Privacy Risk Assessments:
A Prerequisite to Privacy Risk Management

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

NIST

Friction in Our Digital World

45% of online households reported that privacy or security concerns stopped them from:*

- Conducting financial transactions;
- Buying goods or services;
- Posting on social networks; or
- Expressing opinions on controversial or political issues via the Internet.

*July 2015 data collected for NTIA at https://www.ntia.doc.gov/blog/2016/first-look-internet-use-2015

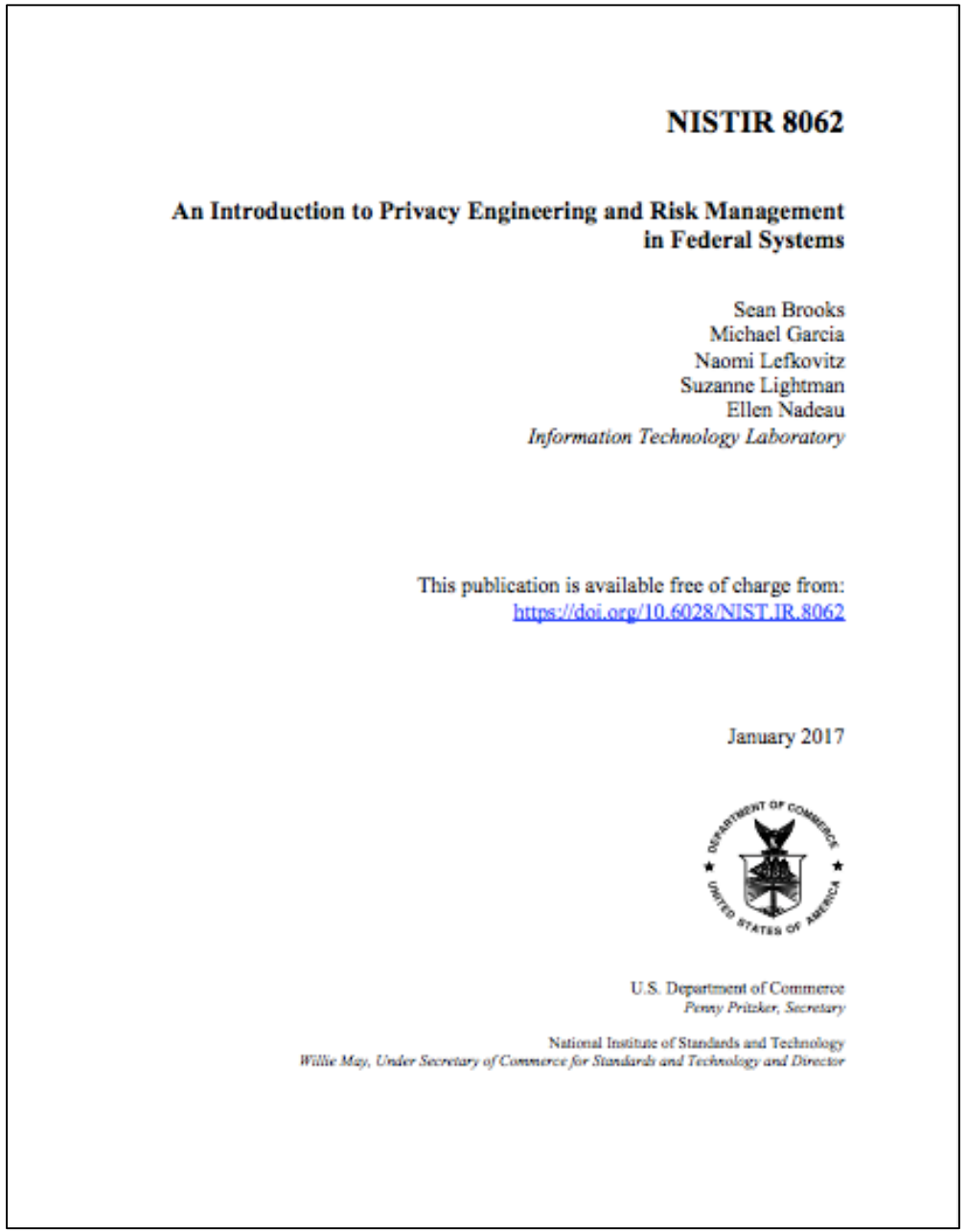
Primary Federal Driver

OMB July 2016 update to Circular A-130 clarified that:

- Agencies' obligations with respect to managing privacy risk and information resources extends beyond compliance with privacy laws, regulations, and policies
- Agencies must apply the NIST Risk Management Framework in their privacy programs

NISTIR 8062

An Introduction to Privacy Engineering and Risk Management in Federal Systems



NISTIR 8062

An Introduction to Privacy Engineering and Risk Management in Federal Systems

Sean Brooks
Michael Garcia
Naomi Lefkovitz
Suzanne Lightman
Ellen Nadeau
Information Technology Laboratory

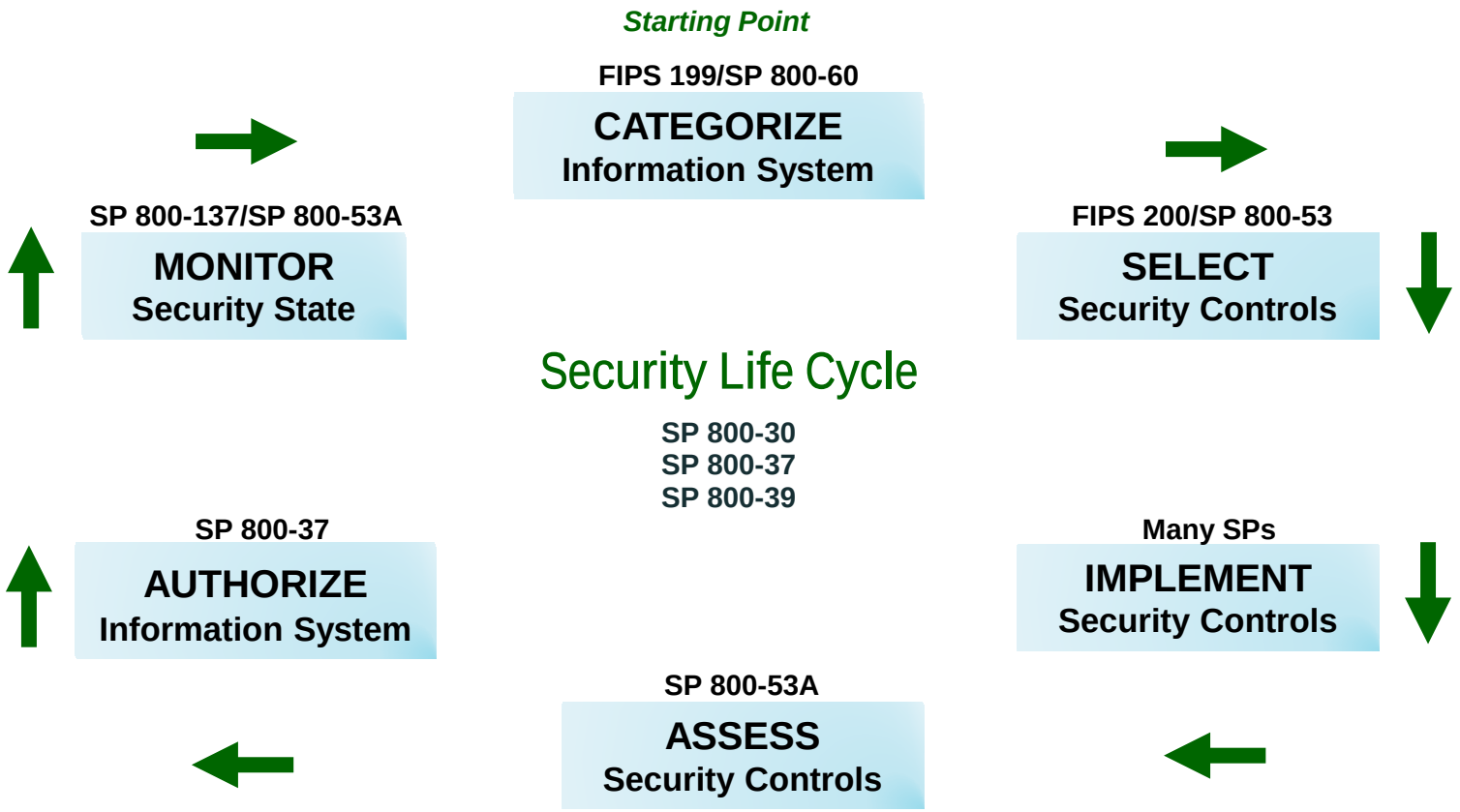
This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8062

January 2017

U.S. Department of Commerce
Penny Pritzker, Secretary

National Institute of Standards and Technology
Willie May, Under Secretary of Commerce for Standards and Technology and Director

NIST Risk Management Framework



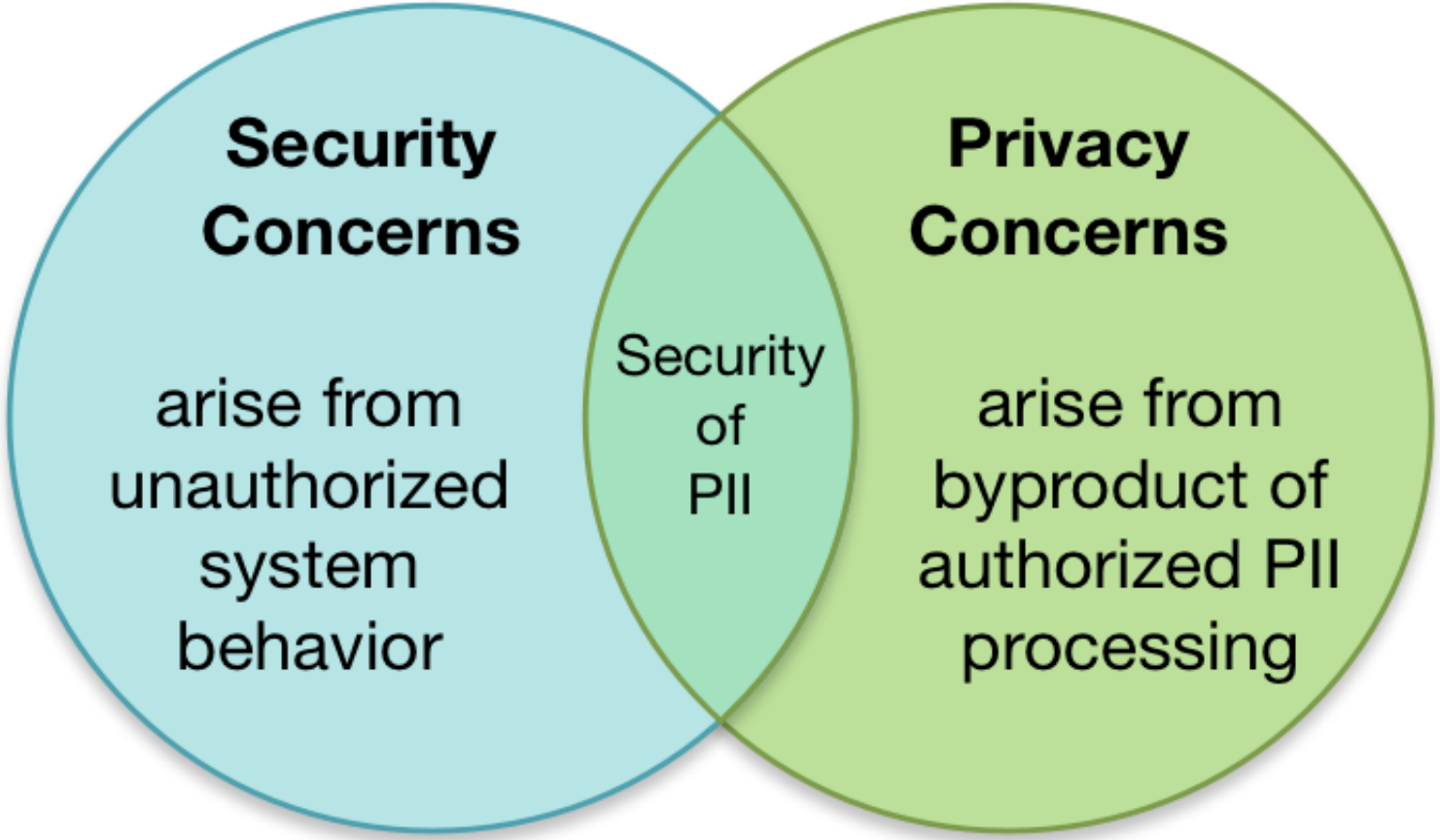
What is privacy risk?

Risk Analysis

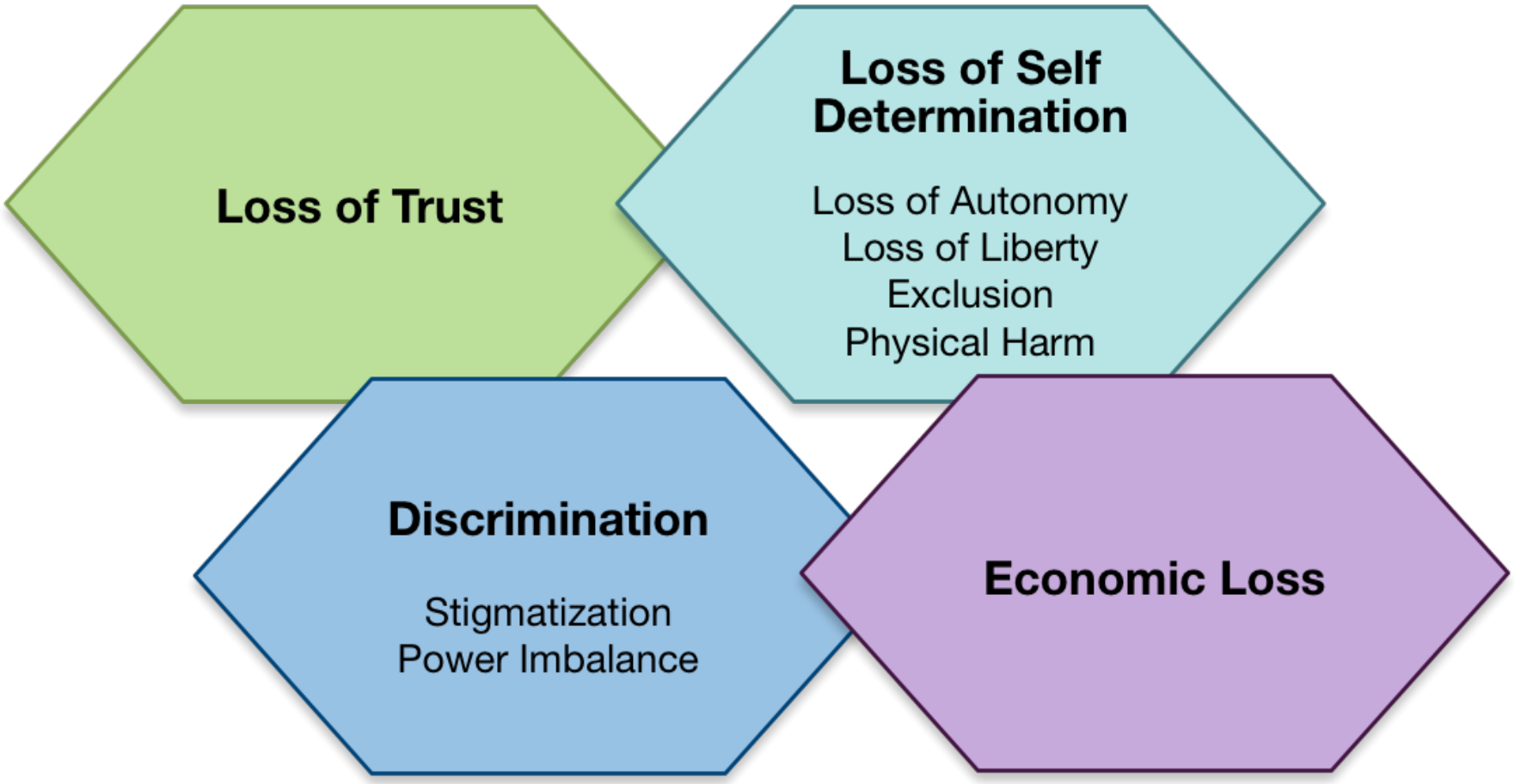
Risk is a function of:

- Likelihood of occurrence of adverse event
- Impact from the occurrence

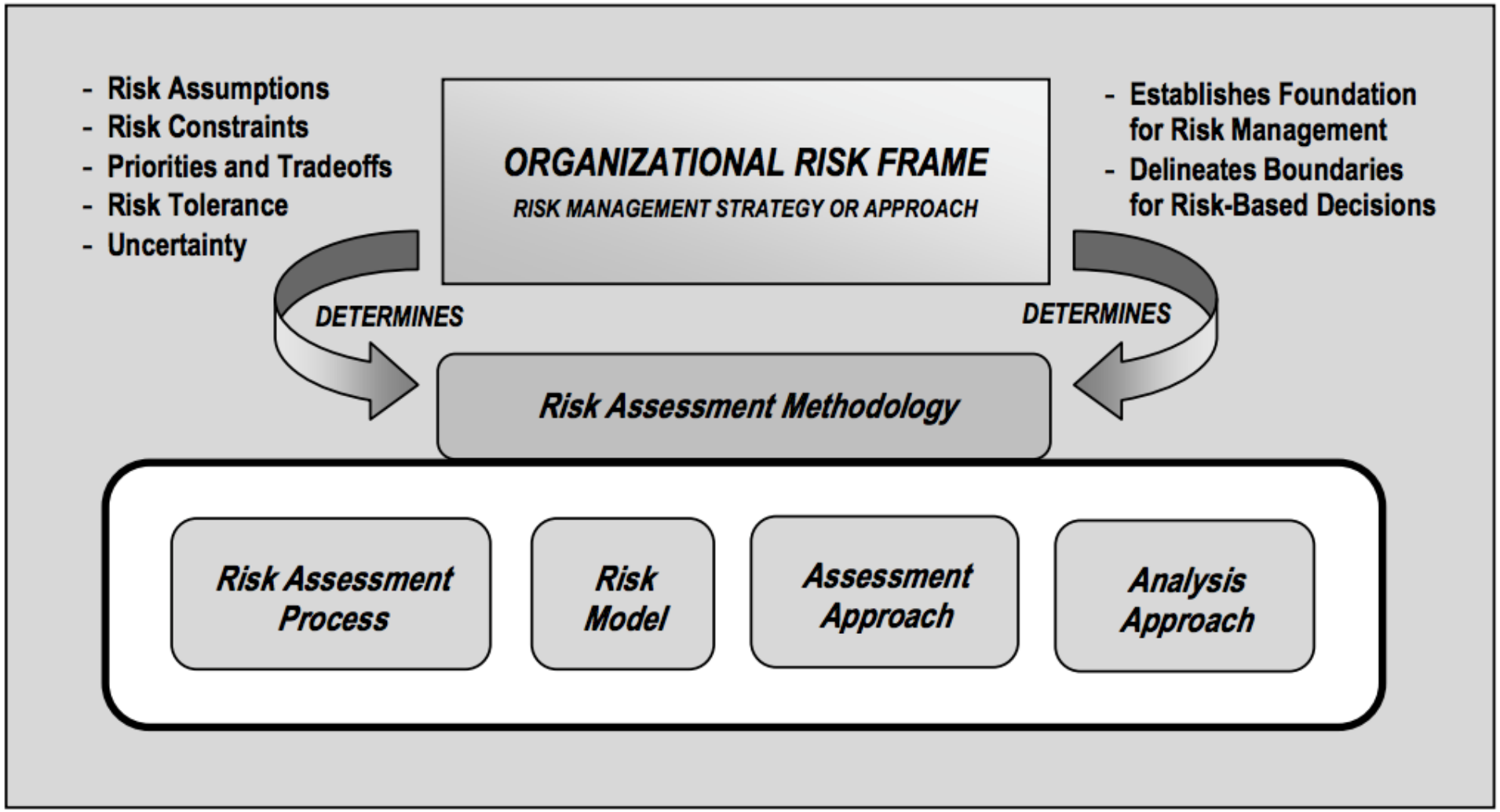
Information Security and Privacy: Boundaries and Overlap



Processing PII Can Create Problems for Individuals



Risk Assessment Components



NIST Special Publication 800-30

Risk Model

Risk models define the ***risk factors*** to be assessed and the relationships among those factors.

Risk factors are inputs to determining levels of risk.

Security Risk Model

Risk factors:

Likelihood |Vulnerability | Threat | Impact

NIST Working Model for System Privacy Risk

Privacy Risk Factors: Likelihood |Problematic Data Action |Impact

Likelihood is a contextual analysis that a data action is likely to create a problem for a representative set of individuals

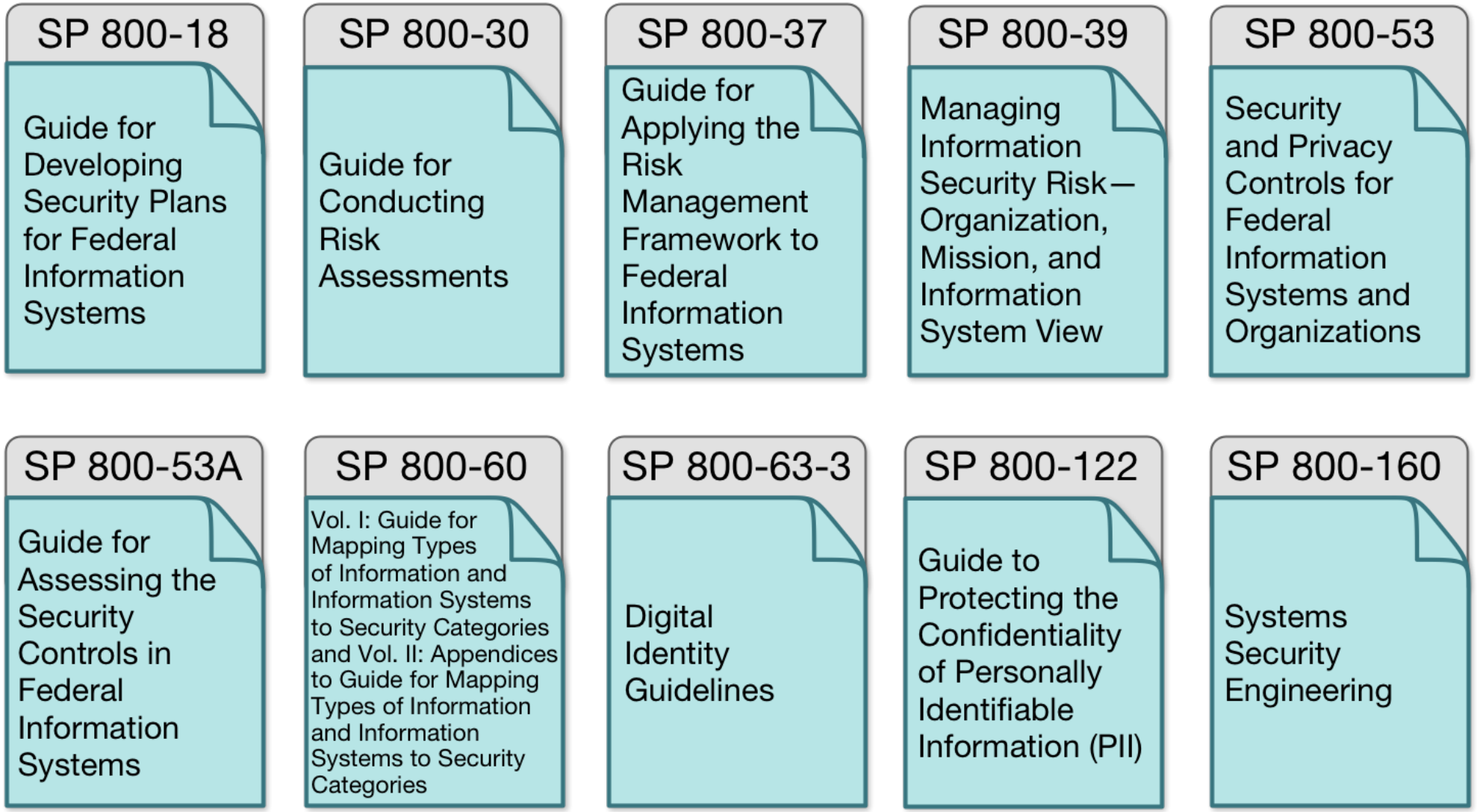
Impact is an analysis of the costs should the problem occur

Note: Contextual analysis is based on the data action performed by the system, the PII being processed, and a set of contextual considerations

Discussion for the Breakouts

- How can organizations effectively do risk assessments for privacy?
- Does a risk model for privacy differ from other risk models?
- What should be the factors for analysis?

Guidance Roadmap



What Should NIST Do Next?

- Which (if any) security-focused RMF documents require privacy parallels or additions?
- What other tools are needed for organizations to effectively do privacy risk management?
- What should be the prioritization?

NIST Privacy Risk Assessment Methodology (PRAM)