Privacy Engineering Objectives and Risk Model

Objective-Based Design for Improving Privacy

in Information Systems

NIST

NIST research has a broad impact

G. Hooijer/shutterstock.com

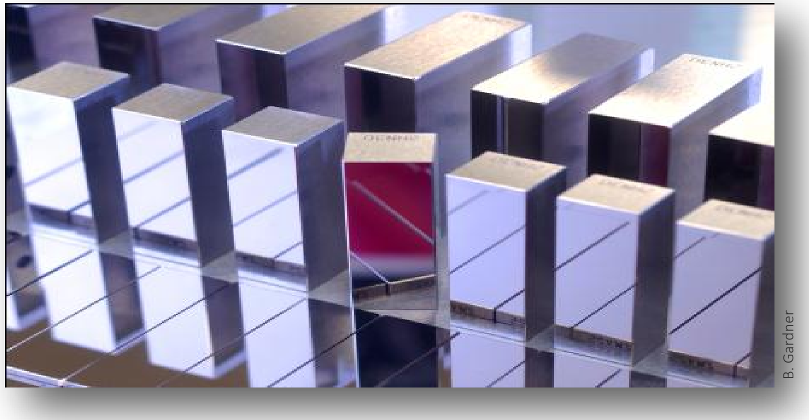
Facilitates trade and fair commerce

D. Stork/shutterstock.com

Improves public safety and security

06photo

Advances manufacturing and services



B. Gardner

Improves quality, ensures uniformity

NIST Partnerships

Industry

Agilent Technologies

intel

Dow

GM

IBM

Pfizer

Universities

University of Maryland

University of Colorado at Boulder

Penn
University of Pennsylvania

The University of Wisconsin Madison

Nonprofits

AdvaMed
Advanced Medical Technology

ASTM International
Standards Worldwide

USCAR

ITRS
International Technology Roadmap for Semiconductors

ADA

Government

NASA

NSF

U.S. Department of Homeland Security
Homeland Security

National Institutes of Health

United States Environmental Protection Agency

Department of Defense United States of America

Department of Justice
Qui Pro Domina Justitia Sequitur

NIST

First Privacy Engineering Workshop

Purpose:

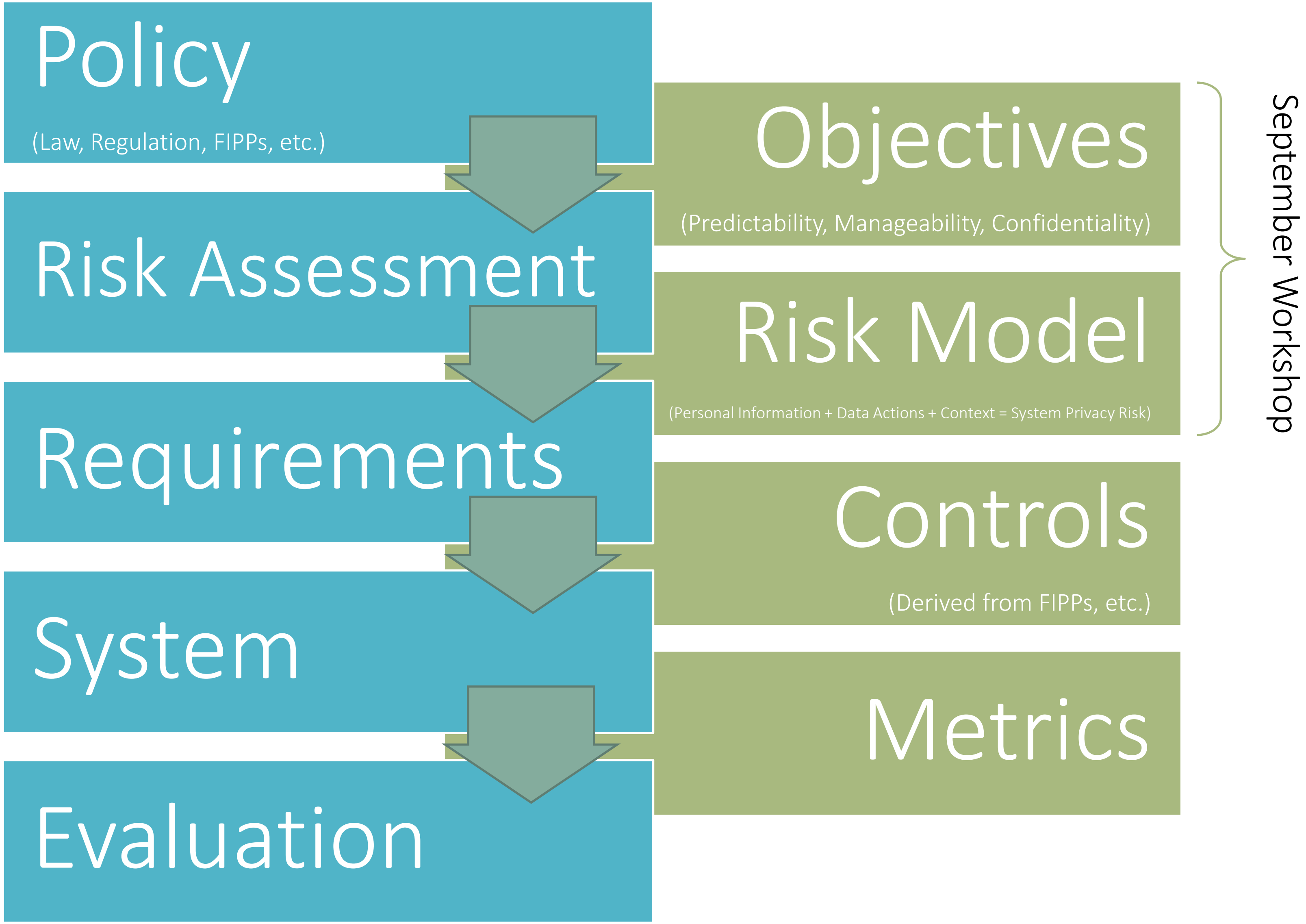
- Consider analogous models
  - Focus on objectives
- Identify distinctions

Key Outcomes:

- Communication gap
- Positive interest in a risk management model

Model Privacy Risk Management Framework

Privacy Engineering Components



Policy

(Law, Regulation, FIPPs, etc.)

Risk Assessment

Requirements

System

Evaluation

Objectives

(Predictability, Manageability, Confidentiality)

Risk Model

(Personal Information + Data Actions + Context = System Privacy Risk)

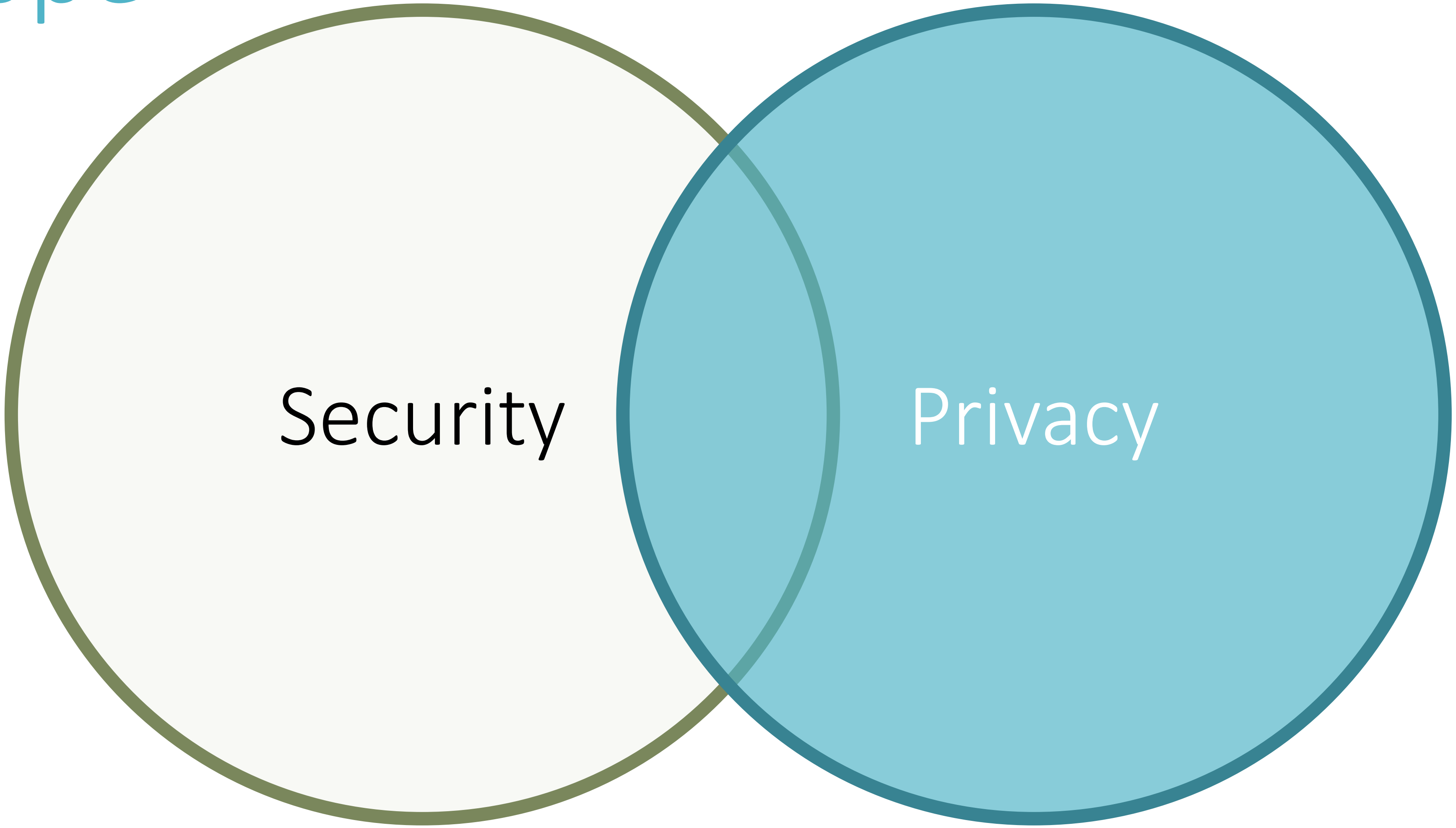
Controls

(Derived from FIPPs, etc.)

Metrics

September Workshop

Scope

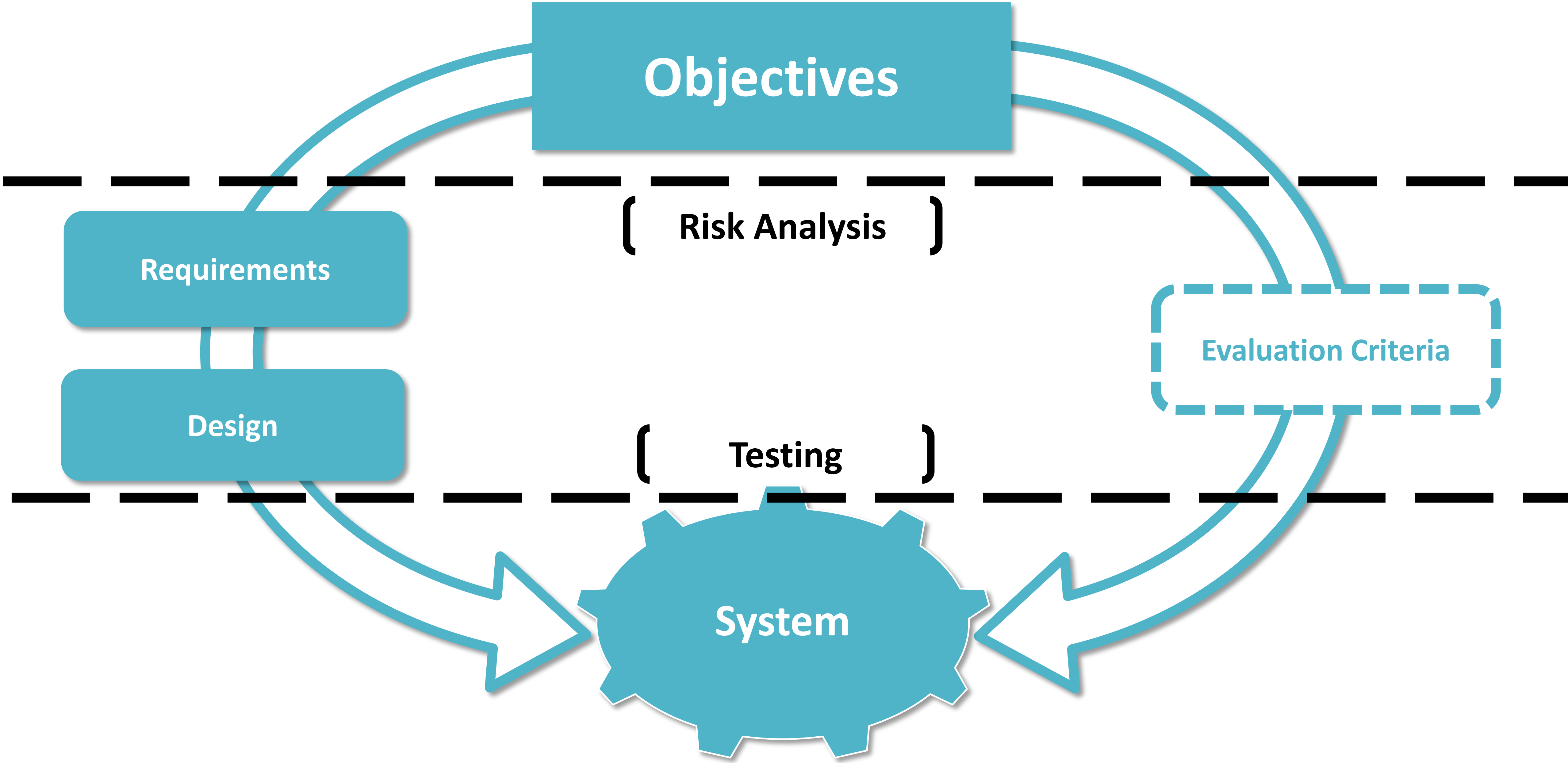


Key Terms

- Privacy Engineering Objectives
- Problematic Data Actions
- Privacy Engineering
- Data Lifecycle
- Context
- Data Actions
- Privacy Harms

Privacy Engineering Objectives

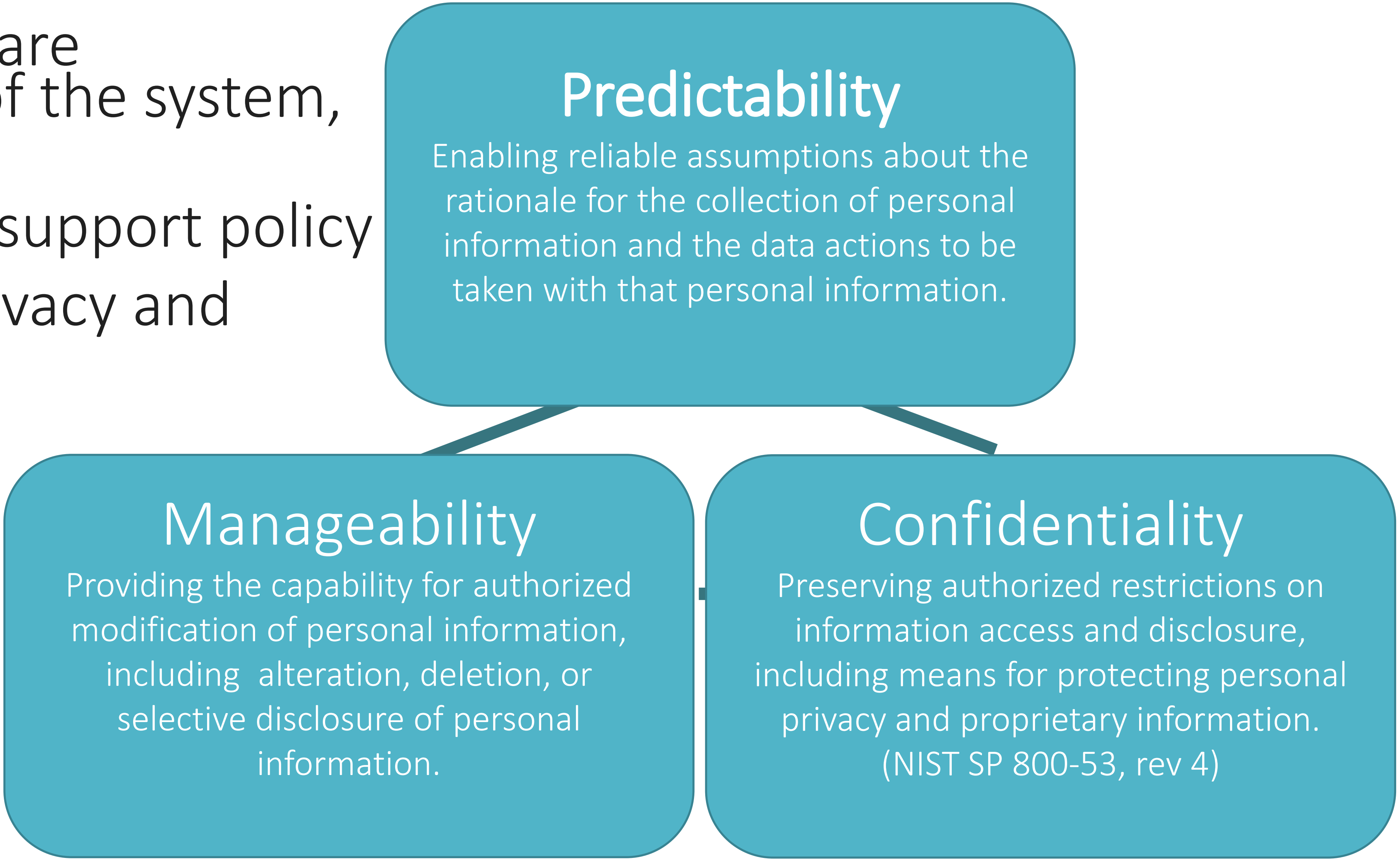
Outcome-based objectives that guide design requirements to achieve privacy-preserving information systems.



Objectives
Risk Analysis
Requirements
Design
Evaluation Criteria
Testing
System

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)

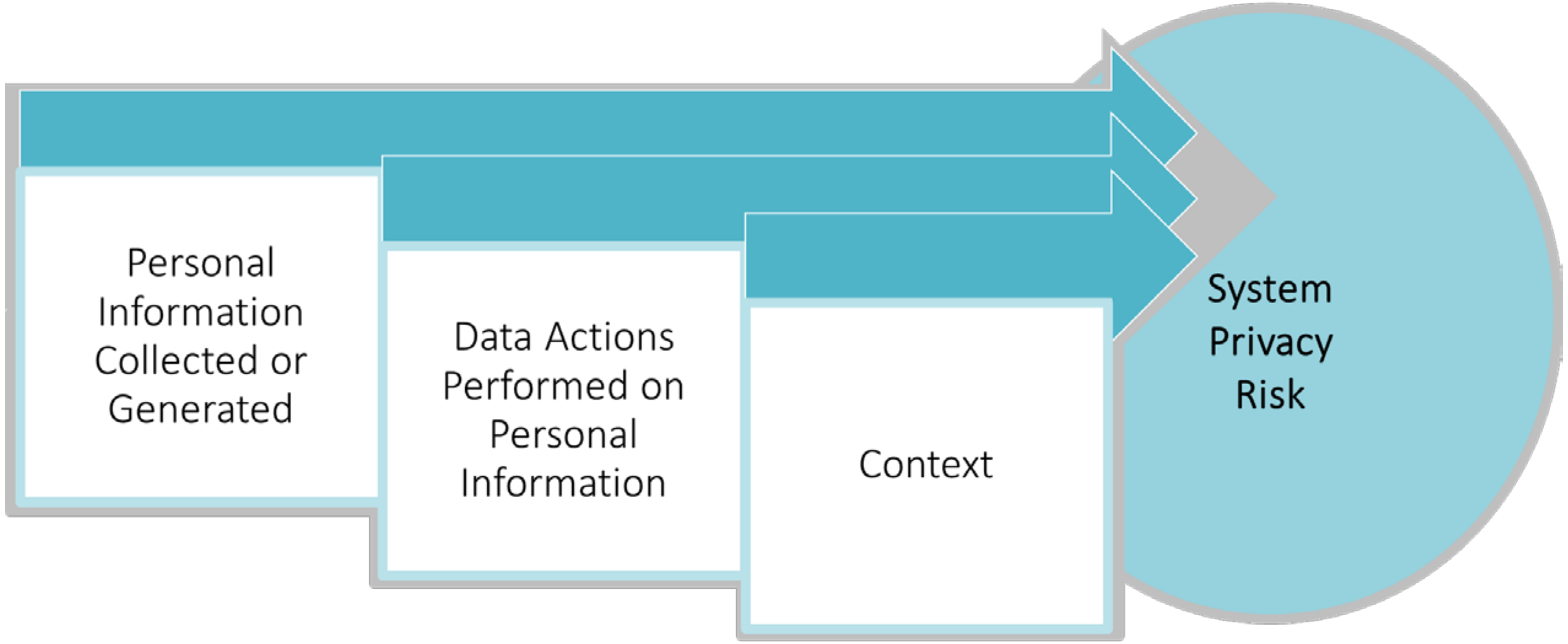
System Privacy Risk Model

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 Personal Information
Context
System Privacy Risk

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

Next Steps

Webinar: September 26, 2014

Publish a NIST Interagency Report

- Public comment period between draft and final versions

Comments may be sent to privacyeng@nist.gov until October 10, 2014.

Goals for Breakout Sessions

- **Privacy Engineering:** Is this definition useful? Should harms be part of the definition? Wordsmithing is welcome.
- **Privacy Engineering Objectives:** Do these objectives support policies, but not determine them? Is that how they should work? Are there any gaps? Wordsmithing is welcome.
- **System Privacy Risk Equation:** Does this equation seem likely to be effective in identifying system privacy risks? Should it hinge on identifying problematic data actions? If not, how should system privacy risk be identified?
- **Context:** Are these relevant factors? Should we include more?
- **Problematic Data Actions and Harms:** Goal is not to wordsmith the examples, but treat them as source data for validating whether the objectives and the risk model work in a range of use cases. Are any irrelevant? Should we provide other examples?
- **Use Cases:** Are there particular scenarios that would help to test or demonstrate how this model works?
- **What else?**