

Privacy Engineering Objectives and Risk Model

Objective-Based Design for Improving Privacy
in Information Systems

NIST research has a broad impact



G. Muehler / shutterstock.com

Facilitates trade and fair commerce



G. Muehler / shutterstock.com

Improves public safety and security



06photo

Advances manufacturing and services



B. Gardner

Improves quality, ensures uniformity

NIST Partnerships

Industry



Universities



Nonprofits



International Technology Roadmap for Semiconductors



Government



First Privacy Engineering Workshop

Purpose:

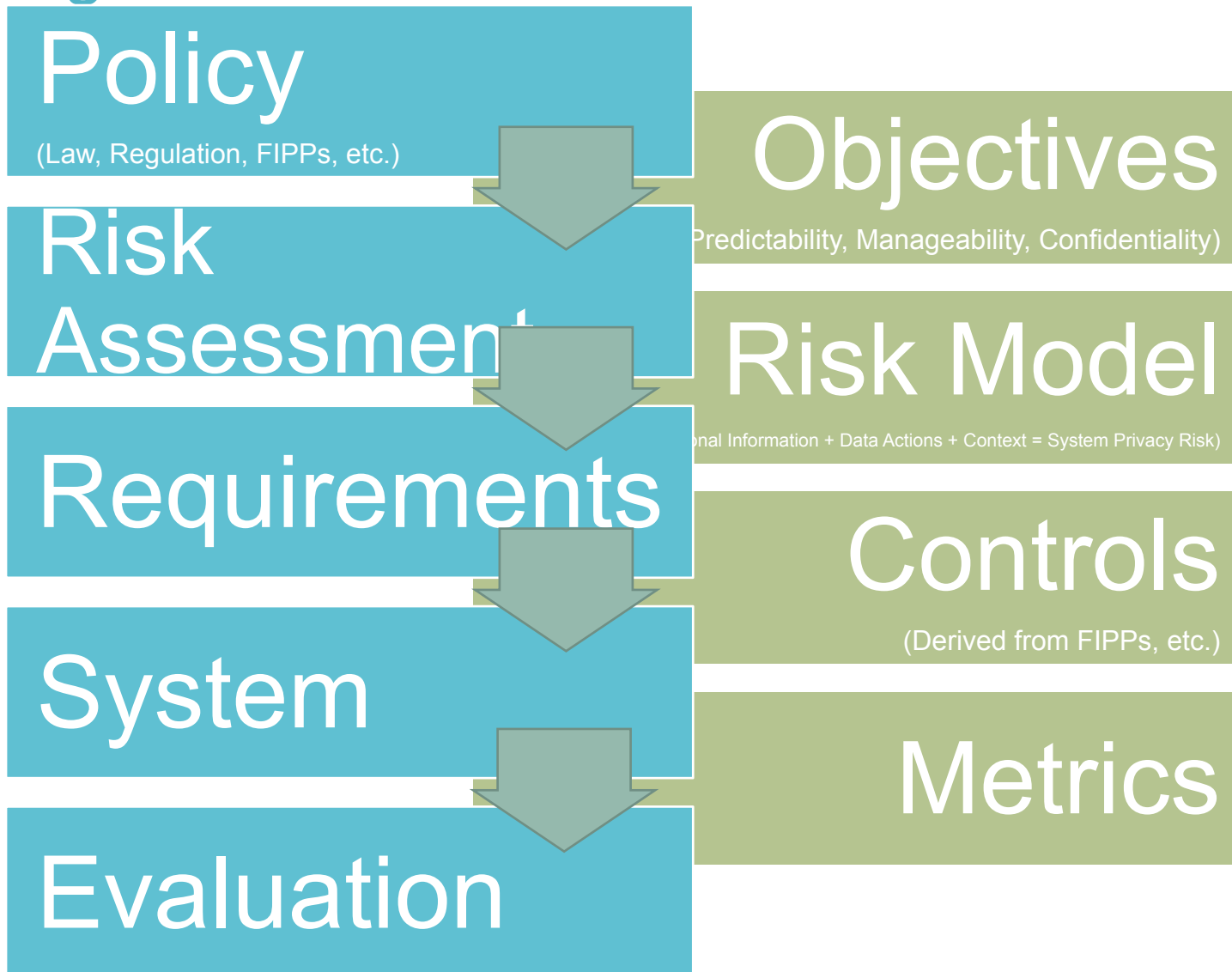
- Consider analogous models
 - Focus on objectives
- Identify distinctions

Key Outcomes:

- Communication gap
- Positive interest in a risk management model

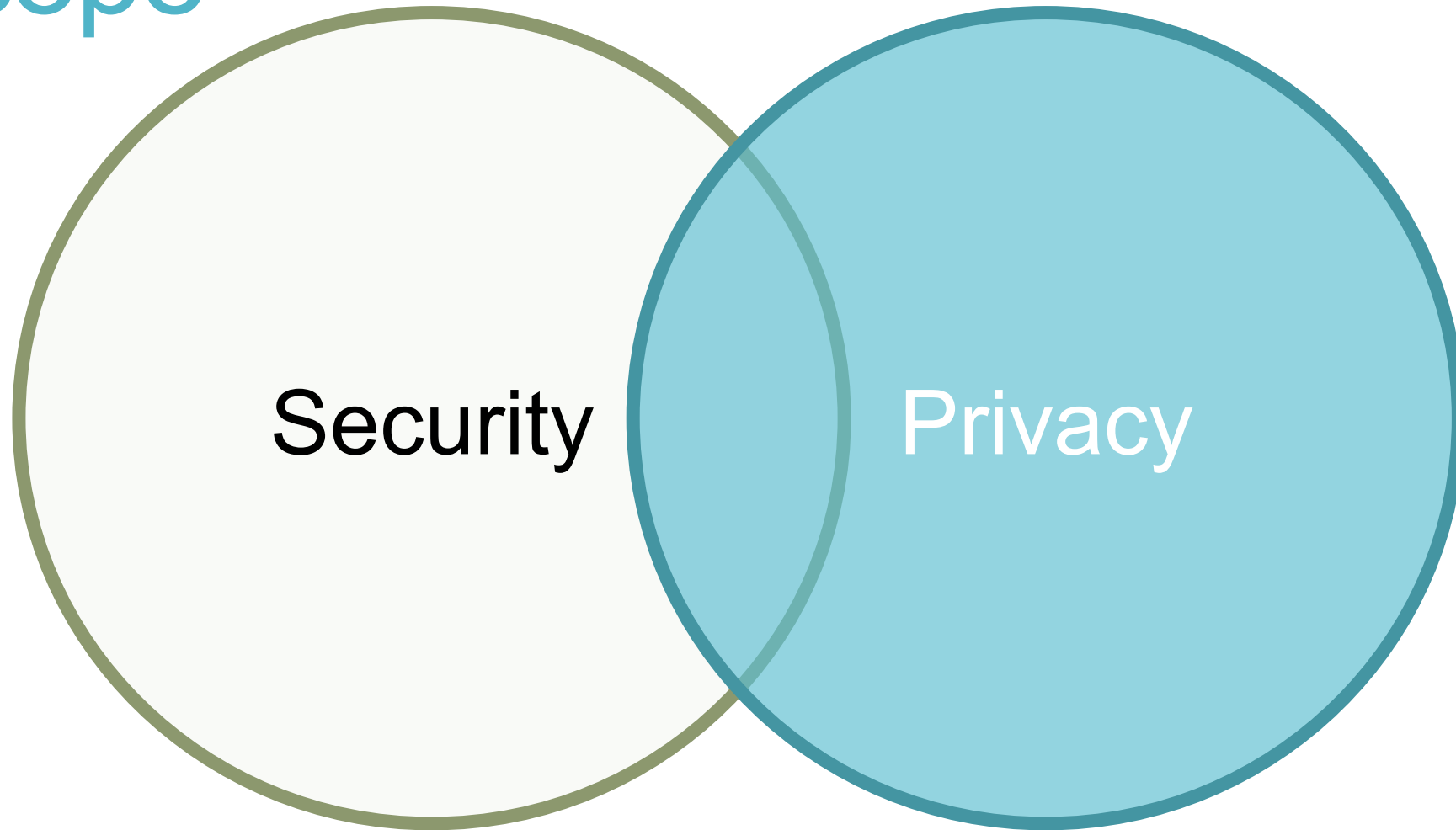
Model Privacy Risk Management Framework

Privacy Engineering Components



September Workshop

Scope



Key Terms

Privacy Engineering
Objectives

Problematic Data
Actions

Privacy Engineering

Data Lifecycle

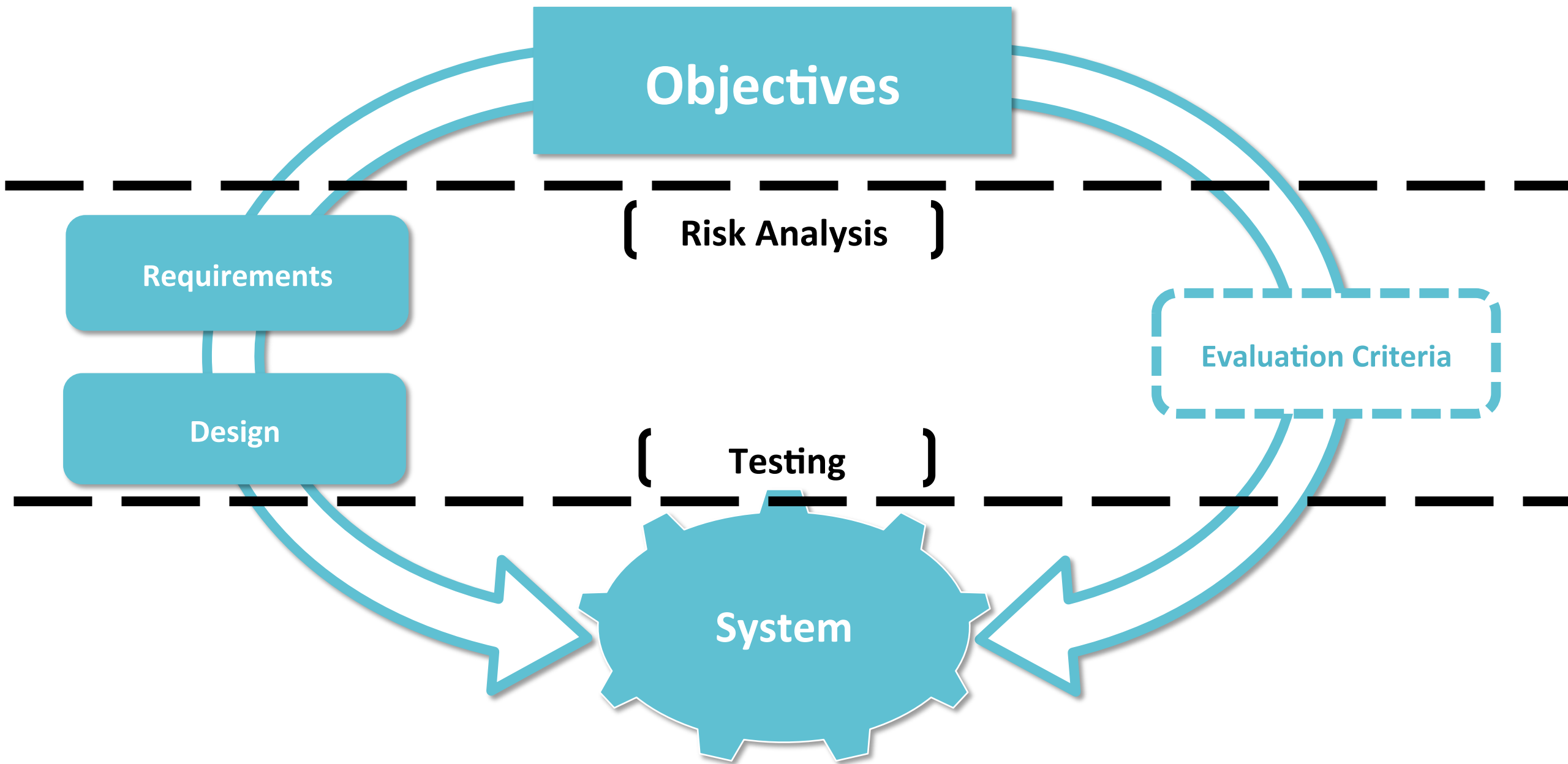
Context

Data Actions

Privacy Harms

Privacy Engineering Objectives

Outcome-based objectives that guide design requirements to achieve privacy-preserving information systems.



The Privacy Triad

- The objectives are characteristics of the system, not role-based.
- The objectives support policy
- Aligning the privacy and security overlap

Predictability

Enabling reliable assumptions about the rationale for the collection of personal information and the data actions to be taken with that personal information.

Manageability

Providing the capability for authorized modification of personal information, including alteration, deletion, or selective disclosure of personal information.

Confidentiality

Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.

(NIST SP 800-53, rev 4)

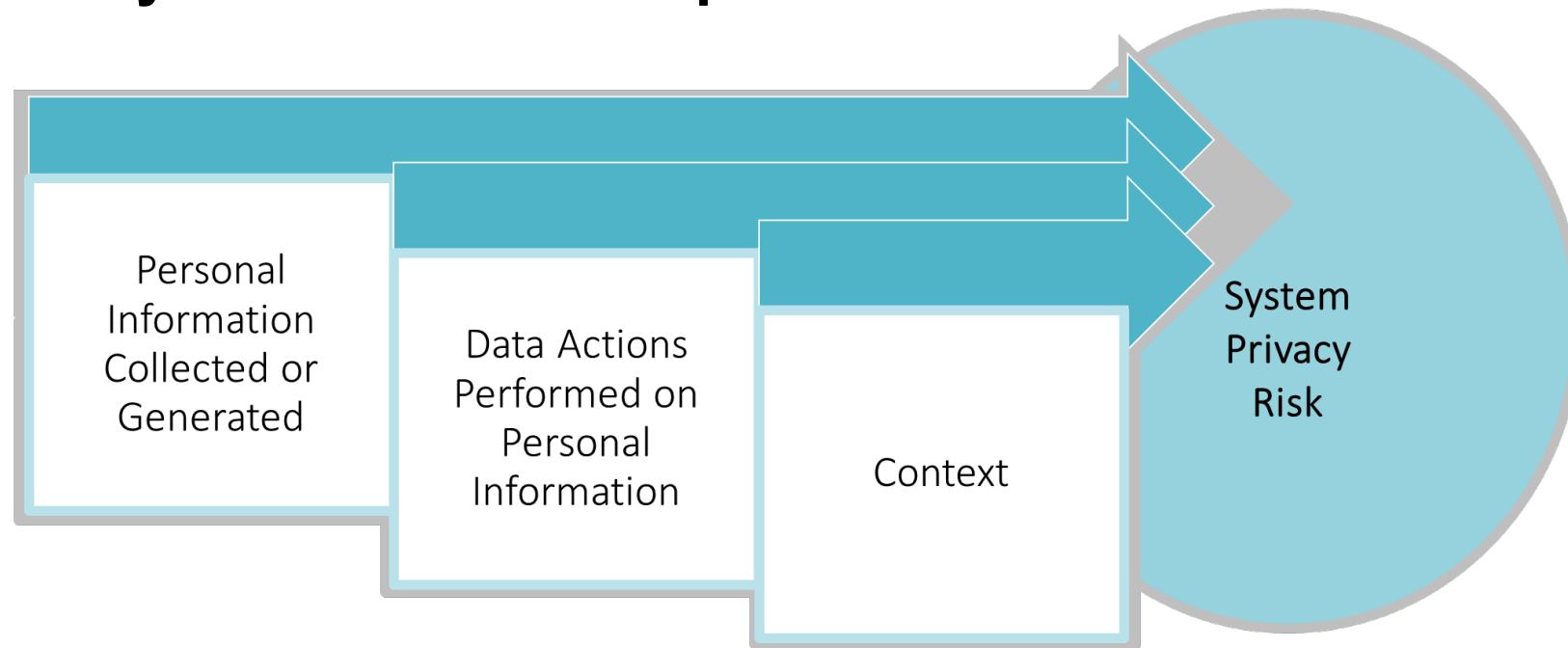
System Privacy Risk Model

Security Risk Equation

**Security Risk = Vulnerability * Threat *
Impact**

System Privacy Risk Equation

System privacy risk is the risk of problematic data actions occurring



Personal Information Collected or Generated * Data Actions Performed on that Information * Context = System Privacy Risk

Context

“Context” means the circumstances surrounding a system’s collection, generation, processing, disclosure and retention of personal information.

Problematic Data Actions and Privacy Harms

Distinguish data actions that give rise to harms and actual harms

Problematic Data Actions

Validation of the objectives and the risk model

Privacy Harms

Privacy Engineering Definition

Privacy engineering is a collection of methods to support the mitigation of risks to individuals of loss of self-determination, loss of trust, discrimination and economic loss by providing predictability, manageability, and confidentiality of personal information within information systems.

Information Security: *The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.*
[44 U.S.C., SEC. 3542]

Illustrative Mapping of Privacy Engineering Objectives to Problematic Data Actions

Data Lifecycle Phase	Normal Data Action	Problematic Data Action	Potential Harms
Predictability			
Collection	Service Initiation	Induced Disclosure	Power Imbalance, Loss of Autonomy
Processing	Aggregation	Unanticipated Revelation	Stigmatization, Power Imbalance, Loss of Trust, Loss of Autonomy
Processing	System monitoring	Surveillance	Power Imbalance, Loss of Trust, Loss of Autonomy, Loss of Liberty
Manageability			
Disclosure	Authorized Attribute Sharing	Distortion	Stigmatization, Power Imbalance, Loss of Liberty
Disposal	Normal Account Deletion	Unwarranted Restriction	Exclusion, Economic Loss, Loss of Trust
Confidentiality			
Use	Authorized Use	Appropriation	Loss of Trust, Economic Loss, Power Imbalance
Retention	Secure Storage	Insecurity	Economic Loss, Stigmatization

What's Next?

Webcast: 2:00pm, ET, October 2, 2014

Publish a NIST Interagency Report

- Public comment period between draft and final versions

Comments may be sent to privacyeng@nist.gov until October 15, 2014.