TOZNY

Understanding, Assessing, and Managing Privacy Risks

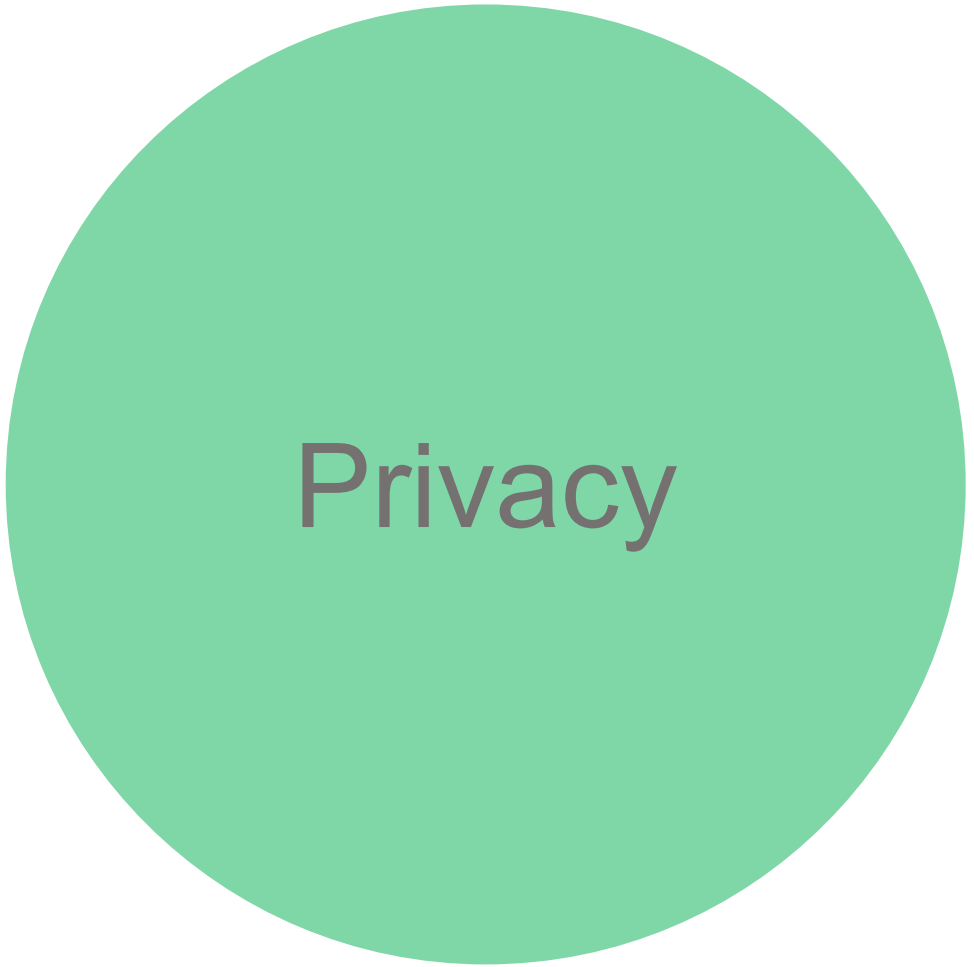
NWACC · Information Security Workshop

TOZNY

Understanding …

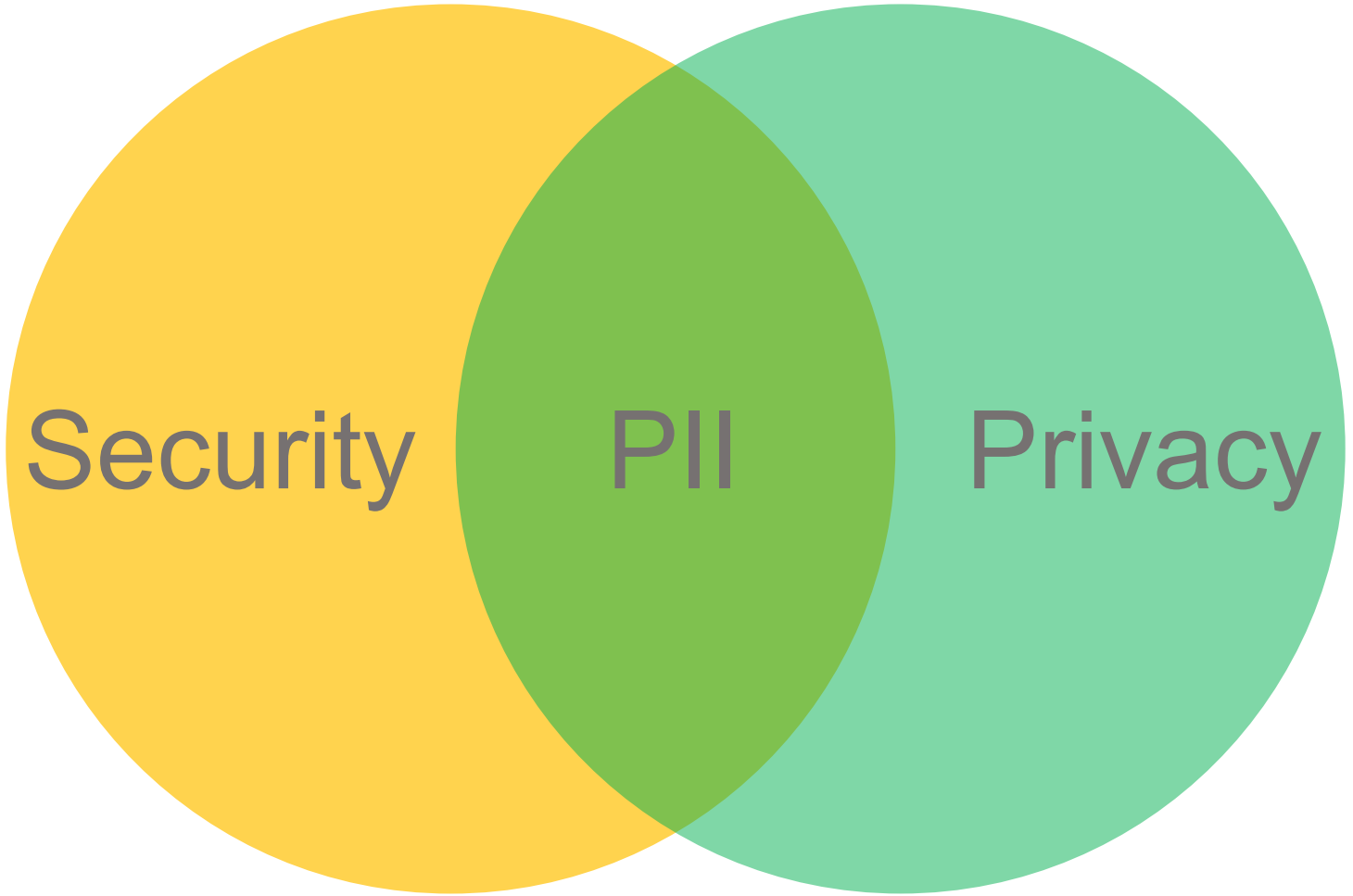
TOZNY

Understanding …



TOZNY

Understanding …



TOZNY

Understanding …

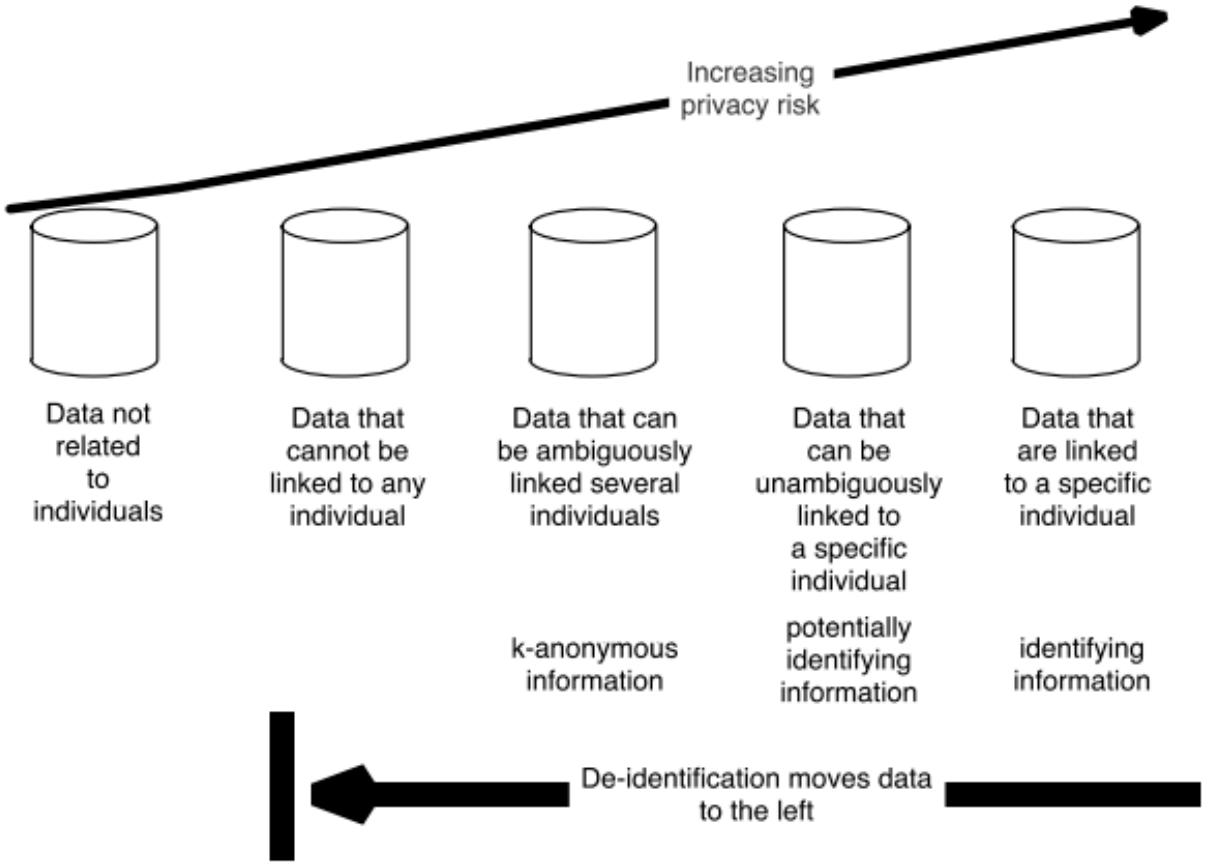
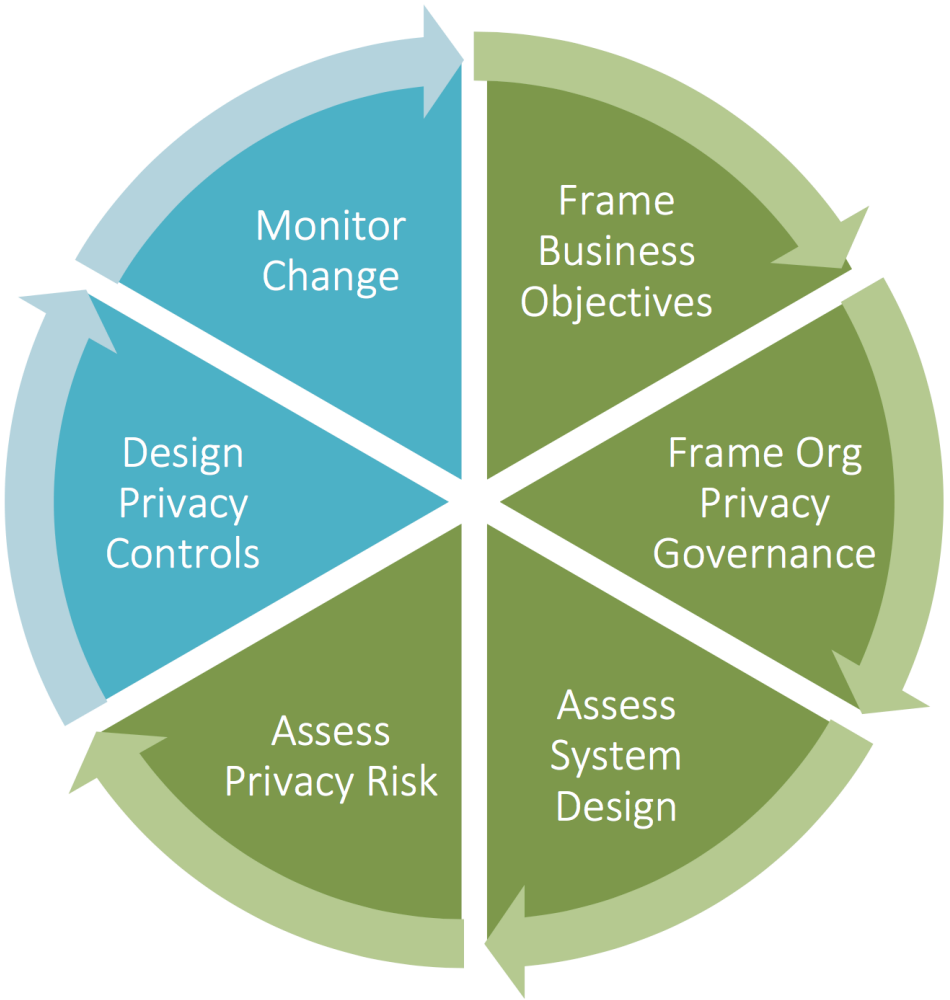


Figure 1: The Data Identifiability Spectrum.

TOZNY

Assessing …

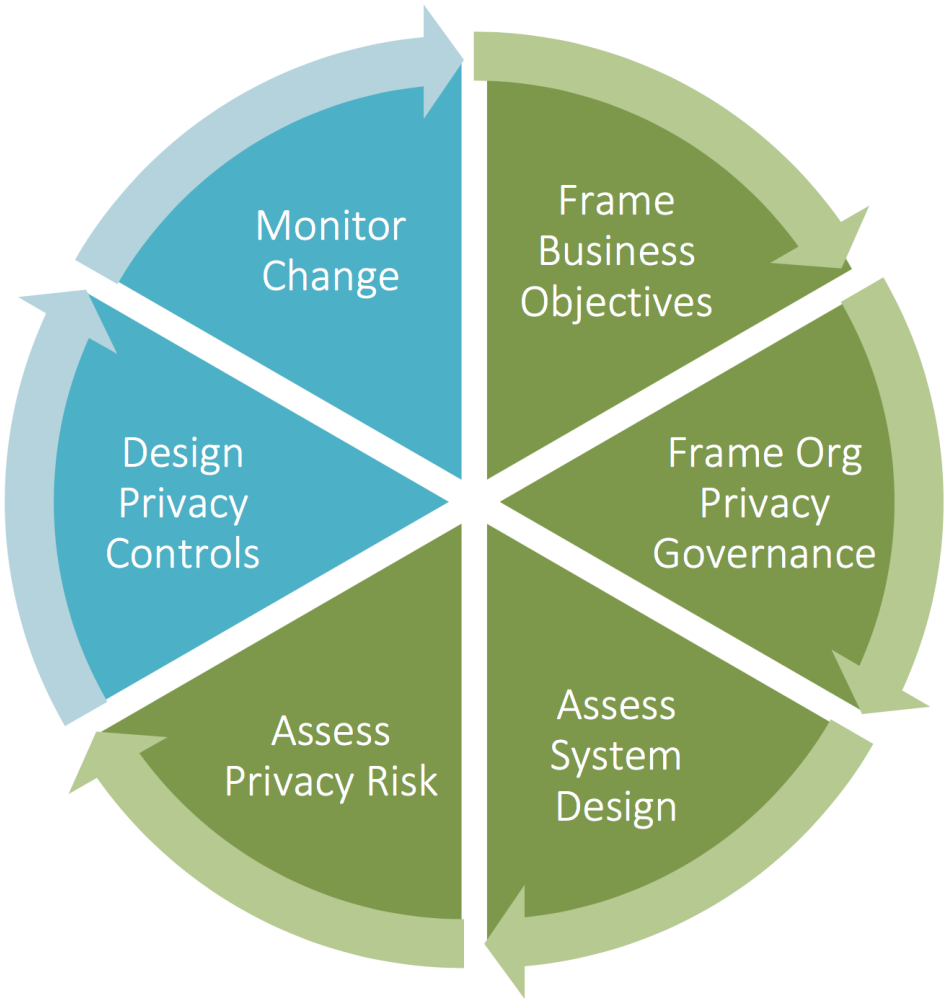
- Frame business objectives
- Frame organization privacy governance
- Assess system design
- Assess privacy risk
- Design privacy goals
- Monitor change



TOZNY

Assessing …

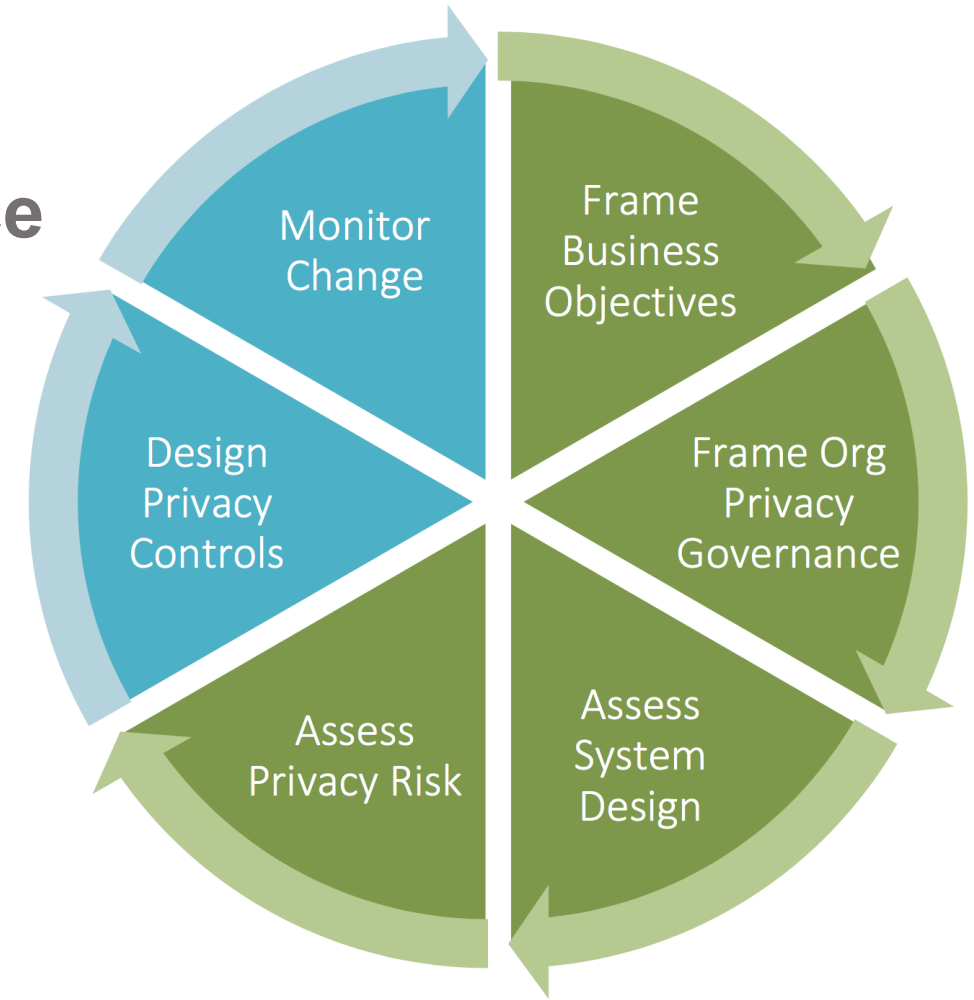
- **Frame business objectives**
- Frame organization privacy governance
- Assess system design
- Assess privacy risk
- Design privacy goals
- Monitor change



TOZNY

Assessing …

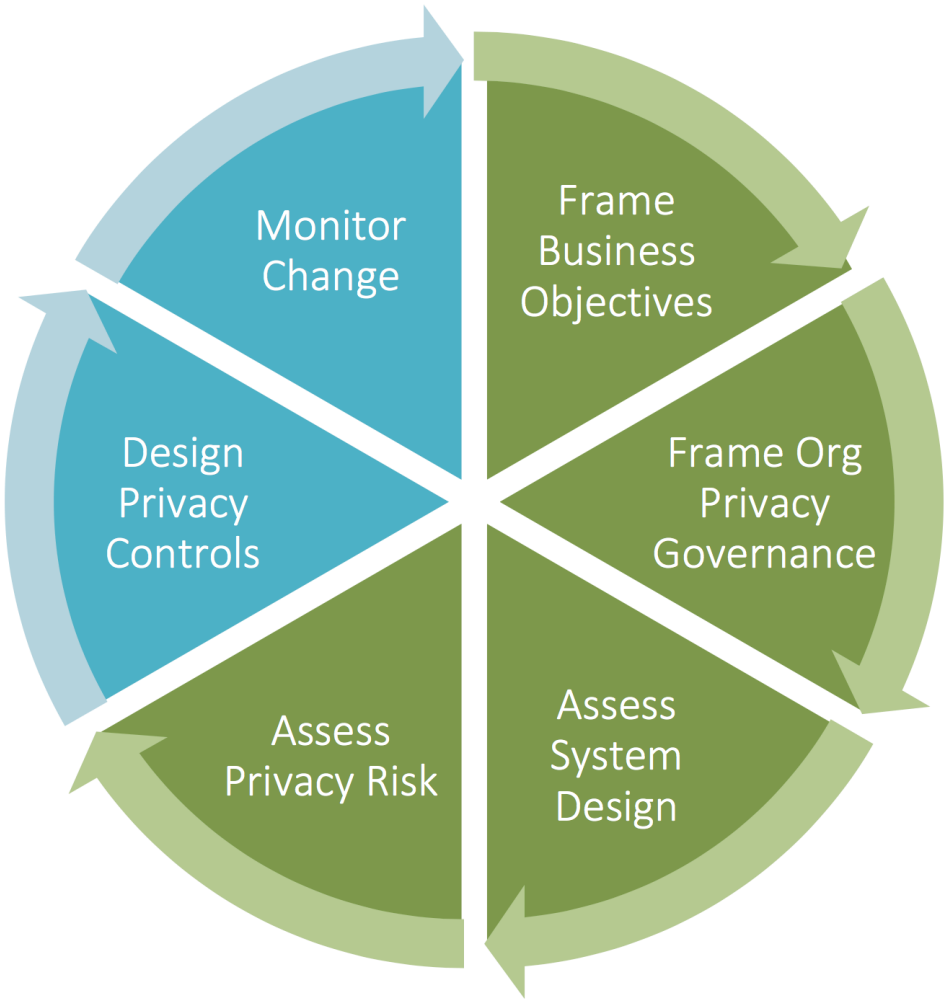
- Frame business objectives
- **Frame organization privacy governance**
- Assess system design
- Assess privacy risk
- Design privacy goals
- Monitor change



TOZNY

Assessing …

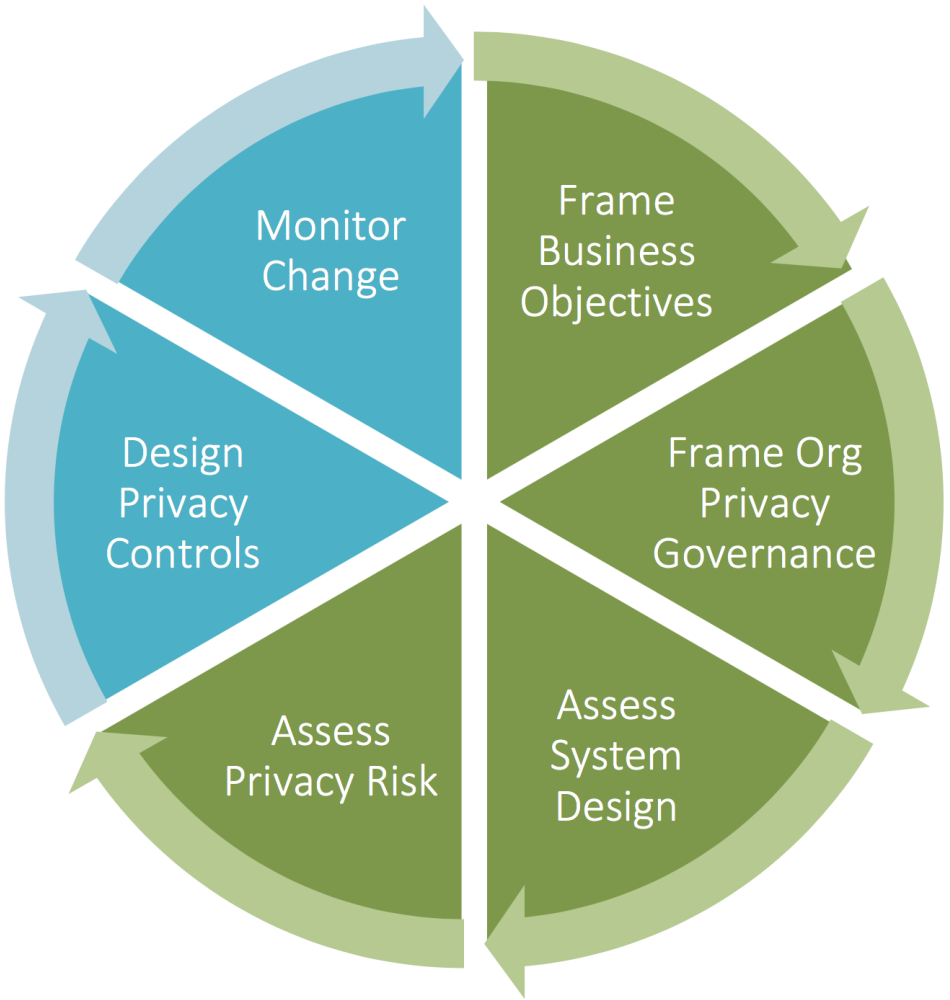
- Frame business objectives
- Frame organization privacy governance
- **Assess system design**
- Assess privacy risk
- Design privacy goals
- Monitor change



TOZNY

Assessing …

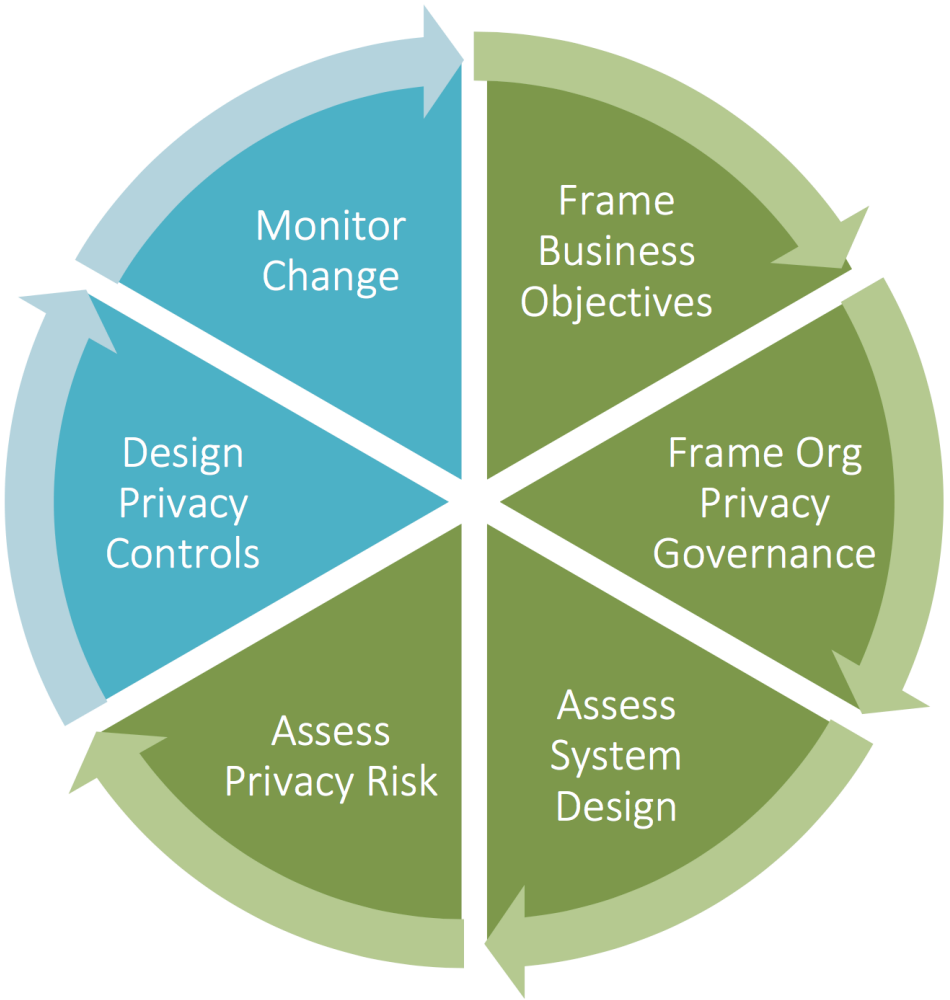
- Frame business objectives
- Frame organization privacy governance
- Assess system design
- **Assess privacy risk**
- Design privacy goals
- Monitor change



TOZNY

Assessing …

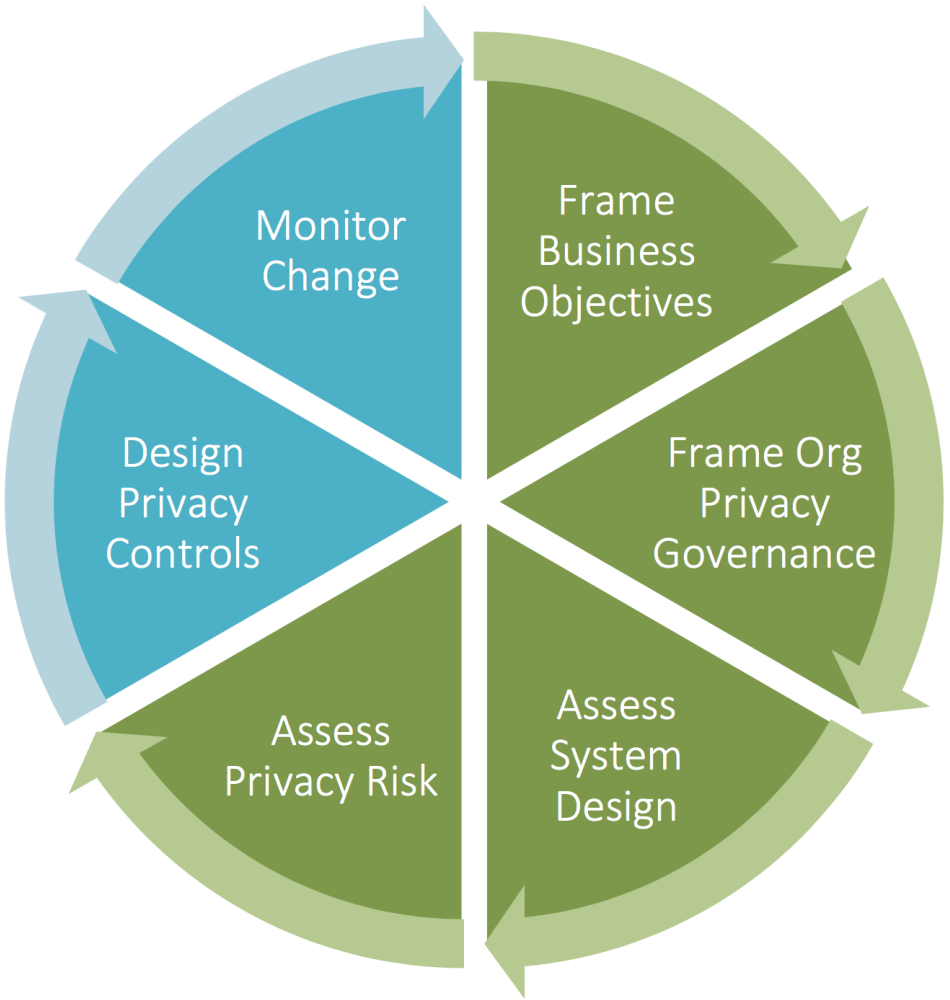
- Frame business objectives
- Frame organization privacy governance
- Assess system design
- Assess privacy risk
- **Design privacy goals**
- Monitor change



TOZNY

Assessing …

- Frame business objectives
- Frame organization privacy governance
- Assess system design
- Assess privacy risk
- Design privacy goals
- **Monitor change**



TOZNY

What's the Purpose

- Ensure **Predictability** – enable reliable assumptions about personal information and how it will be processed
- Promote **Manageability** – provide for granular administration of personal information, including alteration, deletion, and disclosure
- Enable **Disassociability** – allow the processing of personal data without associating to individuals beyond requirements

TOZNY

Assessment Example

USE CASE: USERS ENCRYPTING THEIR OWN DATA

TOZNY

Assessing … An Example

- Encrypt at the point of origin, decrypt at the point of use
  - Compare to full-disk and network encryption (TLS)
  - Implies intermediate parties *have no data access*
- Applies in multiple scenarios:
  - Two or more end users
  - Client and server communication
  - Inter-server communication
- Results in **data minimization**
  - Users encrypt, no one else has access!

TOZNY

Assessing … An Example

USE CASE: USERS ENCRYPTING THEIR OWN DATA

- **Data Event:** Storage and Retrieval of Encrypted data
- **Problematic data actions:** Availability failure (loss of key)
- **Selected controls:** User-to-user encryption for selected data
- **Considerations:** Could make code more complex. Difficult to trust users to maintain keys – *severe* availability risks if keys are lost
  Extremely effective in ensuring privacy.

TOZNY

Assessing … An Example

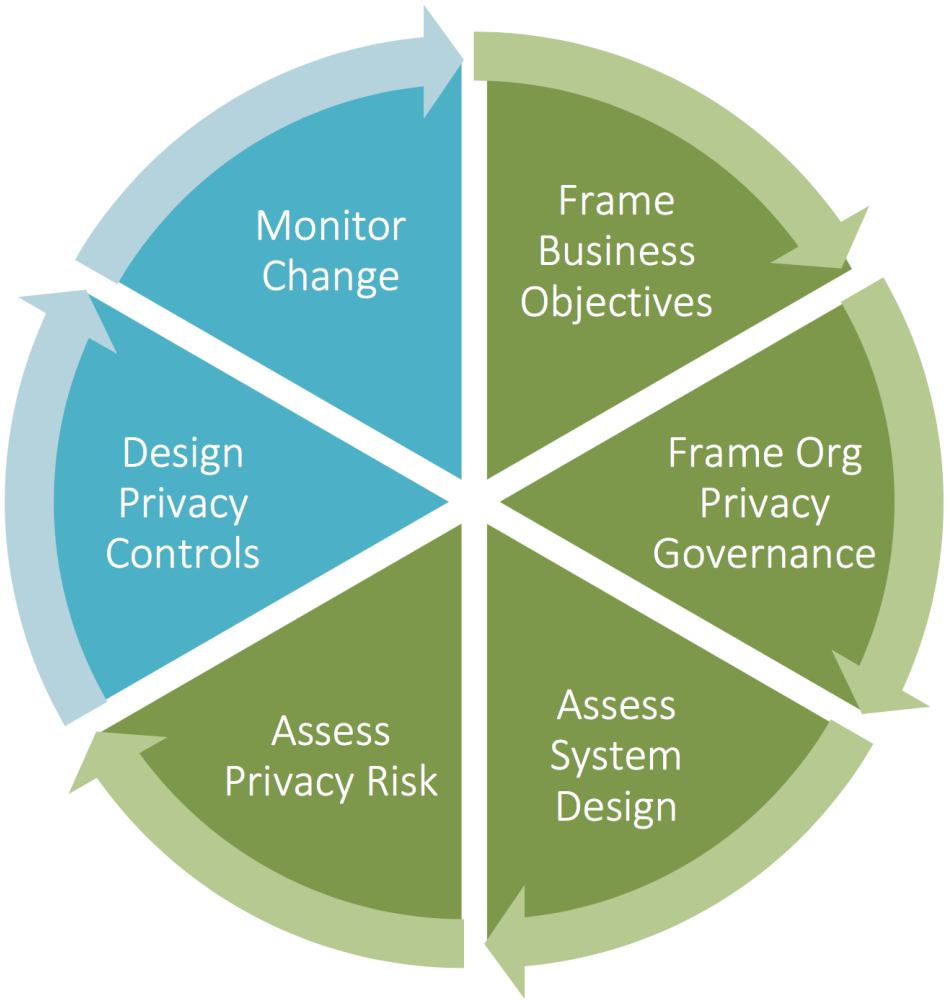
USE CASE: USERS ENCRYPTING THEIR OWN DATA

- Balance the risks on either side
  - Which is greater, risk of key loss or risk of data breach?
- System design implications hinge off this assessment
- Future changes likewise follow from this consideration

TOZNY

Management …

- Ongoing management requires review
  - Have systems changed?
  - Have objectives changed?
  - Has the organization changed?
  - Have new risks been presented?
- Management equates to ongoing reassessment and adjustment



TOZNY

Resources

- NIST Internal Report 8062
  - An Introduction to Privacy Engineering and Risk Management in Federal Systems
  - Both the final January 2017 report *and* the May 2015 draft
- NIST Internal Report 8053
  - De-Identification of Personal Information
- NIST Special Publication 800-30
  - Guide for Conducting Risk Assessments
- NIST Special Publication 800-39
  - Managing Information Security Risk

TOZNY

Questions?

TOZNY

THANK YOU!

info@tozny.com
(844) 628-2872
www.tozny.com