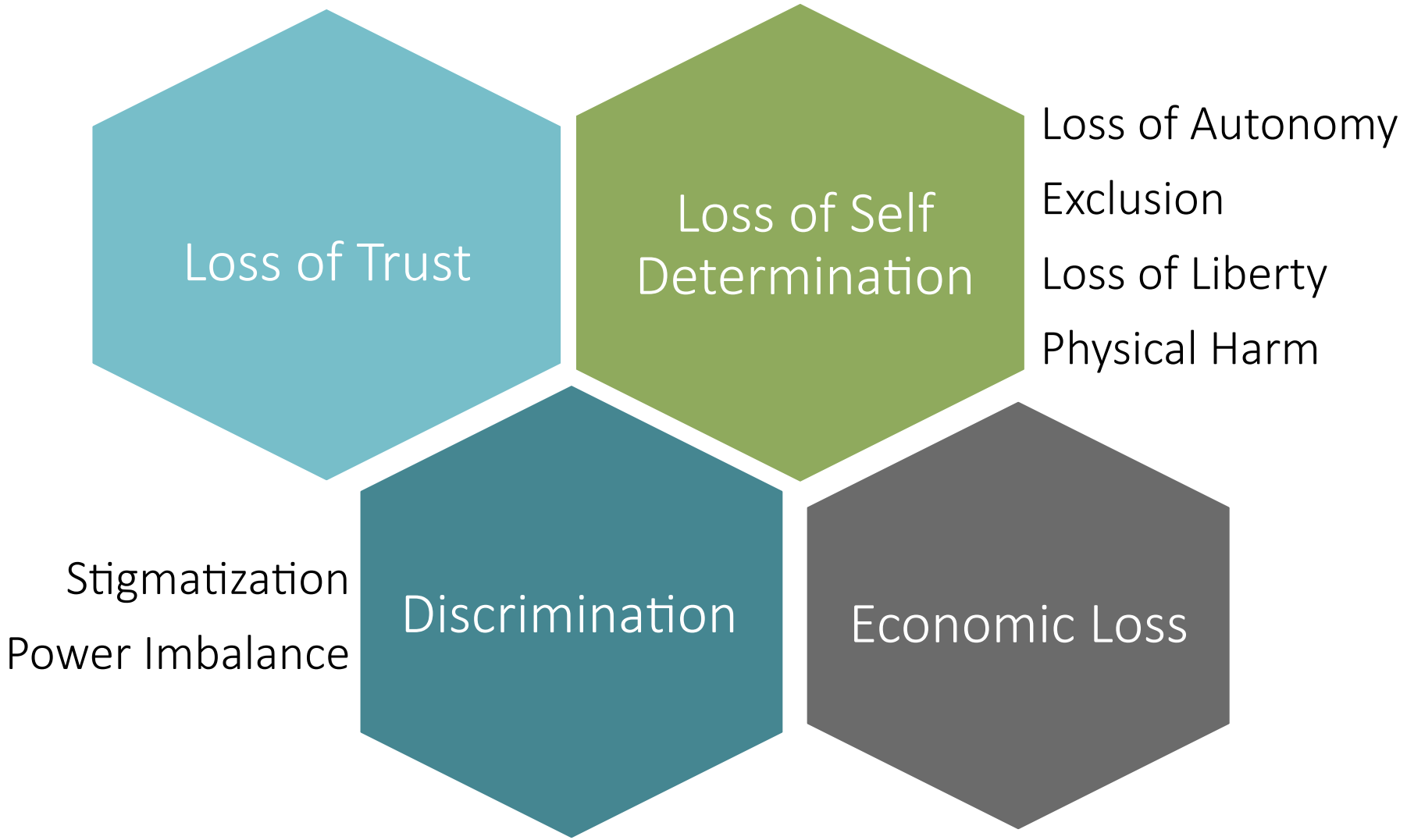
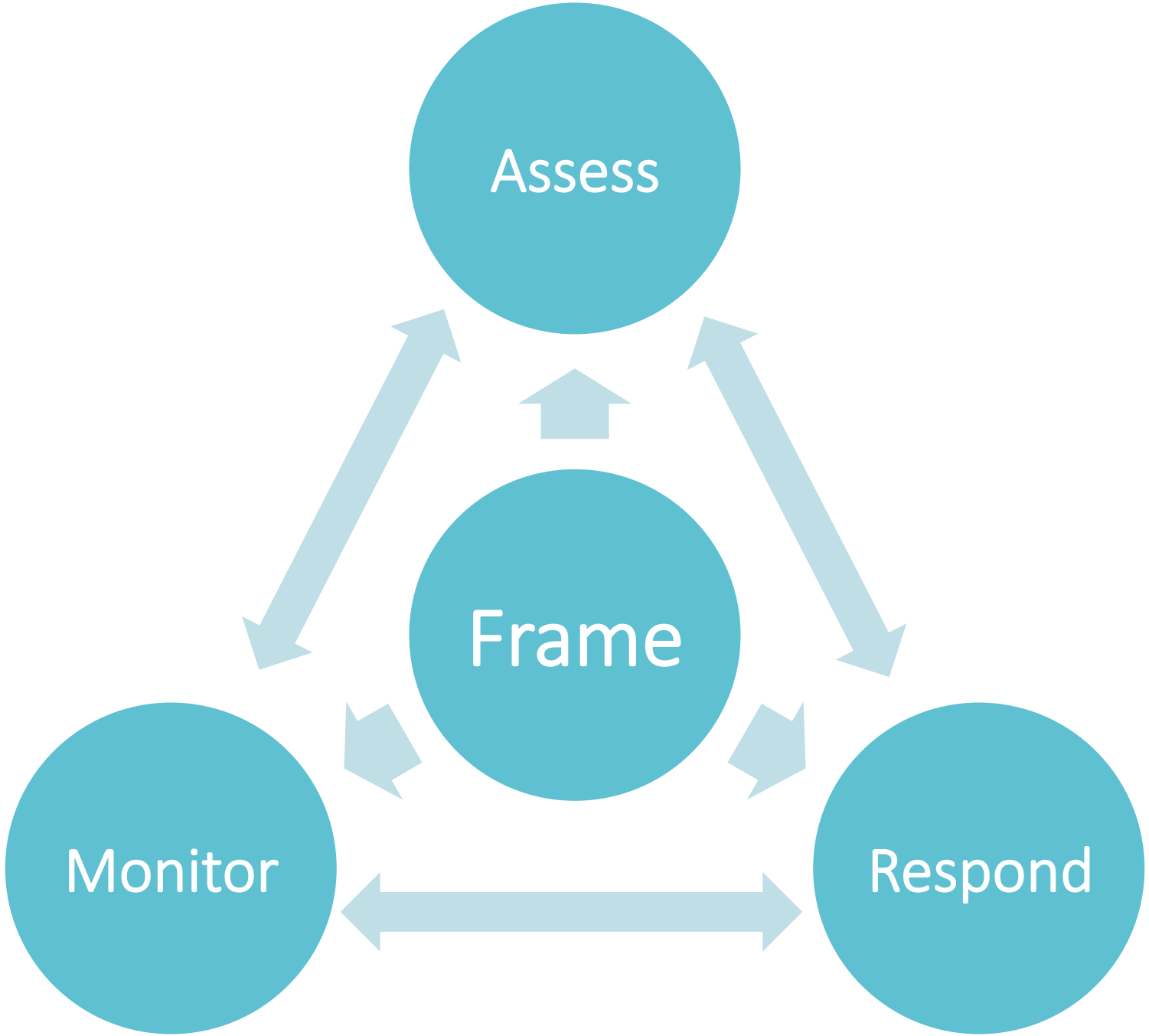
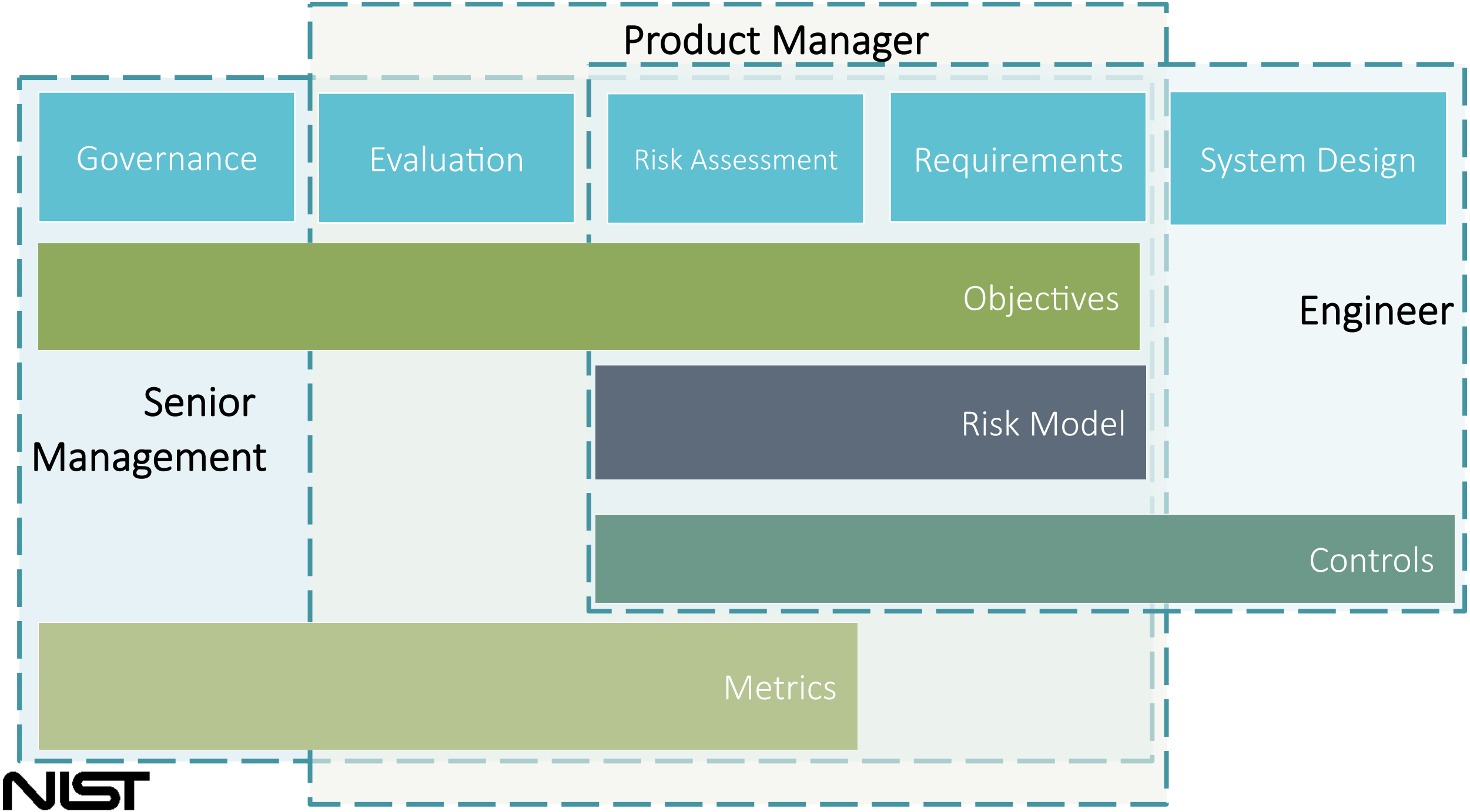
Using Risk Management to Improve Privacy in Information Systems

Potential Problems for Individuals




Assess
Frame
Monitor
Respond


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

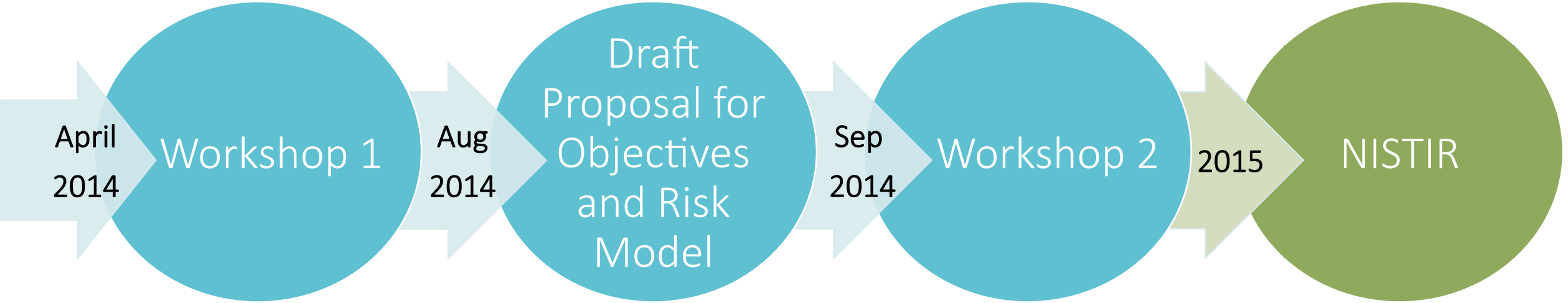
- Transparency
- Individual Participation
- Purpose Specification
- Data Minimization
- Use Limitation
- Data Quality and Integrity
- Security
- Accountability and Auditing

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

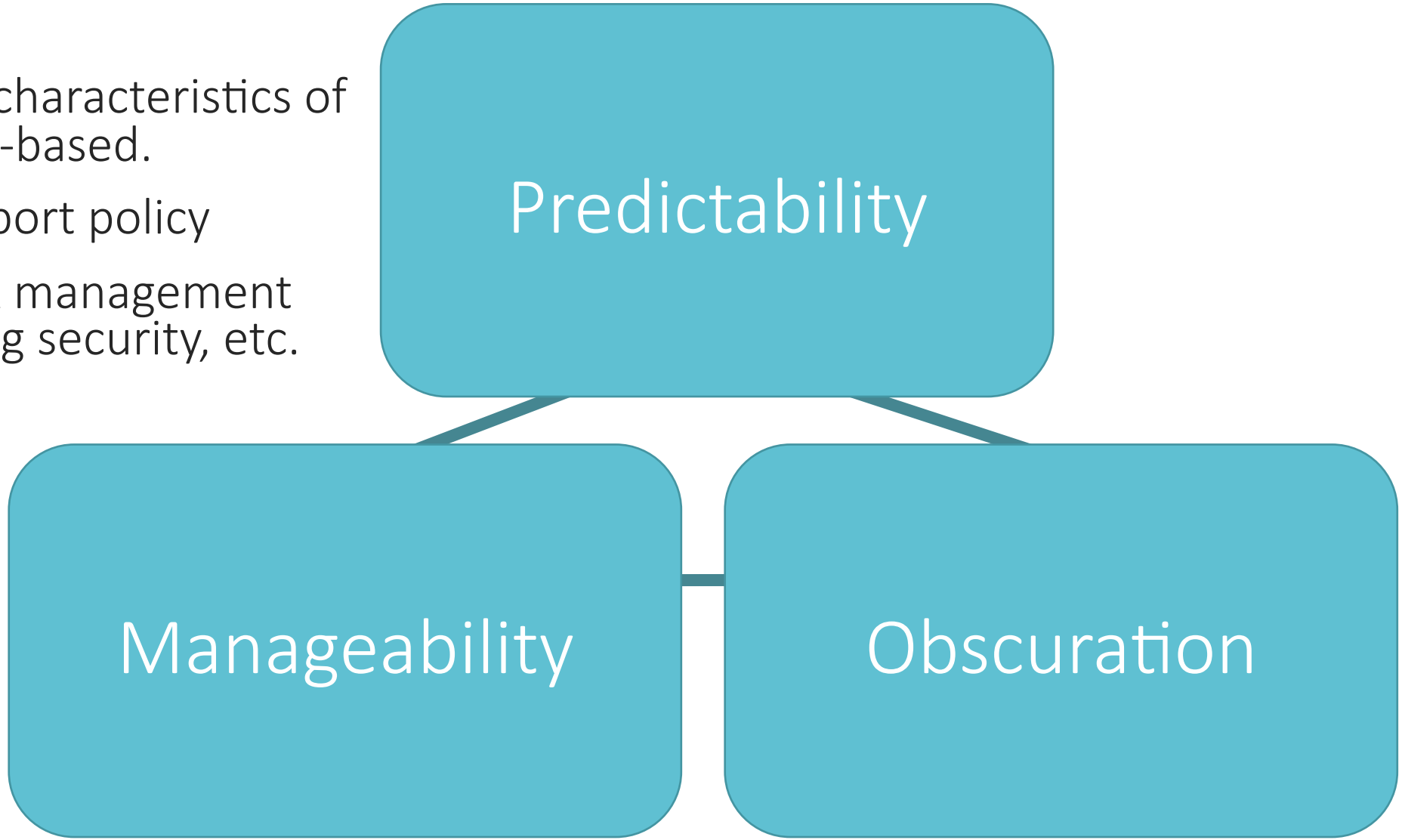
NIST

NIST Process



Developing a Privacy Triad: Draft Objectives

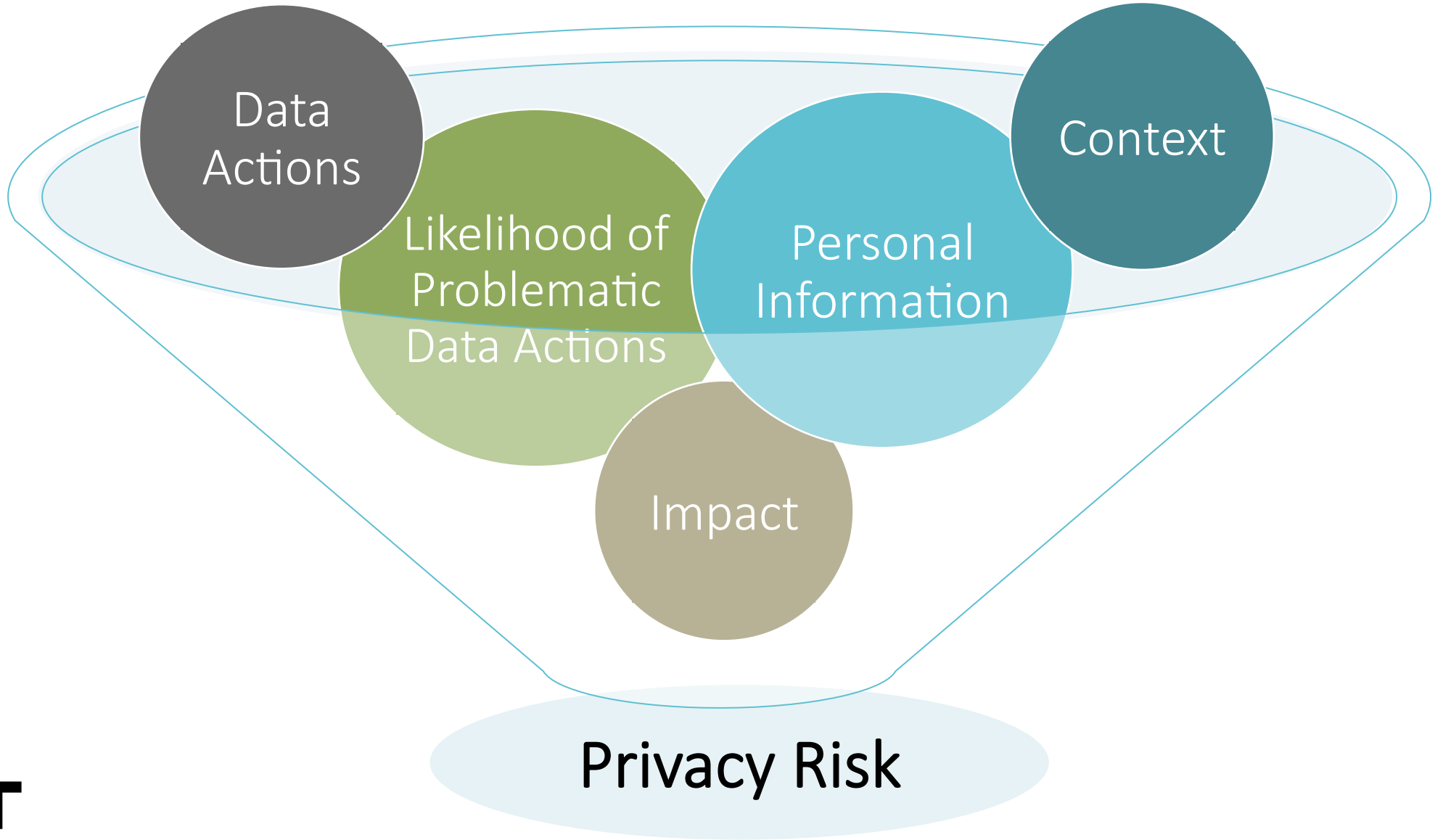
- The objectives are characteristics of the system, not role-based.
- The objectives support policy
- Part of broader risk management framework, including security, etc.



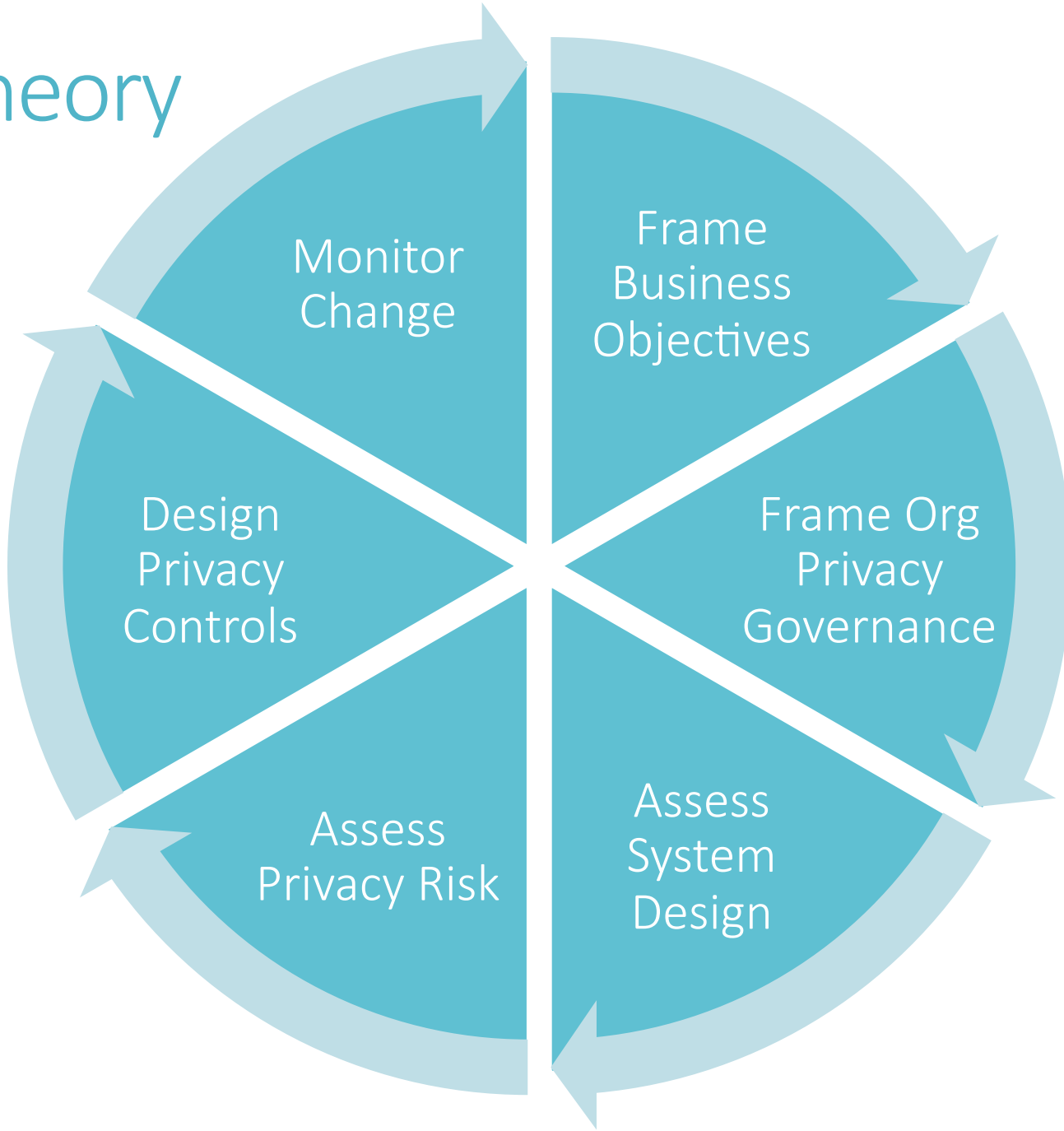
Security Risk Equation

Security Risk = Vulnerability * Threat * Impact

Identifying System Privacy Risk



Testing the Theory



Objectives and Research

- How can researchers effectively communicate the goals of their research?
- Without understanding how new technical privacy controls impact core components of privacy, it is tempting to see solutions as more widely (or narrowly) applicable than they are (ex: encryption).

Objectives provide a common, affirmative language to frame the pursuit of privacy-enhancing technologies, and further understanding of the social, cultural, and economic contextual factors necessary for effective risk analysis

Resources

NIST Privacy Engineering Website:

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