



# Privacy & Data Protection

Presented to:

New Orleans ISACA Chapter

Presented by:

Raj Mehta, CPA, CITP, CISA, CISSP, CIPP

May 31, 2007

# Agenda

---

- **What is Privacy and Personally Identifiable Information (PII)?**
- **Privacy Legal Landscape**
- **How does it apply to my organization?**
- **Enterprise Privacy Drivers**
- **How to address Privacy**

# Defining Privacy

---

Generally, there are **three social concerns** that drive the issue of privacy. These include individuals' fears about:

- How PII is **used**
- How PII is **protected**; and
- Who is **accountable**

There are many definitions and classifications of personal information:

- **California SB 1386: “Personal Information”** - An individual's name, social security number, driver's license number or identification card number; or an account number, credit or debit card number, in combination with a required security code, access code, or password that would permit access to an individual's financial account
- **Gramm-Leach-Bliley: “Nonpublic Personal Information”** - Information not publicly available such as social security number, account information, financial information
- **Louisiana SB 205** - The bill requires that state residents be notified when there has been an unauthorized access of their PII.
- **COPPA: “ Personal Information”** - Individually identifiable information about an individual collected online including name, home address, email address, telephone number, social security number, any other identifier concerning the client child or the parents of that child that the website collects
- **HIPAA:** Health Insurance Portability & Accountability Act

*Companies have the difficult task of developing their own definition of customer and employee personal information*

# Regional Differences

---

**Despite the similarities that exist amongst various privacy models, there are fundamental regional differences that exist in the world today:**

## **\* U.S. \***

The prevailing concept is that once an individual provides PII to an organization, the organization becomes the data owner. Baring any sector specific privacy legislation, the organization can determine the use of that information.



## **\* EU\***

The prevailing concept is that the individual data subject retains rights in his/her PII. The organization has the responsibilities of a custodian for protecting that PII and using it only in accordance with the rights conveyed by the individual.

## **\* APEC \***

The prevailing concept is accountability. Organization must design privacy protections to prevent harm to individuals from wrongful collection or misuse. The organization is accountable and obligated to exercise due diligence.

# Defining PII: Commonalities

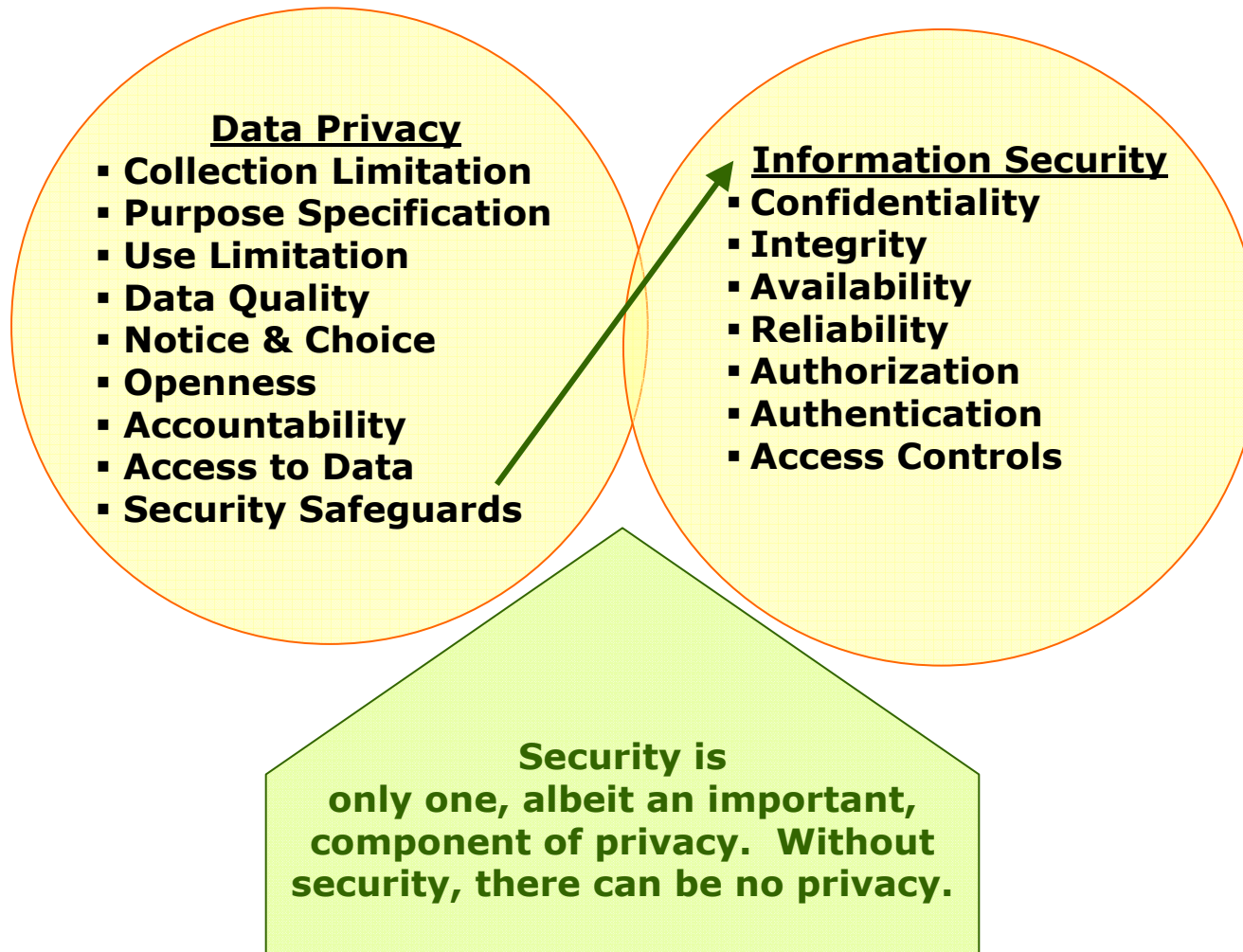
---

PII is generally defined as **any information relating to an identified or identifiable natural person**. It may be referred to as personal data, personal information, non-public personal information, etc. For purposes of this training we will use the term PII. Examples include (but are not limited to):

PERSONAL INFORMATION	<ul style="list-style-type: none"><li>• <b>Name</b></li><li>• <b>Gender</b></li><li>• <b>Date of birth</b></li><li>• <b>Home address</b></li><li>• <b>Personal telephone number</b></li><li>• <b>Personal email address</b></li><li>• <b>Biometric identifier</b></li><li>• <b>Photograph or video identifiable to an individual</b></li><li>• <b>Behavioral information (e.g., in a CRM system)</b></li></ul>
HEALTH INFORMATION	<ul style="list-style-type: none"><li>• <b>Medical records</b></li><li>• <b>Health plan beneficiary information</b></li><li>• <b>Physical or mental health information</b></li><li>• <b>Provided health services or any information collected during the health service</b></li></ul>
FINANCIAL INFORMATION / SPECIAL HANDLING PII	<ul style="list-style-type: none"><li>• <b>Government identifiers (Social Security Numbers)</b></li><li>• <b>Account numbers (bank accounts, credit cards, etc.)</b></li><li>• <b>Personal Identification Numbers (PINs) and passwords to financial accounts</b></li></ul>
SENSITIVE INFORMATION	<ul style="list-style-type: none"><li>• <b>Racial or ethnic origin</b></li><li>• <b>Religious or philosophical beliefs</b></li><li>• <b>Trade-union membership</b></li><li>• <b>Health or sexual orientation</b></li><li>• <b>Offenses, criminal convictions or security measures</b></li><li>• <b>Combinations of certain information (e.g., name and ssn)</b></li></ul>

# Privacy & Security Relationships

---



# Global Response: Proliferation of Privacy and Data Protection Laws & Regulations

---



# EU Data Protection Directive 95/46/EC

---

- **Enacted in 1995, effective 1998**
- **Each country has its own national data protection law – the directive sets the floor**
- **Prohibits transfer of personal data to non-EU jurisdictions unless “adequate level of protection” is guaranteed or another exception applies**
- **US is not adequate, but enforcement was limited prior to Safe Harbor**
- **Enforcement remains spotty, but recent high profile cases have changed the compliance landscape**
- **Personal Data** - any and all data that relates to an identifiable individual
- **Special Categories of Data** - any and all data revealing race, ethnic origin, political opinions, religion or beliefs, trade union membership, sexual orientation or sex life, or criminal offenses...as well as biometric, health or disability data, national id numbers
- **Processing** - any and all operations on personal data (including collection, storage, handling, use, disclosure and deletion) - regardless of form or format (manual or automatic processing)

# Transferring Data Outside the EU

---

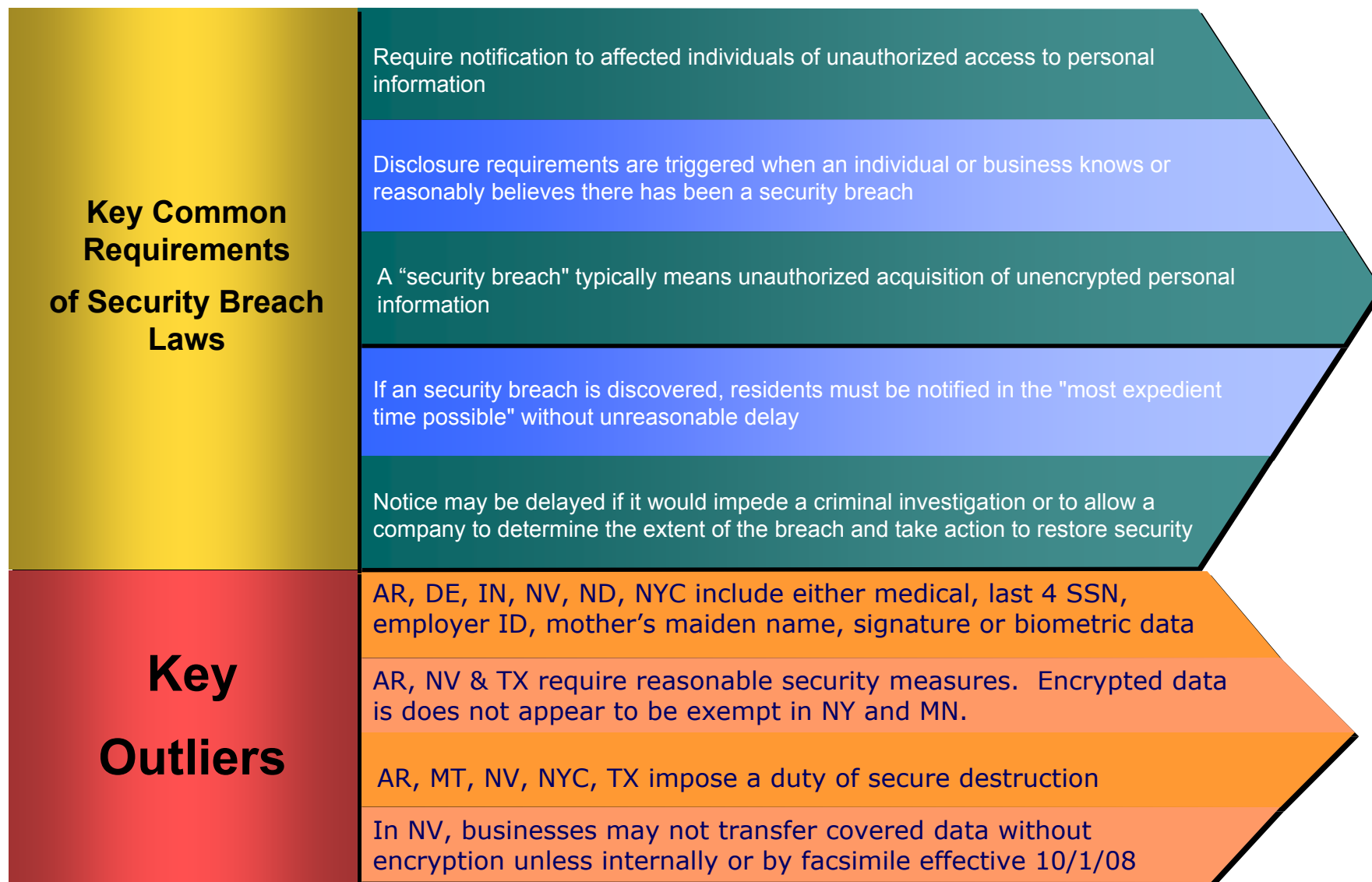
- **Data transfers are acceptable under the following conditions:**
  - To a country that has been declared adequate (e.g., Switzerland, Canada)
  - Within the Safe Harbor framework (from EU to US only)
  - To any country, if a contract ensures adequate protection (e.g., using model clauses)
  - With “unambiguous consent” from the data subject
  - Upon authorization of EU Member State from which data is transferred

# Safe Harbor

---

- **US Dept of Commerce created a series of documents that describe privacy principles similar to those in the Directive**
- **EU agreed that companies that self-certify are following the principles and are in an adequate safe harbor**
- **FTC agreed that not following a self-certified standard is unfair/deceptive and subject to enforcement**
- **Companies implement a privacy program, then certify annually to DOC that they are compliant**
- **Not available to financial institutions and others who are not regulated by the FTC or Dept of Transportation**

# State Breach Notification Laws: Commonalities & Outliers



# Privacy Requirements – Recent Developments

---

## Federal

- **Increasing FTC enforcement** moving from deceptive trade practices allegations to unfair privacy and security practices (fines and/or mandatory audits)
- Various **federal breach notification** bills in both the House and Senate
- Vigorous federal agency pursuit of **cell-phone record sales**
- **Various federal bills restricting the use of SSN**
- **12 privacy and security related bills** were introduced on the first session of congress in Jan 07
- AICPA/CICA **Generally Accepted Privacy Principles (May 2006)**

## State

- 34 states and the municipality of New York City now have **final or proposed Breach Notification Laws** similar to California SB1386 (as of 12/07/2006)
- California SB 433 prohibits the use of RFID devices in CA drivers licenses and state ID cards (2006)
- 38 states with pending bills restricting the use of SSNs

## International

- EU Article 29 Data Protection Working Party Opinions:
  - Privacy issues related to the provision of **email screening** services (Feb 2006)
  - The application of EU data protection rules to internal **whistle blowing** schemes (Jan 2006)
- Canadian PIPEDA under Parliament review in 2006 – Results not yet available

## How does it apply to my organization?

---

- PII protection requirements apply to Customers, Business Partners, and **Employees**
- State of Louisiana has Privacy and Security Requirements
- In general, protection applies to Electronic and Paper information
- Most organizations have multiple data privacy and security related regulatory requirements

## Source of Privacy Notifications (Jan '06 – Dec '06)

---

Cause of Breach Notification	Approximate % of Incidents
Stolen/Missing Laptops	33%
Lost/Missing/Stolen Backup Tapes/Removable Media	15%
Data Exposed Via Hacking	18%
Inadvertently Exposed Data/Unaware of Procedures/Disposed off paper records	27%
Dishonest Employees	7%

**Source: Privacy Rights Clearinghouse**

# Enterprise Privacy Drivers



# How Companies Have Gotten Into Trouble

---

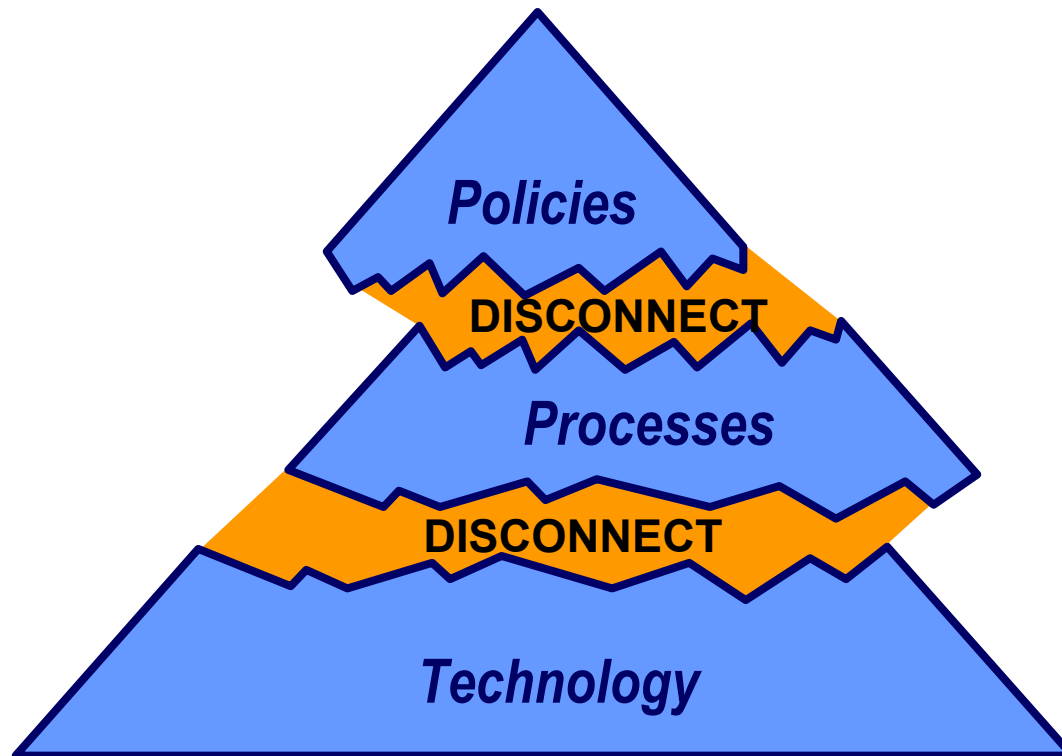
Examples of activities related to Privacy & Data Protection that **led to enforcement actions, law suits, or monetary fines:**

- **Nonexistent policies or differences between practice and policy**
- **Misrepresenting the purpose** for collecting PII
- **Failure to disclose the means used to collect PII** (i.e., the use and/or duration of cookies, web bugs, spyware, tracking technologies)
- **Failure to adequately train** personnel on privacy representations
- Disclosing, sharing, or **selling PII to third parties contrary to the organization's privacy policy**
- **Exporting PII contrary to the privacy laws** of the originating country
- **Misrepresenting the security protection** of PII

# Avoiding the Disconnect

---

A “disconnect” between corporate policies, actual operational practices and technology infrastructure reduces ability to implement changes into the business environment



# Privacy In The Enterprise

---

## Enterprise Resource Planning:

- Provision of access and correction rights
- Data integration could increase attributes which could increase sensitivity which could increase obligations for extra controls
- Data retention and destruction considerations

## Customer Relationship Management:

- Collection and use to align with primary purpose aligned with notice and consent if applicable
- Training and processes to support inquiries and complaints
- Social engineering vulnerabilities

## Mergers & Acquisitions:

- Privacy due-diligence for assessing privacy obligations and current state
- Reconciling different policies, notices and cross-border transfer mechanisms
- Use of the acquiring entity's data could be severely restricted diminishing the value of the asset

## System Development Life Cycle:

- Lack of privacy considerations could result in costly retrofits
- Considerations for notice, choice, access, security, retention and destruction

## Extended Enterprise Relationships:

- Privacy policies for handling third party data
- Vendor selection, due diligence, contracting and monitoring
- Unique considerations for consultants and contract workers

## Outsourcing & Offshoring:

- Reconciling different laws and policies
- Contracts may not be enforceable
- Potential brand impact
- May require notice and consent
- Encryption export considerations

# Common Privacy Challenges

---

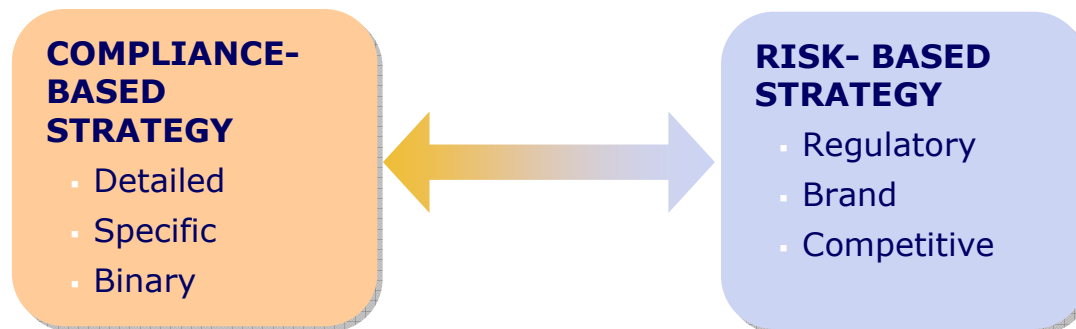
There are several common challenges faced by today's organizations when meeting privacy's demands:

- Creating a privacy strategy that accounts for a **complex, multi-regulatory**, and **changing** environment
- Managing **customer** and **employee concerns and perceptions** across **differing cultures** and multiple industries (e.g., diversified multinational firms)
- 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 it is disposed of
- Reconciling inconsistent practices among affiliates and regions
- Driving policy into business **practices** and **technology**
- **Adopting privacy values** throughout the enterprise
- Coordinating **incident response & investigations**

# Compliance vs. Risk-Based Approach

---

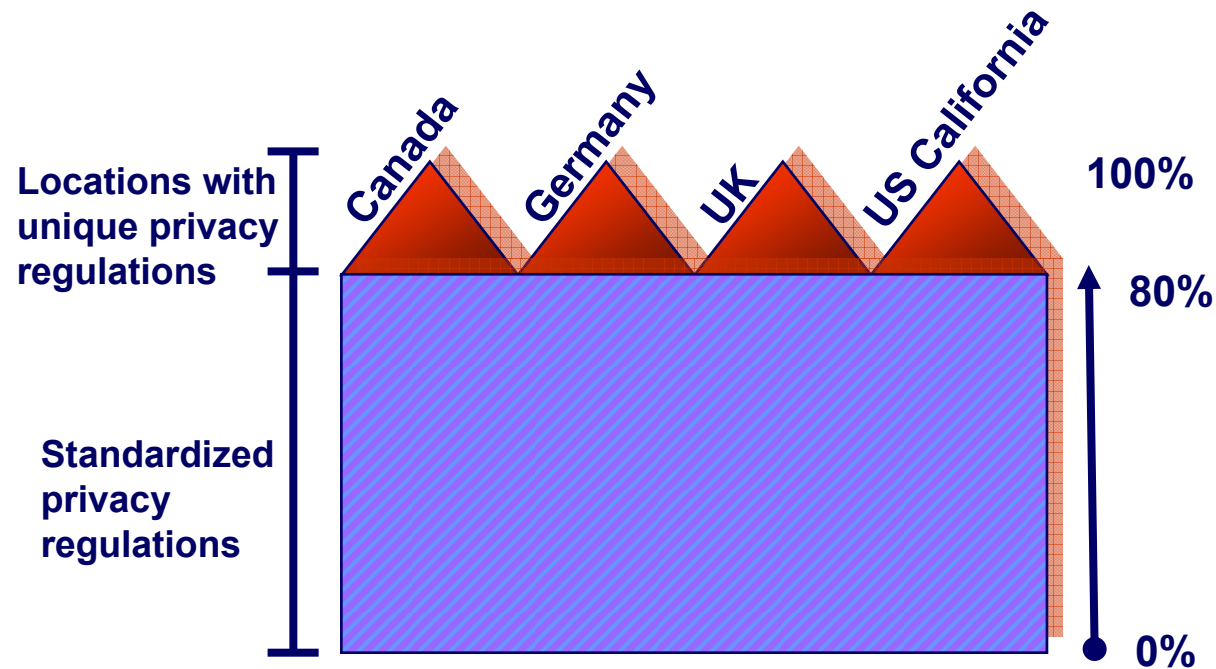
The approach to solving privacy-related issues ranges between adopting a compliance strategy to a risk-based strategy:



Advantages of the risk-based approach:

- Free the company from reactionary cycles
- Allocate scarce resources efficiently and according to level of threat
- Deliver value as quickly as possible

# Risk-Based and Rationalized Approach to Privacy



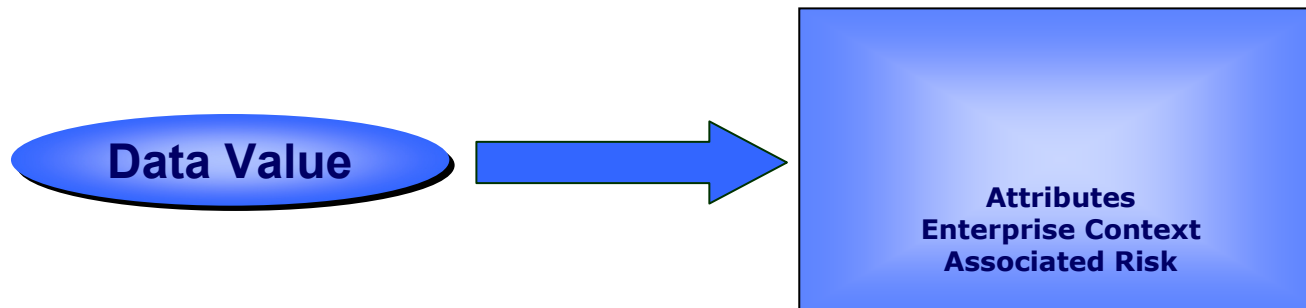
**Identify where the highest risks exist and tackle the major, common issues.**

**Deal with local unique privacy requirements on a case-by-case basis.**

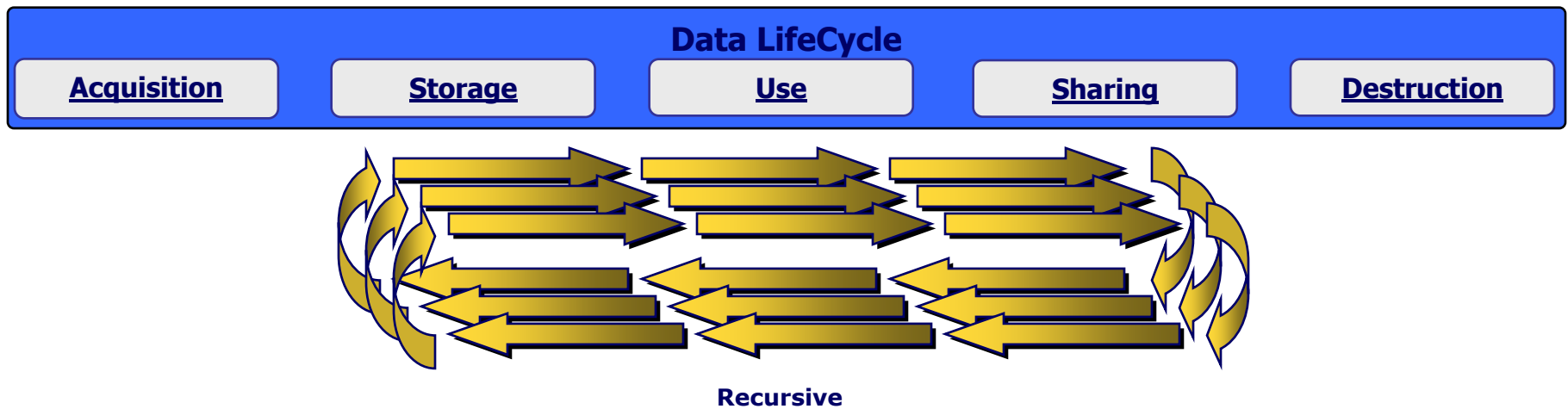
# Data as an Asset

---

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



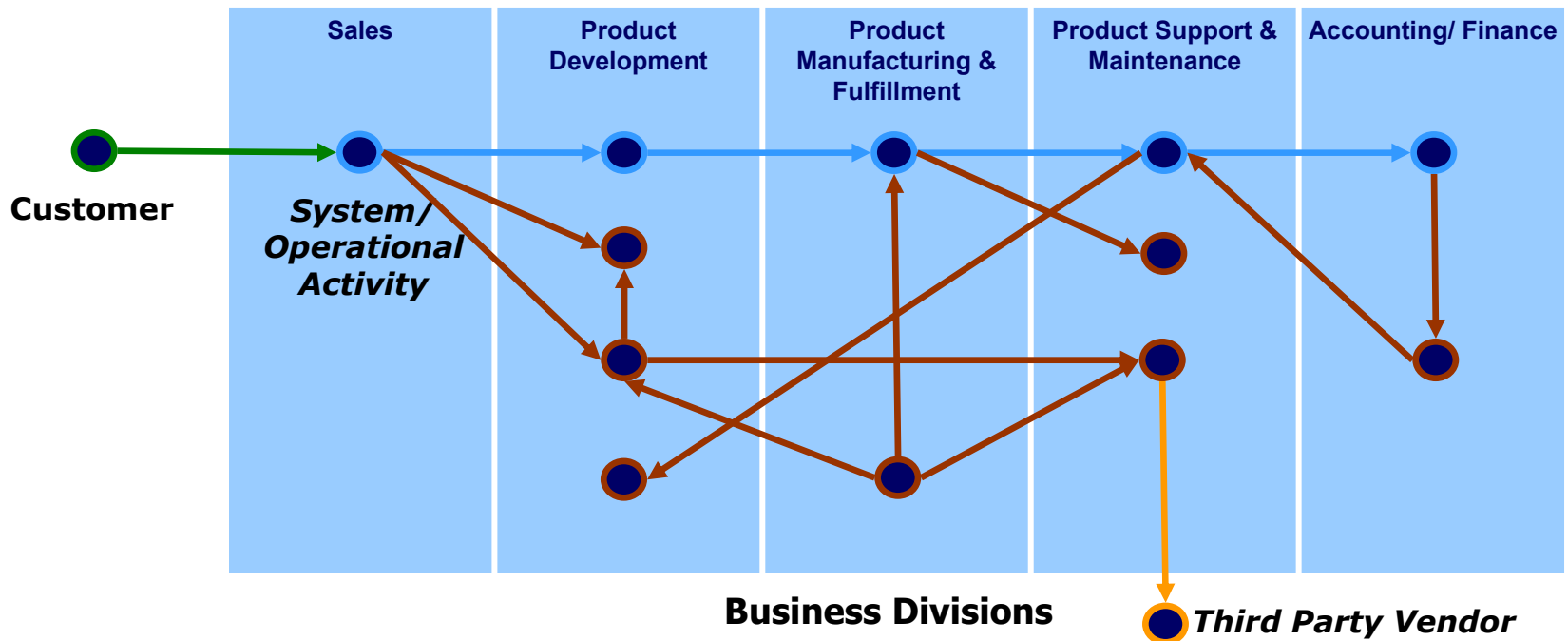
The nature of data changes over time, as it is stored, used and shared.



# Challenge - Understanding the Movement of Data

---

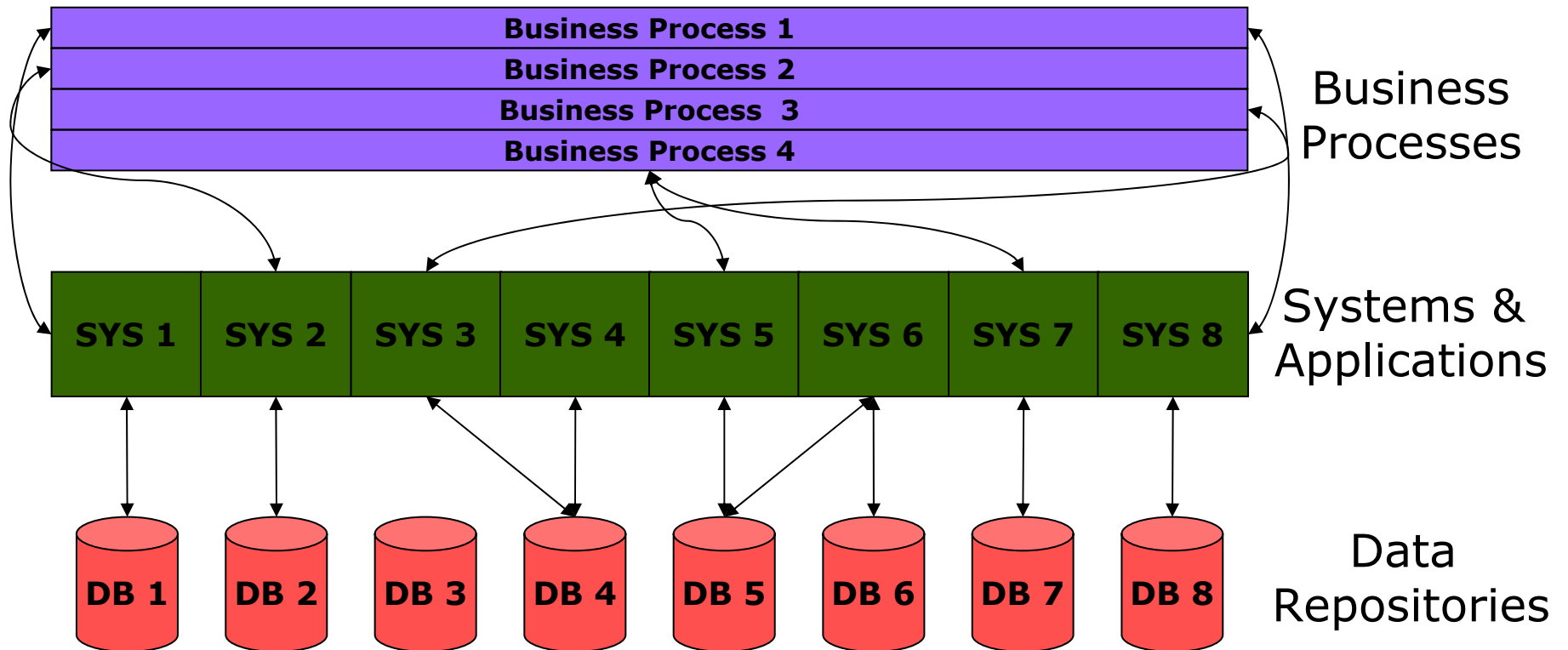
- Companies are organized by vertical business units
- Data (i.e., IP, customer information, financial) moves horizontally in an organization (e.g., order fulfillment process)
- Companies quite often do not have a good understanding of the proliferation and evolution of data within their organization



# Method of Data Analysis

---

Understanding how an organization processes data assets entails taking a risk-based view of its business processes, supporting systems and associated data repositories that contain data.

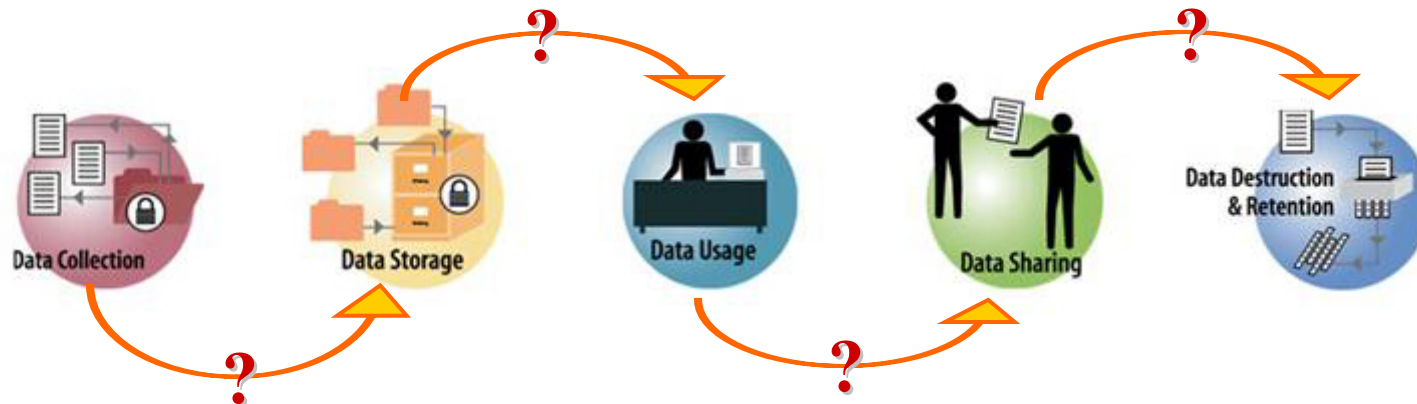


# Data Life Cycle Issues to Manage

---

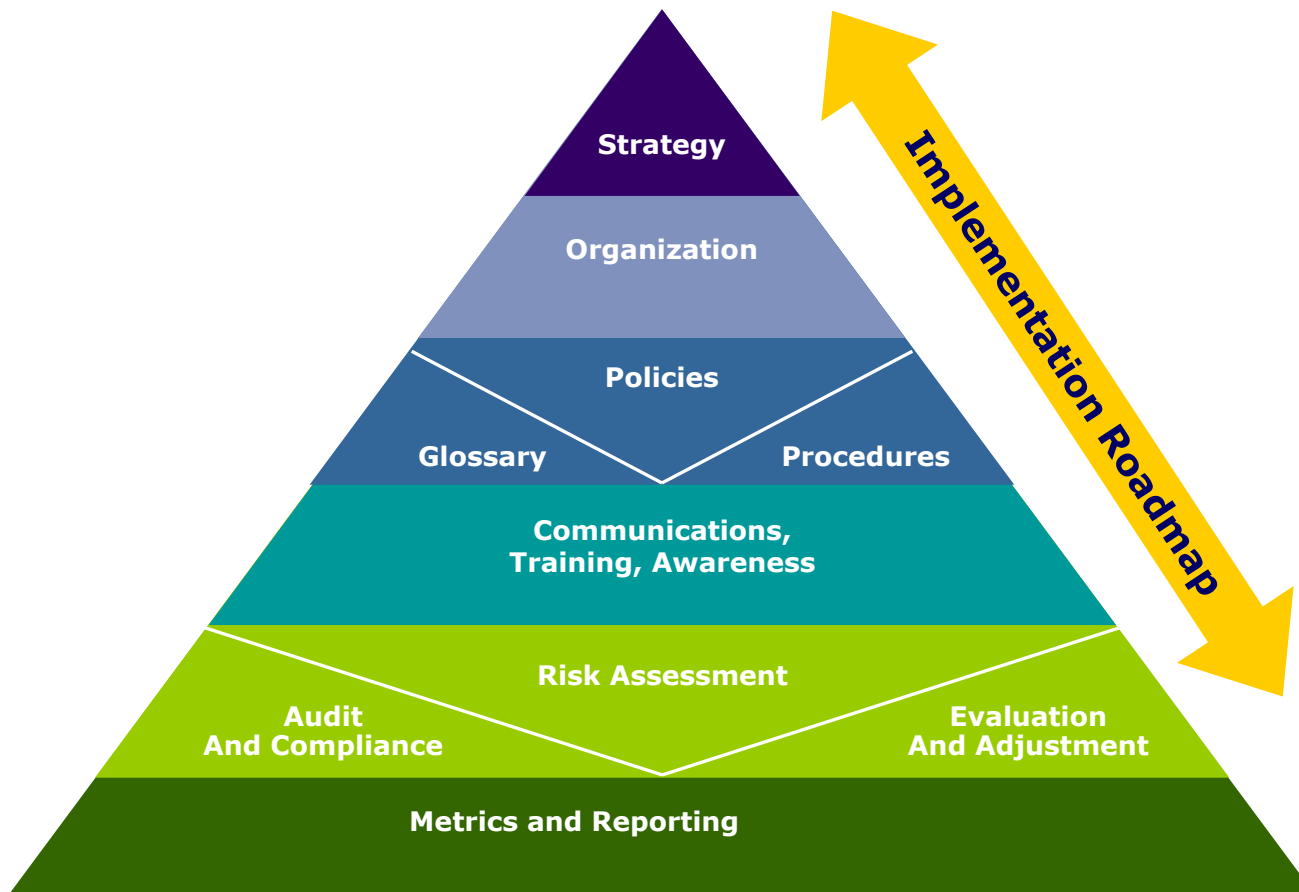
An adequate understanding of the movement of personal information must be gained:

- What data exists?
- How is it collected?
- How is it protected?
- Where is it stored?
- How is the data used?
- Who do you share it with?
- How is it destroyed?



# A Holistic Enterprise Privacy Program

---



# Interfaces for a Privacy Program

---

The privacy program should be closely integrated with other data management initiatives within the enterprise



---

# Deloitte.