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

Federal Security and Privacy Legal Frameworks

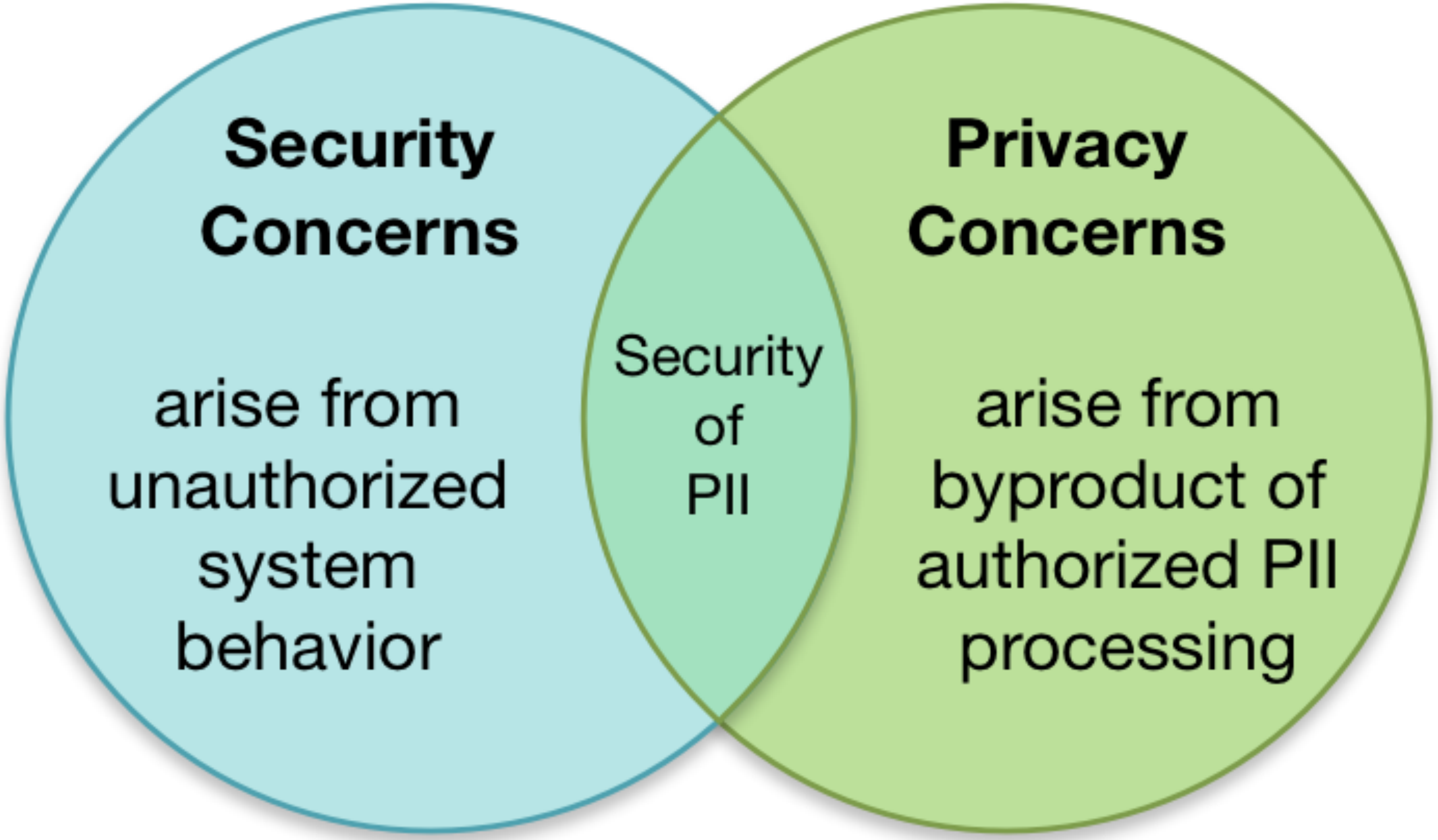
- ➢ FISMA – Federal Information Security Management Act

Requires implementation of “information security protections commensurate with the risk and magnitude of the harm”

- ➢The Privacy Act of 1974

Establishes a code of fair information practices that governs the collection, maintenance, use, and dissemination of information about individuals that is maintained in systems of records by federal agencies.

Information Security and Privacy: Boundaries and Overlap



Security Concerns

arise from unauthorized system behavior

Security of PII

Privacy Concerns

arise from byproduct of authorized PII processing

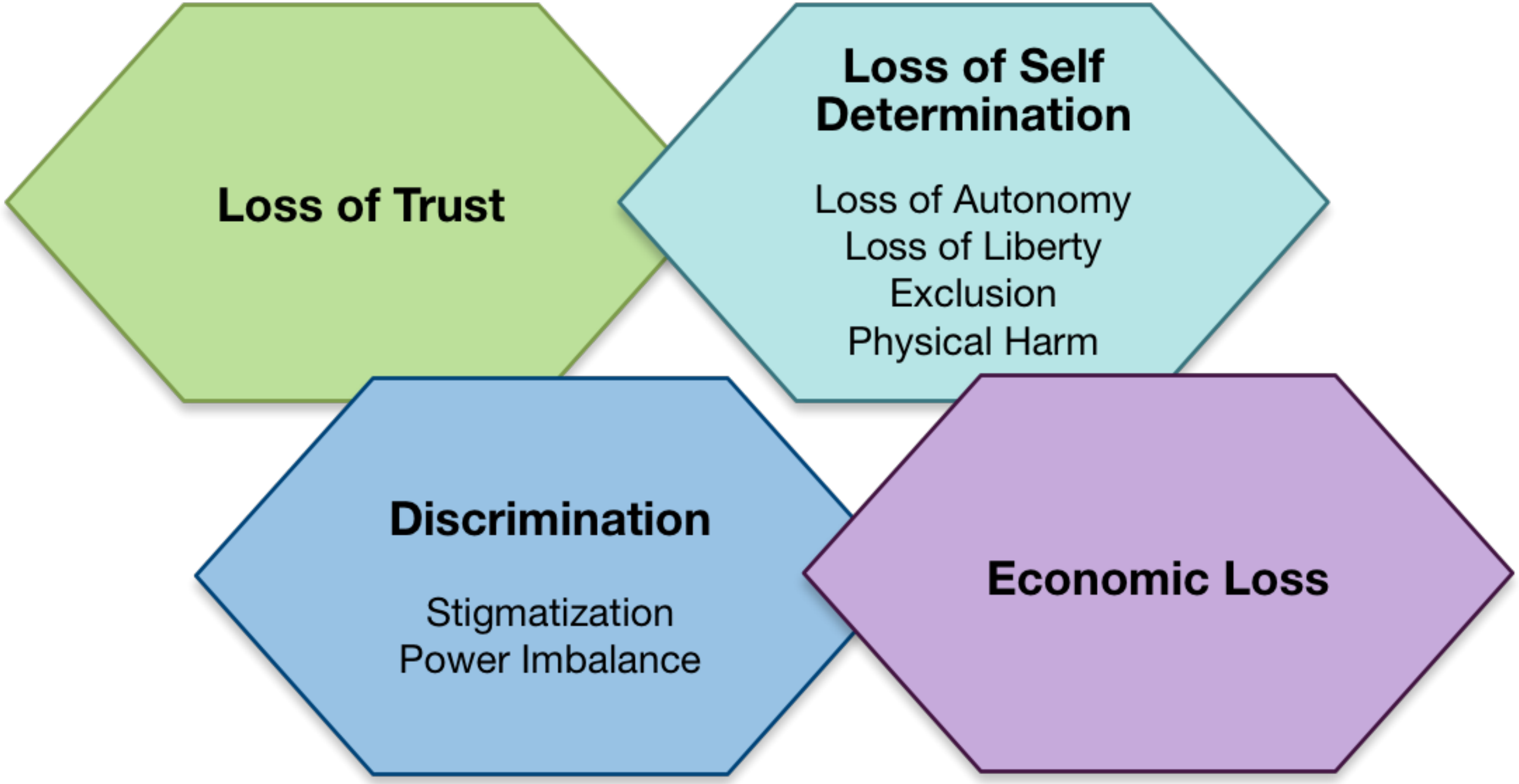
Identifying Risk

Risk is a function of:

- Likelihood of occurrence of adverse event
- Impact that would occur

Security Risk = Vulnerability * Threat * Impact

Processing PII Can Create Problems for Individuals



Loss of Trust

Loss of Self Determination

Loss of Autonomy
Loss of Liberty
Exclusion
Physical Harm

Discrimination

Stigmatization
Power Imbalance

Economic Loss

NIST Working Model for System Privacy Risk

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 costs 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

NIST

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.)

Systems Engineering

- **Systems Engineering**: An engineering discipline whose responsibility is creating and executing an interdisciplinary process to ensure that the customer and all other stakeholder needs are satisfied in a high-quality, trustworthy, cost-efficient, and schedule-compliant manner throughout a system's entire life cycle.
  - 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.
  - "Privacy engineers" can take individuals' privacy interests into account, resulting in a system that may be less likely to create problems for them.

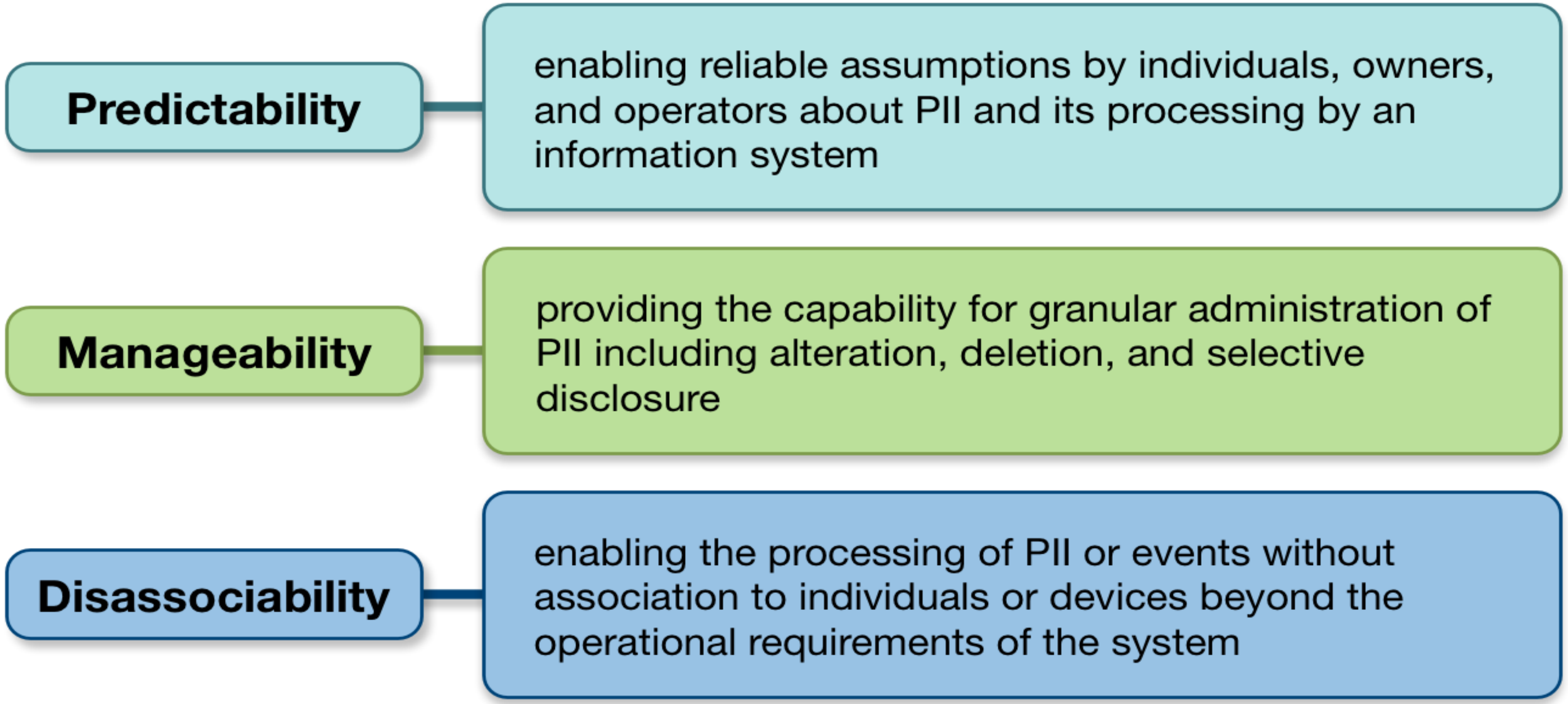
NIST Working Definition of Privacy Engineering

A specialty discipline of systems engineering focused on achieving freedom from conditions that can create problems for individuals with unacceptable consequences that arise from the system as it processes PII.

*Is PII the correct term in light of IoT systems' impact on people, not just data?

NIST Privacy Engineering Objectives

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



Predictability

enabling reliable assumptions by individuals, owners, and operators about PII and its processing by an information system

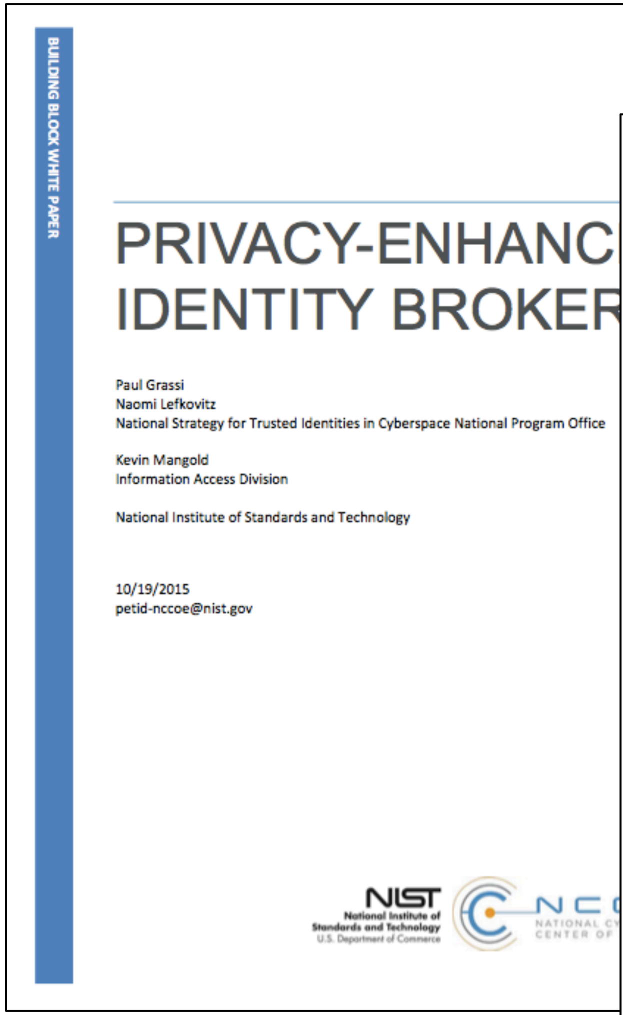
Manageability

providing the capability for granular administration of PII including alteration, deletion, and selective disclosure

Disassociability

enabling the processing of PII or events without association to individuals or devices beyond the operational requirements of the system

A Driver for System Capabilities



BUILDING BLOCK WHITE PAPER

PRIVACY-ENHANC
IDENTITY BROKER

Paul Grassi
Naomi Lefkovitz
National Strategy for Trusted Identities in Cyberspace National Program Office

Kevin Mangold
Information Access Division

National Institute of Standards and Technology

10/19/2015
petid-nccoe@nist.gov

NIST
National Institute of Standards and Technology
U.S. Department of Commerce
NC
NATIONAL C
CENTER OF

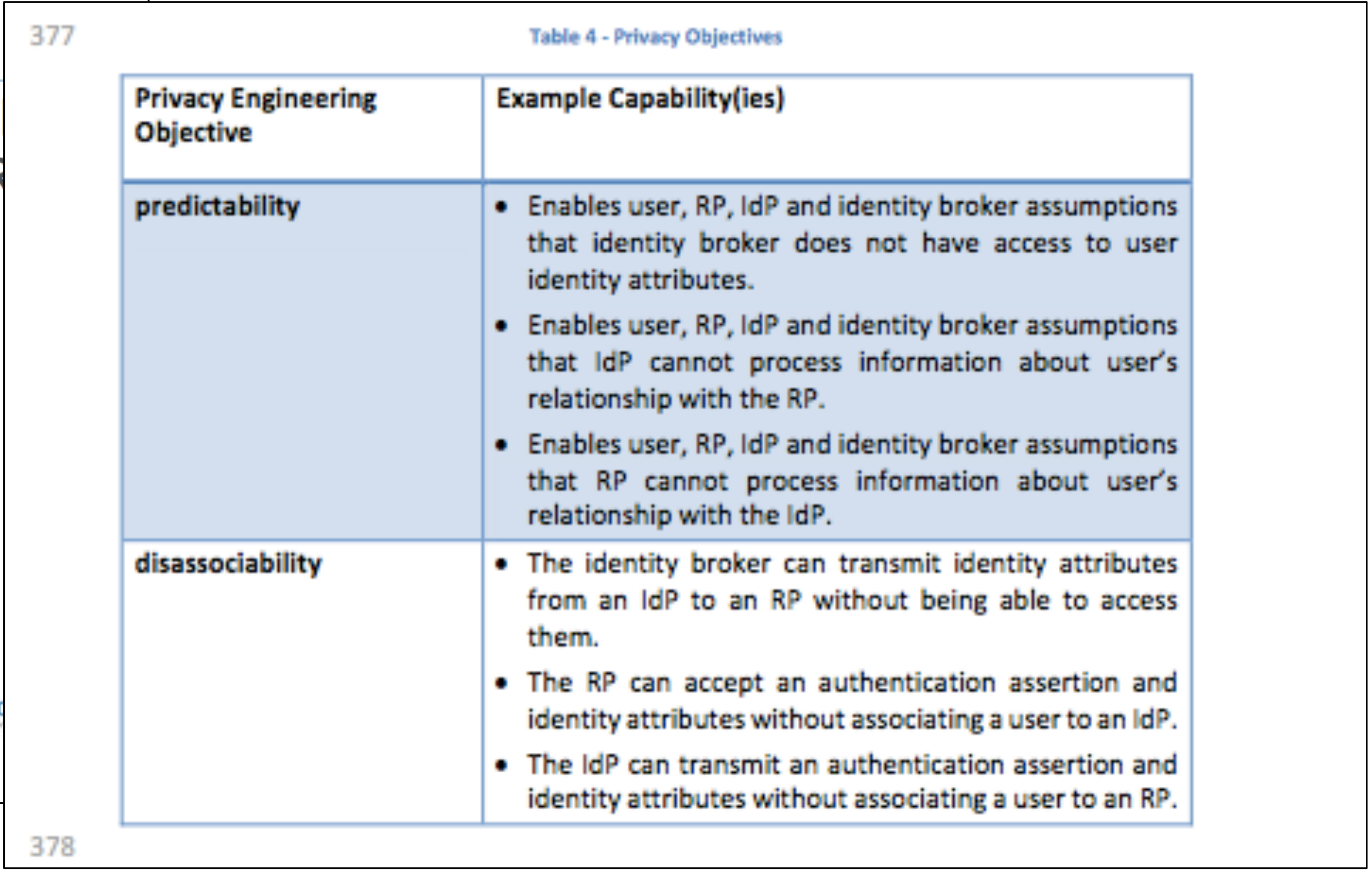
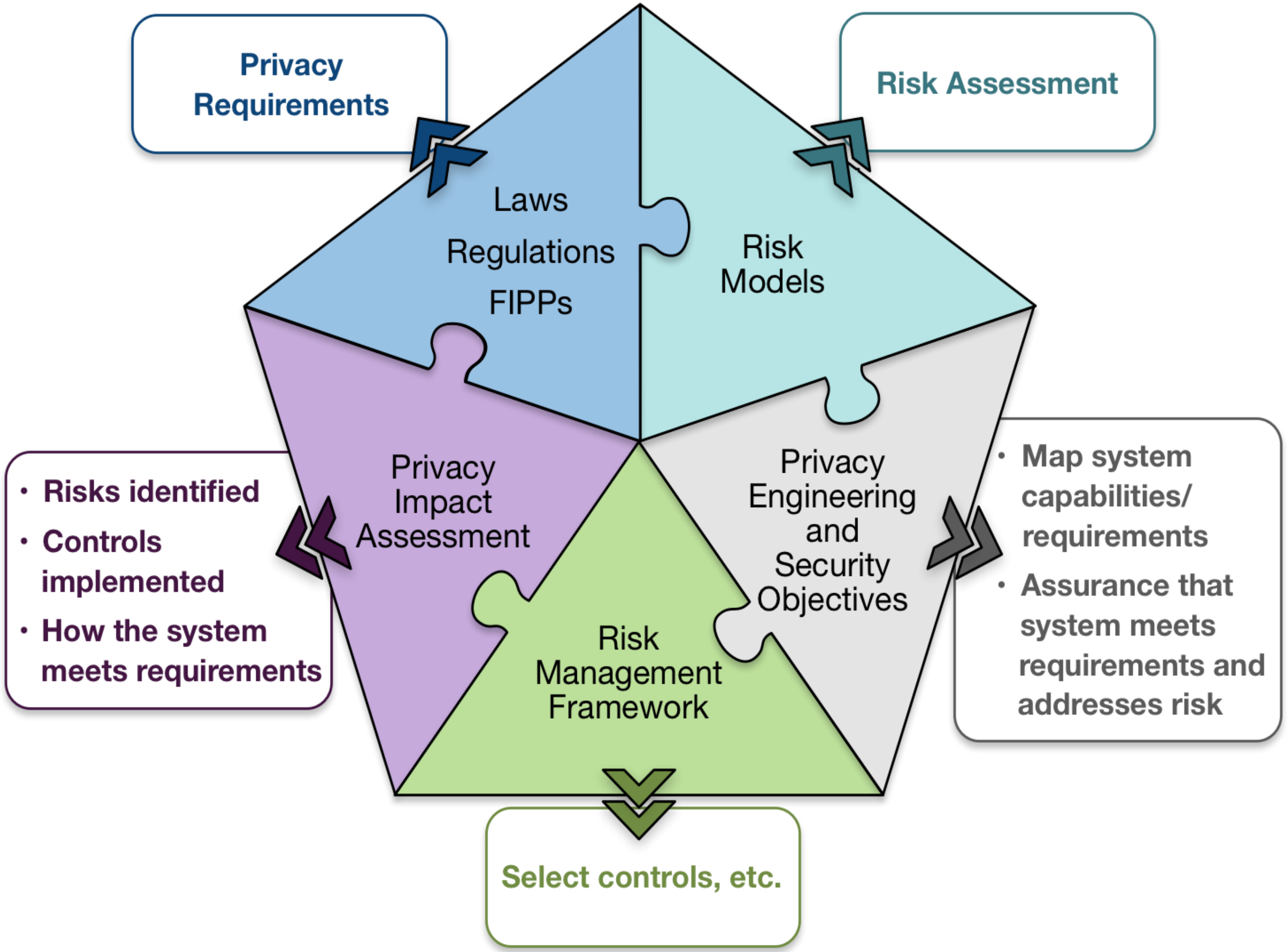


Table 4 - Privacy Objectives

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.

Putting It All Together


Laws
Regulations
FIPPs
Risk Models
Privacy Impact Assessment
Privacy Engineering and Security Objectives
Risk Management Framework

Privacy Requirements

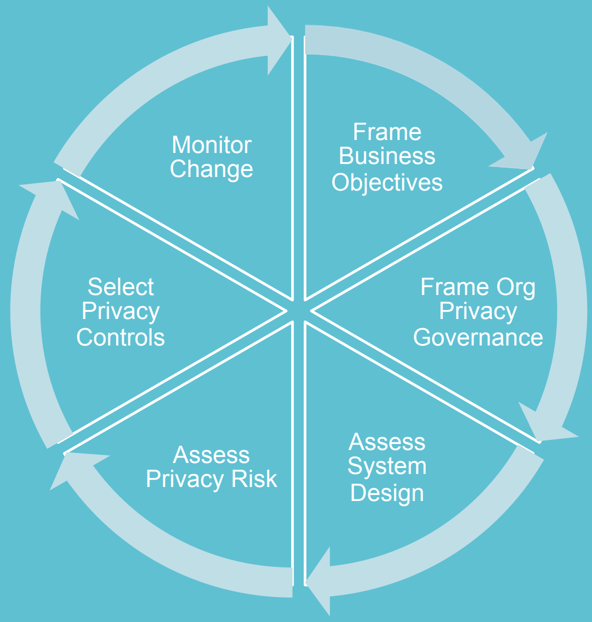
Risk Assessment

- **Risks identified**
- **Controls implemented**
- **How the system meets requirements**

- **Map system capabilities/ requirements**
- **Assurance that system meets requirements and addresses risk**

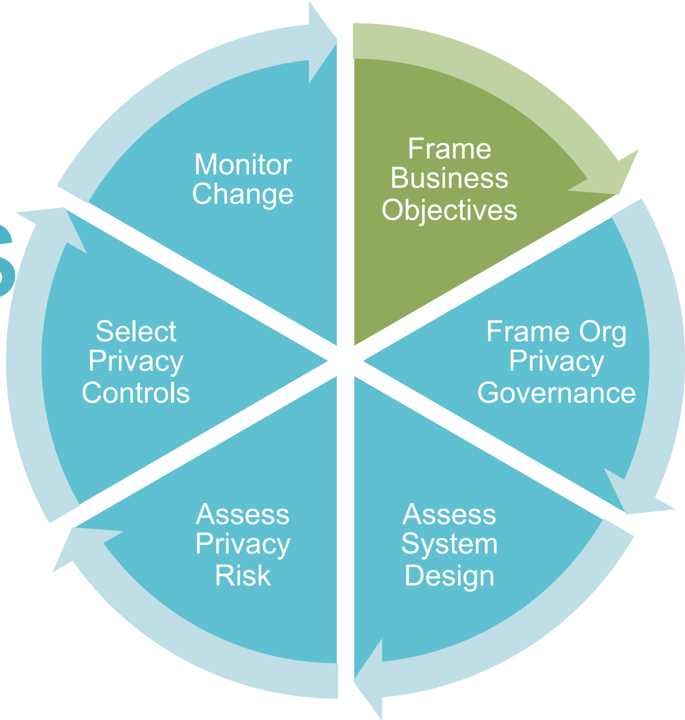
Select controls, etc.

NIST



Privacy Risk Assessment Methodology (PRAM)

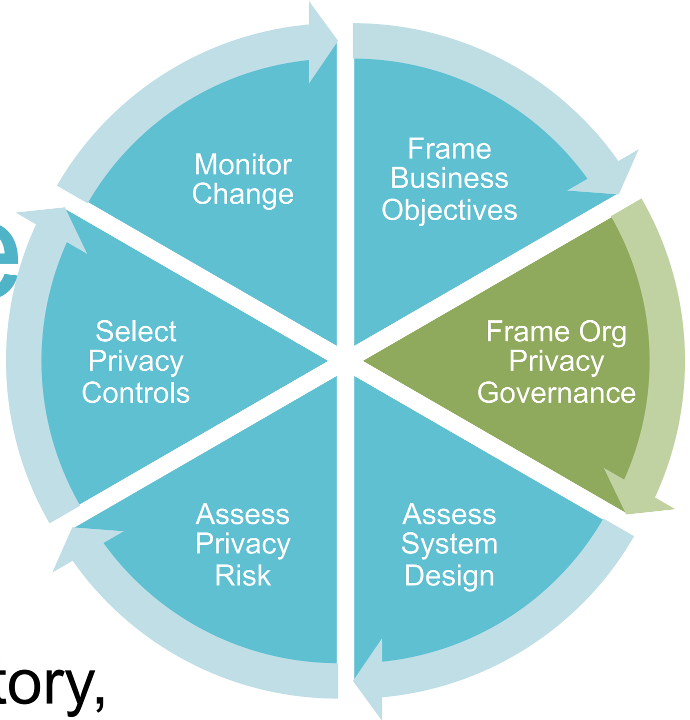
Frame Business Objectives



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.

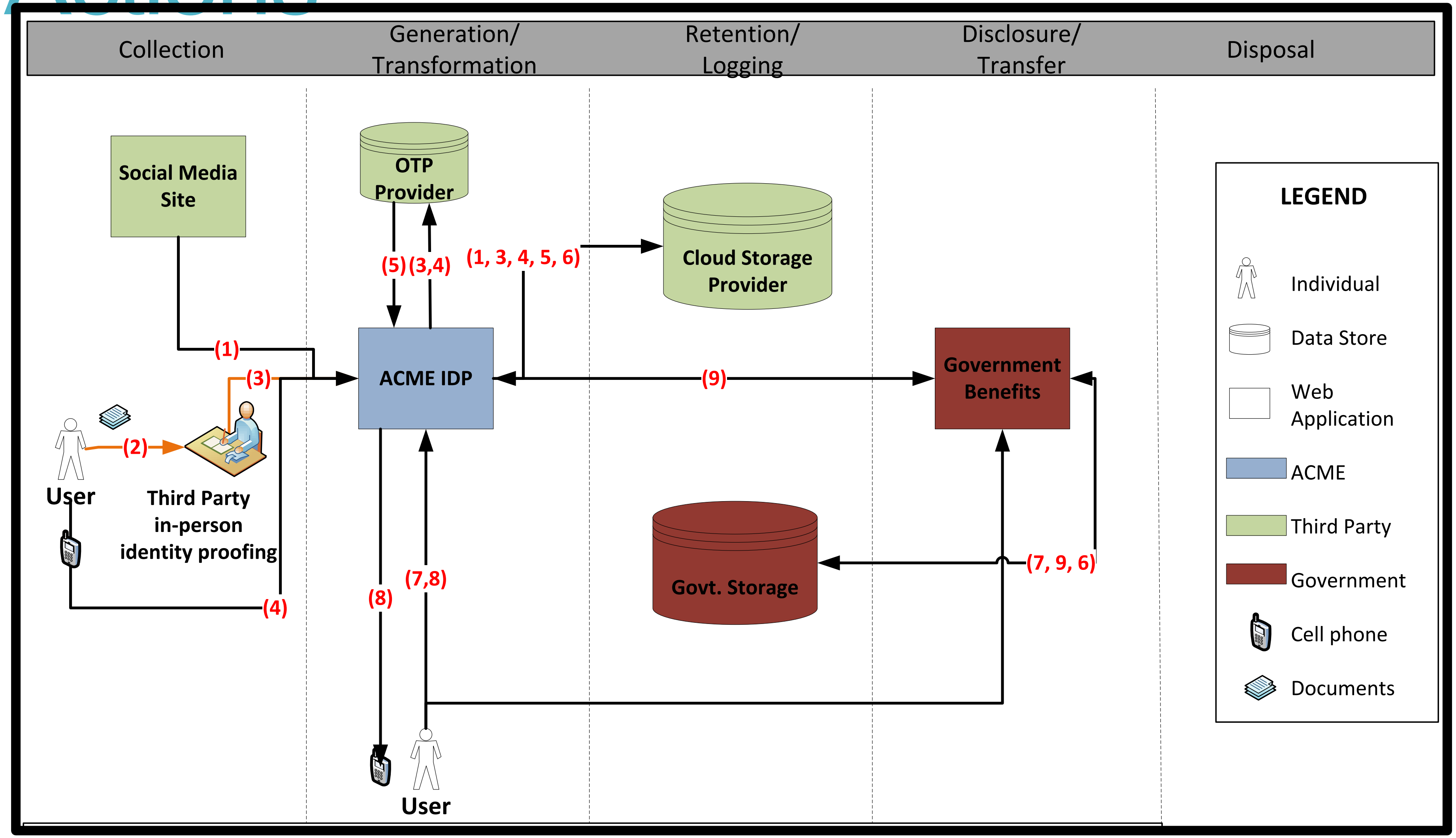
Frame Privacy Governance

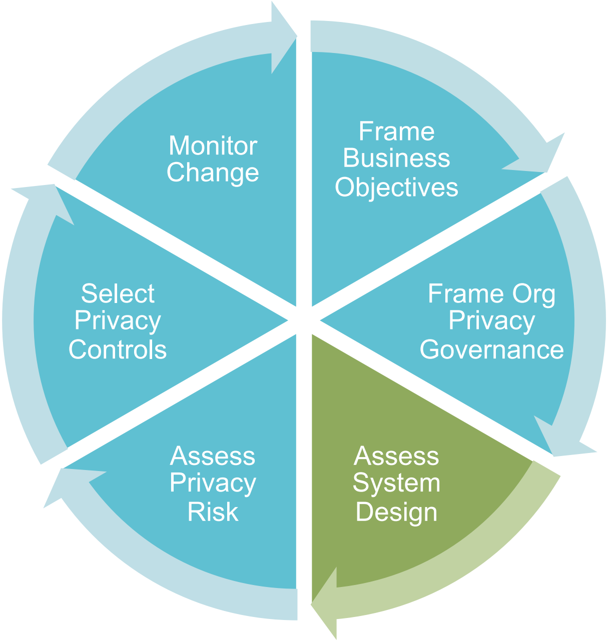


Frame the organizational privacy governance by identifying privacy-related legal obligations, principles, organizational goals and other commitments.

- 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





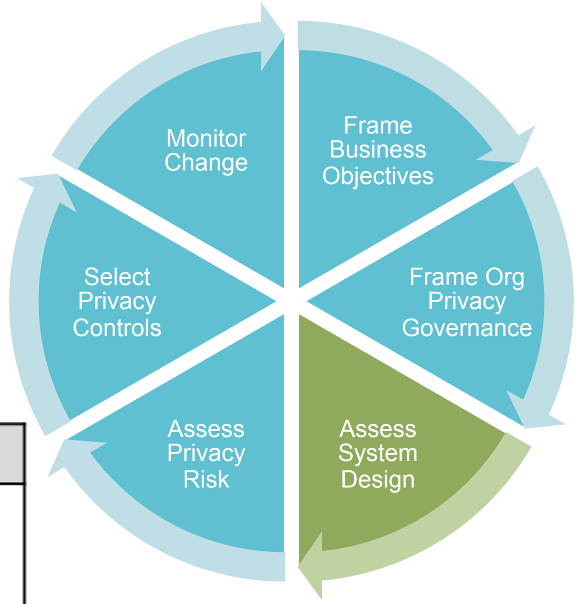
Assess System Design - Context

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.

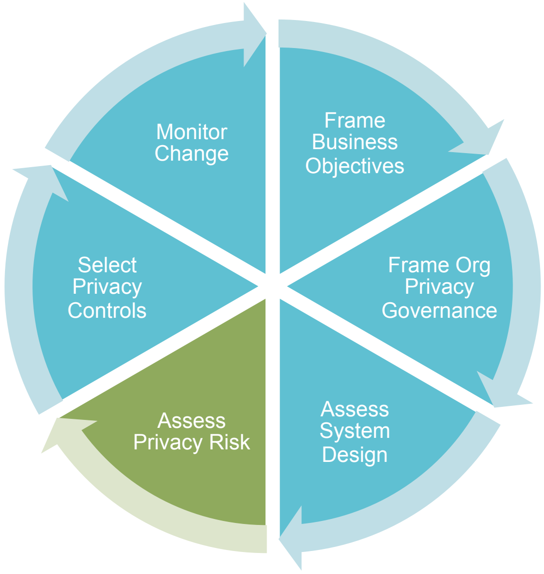
Data Action	Personal Information	Specific Context	Summary Issues
Collection from the Social Media Site	- Self-Asserted Full Name - Validated Email -List of Friends -Profile Photograph	- One-time action (per user) between social credential and ACME IDP, but establishes an ongoing relationship between 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



NIST

Assess Privacy Risk

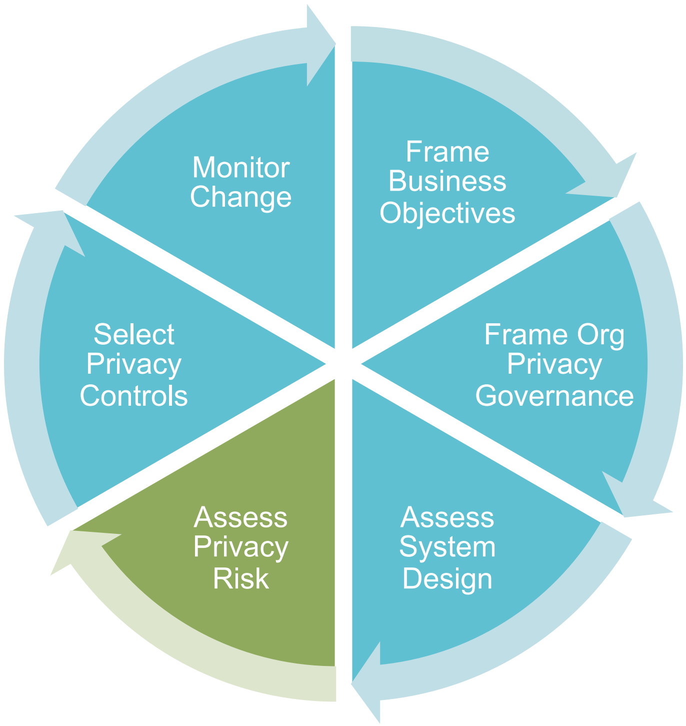


SAMPLE TABLE

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

Assess Privacy Risk



Monitor Change

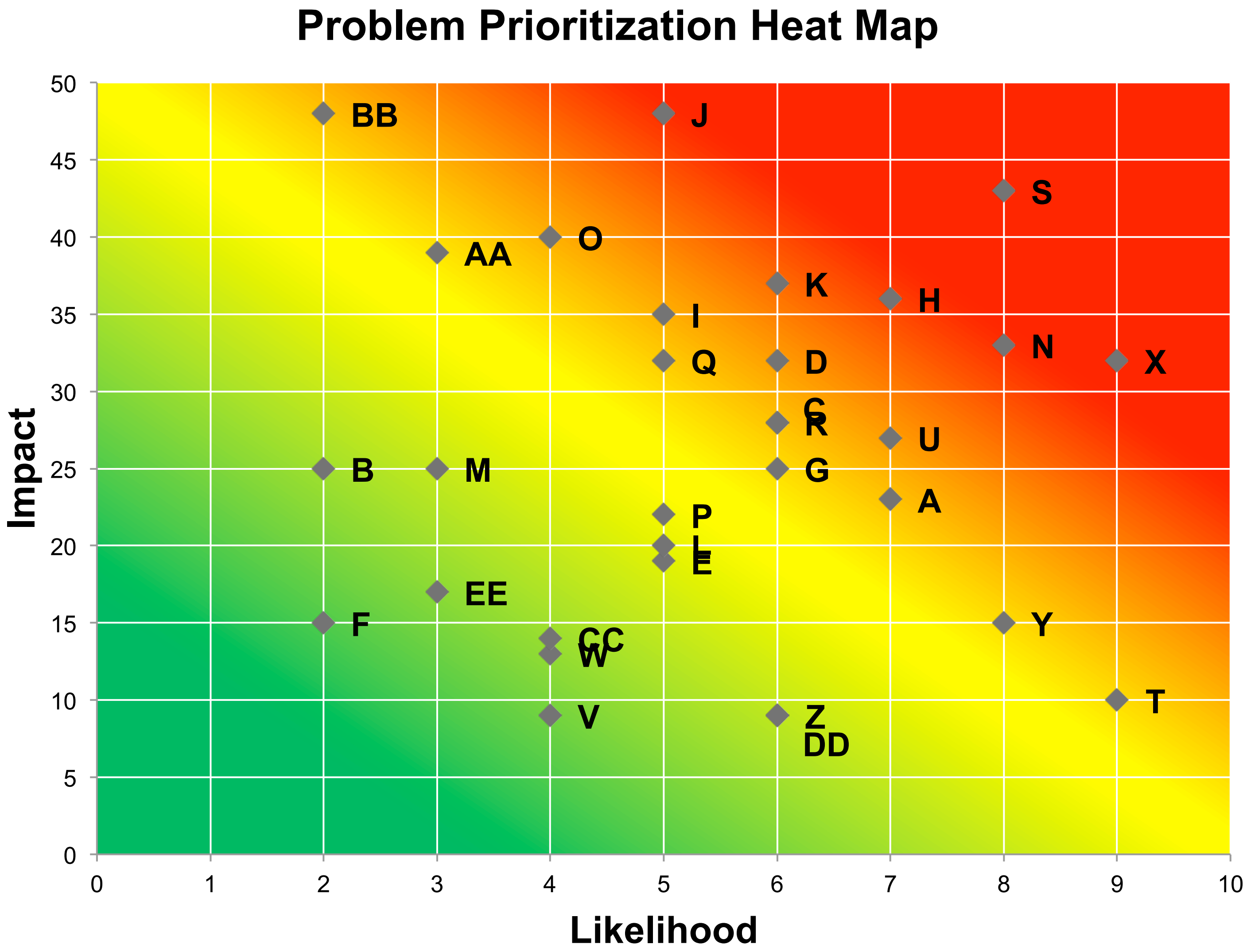
Frame Business Objectives

Frame Org Privacy Governance

Assess System Design

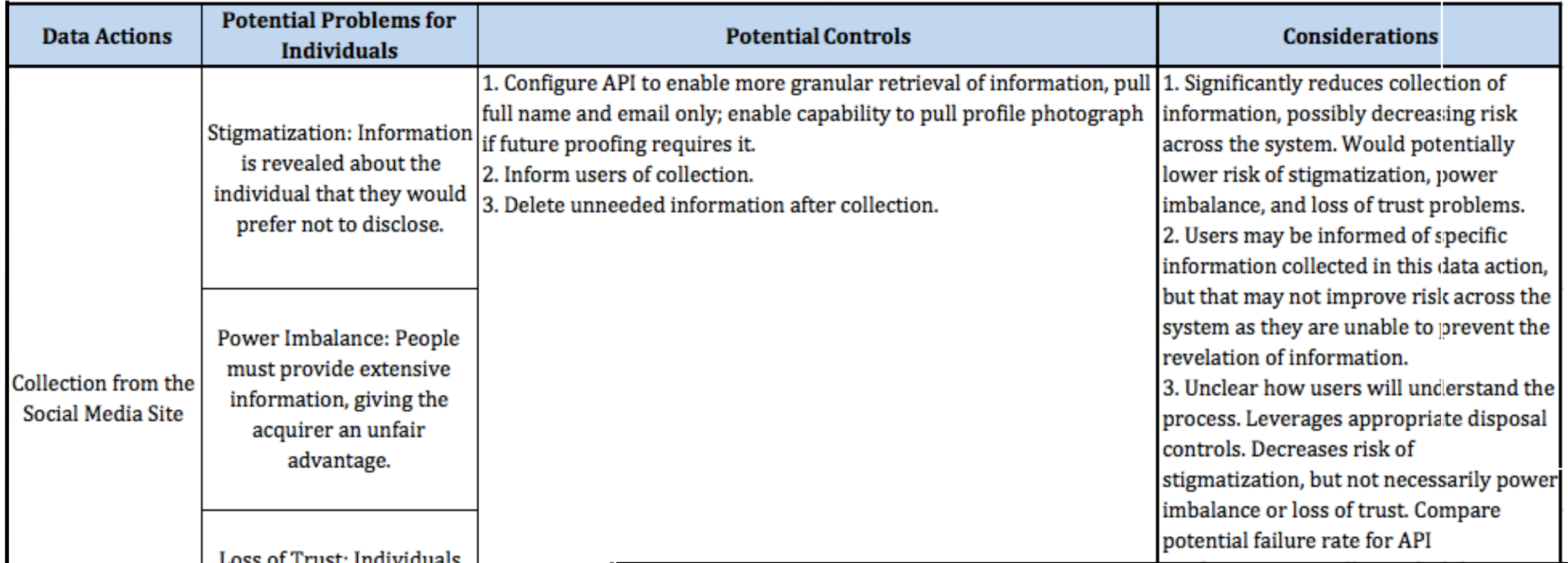
Assess Privacy Risk

Select Privacy Controls

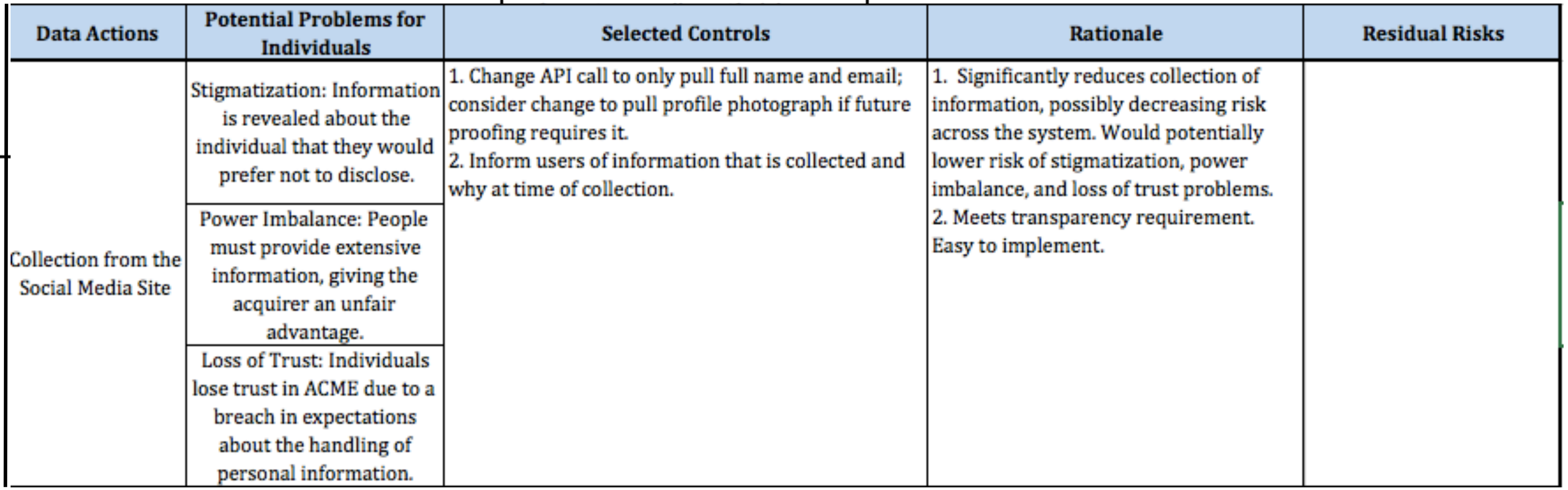


Problem Prioritization Heat Map

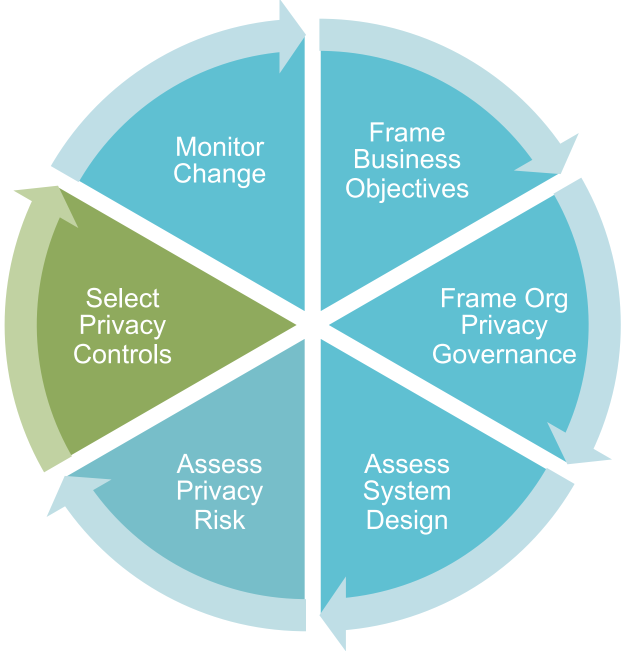
Select Privacy Controls



Data Actions	Potential Problems for Individuals	Potential Controls	Considerations
Collection from the Social Media Site	Stigmatization: Information is revealed about the individual that they would prefer not to disclose.	1. Configure API to enable more granular retrieval of information, pull full name and email only; enable capability to pull profile photograph if future proofing requires it. 2. Inform users of collection. 3. Delete unneeded information after collection.	1. Significantly reduces collection of information, possibly decreasing risk across the system. Would potentially lower risk of stigmatization, power imbalance, and loss of trust problems. 2. Users may be informed of specific information collected in this data action, but that may not improve risk across the system as they are unable to prevent the revelation of information. 3. Unclear how users will understand the process. Leverages appropriate disposal controls. Decreases risk of stigmatization, but not necessarily power imbalance or loss of trust. Compare potential failure rate for API
	Power Imbalance: People must provide extensive information, giving the acquirer an unfair advantage.		
	Loss of Trust: Individuals lose trust in ACME due to a breach in expectations about the handling of personal information.		



Data Actions	Potential Problems for Individuals	Selected Controls	Rationale	Residual Risks
Collection from the Social Media Site	Stigmatization: Information is revealed about the individual that they would prefer not to disclose.	1. Change API call to only pull full name and email; consider change to pull profile photograph if future proofing requires it. 2. Inform users of information that is collected and why at time of collection.	1. Significantly reduces collection of information, possibly decreasing risk across the system. Would potentially lower risk of stigmatization, power imbalance, and loss of trust problems. 2. Meets transparency requirement. Easy to implement.	
	Power Imbalance: People must provide extensive information, giving the acquirer an unfair advantage.			
	Loss of Trust: Individuals lose trust in ACME due to a breach in expectations about the handling of personal information.			



Proposal for First Draft of NIST Special Publication 800-53 Rev. 5

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 extend beyond compliance with privacy laws, regulations, and policies, and that agencies must incorporate the NIST Risk Management Framework (NIST RMF) in their privacy programs

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

Security and SP 800-53

The security controls express security requirements

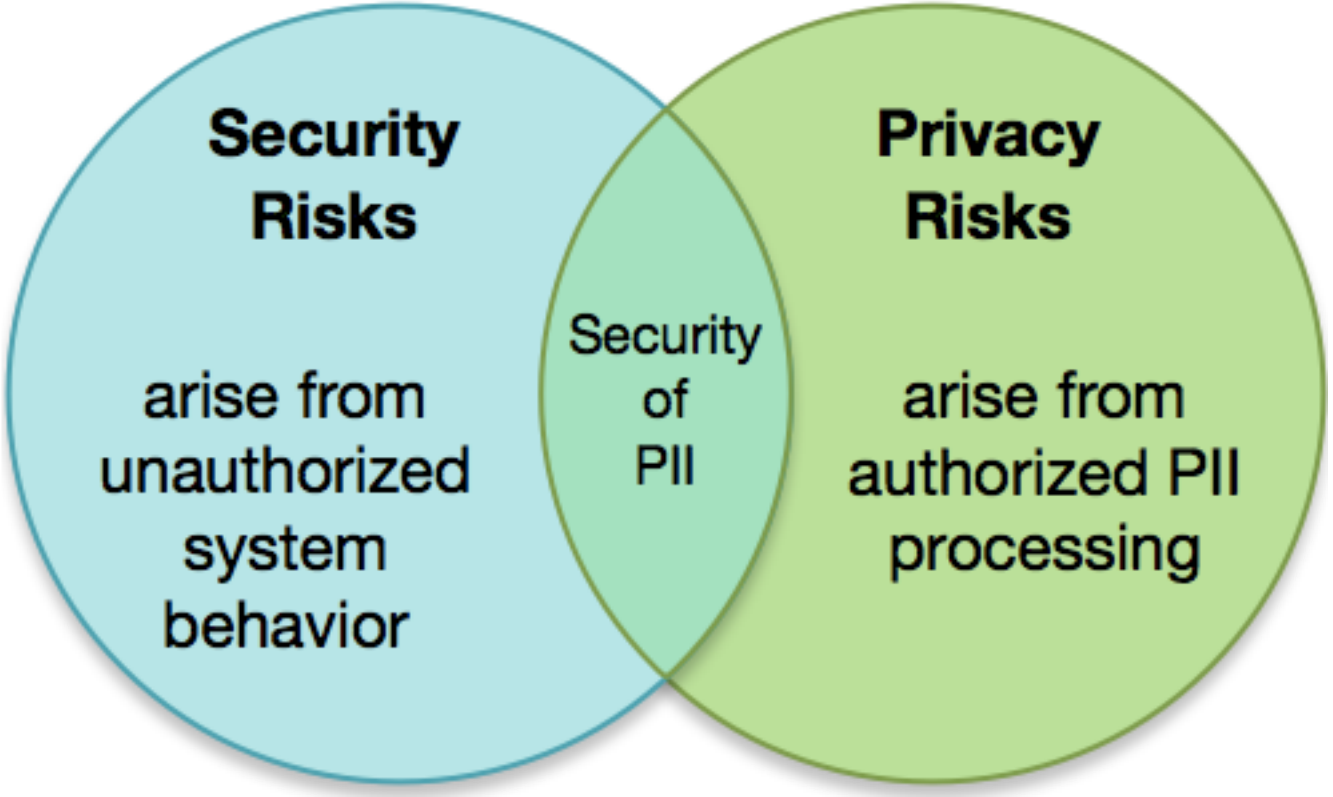
- menu of options
- cybersecurity officials and engineers use to manage assessed risks in their systems

Appendix J Workshop: What We Learned

September 8, 2016

- Benefits of App J:
  - Gives clout to privacy, helps agencies understand how to set up a privacy program
- Challenges of App J:
  - Integration and implementation is a challenge; security groups are the big gorilla resource-wise, and App J can get easily overlooked
  - Better integration shouldn't lead to loss of privacy oversight

Information Security and Privacy Relationship


Security Risks
arise from unauthorized system behavior
Security of PII
Privacy Risks
arise from authorized PII processing

- There is a clear recognition that confidentiality of personal data plays an important role in the protection of privacy

- However, both privacy and security have issues that are distinct from each other

- Appendix J controls address the right side of the diagram

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 Appendix J Reorganization

Appendix J Control	Rev 5 Families
AP-1	PA
AP-2	PA
AR-1	PM
AR-2	PM, RA
AR-3	SA
AR-4	CA
AR-5	AT, PL
AR-6	PM
AR-7	PA, PM, SI
AR-8	PM
DI-1	PM
DI-2	PM, SI
DM-1	PM, SC, SI
DM-2	PM, MP, SI
DM-3	PM
IP-1	IP
IP-2	IP, PM
IP-3	IP
IP-4	PM
SE-1	PM
SE-2	IR
TR-1	IP
TR-2	IP, PM
TR-3	PM
UL-1	PA
UL-2	PA

App J: DM-1 Minimization of Personally Identifiable Information

The organization:

a. Identifies the minimum personally identifiable information (PII) elements that are relevant and necessary to accomplish the legally authorized purpose of collection;

b. Limits the collection and retention of PII to the minimum elements identified for the purposes described in the notice and for which the individual has provided consent; and

c. Conducts an initial evaluation of PII holdings and establishes and follows a schedule for regularly reviewing those holdings [Assignment: organization-defined frequency, at least annually] to ensure that only PII identified in the notice is collected and retained, and that the PII continues to be necessary to accomplish the legally authorized purpose.

Proposed Rev 5: Data Minimization

Examples:

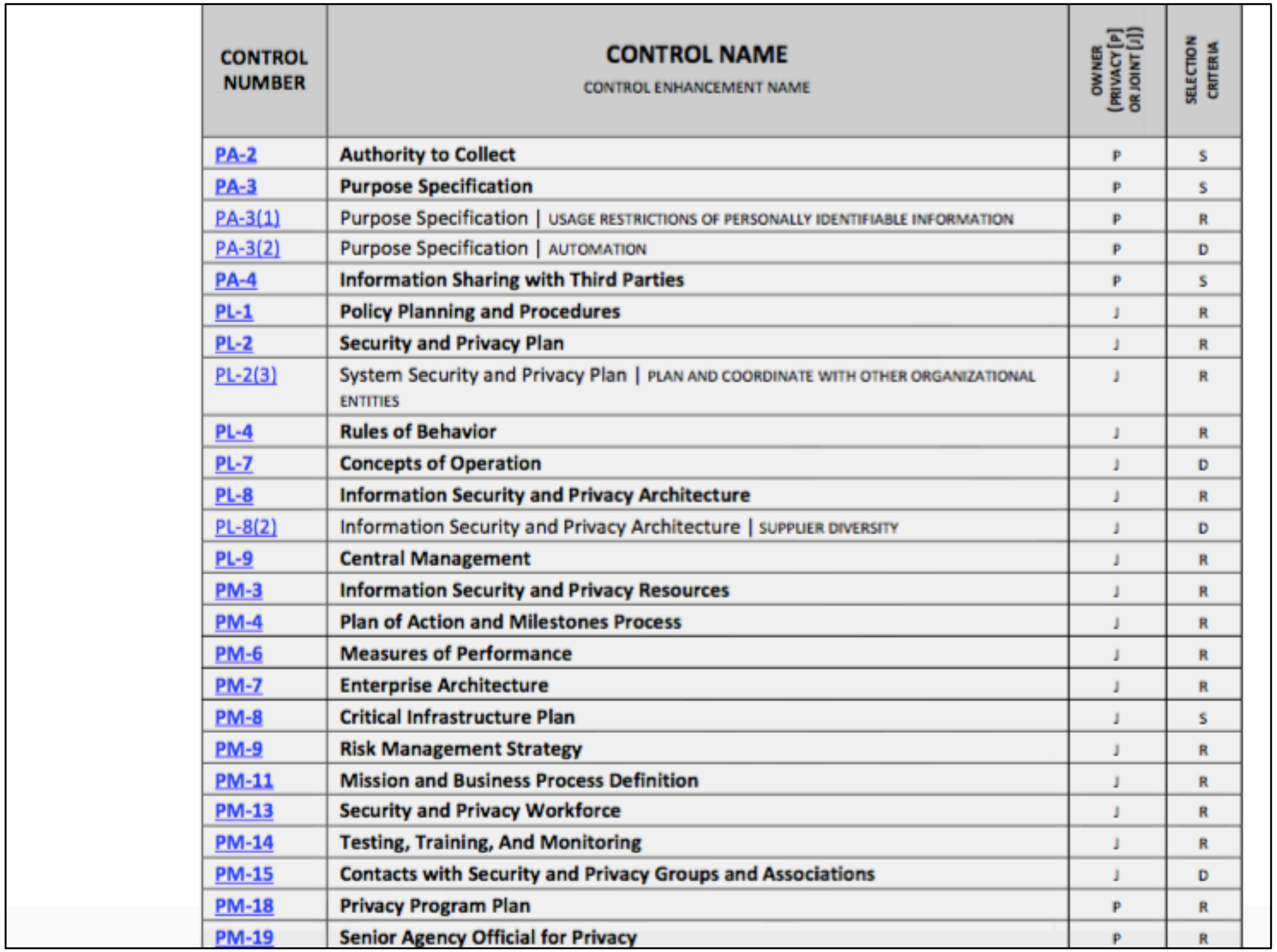
- **SI-12(1) Information Management And Retention | Limit Personally Identifiable Information Elements**

Limit personally identifiable information being processed in the information life cycle to the [Assignment: organization-defined elements] identified in the privacy risk assessment.

- **SC-42(5) Sensor Capability and Data | Collection Minimization**

Employ [Assignment: organization-defined sensors] that are configured to minimize the collection of information about individuals that is not needed.

Draft Summary Privacy Controls Table



CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	OWNER (PRIVACY [P] OR JOINT [J])	SELECTION CRITERIA
PA-2	**Authority to Collect**	P	S
PA-3	**Purpose Specification**	P	S
PA-3(1)	Purpose Specification | USAGE RESTRICTIONS OF PERSONALLY IDENTIFIABLE INFORMATION	P	R
PA-3(2)	Purpose Specification | AUTOMATION	P	D
PA-4	**Information Sharing with Third Parties**	P	S
PL-1	**Policy Planning and Procedures**	J	R
PL-2	**Security and Privacy Plan**	J	R
PL-2(3)	System Security and Privacy Plan | PLAN AND COORDINATE WITH OTHER ORGANIZATIONAL ENTITIES	J	R
PL-4	**Rules of Behavior**	J	R
PL-7	**Concepts of Operation**	J	D
PL-8	**Information Security and Privacy Architecture**	J	R
PL-8(2)	Information Security and Privacy Architecture | SUPPLIER DIVERSITY	J	D
PL-9	**Central Management**	J	R
PM-3	**Information Security and Privacy Resources**	J	R
PM-4	**Plan of Action and Milestones Process**	J	R
PM-6	**Measures of Performance**	J	R
PM-7	**Enterprise Architecture**	J	R
PM-8	**Critical Infrastructure Plan**	J	S
PM-9	**Risk Management Strategy**	J	R
PM-11	**Mission and Business Process Definition**	J	R
PM-13	**Security and Privacy Workforce**	J	R
PM-14	**Testing, Training, And Monitoring**	J	R
PM-15	**Contacts with Security and Privacy Groups and Associations**	J	D
PM-18	**Privacy Program Plan**	P	R
PM-19	**Senior Agency Official for Privacy**	P	R

Guidance Roadmap

SP 800-18

Guide for Developing Security Plans for Federal Information Systems

SP 800-30

Guide for Conducting Risk Assessments

SP 800-37

Guide for Applying the Risk Management Framework to Federal Information Systems

SP 800-39

Managing Information Security Risk—Organization, Mission, and Information System View

SP 800-53

Security and Privacy Controls for Federal Information Systems and Organizations

SP 800-53A

Guide for Assessing the Security Controls in Federal Information Systems

SP 800-60

Volume I: Guide for Mapping Types of Information and Information Systems to Security Categories and Volume II: Appendices to Guide for Mapping Types of Information and Information Systems to Security Categories

SP 800-122

Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)

SP 800-160

Systems Security Engineering

Resources

Naomi Lefkovitz

Naomi.lefkovitz@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