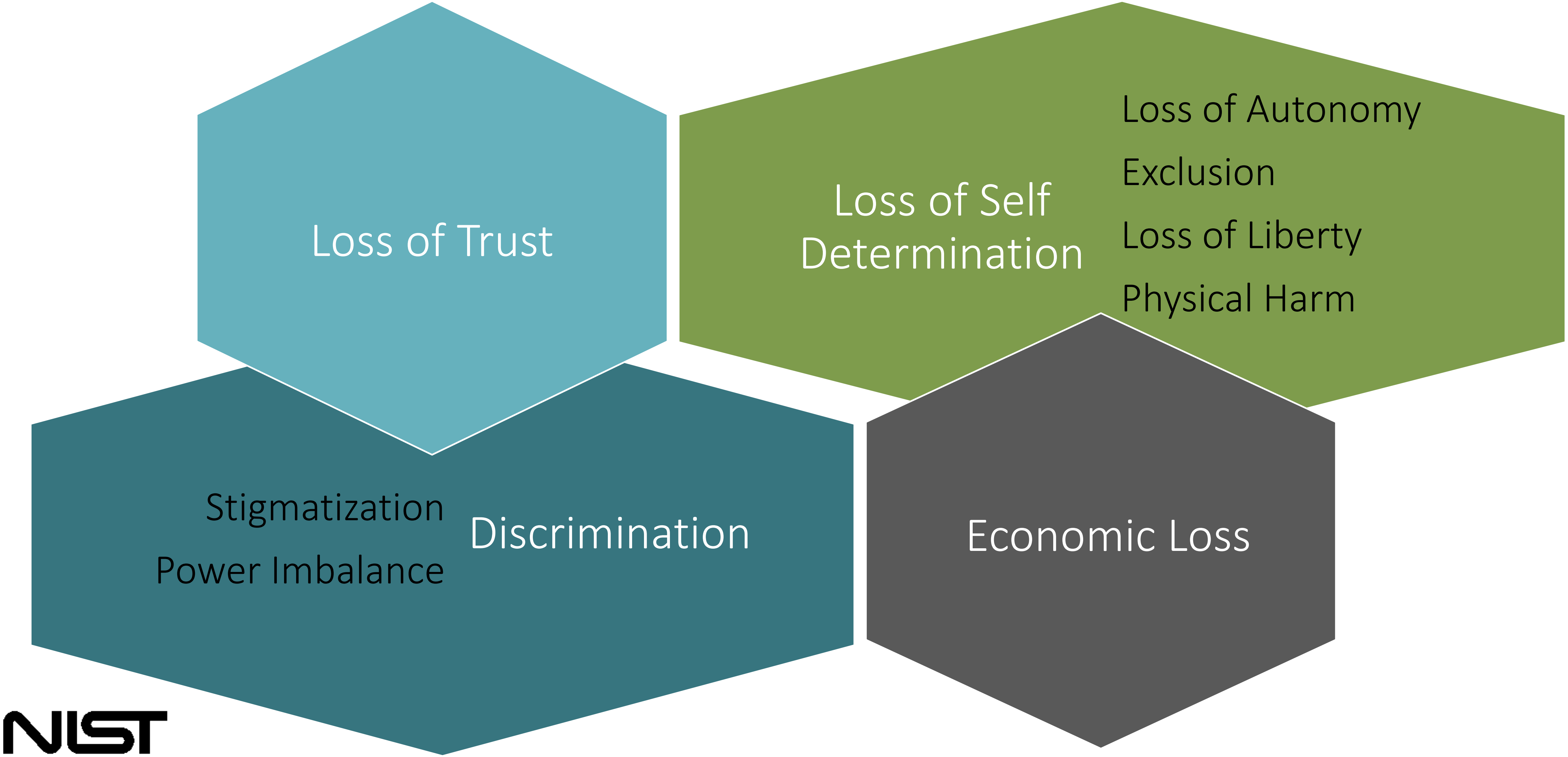
Using Risk Management to Improve Privacy in Information Systems

Potential Problems for Individuals



Loss of Trust

Loss of Self Determination

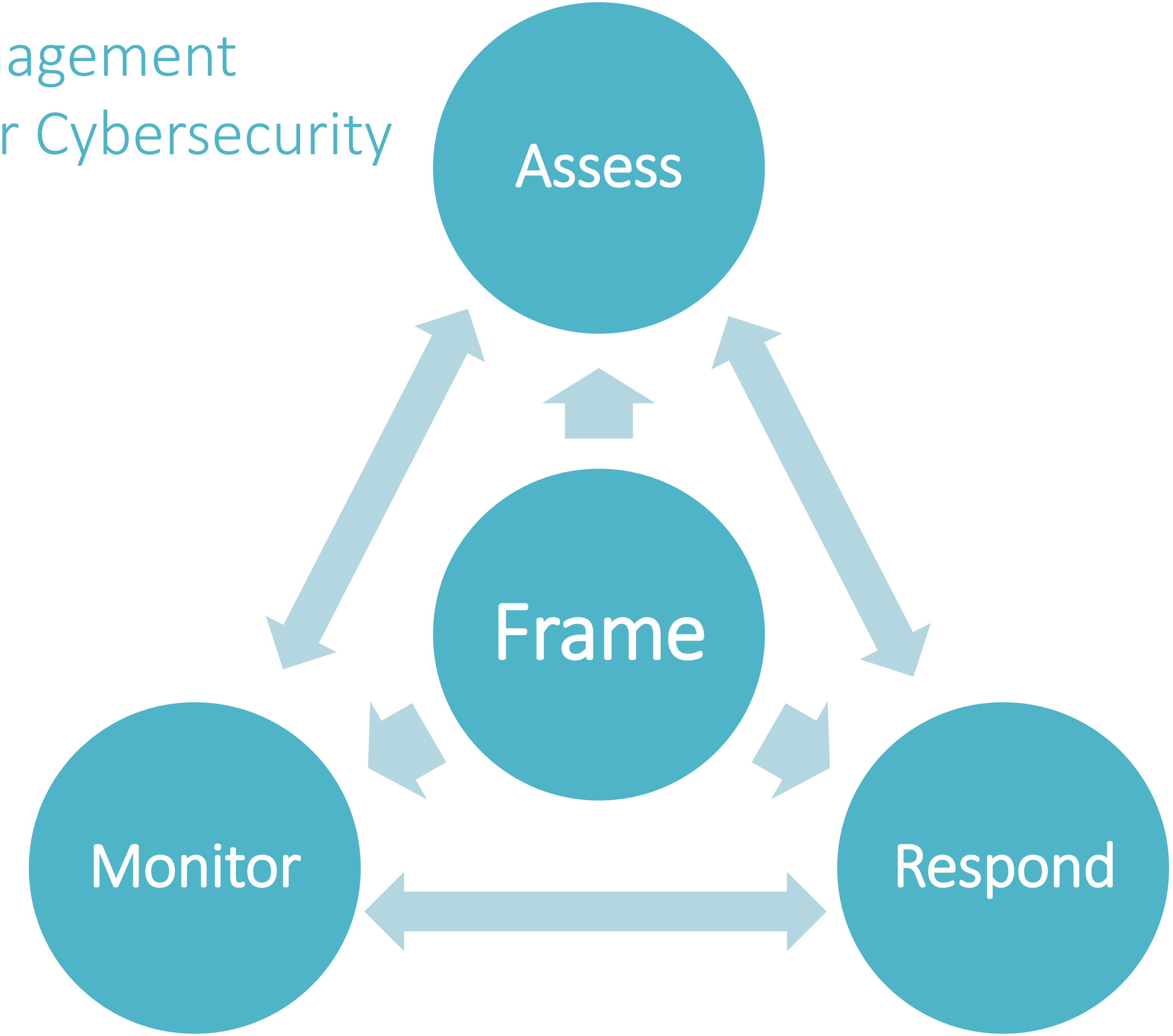
- Loss of Autonomy
- Exclusion
- Loss of Liberty
- Physical Harm

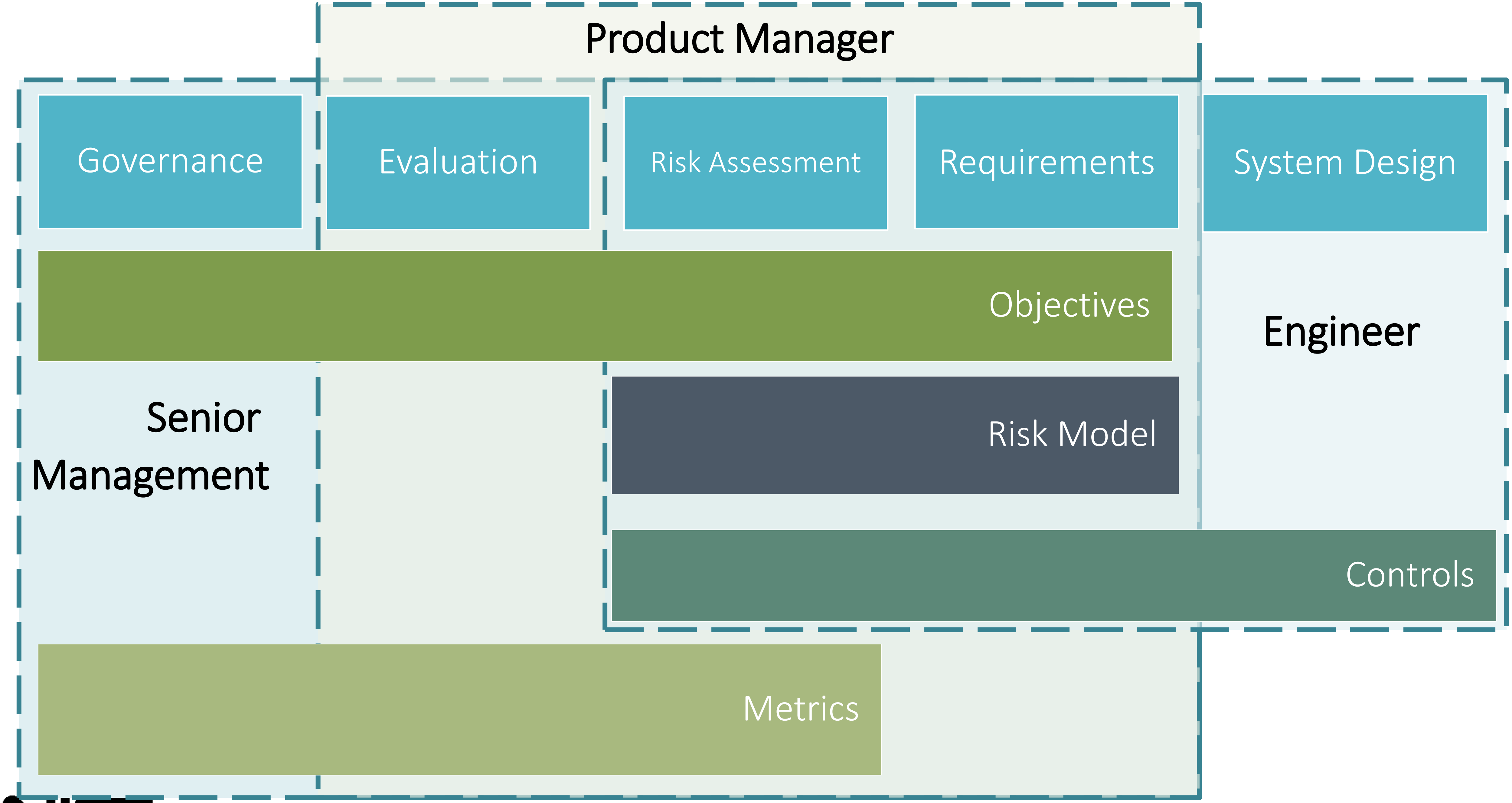
Discrimination

- Stigmatization
- Power Imbalance

Economic Loss

NIST Risk Management Framework for Cybersecurity




Product Manager
Governance
Evaluation
Risk Assessment
Requirements
System Design
Objectives
Engineer
Senior Management
Risk Model
Controls
Metrics

The Right Tool for the Job

Many current privacy approaches are some mixture of governance principles, requirements and controls.

USG FIPPs

Transparency
Individual Participation
Purpose Specification
Data Minimization
Use Limitation
Data Quality and Integrity
Security
Accountability and Auditing

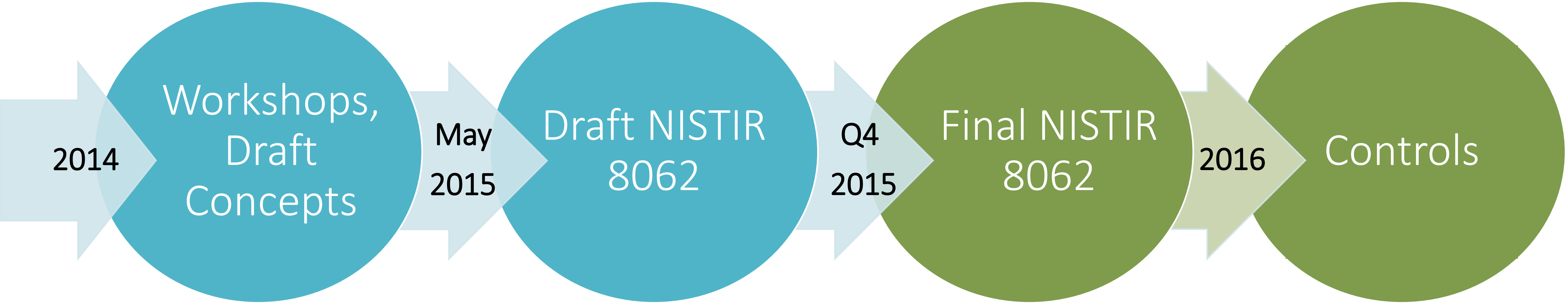
NIST SP 800-53, Appendix J

Authority and Purpose
Accountability, Audit, and Risk Management
Data Quality and Integrity
Data Minimization and Retention
Individual Participation and Redress
Security
Transparency
Use Limitation

NIST IR 8062

Privacy Risk Management for Federal Information Systems

NIST Process



2014

Workshops, Draft Concepts

May 2015

Draft NISTIR 8062

Q4 2015

Final NISTIR 8062

2016

Controls

Draft Privacy Engineering Objectives

- Design characteristics or properties of the system
- Support policy
- Support control mapping

Predictability is the enabling of reliable assumptions by individuals, owners, and operators about personal information and its processing by an information system.

Manageability is providing the capability for granular administration of personal information including alteration, deletion, and selective disclosure.

Disassociability is enabling the processing of personal information or events without association to individuals or devices beyond the operational requirements of the system.

Security Risk Equation

Security Risk = Vulnerability * Threat * Impact

Privacy Risk Equation

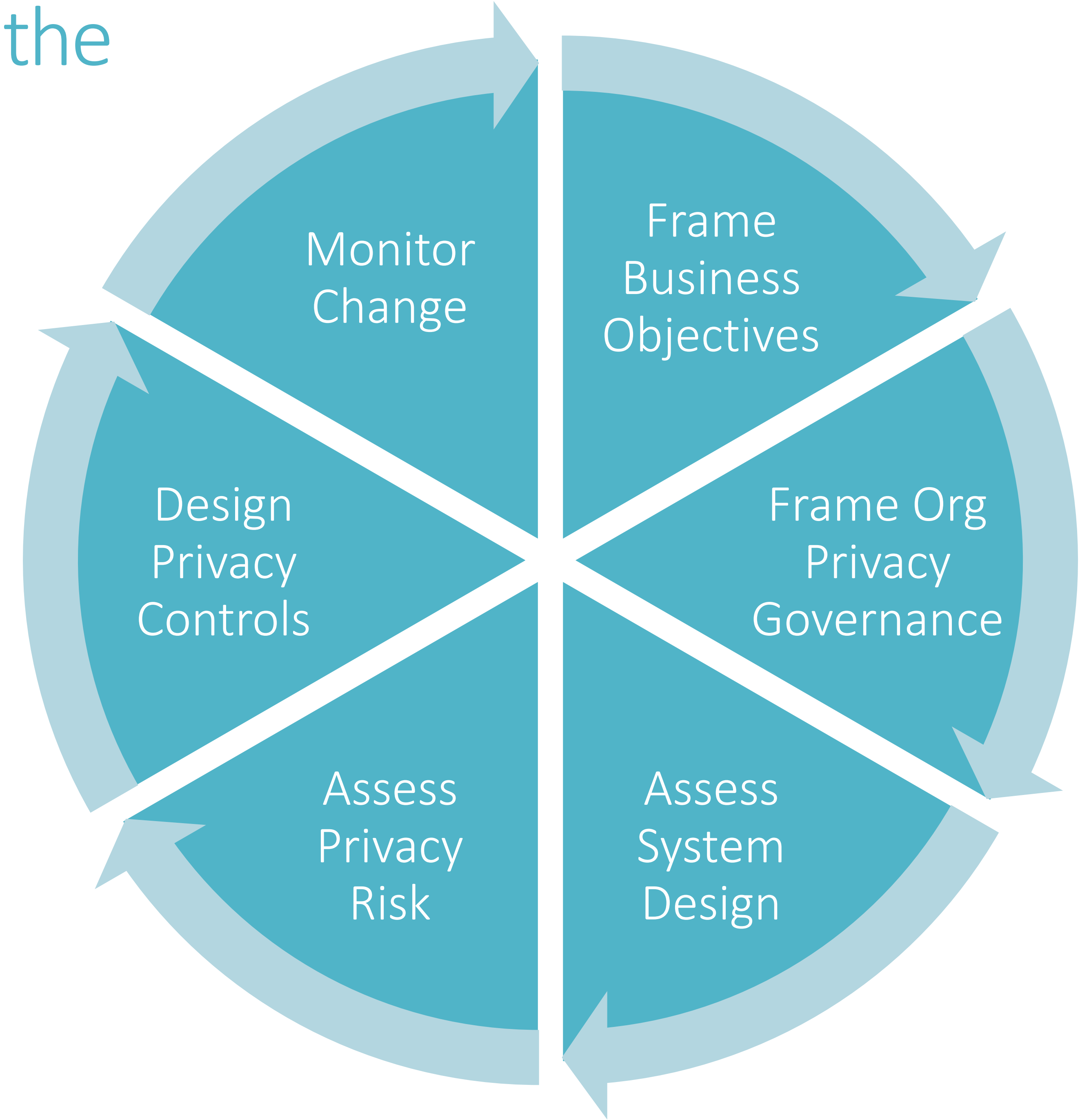
Privacy Risk = Likelihood of a Problematic Data Action * Impact

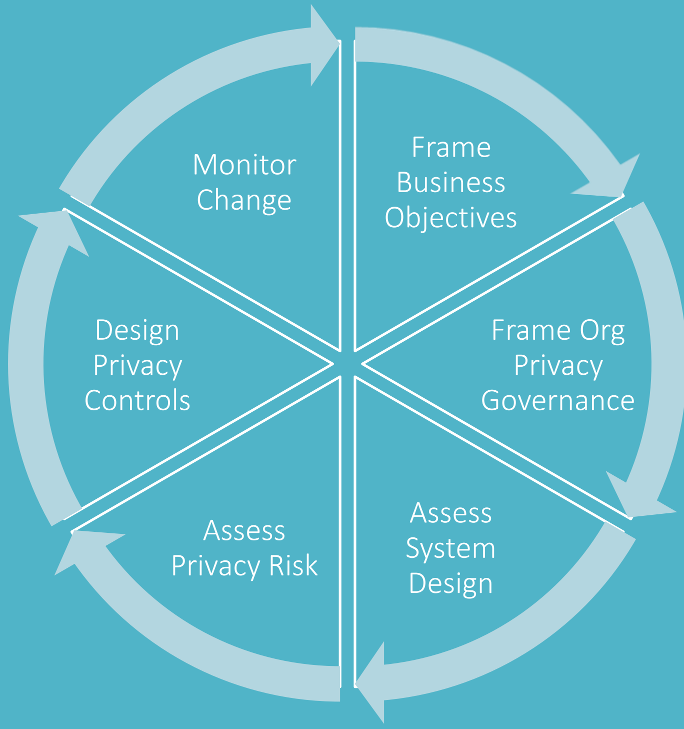
Likelihood is determined by contextually-based analysis that a data action is likely to create a problem for representative set of individuals

Impact is determined by an analysis of the adverse affects on an organization of creating the potential for privacy problems

Note: Contextual analysis is the comparison of Data Actions, the personal information on which they act, and contextual considerations

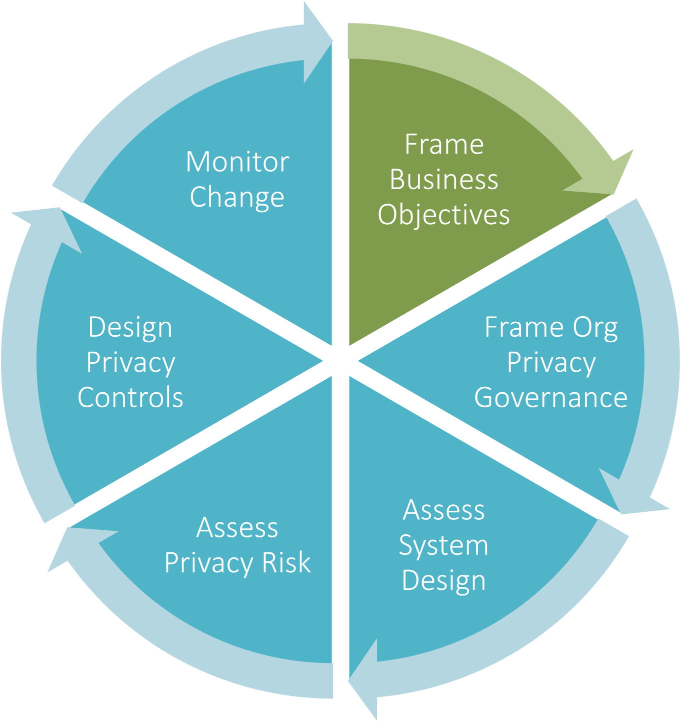
Implementing the Theory





Privacy Risk Assessment Methodology

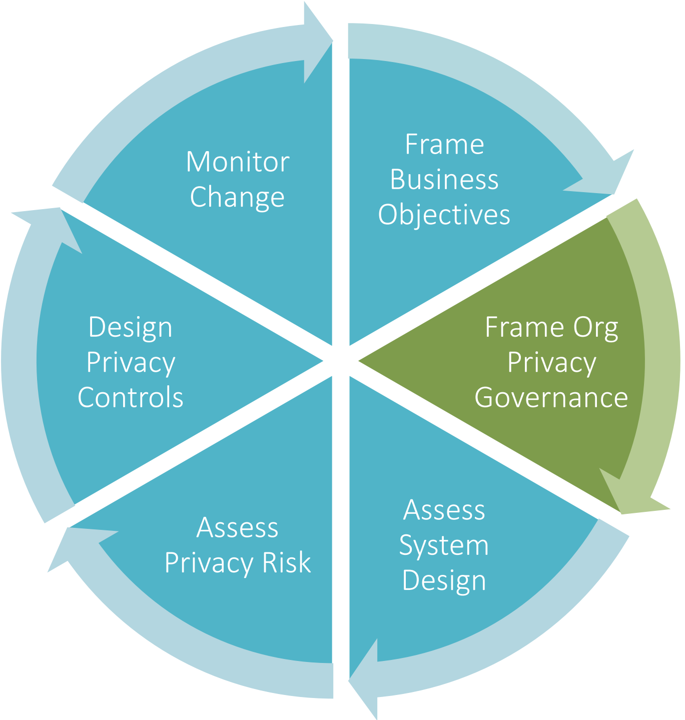
Frame Business Objectives



Frame the business objectives for the system(s), including the organizational needs served.

- Describe the functionality of your system(s).
- Describe the business needs that your system(s) serve.
- Describe how your system will be marketed, with respect to any privacy-preserving functionality.

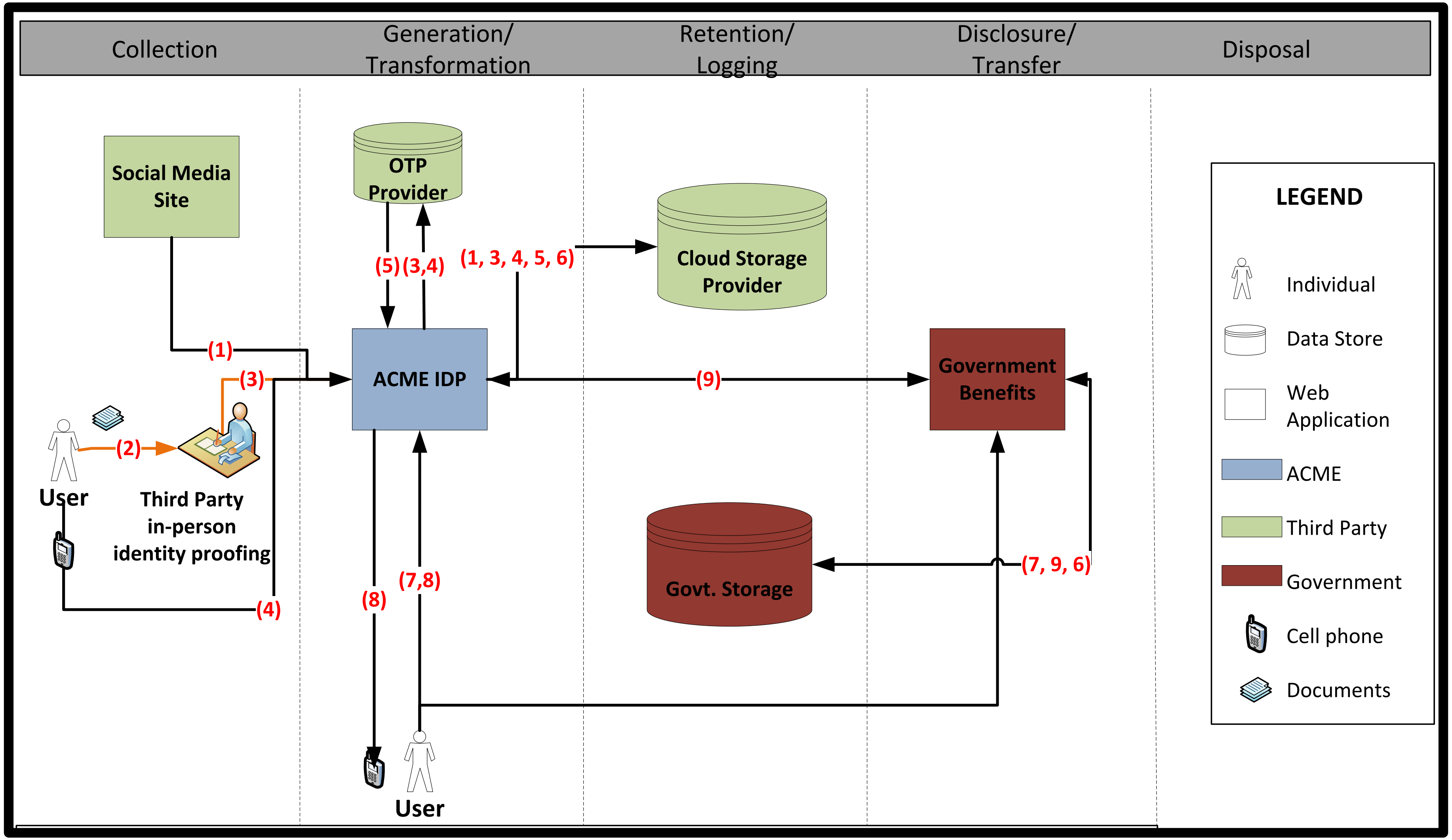
Frame Privacy Governance

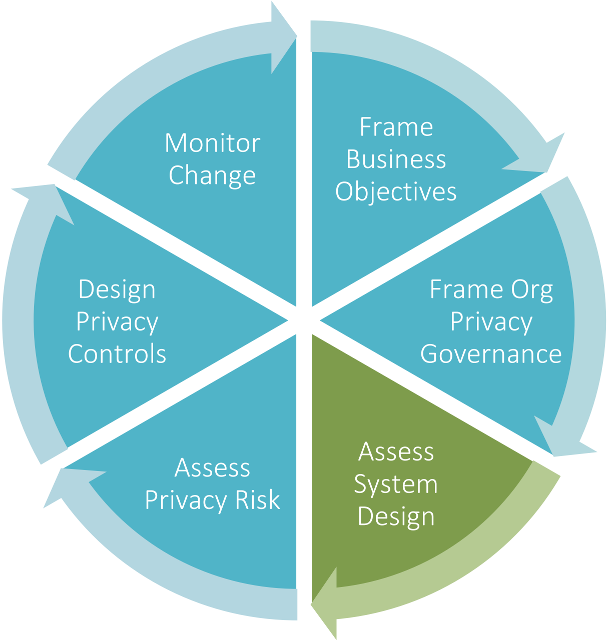


Frame the organizational privacy governance by identifying privacy-related legal obligations, principles, organizational goals and other commitments.

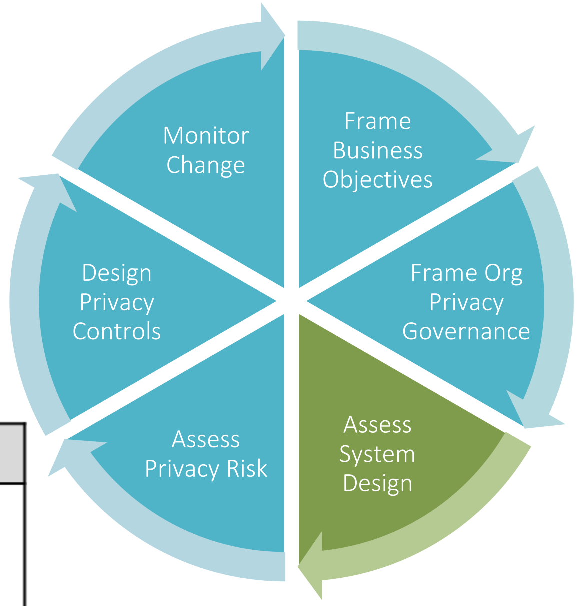
- Legal Environment: Identify any privacy-related statutory, regulatory, contractual and/or other frameworks within which the pilot must operate.
- Identify any privacy-related principles or other commitments to which the organization adheres (FIPPs, Privacy by Design, etc.).
- Identify any privacy goals that are explicit or implicit in the organization's vision and/or mission.
- Identify any privacy-related policies or statements within the organization, or business unit.

Assess System Design – Data Actions





Assess System Design - Context



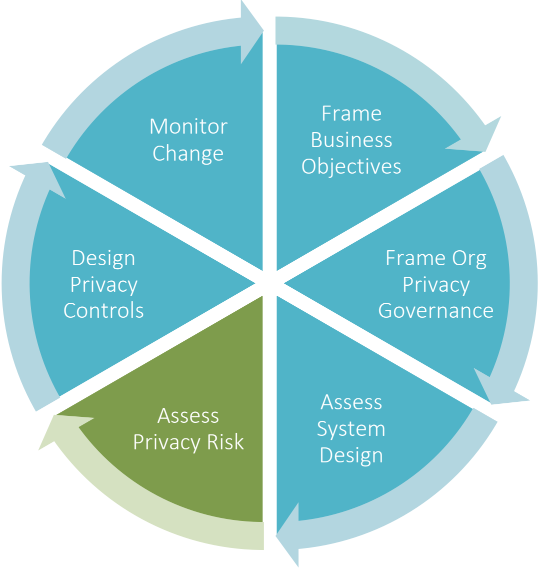
Example:

An individual wishes to use ACME IDP service to augment a social credential with identity proofing and a second authentication factor to create a stronger credential. This stronger credential will be used to access government benefits.

Data Action	Personal Information	Specific Context	Summary Issues
Collection from the Social Media Site	- Self-Asserted Full Name - Validated Email -List of Friends -Profile Photograph	- One-time action (per user) between social credential and ACME IDP, but establishes an ongoing relationship between user's social media presence and ACME IDP - Social credential linking is visible to user - Linking of social credential simplifies access to government benefits system - User profile may contain information the user considers sensitive - User profile may contain information from other users not participating in the system	- Full social credential profile access (including picture and list of friends) is not necessary for fulfilling operational purpose - Will users understand the eventual high-assurance credential is controlled by ACME and not by their social credential provider? - How will perception of the social media organization's privacy practices impact users' willingness to consent to this data action? - Will the user understand ACME will have

Example Contextual Factors
Organizational
System includes both government benefits agency and commercial service providers
Multiple privacy policies governing system
Public perception: high expectation of privacy with government benefits agency, low expectation with social credential provider
Relationships: No pre-existing relationship with ACME IDP, regular interactions with government benefits agency, regular interactions with social credential provider
System
Personal information is not intended to be made public
New system, no history with affected individuals. Low similarity with existing systems/uses of social identity.
Four parties sharing personal information: one public institution, three private
ACME will use 3rd party cloud provider
User
High sensitivity about government benefits provided by system
Users exhibit various levels of technical sophistication
Potential user confusion regarding who "owns" the various segments of each system
20% of users use privacy settings at social provider

Assess Privacy Risk

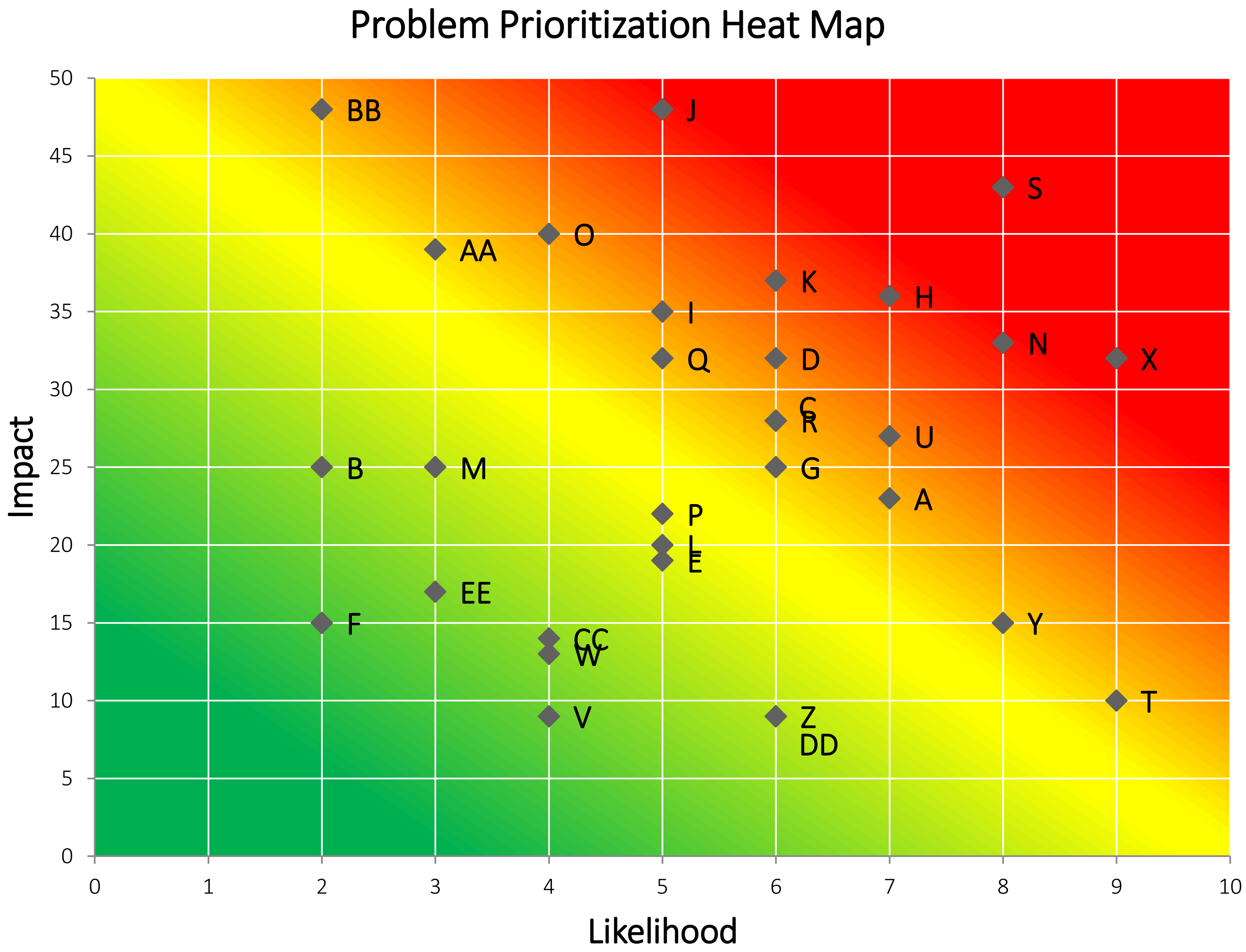


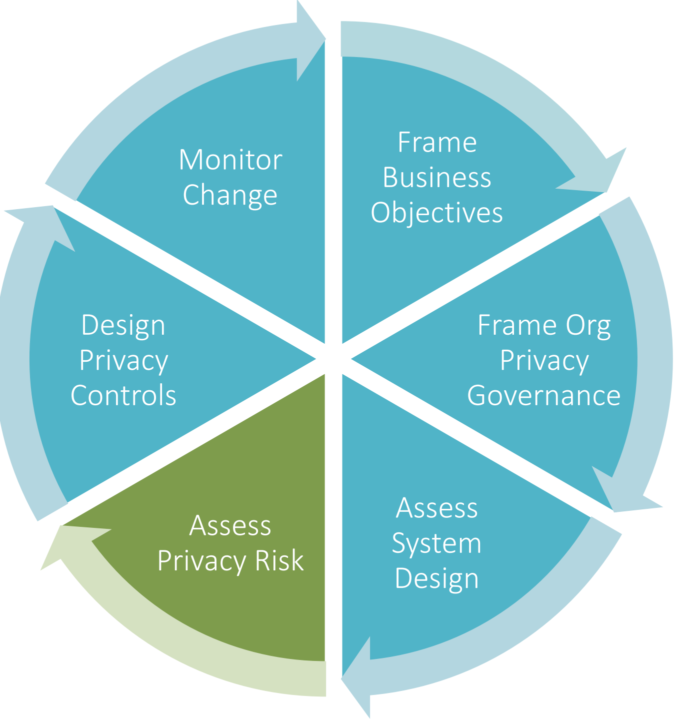
SAMPLE TABLE

Data Actions	Summary Issues	Problematic Data Actions	Potential Problems for Individuals	Likelihood
Collection from the Social Media Site	Full social credential profile access (including picture and list of friends) is not necessary for fulfilling operational purpose.	-Appropriation -Induced disclosure -Surveillance -Unanticipated Revelation	Stigmatization: Information is revealed about the individual that they would prefer not to disclose.	7
			Power Imbalance: People must provide extensive information, giving the acquirer an unfair advantage.	2
	Will users understand the eventual high-assurance credential is controlled by ACME and not by their social credential provider?	-This summary issue will be associated with another data action.		NA
	How will percept organization's priva willingness to con			

Data Actions	Summary Issues	Problematic Data Actions	Potential Problems for Individuals	Business Impact Factors					Total Business Impact (per Potential Problem)
				Noncompliance Costs	Direct Business Costs	Reputational Costs	Internal Culture Costs	Other	
Collection from the Social Media Site	Full social credential profile access (including picture and list of friends) is not necessary for fulfilling operational purpose.	-Appropriation -Induced disclosure -Surveillance -Unanticipated Revelation	Stigmatization	7	6	6	4		23
			Power Imbalance	7	6	8	4		25
	How will perception of the social media organization's privacy practices impact users' willingness to consent to this data action?	-Induced disclosure -Surveillance	Loss of Trust	7	6	8	7		28

Assess Privacy Risk





Resources

NIST Privacy Engineering Website:

http://csrc.nist.gov/projects/privacy_engineering/index.html

Draft NISTIR 8062:

http://csrc.nist.gov/publications/PubsDrafts.html#NIST-IR-8062