Privacy Engineering at NIST

Trustworthy Systems: Foundational to a Digital Society

What makes systems trustworthy?

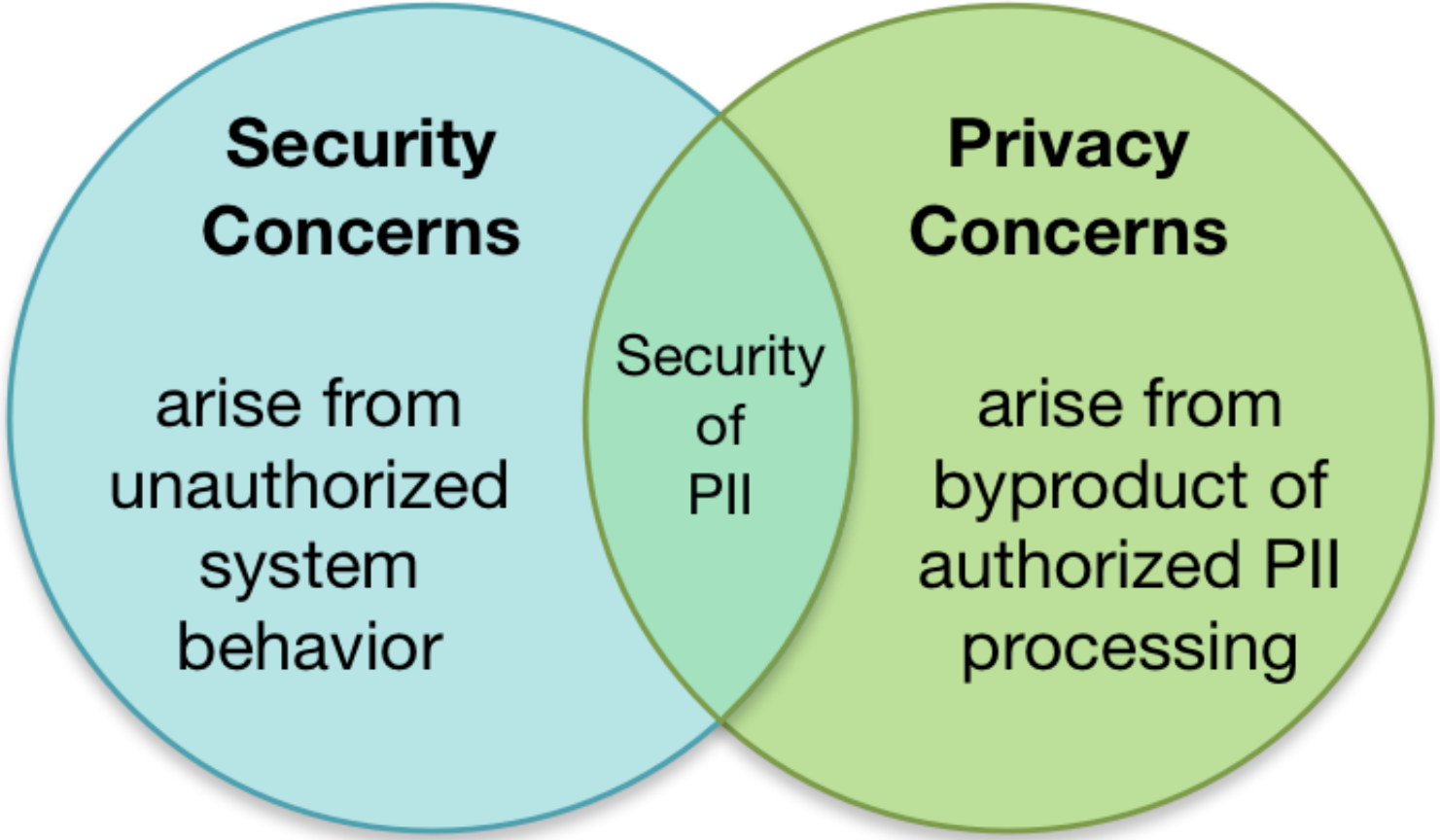
- Multiple attributes of trustworthiness include security, safety, reliability, etc.
- Privacy must be considered one of the attributes

How can we know if systems are trustworthy?

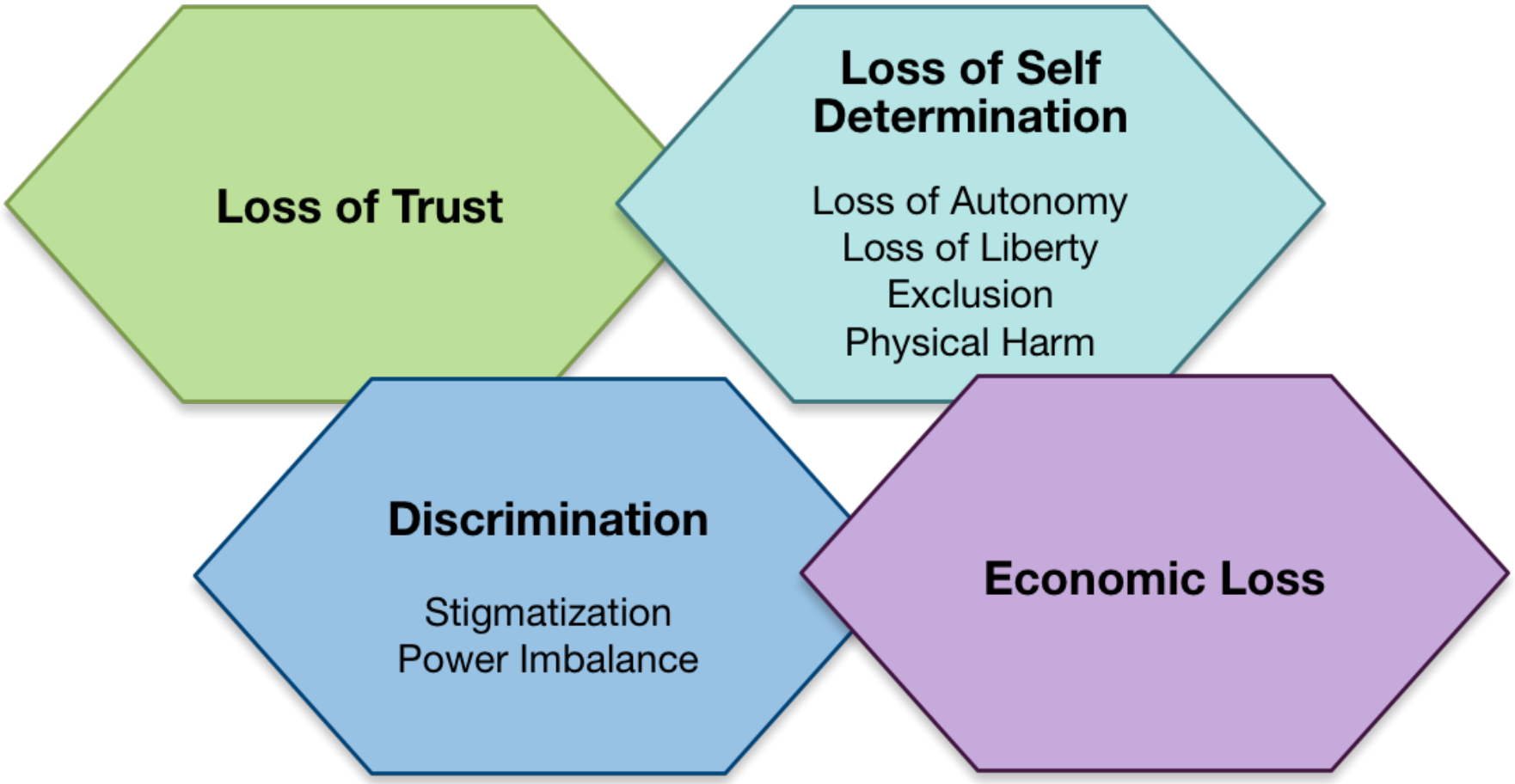
- Repeatable and measurable approaches help provide a sufficient base of evidence
- Privacy needs a body of guidance for repeatable and measurable approaches similar to other attributes of trustworthiness

NIST

Information Security and Privacy: Boundaries and Overlap



Processing PII Can Create Problems for Individuals



Identifying Risk

A measure of the extent to which an entity is threatened by a potential circumstance or event

A function of:

- Likelihood of occurrence
- Adverse impact that would occur

Security Risk = Vulnerability * Threat * Impact

System Privacy Risk Model

Privacy Risk = Likelihood of a Problematic Data Action * Impact of a Problematic Data Action

Likelihood is a contextual analysis that a data action is likely to create a problem for a representative set of individuals

Impact is an analysis of the indirect costs to an organization should the problem occur

Note: Contextual analysis is based on the data action performed by the system, the PII being processed, and a set of contextual considerations

Risk Management

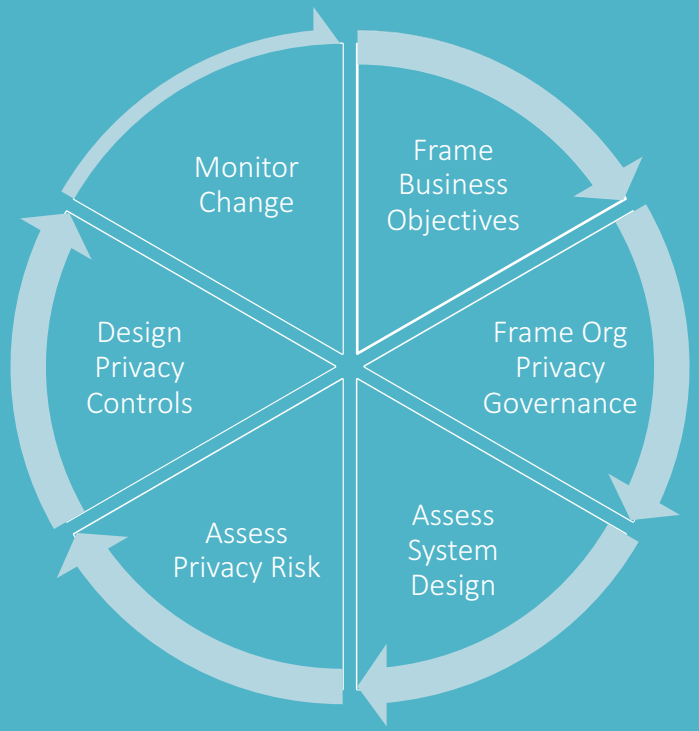
Risk can never be eliminated, so it must be managed.

Risk Responses

- Accept Risk
- Avoid risk
- Mitigate risk
- Transfer/share risk

Risk Decisions

- Organization-wide process
- Optimization factors include: mission objectives; other risk areas (financial, legal, etc.)

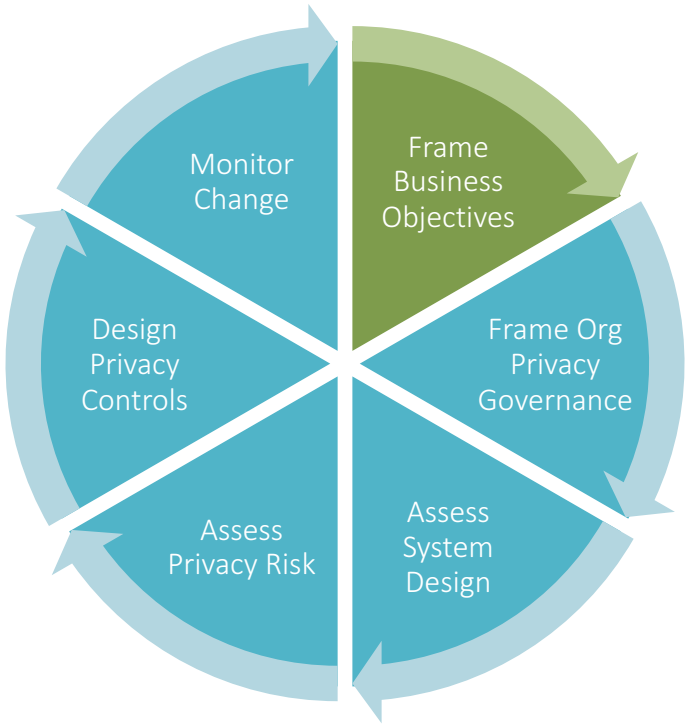


Privacy Risk Assessment

Systems Engineering

- An important objective is to deliver systems that are deemed trustworthy
- Balances the often conflicting design constraints of performance, cost, schedule, and effectiveness to optimize the solution while providing an acceptable level of risk.
- Holistic process that must account for the needs and expectations of stakeholders is particularly relevant for privacy.
  - "Privacy engineers" can take individuals' privacy interests into account, resulting in a system that may be less likely to create problems for them.

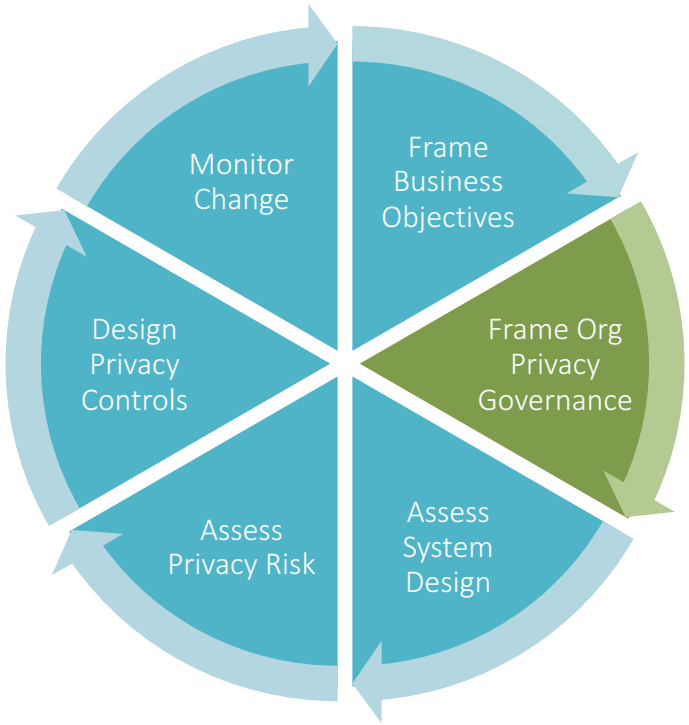
Frame Business Objectives



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

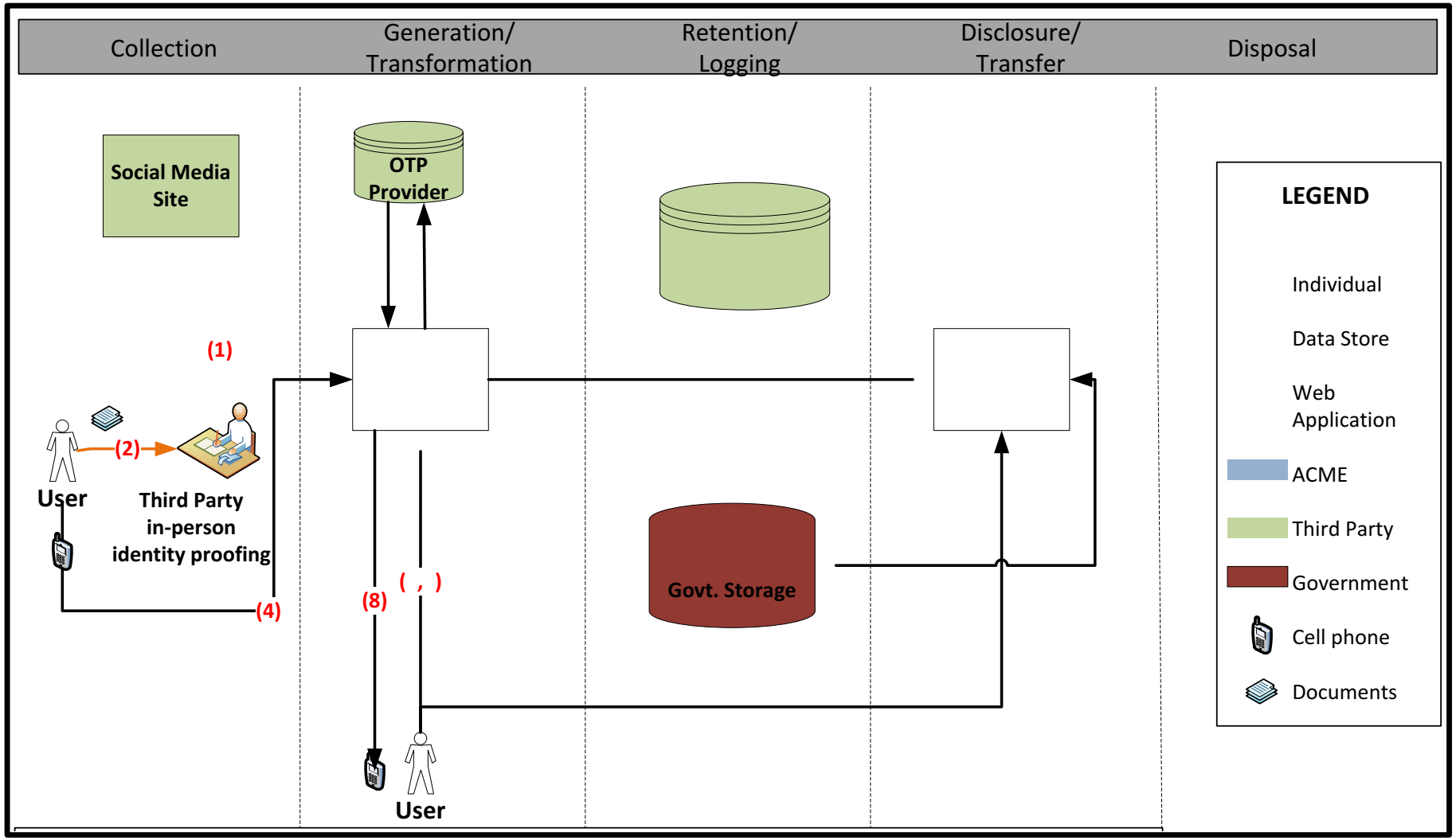


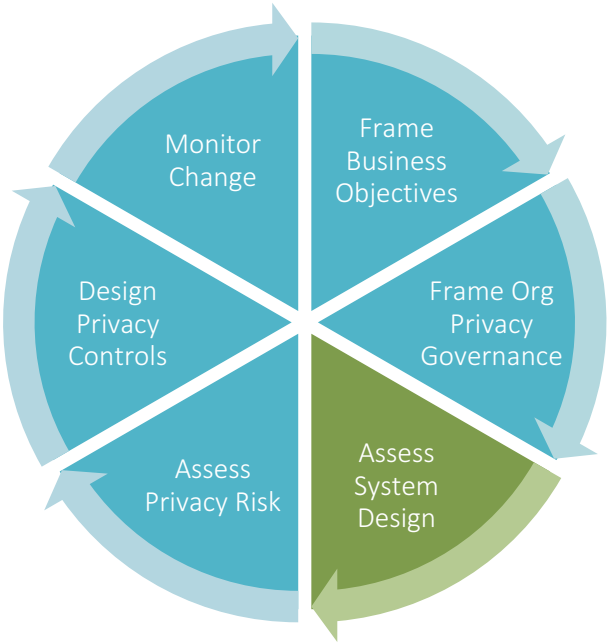
Frame the organizational privacy governance by identifying privacy-related legal obligations, principles, organizational goals and other commitments.

- 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.

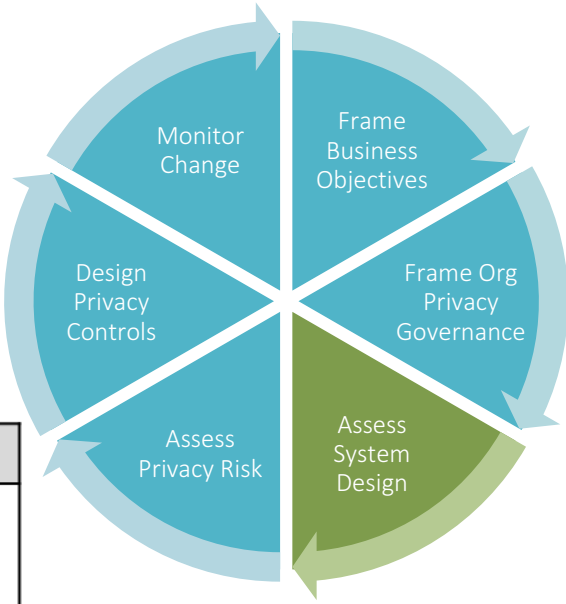
NIST

Assess System Design – Data Actions





Assess System Design - Context



Example:

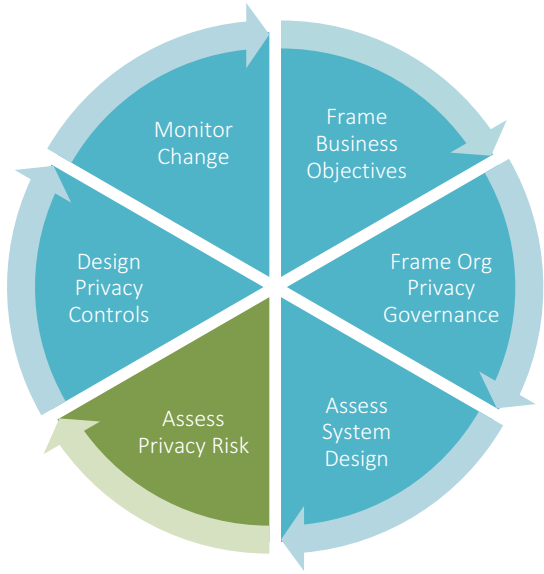
An individual wishes to use ACME IDP service to augment a social credential with identity proofing and a second authentication factor to create a stronger credential. This stronger credential will be used to access government benefits.

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

NIST

Assess Privacy Risk



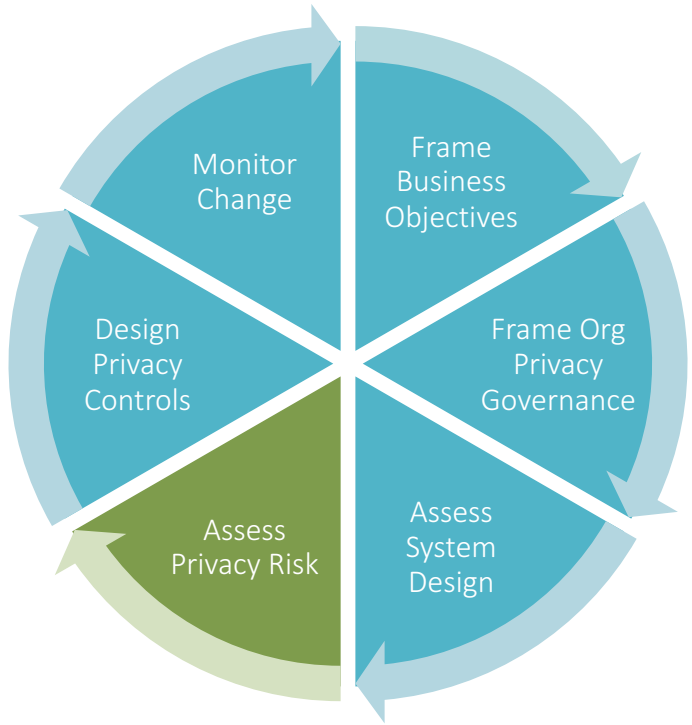
SAMPLE TABLE

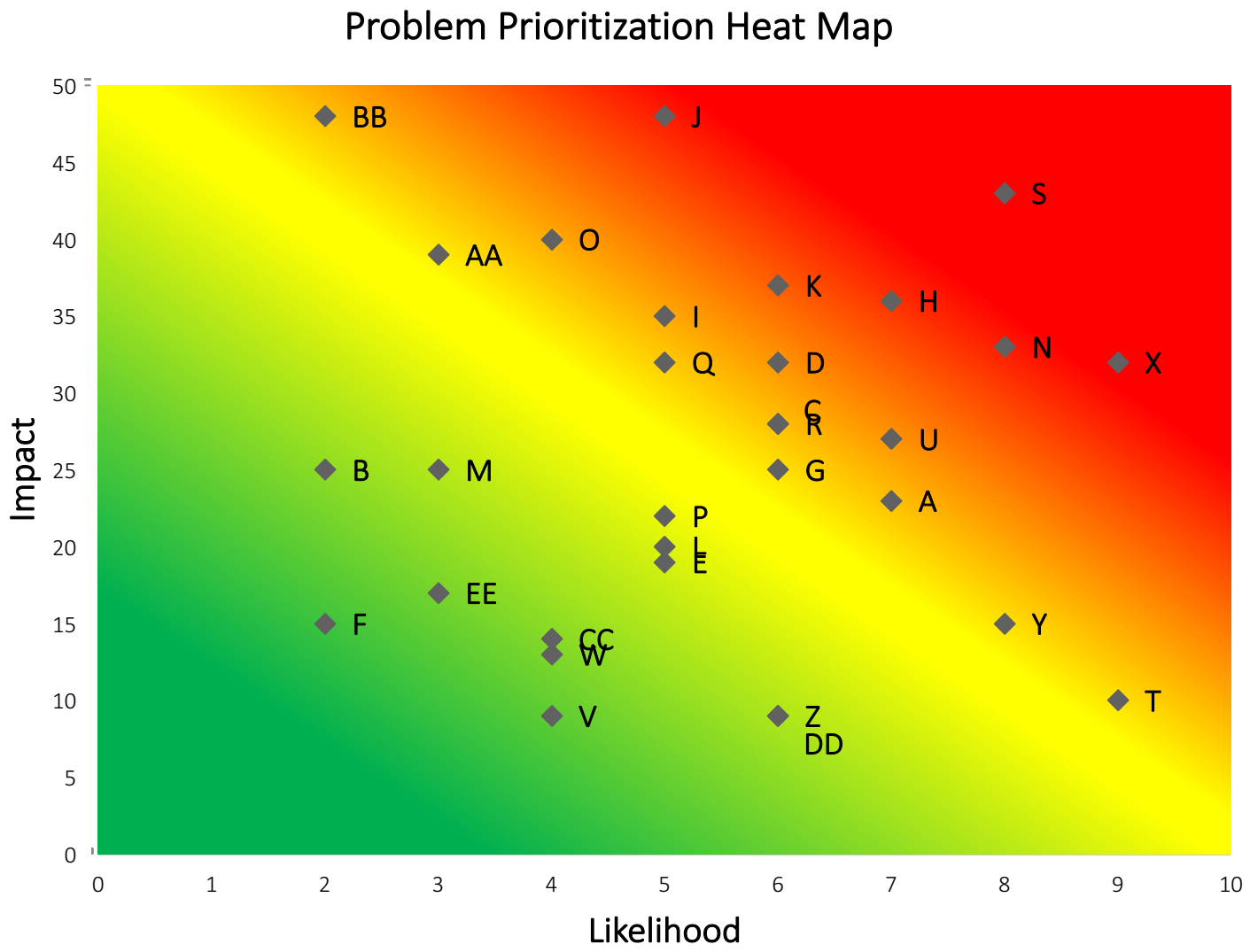
Data Actions	Summary Issues	Problematic Data Actions	Potential Problems for Individuals	Likelihood
Collection from the Social Media Site	Full social credential profile access (including picture and list of friends) is not necessary for fulfilling operational purpose.	-Appropriation -Induced disclosure -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

NIST

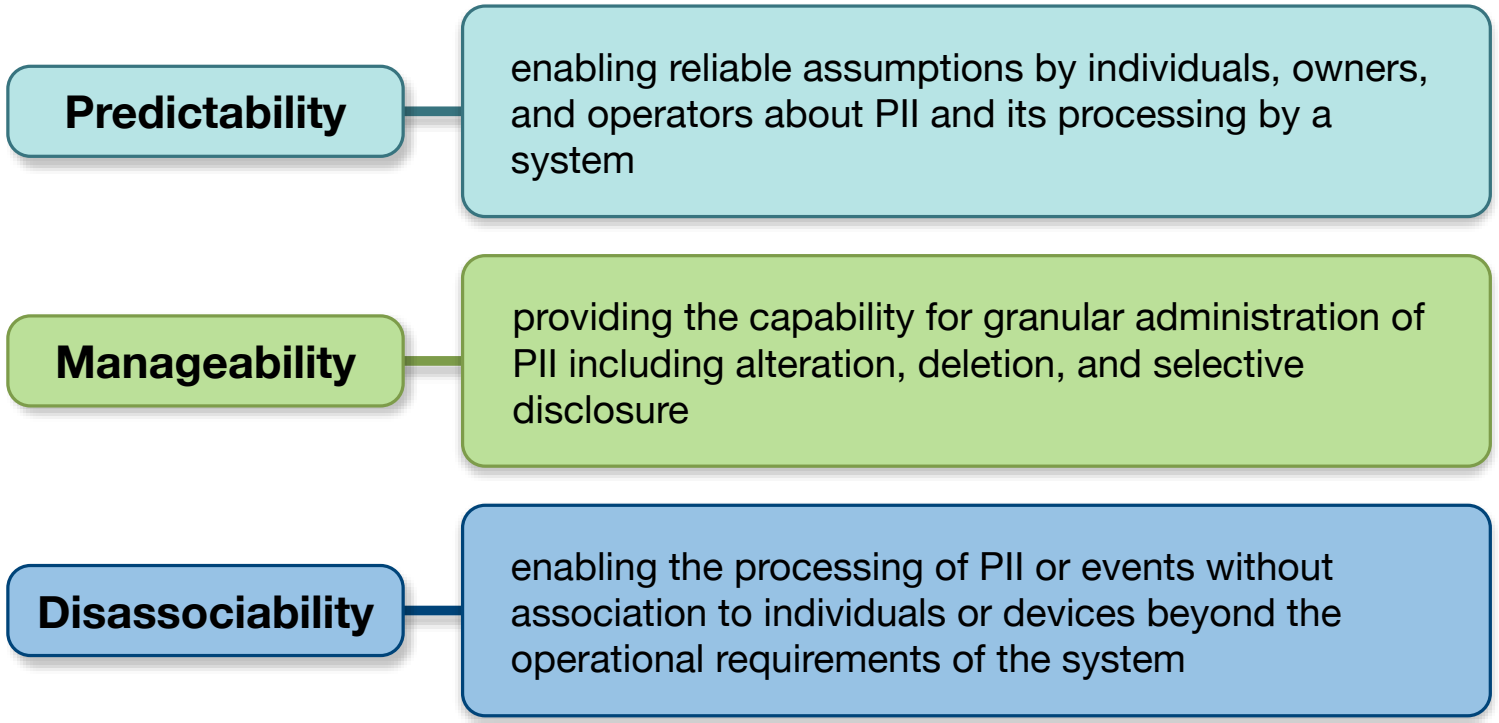
Assess Privacy Risk





NIST Privacy Engineering Objectives

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



A Driver for System Capabilities

377

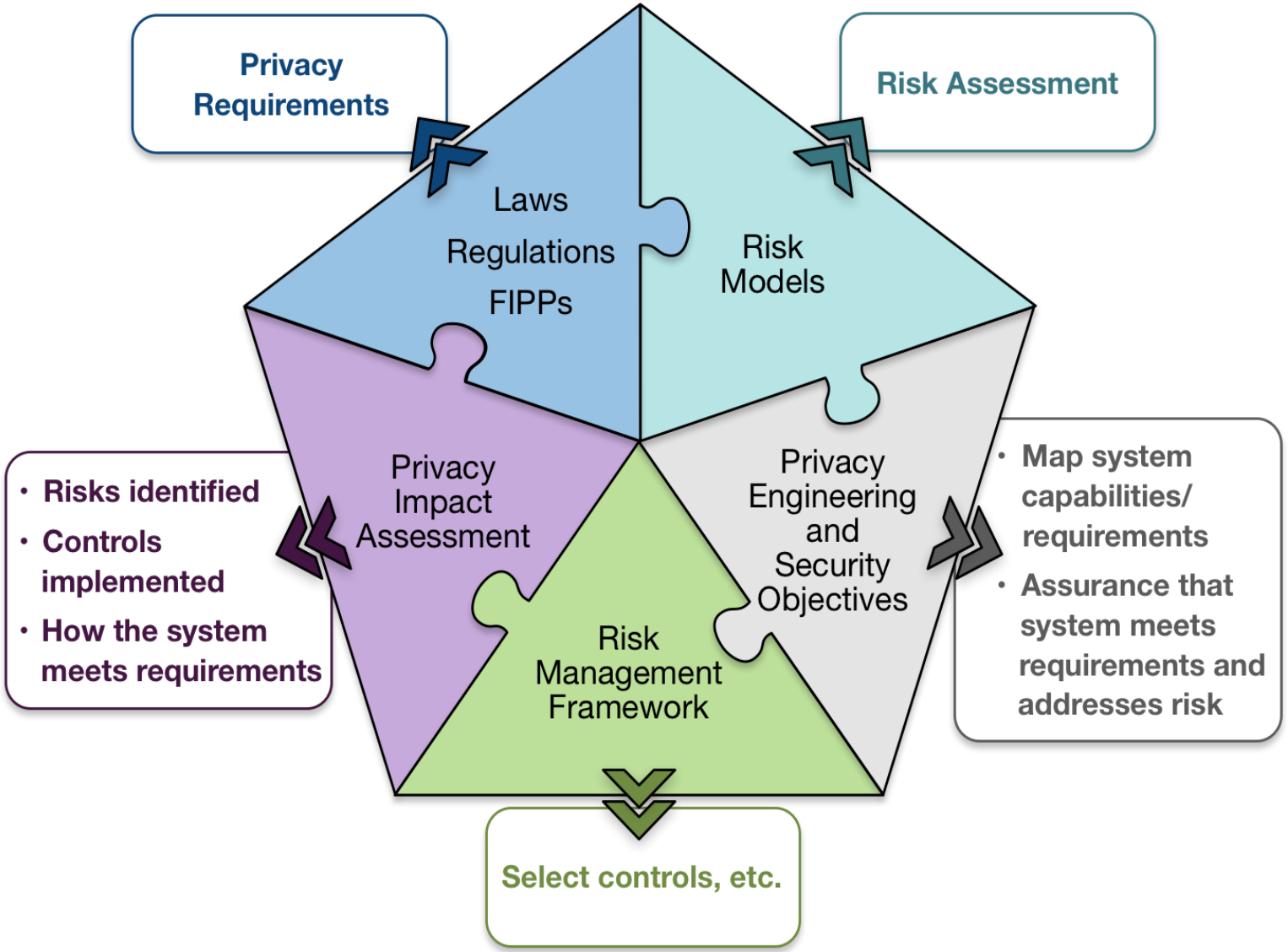
Table 4 - Privacy Objectives

Privacy Engineering Objective	Example Capability(ies)
predictability	• Enables user, RP, IdP and identity broker assumptions that identity broker does not have access to user identity attributes. • Enables user, RP, IdP and identity broker assumptions that IdP cannot process information about user's relationship with the RP. • Enables user, RP, IdP and identity broker assumptions that RP cannot process information about user's relationship with the IdP.
disassociability	• The identity broker can transmit identity attributes from an IdP to an RP without being able to access them. • The RP can accept an authentication assertion and identity attributes without associating a user to an IdP. • The IdP can transmit an authentication assertion and identity attributes without associating a user to an RP.

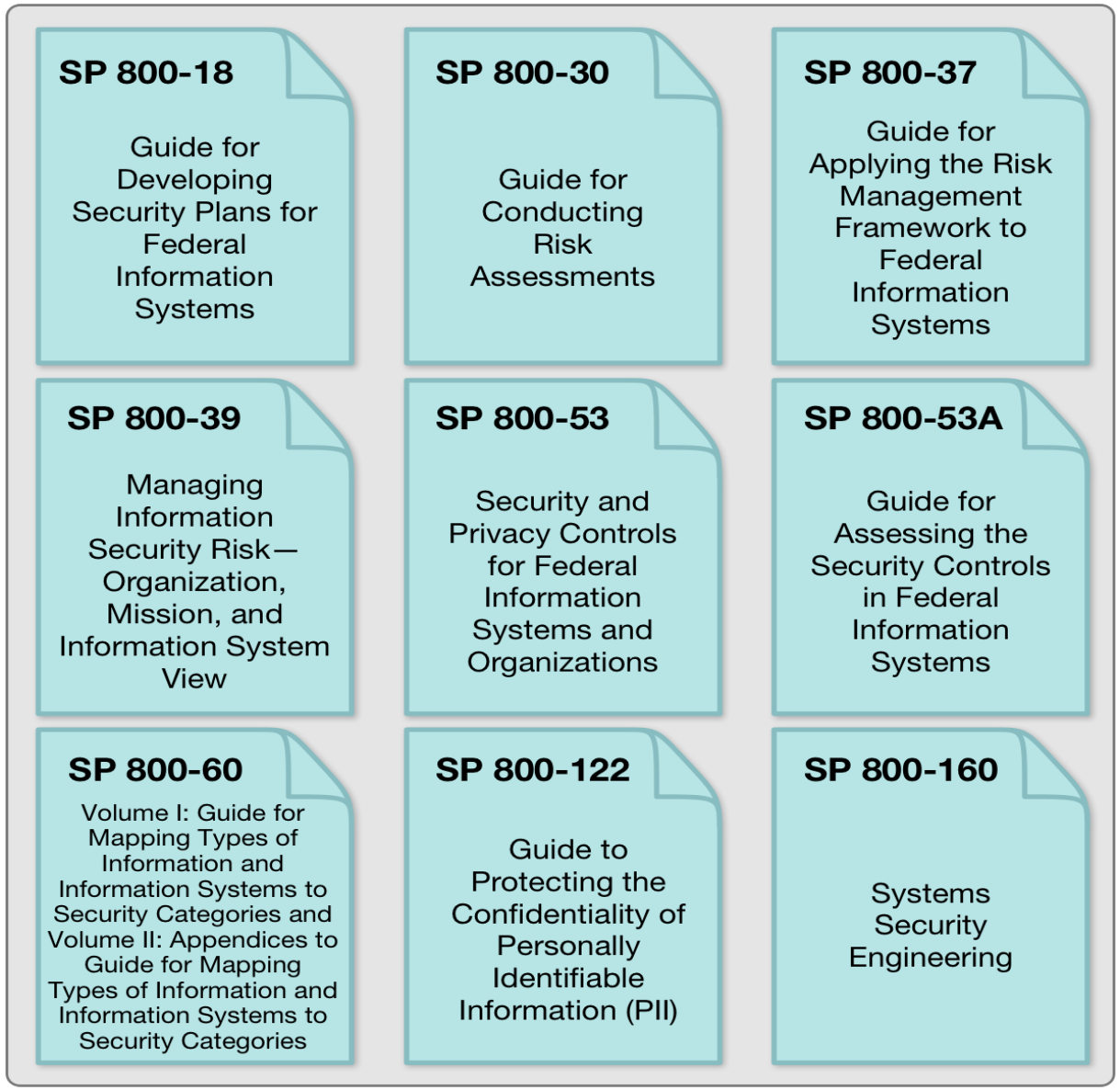
378

NIST

Putting It All Together



Guidance Roadmap



800-53 Current Drivers

- OMB update in July 2016 to Circular A-130 clarified that federal agencies' obligations with respect to managing privacy risk and information resources extends beyond compliance with privacy laws, regulations, and policies, and that agencies must **apply the NIST Risk Management Framework (NIST RMF)** to their privacy programs and Information Systems.

- NIST Special Publication (SP) 800-53 Security and Privacy Controls for Federal Information Systems and Organizations is in the revision 5 cycle now.

800-53 Rev. 5 Proposed Control Families

Control Identifiers and Family Names			
ID	FAMILY	ID	FAMILY
AC	Access Control	MP	Media Protection
AT	Awareness and Training	PA	Privacy Authorization
AU	Audit and Accountability	PE	Physical and Environmental Protection
CA	Assessment and Authorization	PL	Planning
CM	Configuration Management	PM	Program Management
CP	Contingency Planning	PS	Personnel Security
IA	Identification and Authentication	RA	Risk Assessment
IP	Individual Participation	SA	System and Services Acquisition
IR	Incident Response	SC	System and Communications Protection
MA	Maintenance	SI	System and Information Integrity

Proposed New Privacy Families

Privacy Authorization	Individual Participation
PA-1 Privacy Authorization Policy and Procedures	IP-1 Individual Participation Policy and Procedures
PA-2 Authority to Collect	IP-2 Consent
PA-3 Purpose Specification	IP-3 Redress
PA-4 Information Sharing with Third Parties	IP-4 Privacy Notice
	IP-5 Privacy Act Statements
	IP-6 Individual Access

Proposed PM Control Family

Security & Integrated Controls	Privacy Controls
Information Security Program Plan	Agency Privacy Program Plan
Senior Information Security Officer	Senior Agency Official for Privacy
Information Security and Privacy Resources	System of Records Notices
Plan of Action and Milestones Process	Dissemination of Privacy Program Information
System Inventory	Accounting of Disclosures
Information Security and Privacy Measures of Performance	Data Quality Management
Enterprise Architecture	Data Management Board
Critical Infrastructure Plan	Data Integrity Board
Risk Management Strategy	Minimization of Personally Identifiable Information in Testing, Training, and Research
Authorization Process	Individual Access Control
Mission and Business Process Definition	Complaint Management
Insider Threat Program	Inventory of Personally Identifiable Information
Information Security and Privacy Workforce	Privacy Reporting
Testing, Training, and Monitoring	
Contacts with Groups and Associations	
Threat Awareness Program	

Resources

Ellen Nadeau

Ellen.nadeau@nist.gov

NIST Privacy Engineering Website:

https://www.nist.gov/programs-projects/privacy-engineering

NIST Internal Report 8062

https://doi.org/10.6028/NIST.IR.8062