Deloitte.

Enterprise Risk: Privacy and Identity Theft

Ken DeJarnette, CIPP

Principal – Security & Privacy Services, Deloitte & Touche LLP

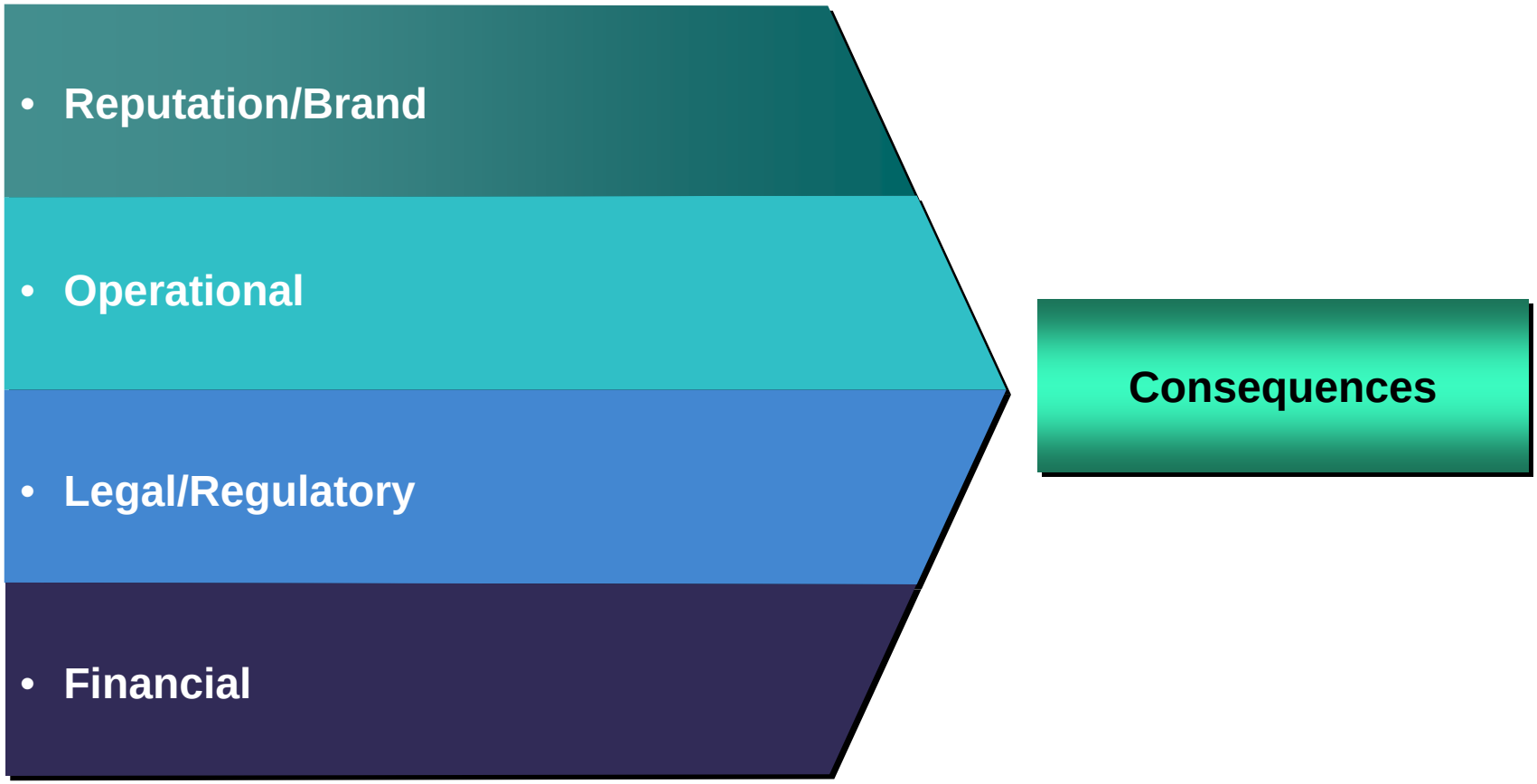
The Privacy Symposium

Harvard, MA

August 21, 2007

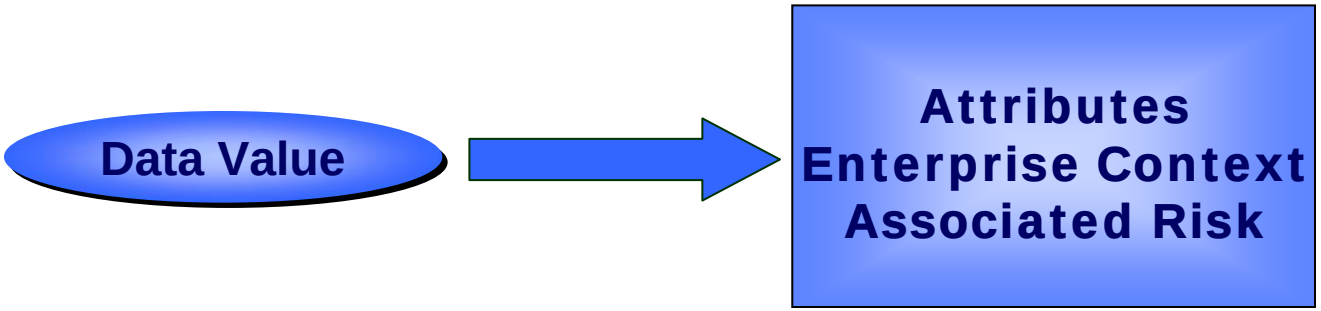
Privacy and ID Theft: Part of a Broader Risk Program

What risk are we trying to manage?

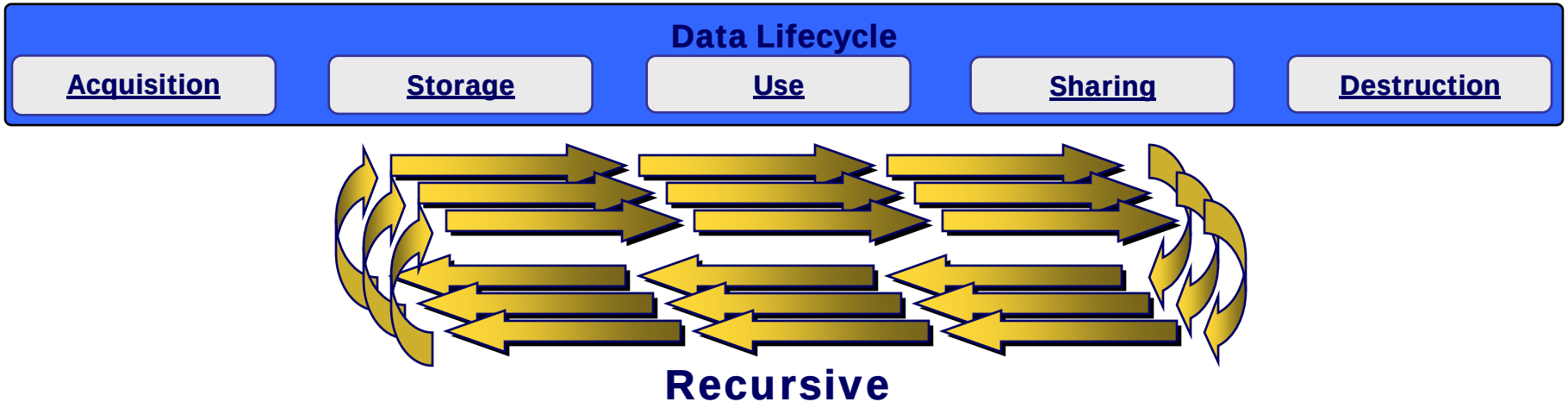


The Nature of PII: Protecting an Evolving Asset

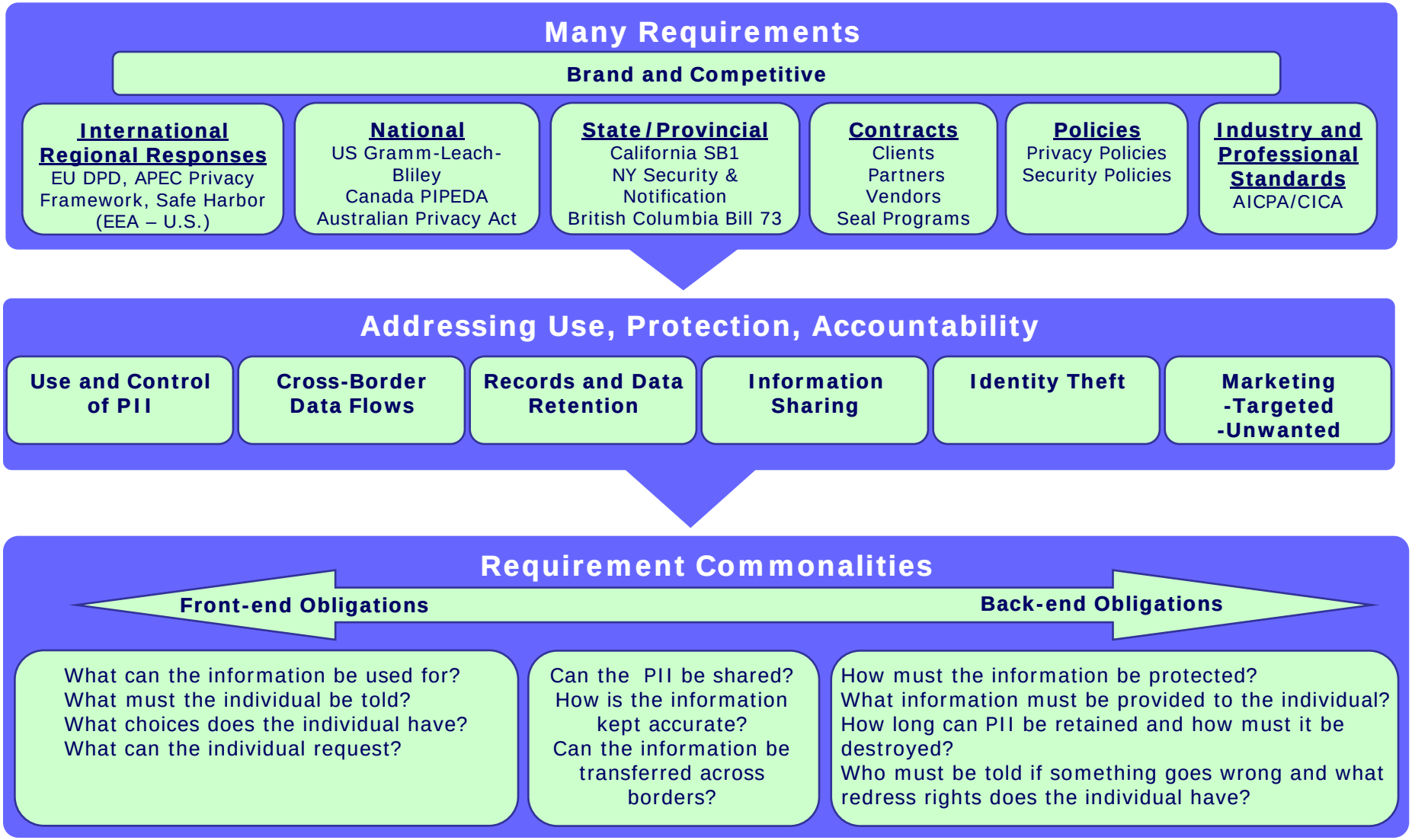
Data is an asset with multiple attributes. The value associated with data is determined by its attributes, context within the enterprise and associated risk.



The nature of data changes over time, as it is stored, used and shared.

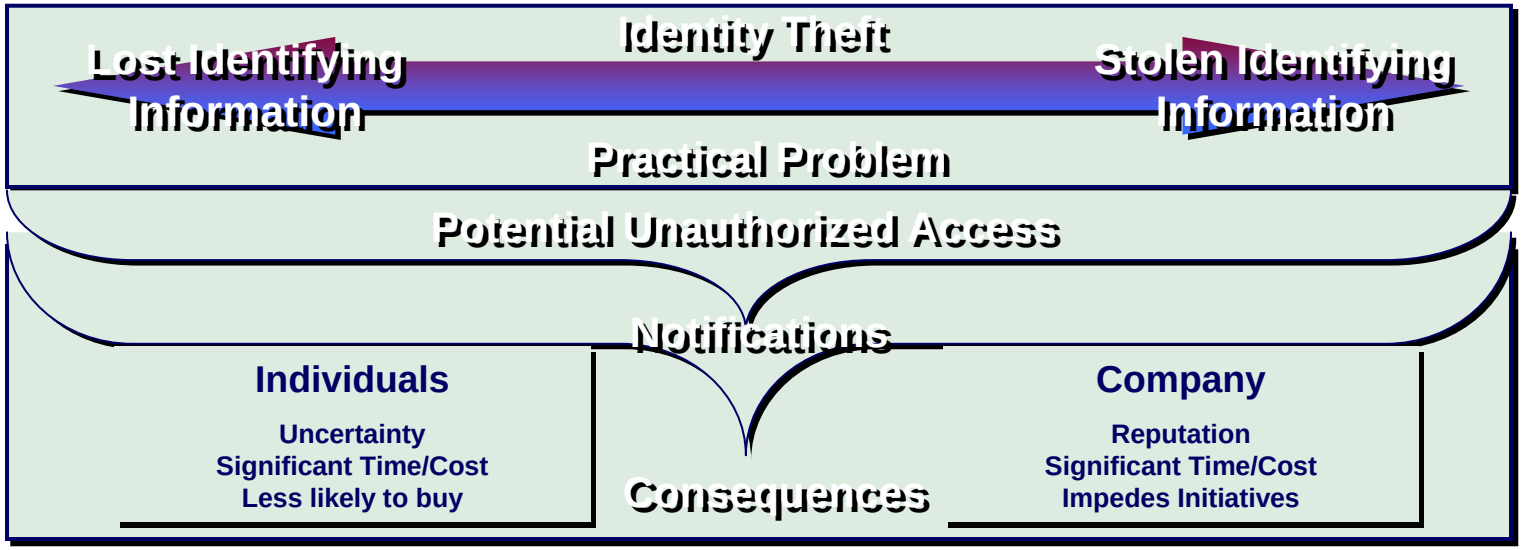


The Privacy and Data Protection Environment



Understanding the Totality of Problem

- **Technical definition:**
  - A fraud committed or attempted using the identifying information of anther person . . .
  - "Identifying information" means a name or number that can be used alone or in conjunction with other information to identify a specific person including:
    - Name, SSN, date of birth, drivers license, alien registration, passport, taxpayer id
    - Unique biometric data
    - Unique electronic identification number, address or routing code
- **However, broader than technical definition:**
  - Disclosure requirements are triggered when an individual or business knows or reasonably believes there has been a security breach impacting personal information (i.e., identifying information) (CA SB-1386)
  - A "security breach" typically means unauthorized acquisition/access of unencrypted personal information (CA SB-1386)



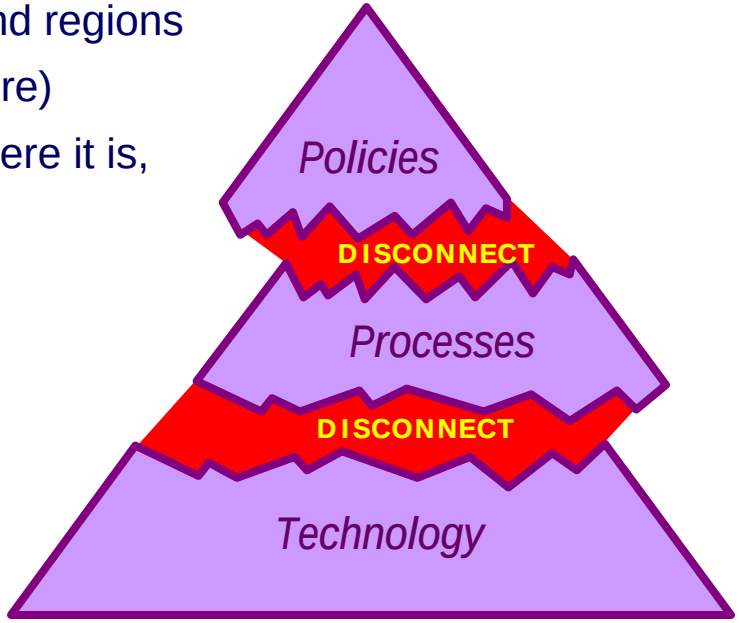
Common Privacy Challenges

Organizations face multiple challenges in meeting privacy demands:

- Creating a privacy strategy that accounts for a complex, multi-regulatory, and changing environment
- Driving policy into business practices and technology
- Managing customer and employee concerns and perceptions across differing cultures and multiple industries
- Reconciling inconsistent practices among affiliates and regions
- Managing the data lifecycle (legacy, current, and future)
- Knowing how PII is acquired, what they do with it, where it is, who it is shared with, and how to dispose of it
- Adopting privacy values throughout the enterprise
- Coordinating incident response and investigations

Most common mistakes:

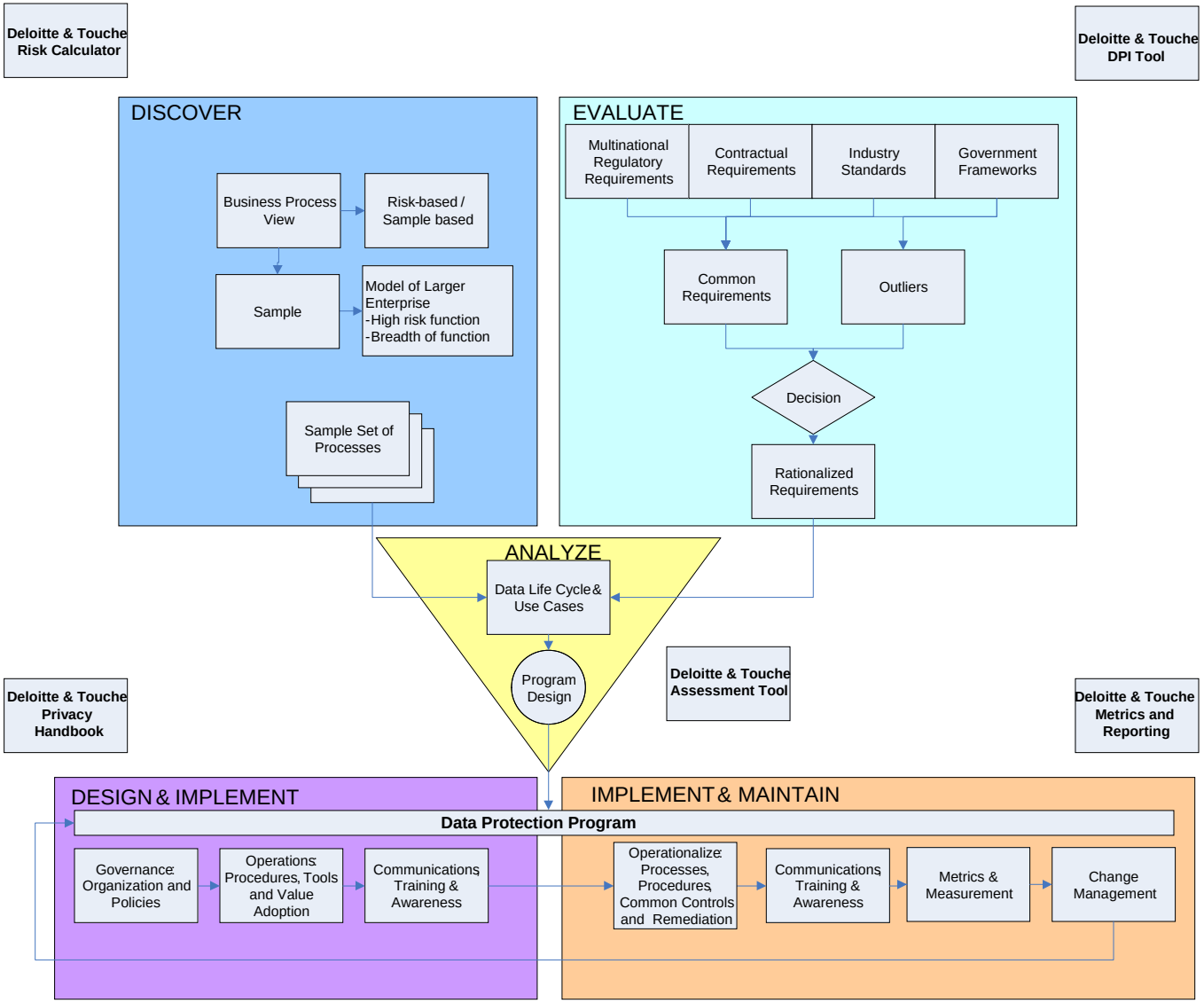
- Rushing to policy
- "Failing to do what you say you do"



Bringing Analytical Rigor

- Understanding environment
  - Process centric
- Rationalizing requirements
- Developing risk criteria
  - Origin
  - Type
  - Use
  - Environment
- Prioritizing
- Use/scenarios
- Common controls

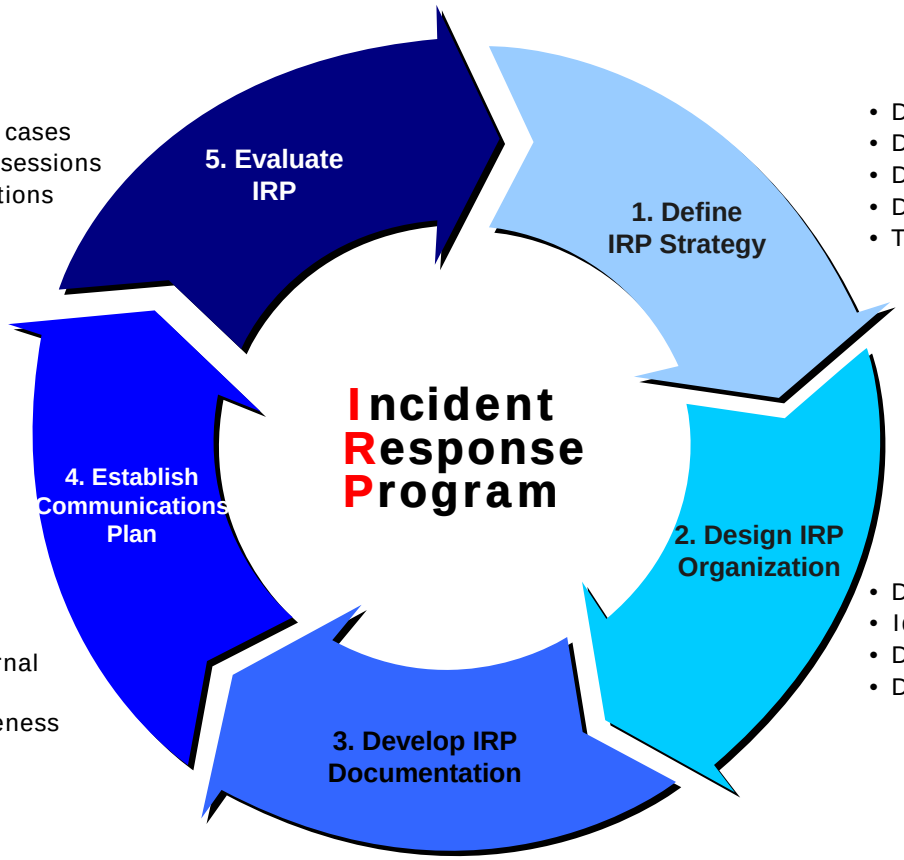
Data Protection Program Methodology Map



Responding to a Privacy Incident

- Privacy incidents can have a broad impact and lasting implications
- Response must be programmatic
  - Thought through
  - Risk-based
  - Tactical and strategic
- Early issue spotting is critical – for instance:
  - Lost data may have the same consequences as a hacking incident
  - Notice (who to tell, what to tell and when) may not be simple
  - Duties and obligations may not be clear and might conflict (customers, partners, regulatory agencies, law enforcement)
- Post-incident analysis is essential
  - Address the root-cause
  - Update the program based on lessons learned
- Practice

Incident Response Program



- Develop executive sponsorship
- Develop objectives
- Define scope
- Document charter and strategy
- Tied to related programs (BCM)

- Define roles and responsibilities
- Identify requirements and resources
- Develop organizational structure
- Define budget

- Develop policies
- Develop standards, including types and levels of incidents
- Develop procedures
- Design templates

- Communicate IRP to stakeholders
- Establish internal and external communications strategy
- Conduct training and awareness

- Create testing schedule
- Develop scenarios and test cases
- Conduct tests and practice sessions
- Prioritize and plan remediations

About Deloitte
Deloitte refers to one or more of Deloitte Touche Tohmatsu, a Swiss Verein, its member firms, and their respective subsidiaries and affiliates. Deloitte Touche Tohmatsu is an organization of member firms around the world devoted to excellence in providing professional services and advice, focused on client service through a global strategy executed locally in nearly 150 countries. With access to the deep intellectual capital of 120,000 people worldwide, Deloitte delivers services in four professional areas – audit, tax, consulting and financial advisory services – and serves more than one-half of the world's largest companies, as well as large national enterprises, public institutions, locally important clients, and successful, fast-growing global growth companies. Services are not provided by the Deloitte Touche Tohmatsu Verein, and, for regulatory and other reasons, certain member firms do not provide services in all four professional areas.

As a Swiss Verein (association), neither Deloitte Touche Tohmatsu nor any of its member firms has any liability for each other's acts or omissions. Each of the member firms is a separate and independent legal entity operating under the names "Deloitte," "Deloitte & Touche," "Deloitte Touche Tohmatsu," or other related names.

In the U.S., Deloitte & Touche USA LLP is the U.S. member firm of Deloitte Touche Tohmatsu and services are provided by the subsidiaries of Deloitte & Touche USA LLP (Deloitte & Touche LLP, Deloitte Consulting LLP, Deloitte Financial Advisory Services LLP, Deloitte Tax LLP and their subsidiaries), and not by Deloitte & Touche USA LLP. The subsidiaries of the U.S. member firm are among the nation's leading professional services firms, providing audit, tax, consulting and financial advisory services through nearly 30,000 people in more than 80 cities. Known as employers of choice for innovative human resources programs, they are dedicated to helping their clients and their people excel. For more information, please visit the U.S. member firm's Web site at www.deloitte.com/us.