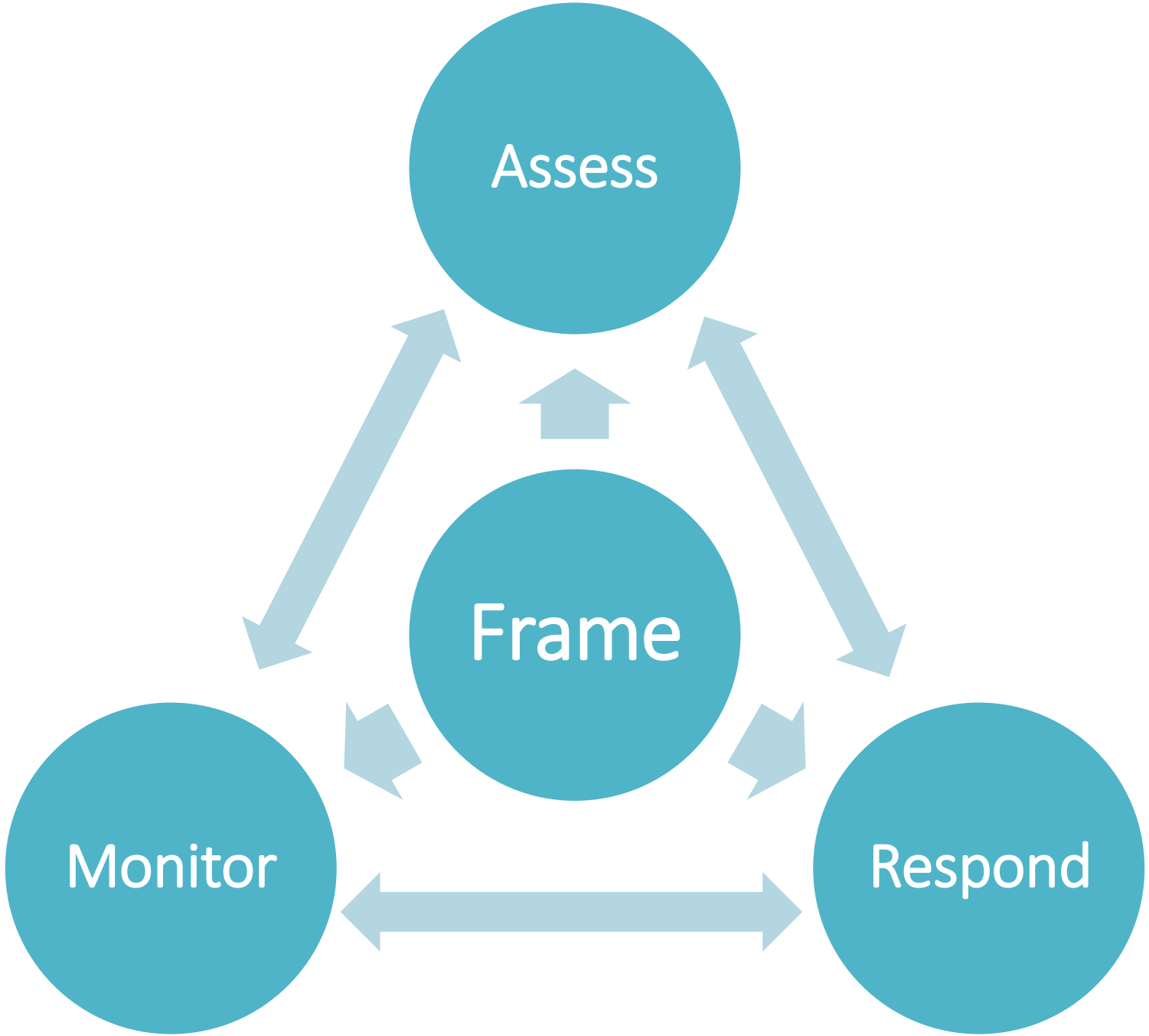
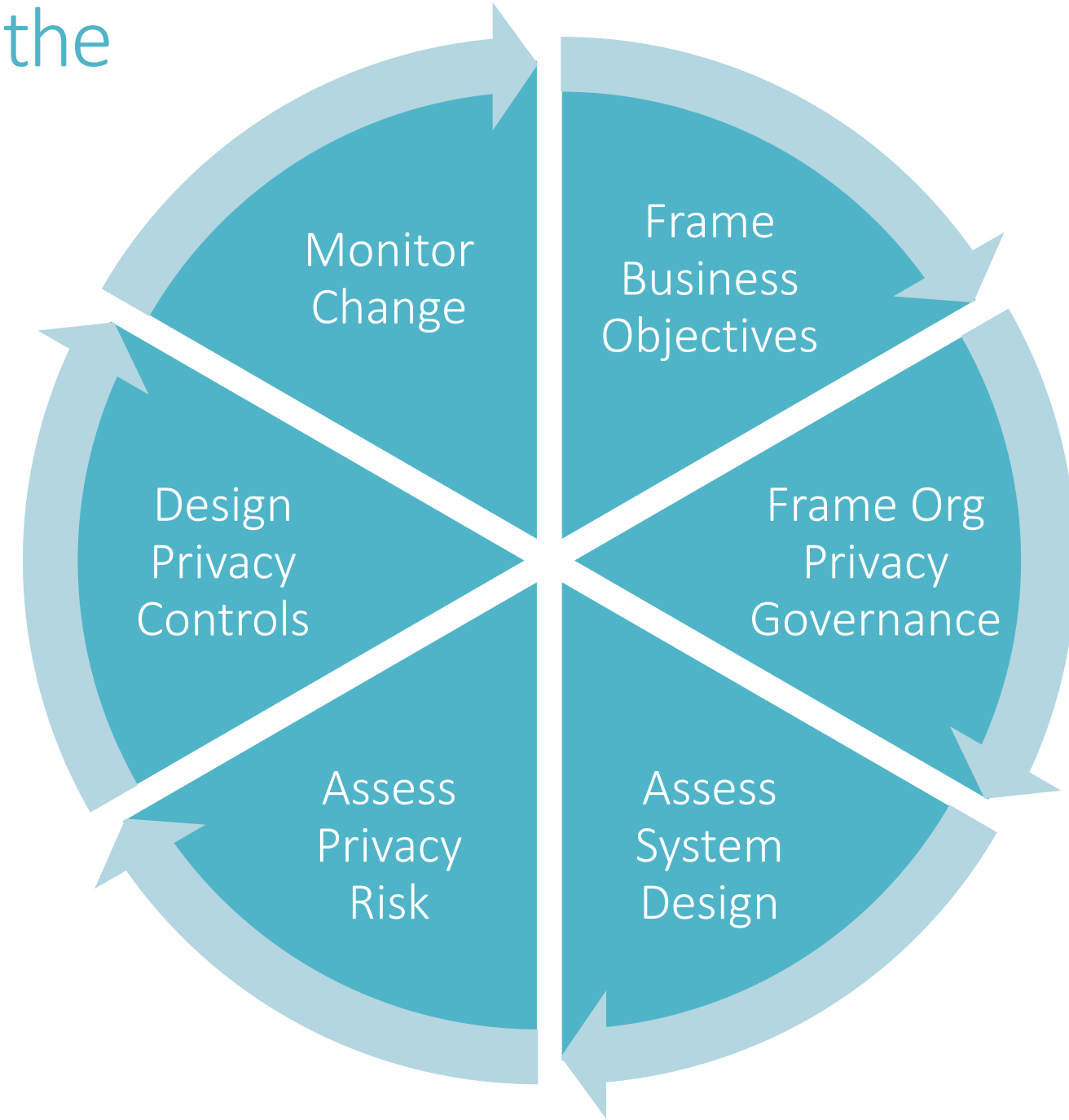
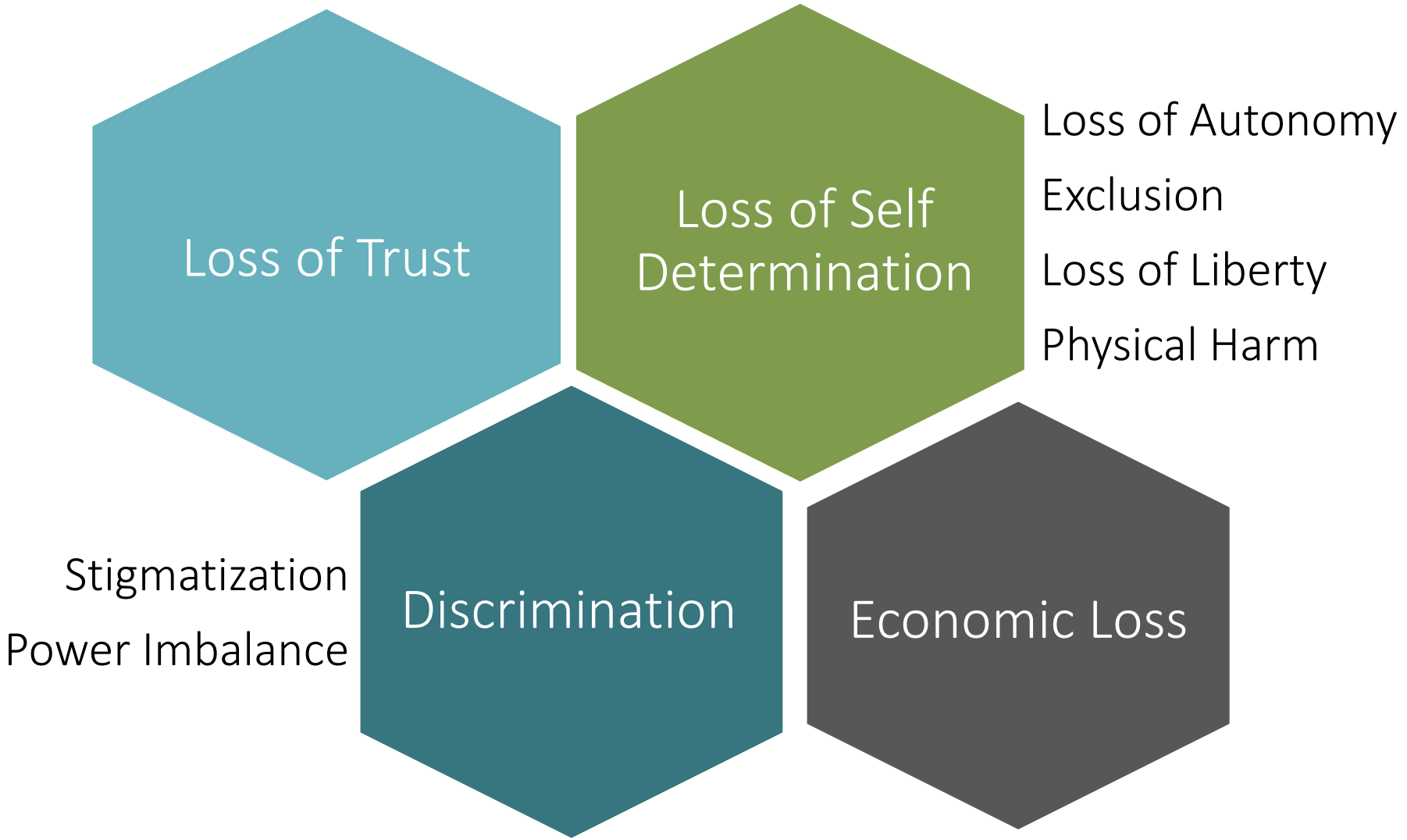
# Using Risk Management to Improve Privacy in Information Systems

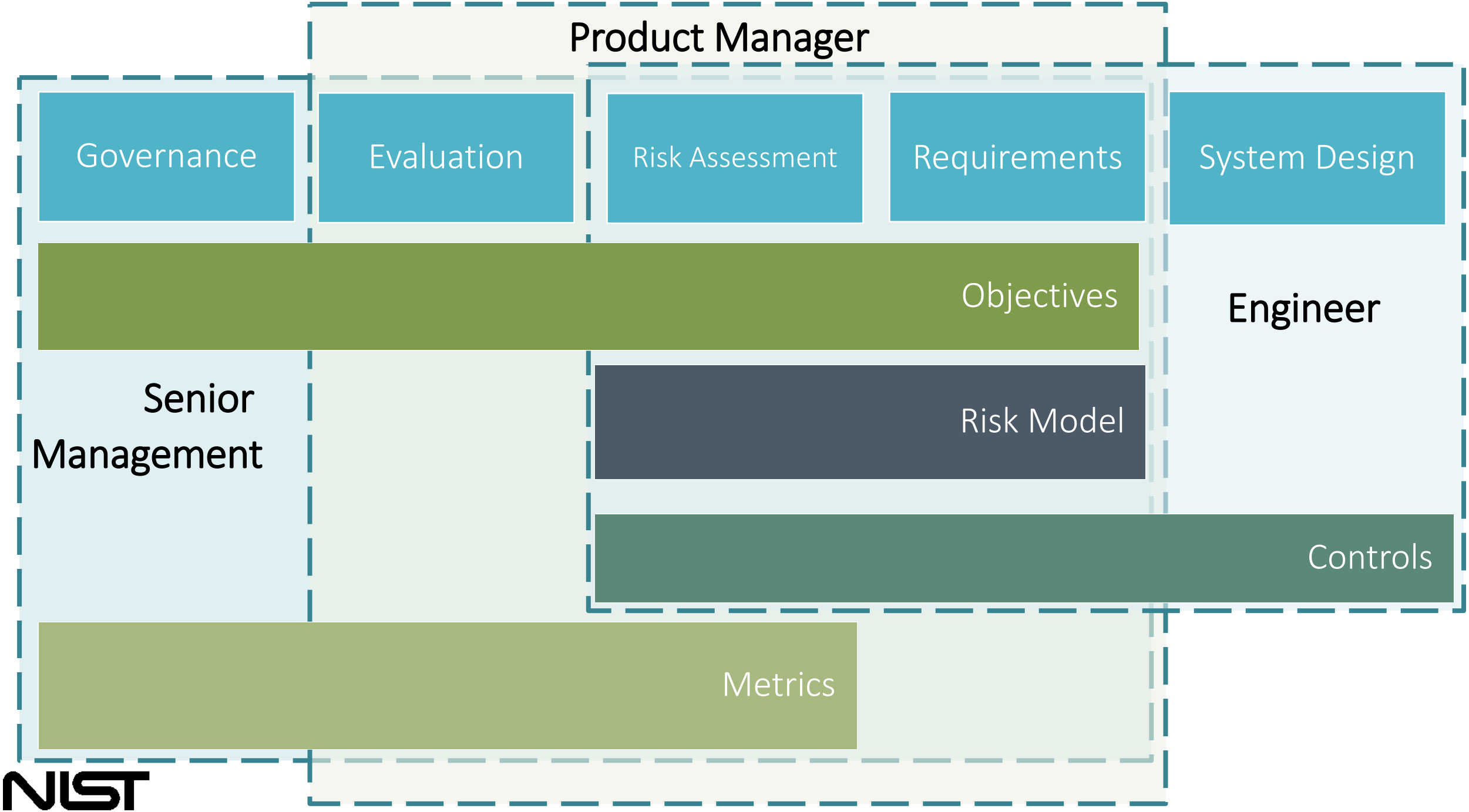

Assess
Frame
Monitor
Respond

# Implementing the Theory



# Potential Problems for Individuals




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

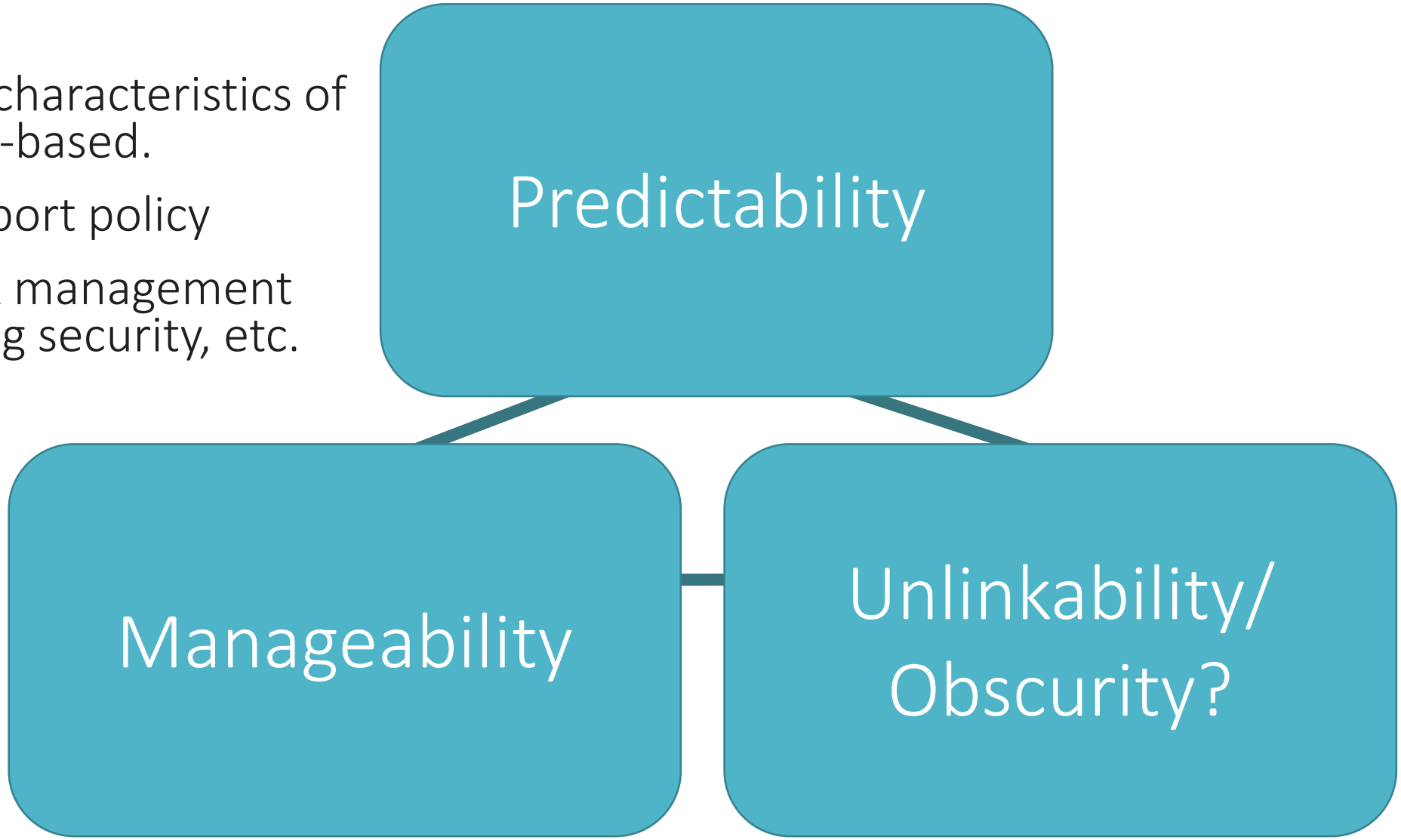
- Authority and Purpose
- Accountability, Audit, and Risk Management
- Data Quality and Integrity
- Data Minimization and Retention
- Individual Participation and Redress
- Security
- Transparency
- Use Limitation

NIST

# NIST Process

# Developing a Privacy Triad: Draft Objectives

- The objectives are characteristics of the system, not role-based.
- The objectives support policy
- Part of broader risk management framework, including security, etc.



# Security Risk Equation

Security Risk = Vulnerability * Threat * Impact

# Inputs for Privacy Risk

- **Likelihood:** Likelihood of a data action becoming problematic (i.e., creating the potential for adverse effects on individuals)

  - the adverse effects that could occur are hypothesized from an assessment of the **data action**, the **personal information** being processed, and the **context** surrounding the data action

- **Impact:** Costs to organizations that would result from the problematic data action

# Resources

NIST Privacy Engineering Website:

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