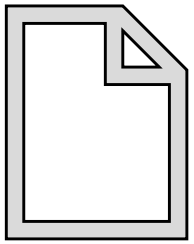
NIST Privacy Framework:
A Tool for Improving Privacy Through Enterprise Risk Management
Preliminary Draft
October 2019

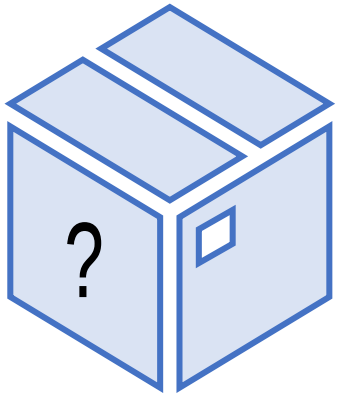
Collaborative Development

Starting Point
Attributes

Current State
Preliminary Draft



Version 1.0



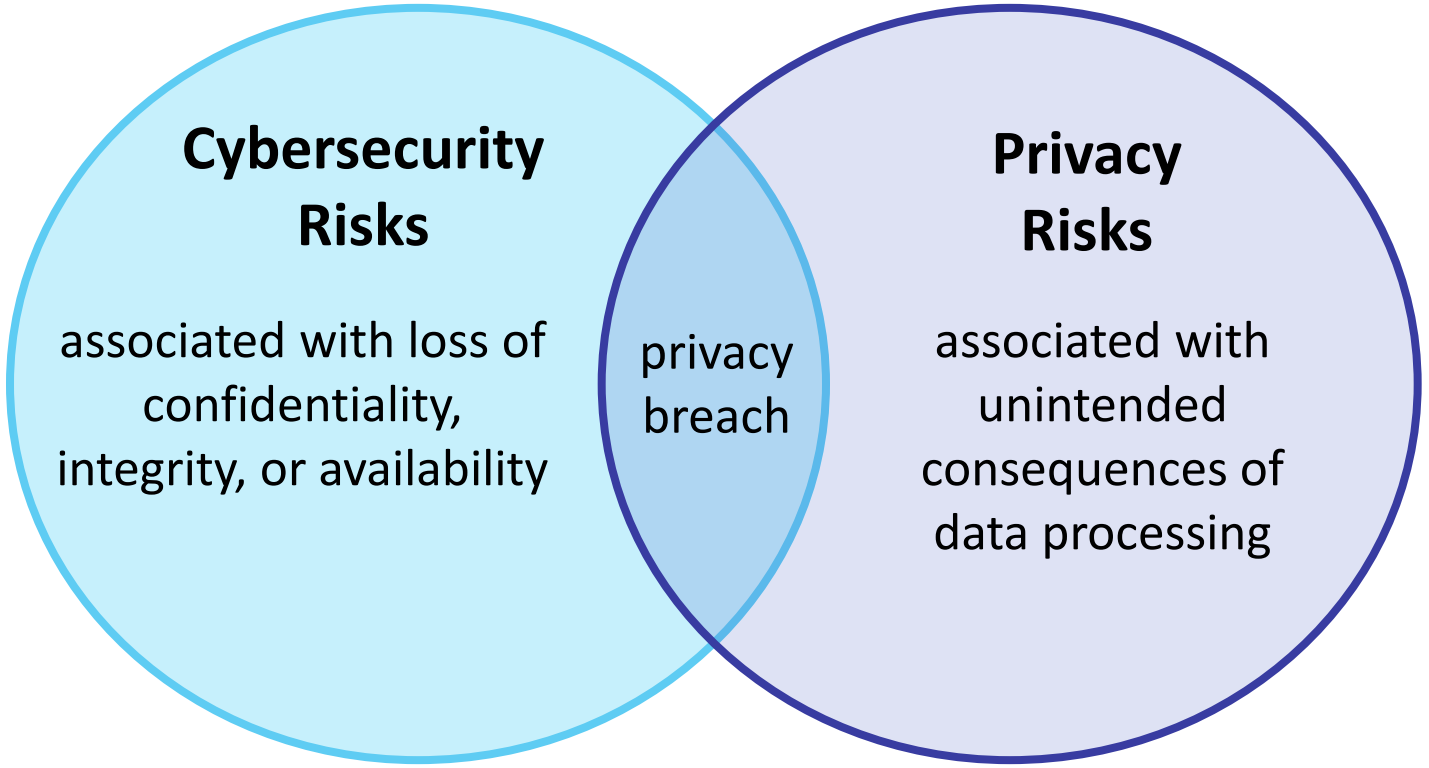
2
public comment periods

3
public workshops

5
webinars

ongoing
stakeholder engagement

Relationship Between Cybersecurity and Privacy Risk



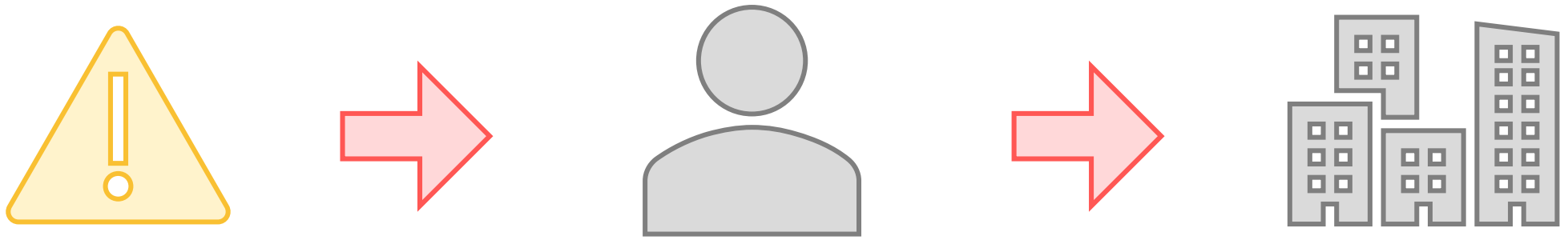
Data: A representation of information, including digital and non-digital formats

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

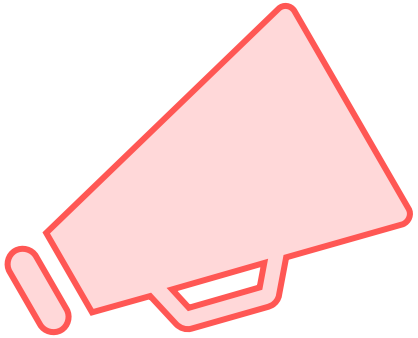
resulting impact
(e.g., customer abandonment, noncompliance costs, harm to reputation or internal culture)

Value Proposition

Privacy Framework supports:

Building customer trust

Fulfilling current compliance obligations



Facilitating communication

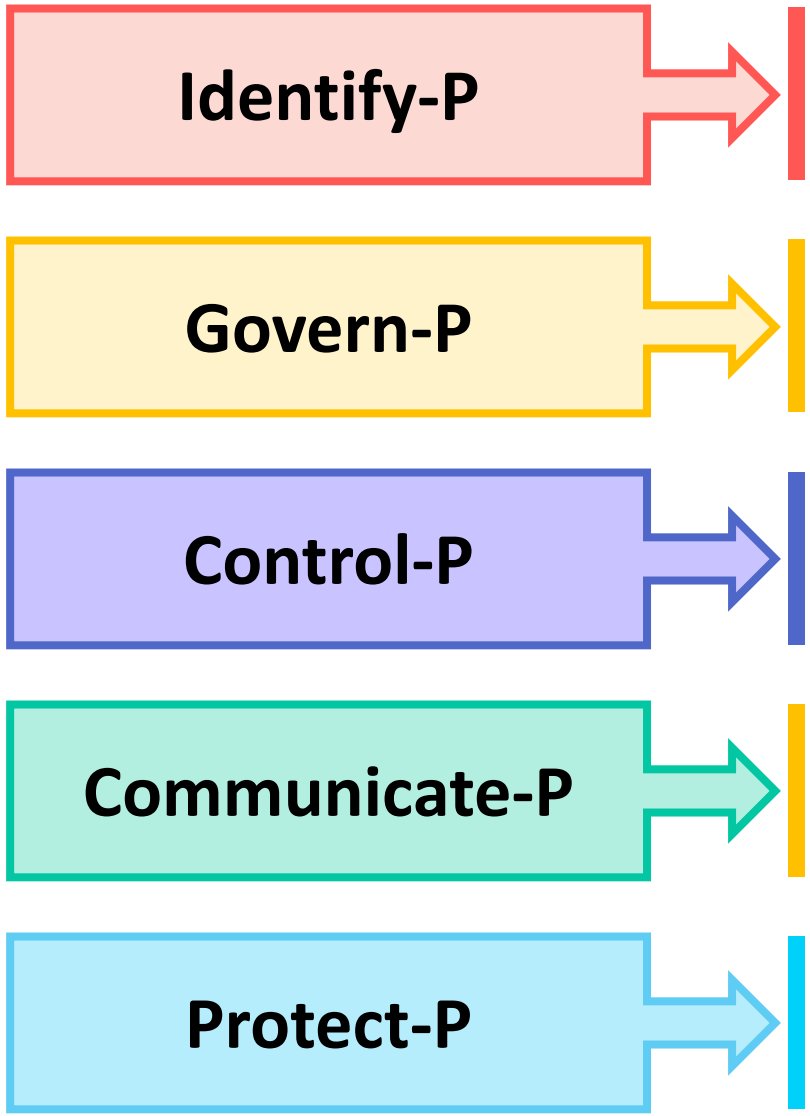
Privacy Framework Structure

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



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

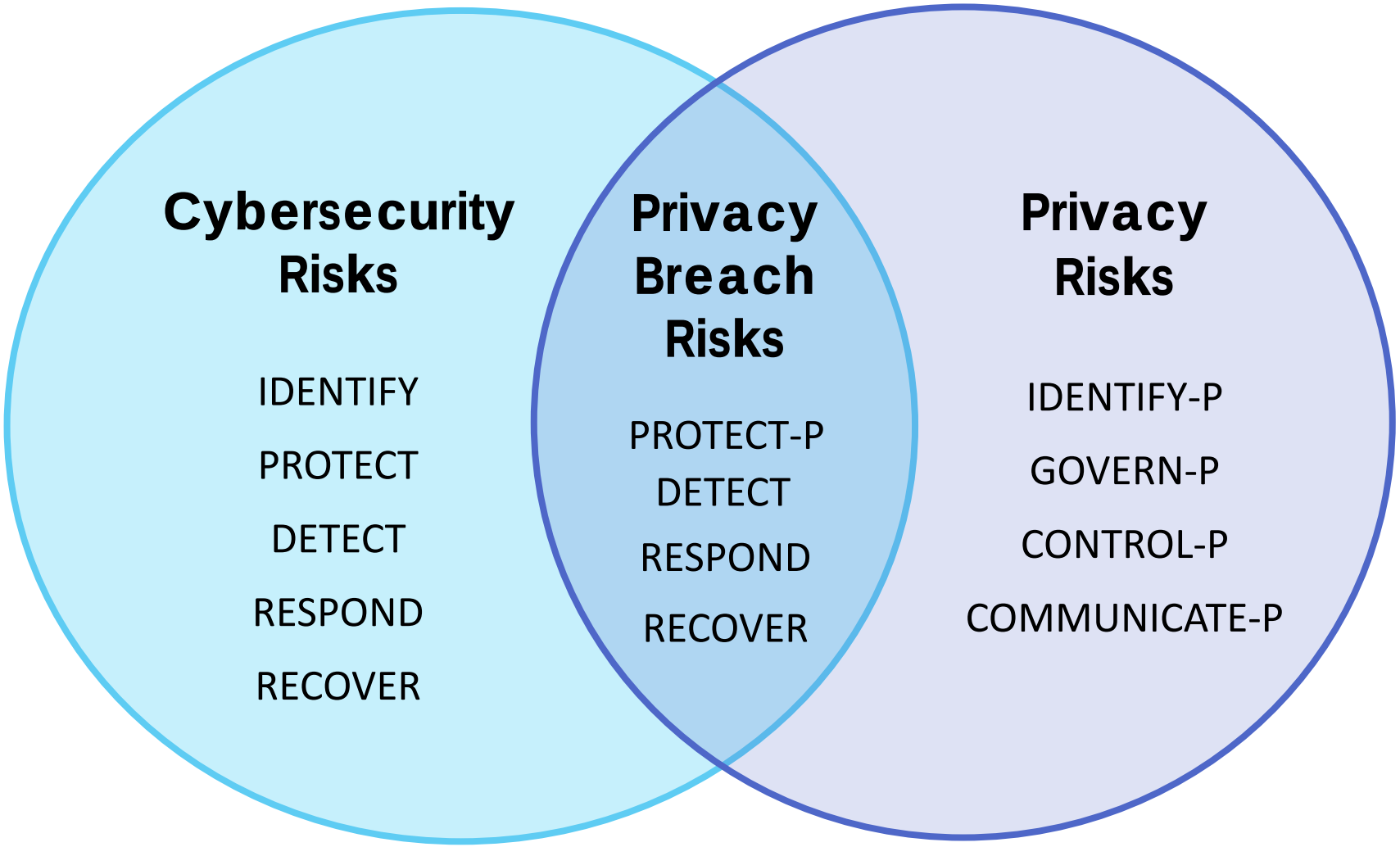
Develop and implement the organizational governance structure to enable an ongoing understanding of the organization's risk management priorities that are informed by privacy risk.

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

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

Develop and implement appropriate data processing safeguards.

Cybersecurity Framework Alignment



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

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** – lead on privacy
- **NIST repository** – provide use cases and informative references
- **Stakeholder engagement** – international focus

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