
A PRIVACY ENGINEERING APPROACH TO PRIVACY RISK

Katie Boeckl

Privacy Risk Strategist

National Institute of Standards and Technology

kaitlin.boeckl@nist.gov

NIST PRIVACY ENGINEERING PROGRAM

NISTIR 8062

An Introduction to
Privacy Engineering and
Risk Management in
Federal Systems

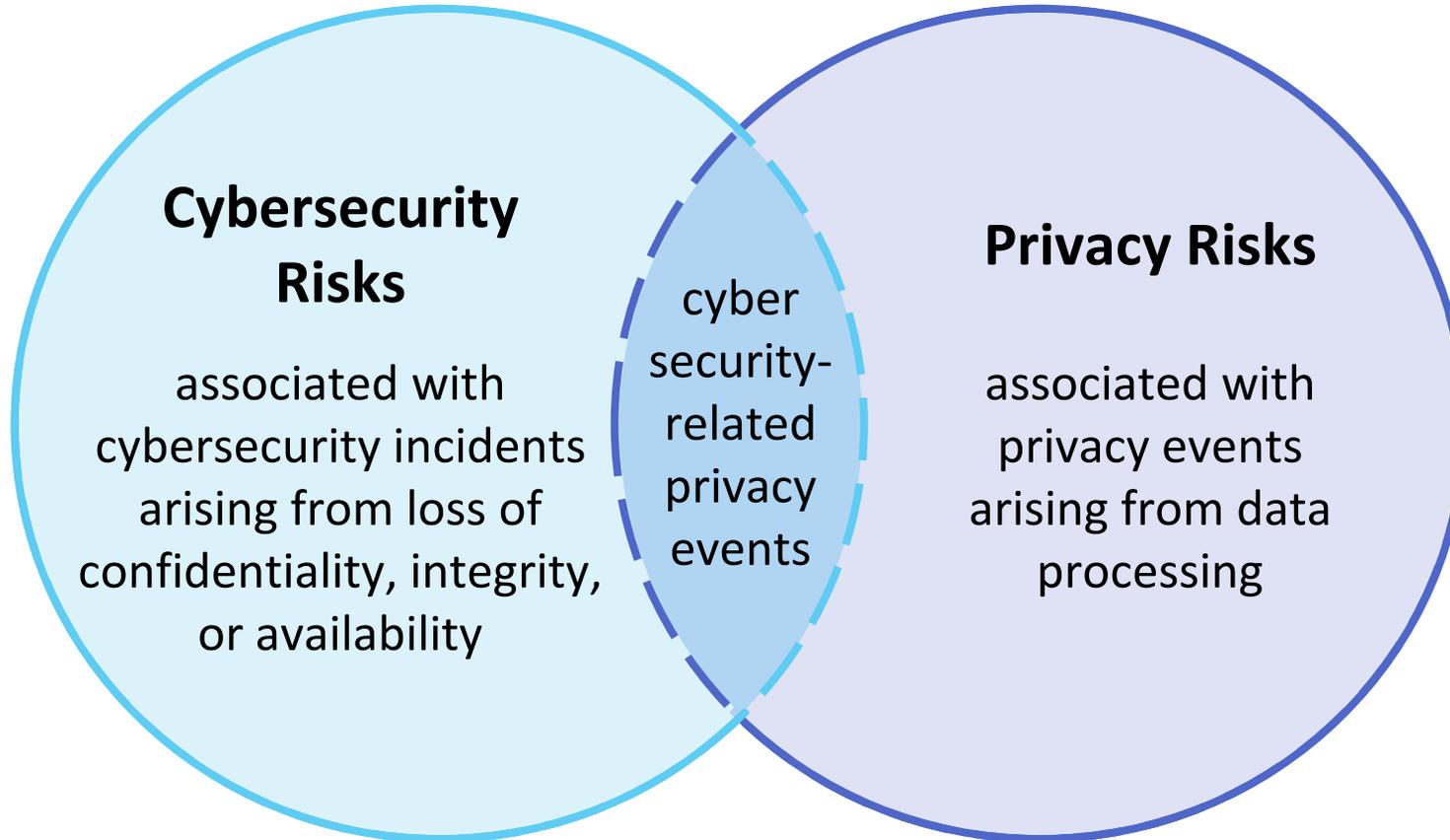
2017

NIST PRIVACY FRAMEWORK

A Tool for Improving
Privacy through
Enterprise Risk
Management

2020

CYBERSECURITY AND PRIVACY RELATIONSHIP



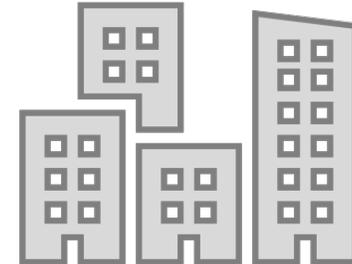
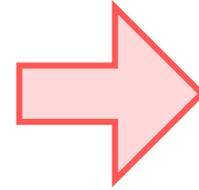
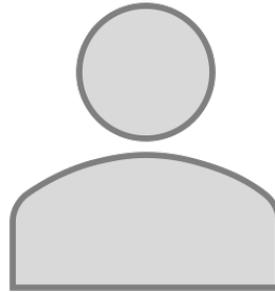
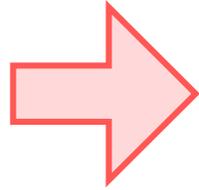
Data: A representation of information, including digital and non-digital formats

Privacy Event: The occurrence or potential occurrence of problematic data actions

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

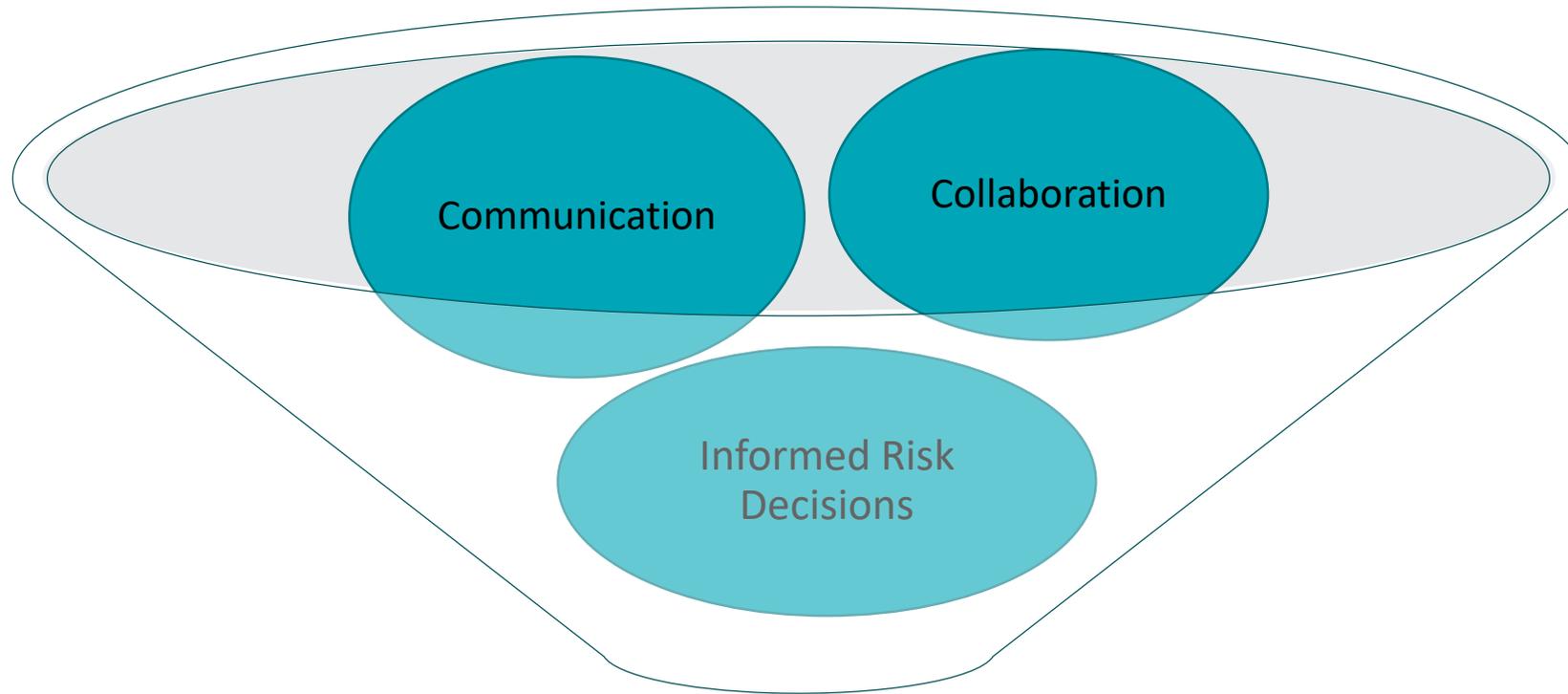
Individual

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

Organization

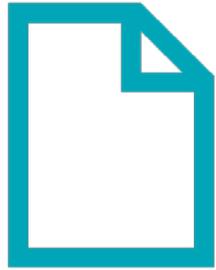
resulting impact
(e.g., customer abandonment, noncompliance costs, harm to reputation or internal culture)

PRIMARY BENEFITS OF PRIVACY RISK ASSESSMENT



Privacy Engineered Solutions

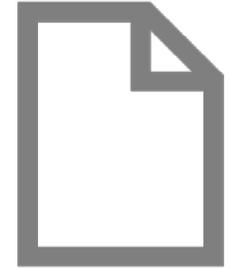
NIST PRIVACY RISK ASSESSMENT METHODOLOGY (PRAM)



Worksheet 1
Framing Business
Objectives and
Organizational
Privacy Governance



Worksheet 2
Assessing System
Design; Supporting
Data Map



Catalog of
Problematic Data
Actions and
Problems



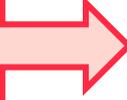
Worksheet 3
Prioritizing Risk



Worksheet 4
Selecting Controls

NIST PRIVACY FRAMEWORK CORE FUNCTIONS

Identify-P



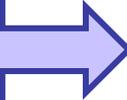
Develop the organizational understanding to manage privacy risk for individuals arising from data processing.

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



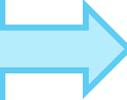
Develop and implement appropriate activities to enable organizations or individuals to manage data with sufficient granularity to manage privacy risks.

Communicate-P



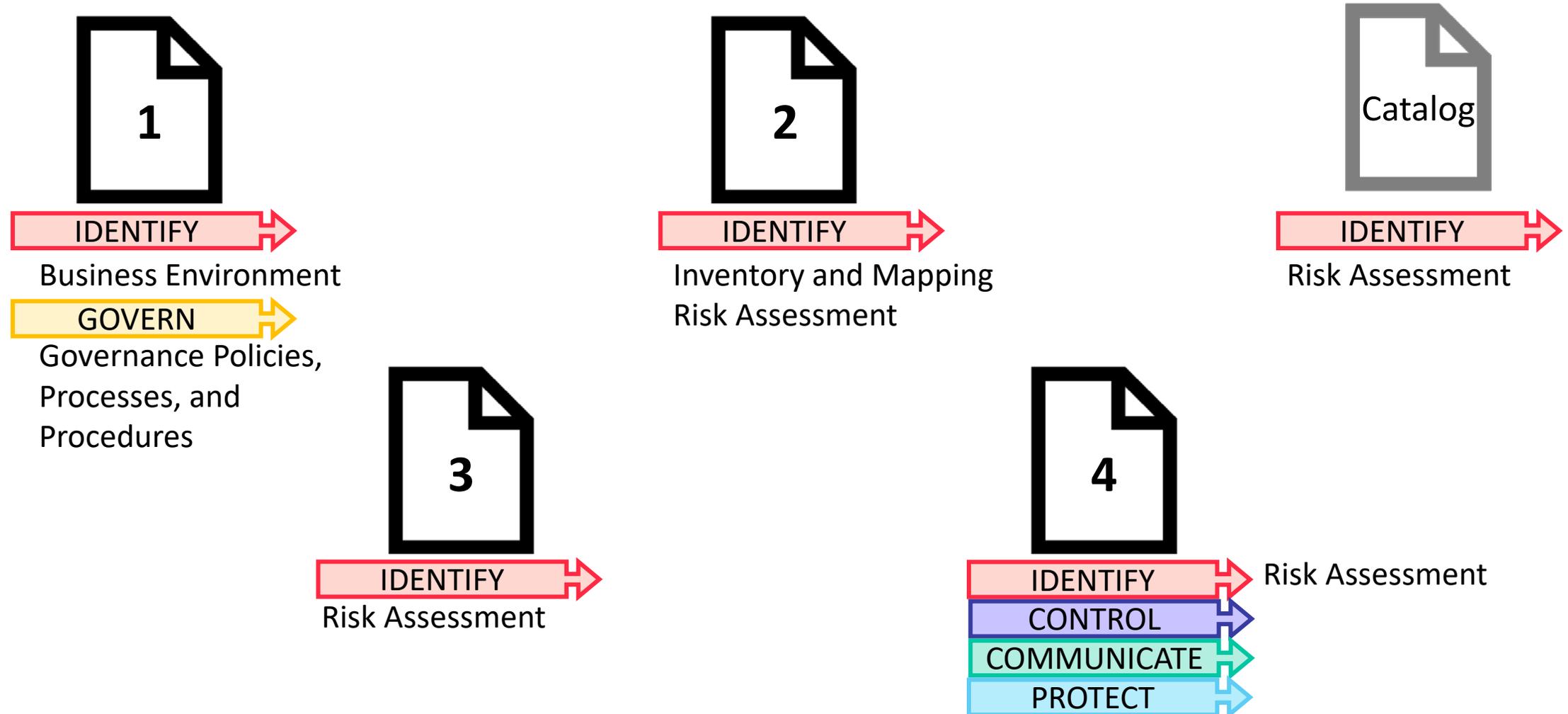
Develop and implement appropriate activities to enable organizations and individuals to have a reliable understanding about how data are processed and associated privacy risks.

Protect-P



Develop and implement appropriate data processing safeguards.

MAPPING THE NIST PRIVACY FRAMEWORK TO THE PRAM



RESOURCES

NIST Privacy Risk Assessment Methodology:

<https://www.nist.gov/itl/applied-cybersecurity/privacy-engineering/resources#pram>

NIST Privacy Framework: <https://www.nist.gov/privacy-framework>