



# Mexico's Personal Data Protection Law



**WTMA – Monthly Meeting August 17, 2011**

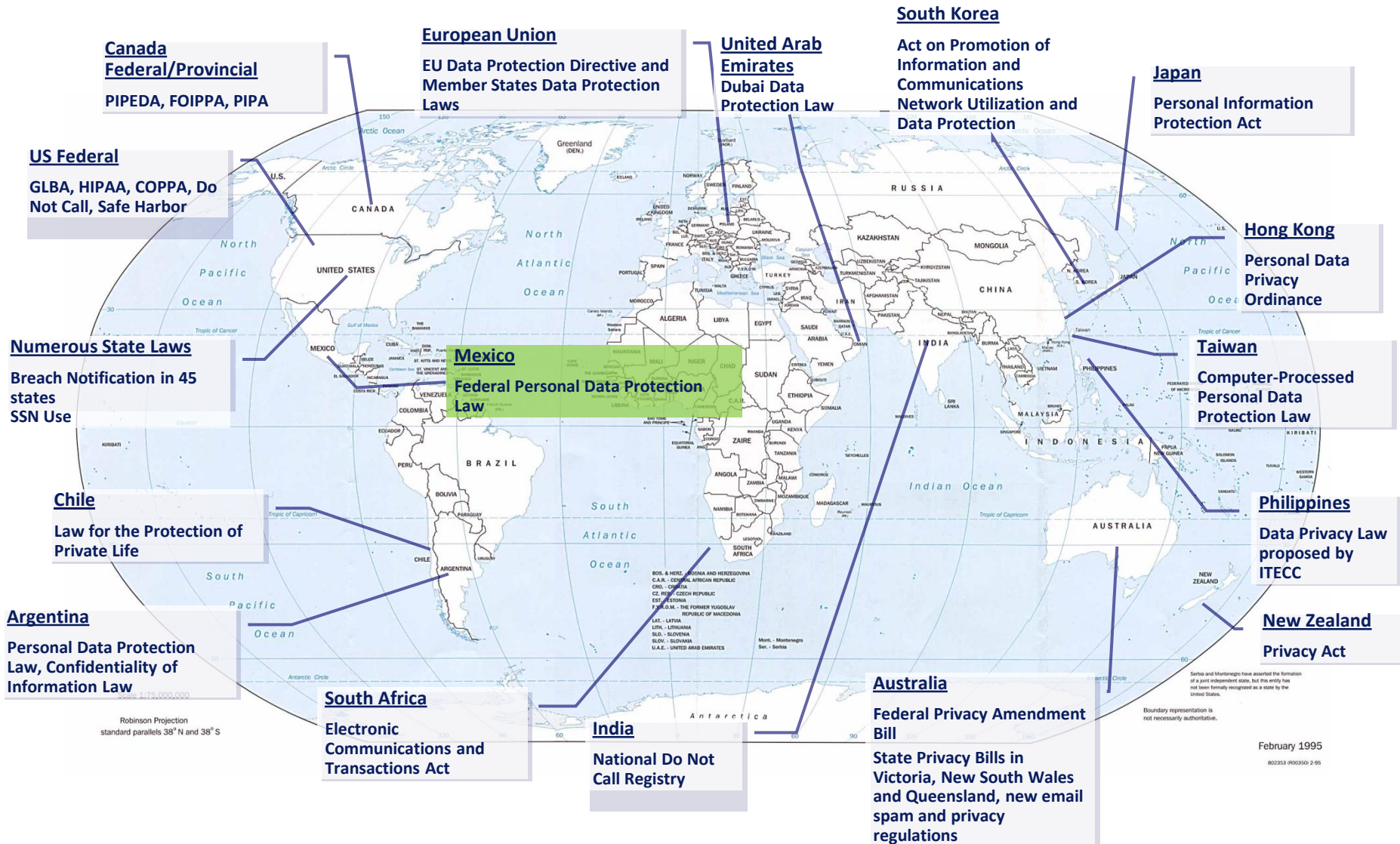
Ivan Curiel, Attorney At Law, Deloitte Tijuana

Antonio Silva, Consulting Director, Deloitte Tijuana



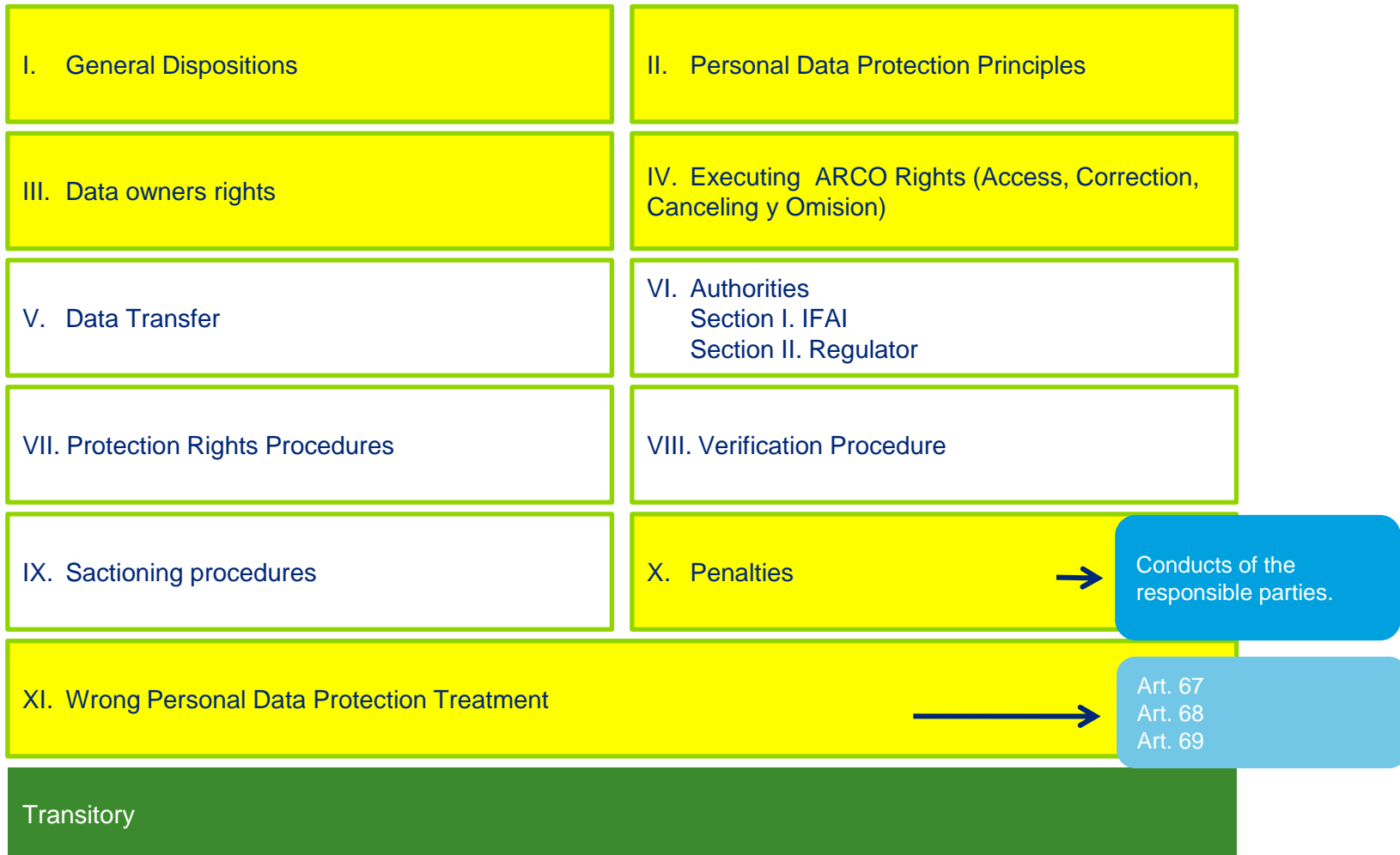
# Personal Data Protection Law 101

# Proliferation of Privacy and Data Protection Laws, Regulations & Standards



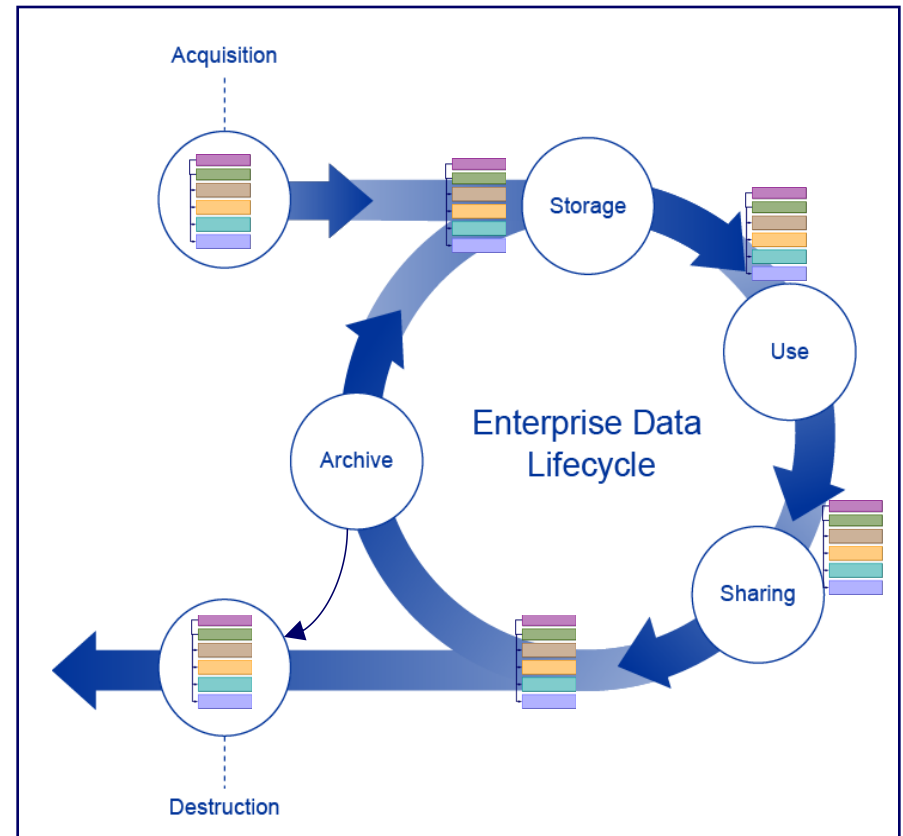
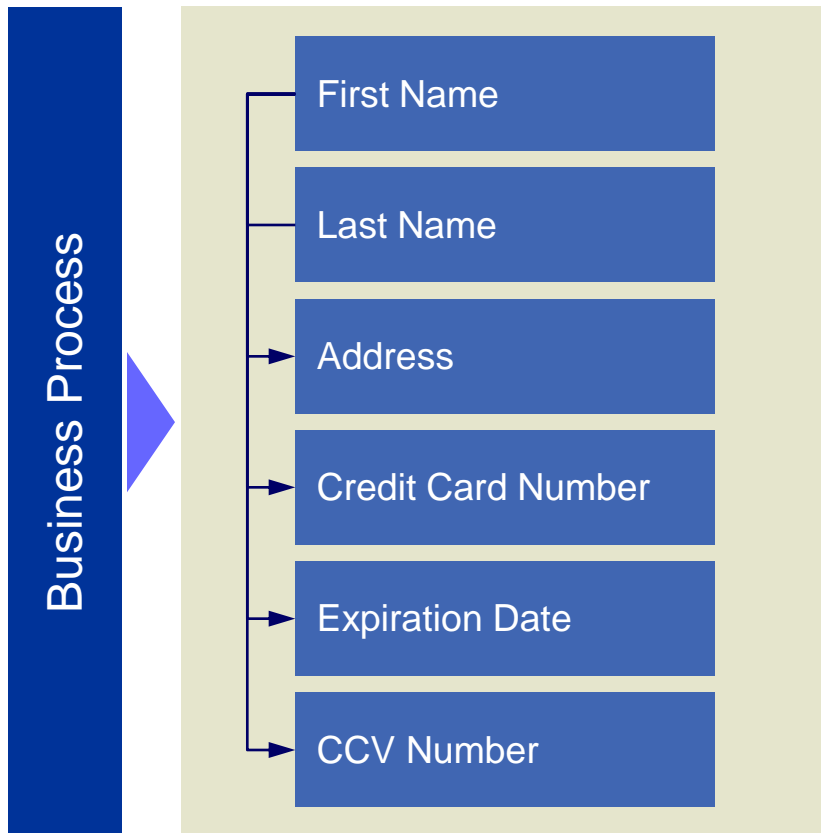
# Structure

## Structure of the LFPDPPP



# Understanding data as an asset

- The business **value** of data is determined by its **attributes**, **context** within the enterprise, and associated **risk**.
- The intrinsic and contextual value of data and its associated risk vary throughout the data lifecycle



# Data in a Global Organization

---

## **Customer Information**

- Government identifiers (e.g., social security numbers)
- Account numbers (e.g., bank accounts, credit card information)
- Customer personal information (e.g., home address, email address, personal phone number)

## **Employee Information**

- Government identifiers (e.g., social security numbers), travel and immigration documents (e.g., visa information, passports, naturalization documents such as permanent resident card), state issued documents of record (state identification, driver's license, birth certificate)
- Account numbers (e.g., bank accounts)
- Employee personal information (e.g., home address, personal phone number)
- HR information (e.g., personal health information, performance management)

## **Third Party Information**

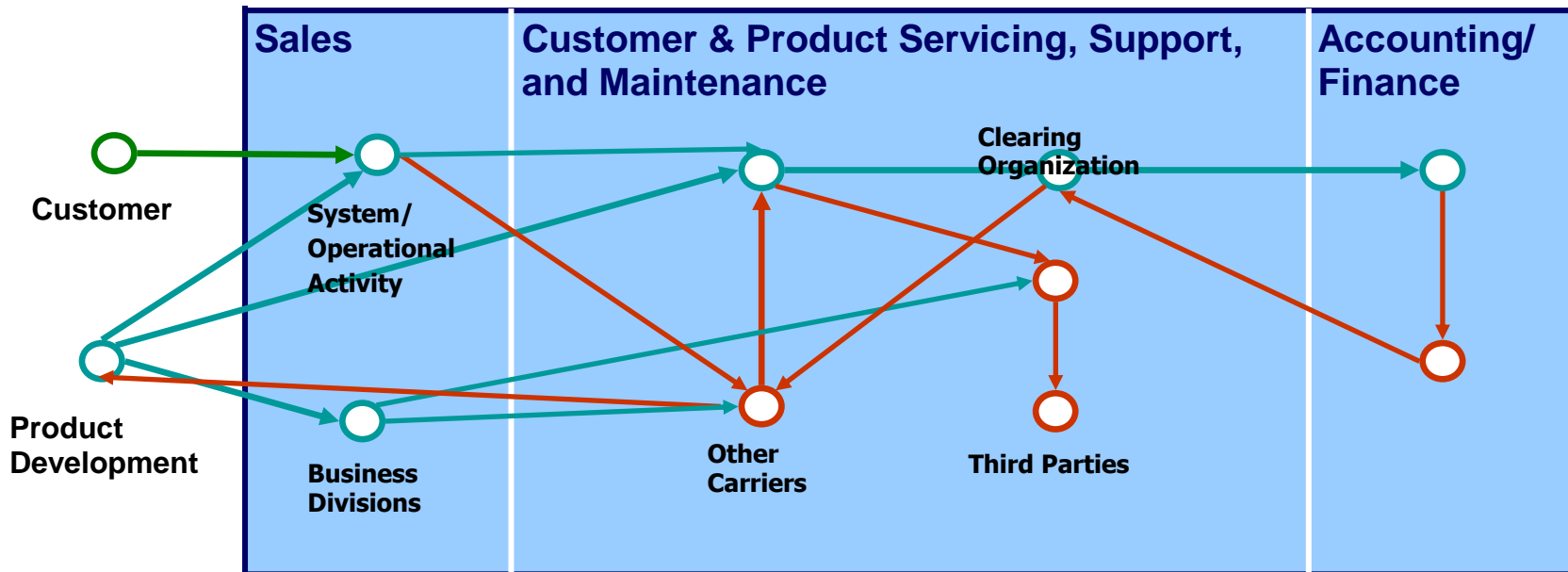
- Business contact information

## **Proprietary and Confidential Information**

- Intellectual capital (e.g., know-how)
- Non-public financial information

# Data movement challenge

- Organizations are made up of vertical business units
- Data (i.e., employee information, customer information, IP) moves horizontally in an organization (e.g., HR, sales and servicing)
- Organizations often do not have a good understanding of the locations, movement, proliferation, and evolution of their data



# Commonalities – Fair information practices

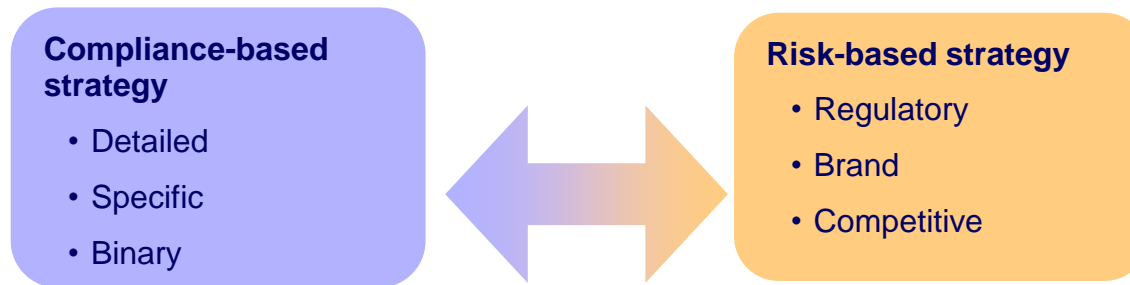
---

- The **Organization for Economic Cooperation and Development (OECD)** established Guidelines on the Protection of Privacy and Trans-border Flows of Personal Data in 1980.
- The guidelines consist of 8 fundamental principles:
  1. Information collection limitation
  2. Data quality
  3. Purpose Specification/Notice
  4. Use limitation
  5. Security
  6. Openness
  7. Individual Participation/Access
  8. Accountability

# A compliance vs. risk-based approach

---

Approaches to solving privacy-related issues tend to fall between the poles of a compliance-based strategy and a risk-based strategy:

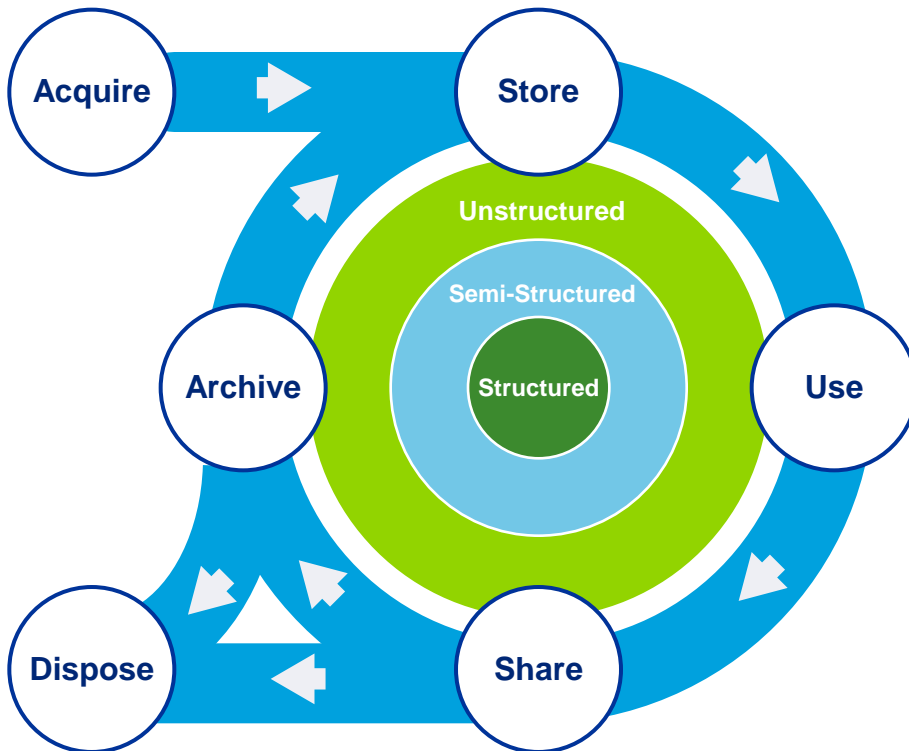


## Advantages of the risk-based approach:

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

# Data lifecycle

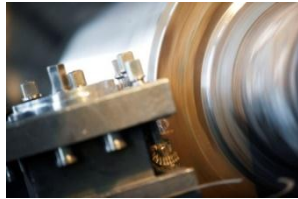
Data Management addresses how an organization manages its data. It is a comprehensive set of capabilities that properly manages the data lifecycle requirements of an enterprise — via the development and execution of **policies**, **procedures**, **architectures**, and use of **technologies**.



“...a data-centric security approach... extends well beyond encryption, covering classification, access controls, use monitoring, retention, and destruction.”

*“Market Overview: IT Security In 2009,” Forrester Research, Inc., April, 2009*

# Data needs to be managed across an organization



**Human resources**

**Manufacturing**

**Sales**

**Corporate**

**Legal**



**Customer data**

- Credit card data
- Personally identifiable data
- Buyer patterns

**Operational data**

- Manufacturing data
- QA data

**Economic**

- Economic forecasts
- Demand forecasts
- Geopolitical trends

**Patents and trade secrets**

- Product feature and design

**Employee data**

- Personally identifiable data
- Compensation

**Product line**

- Upcoming products

**Financial data**

- Budgets
- Financial reports

**Research and development**

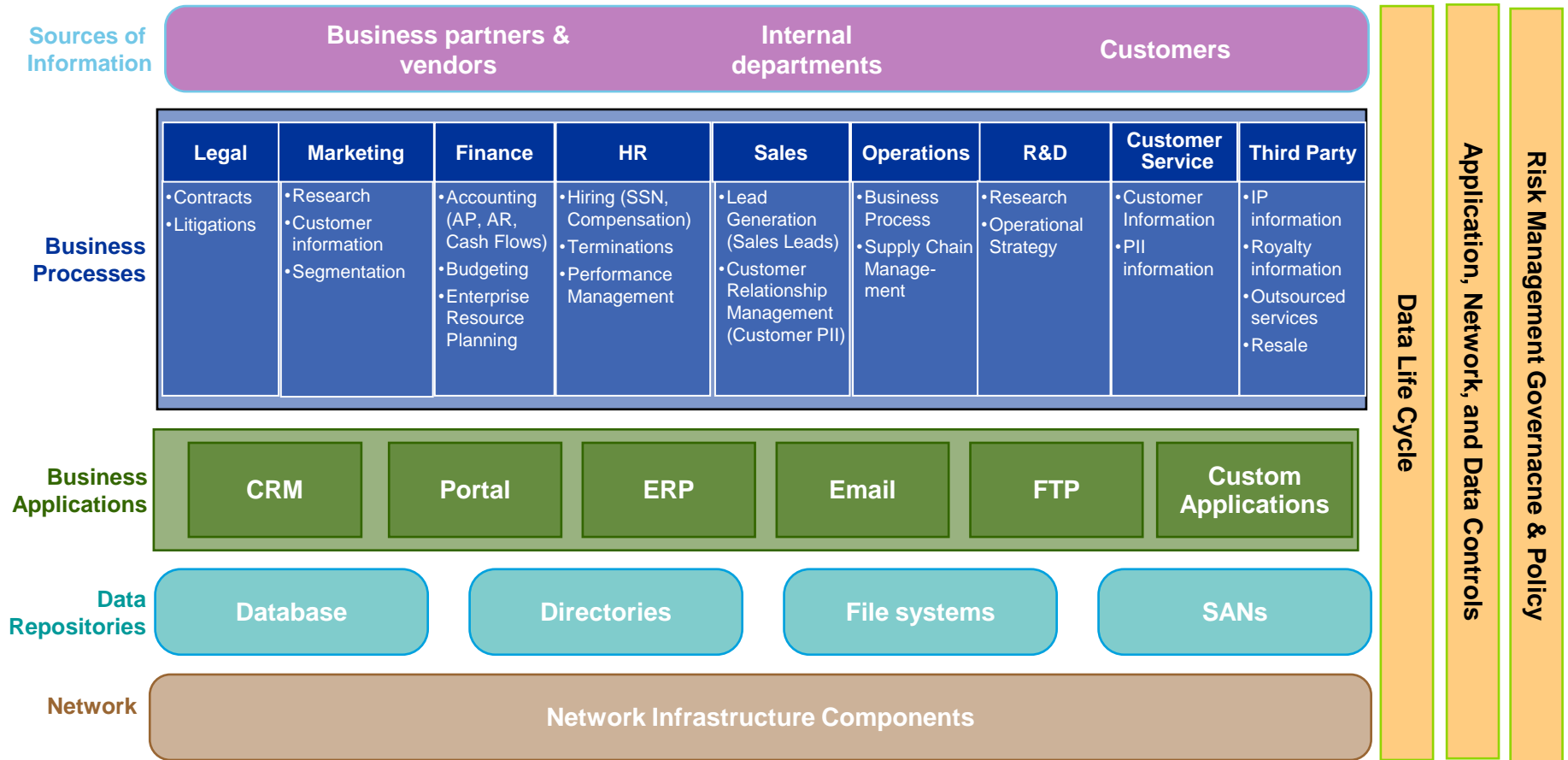
- Internal research and results

**Product line**

- Competitive intelligence
- Consumer preference

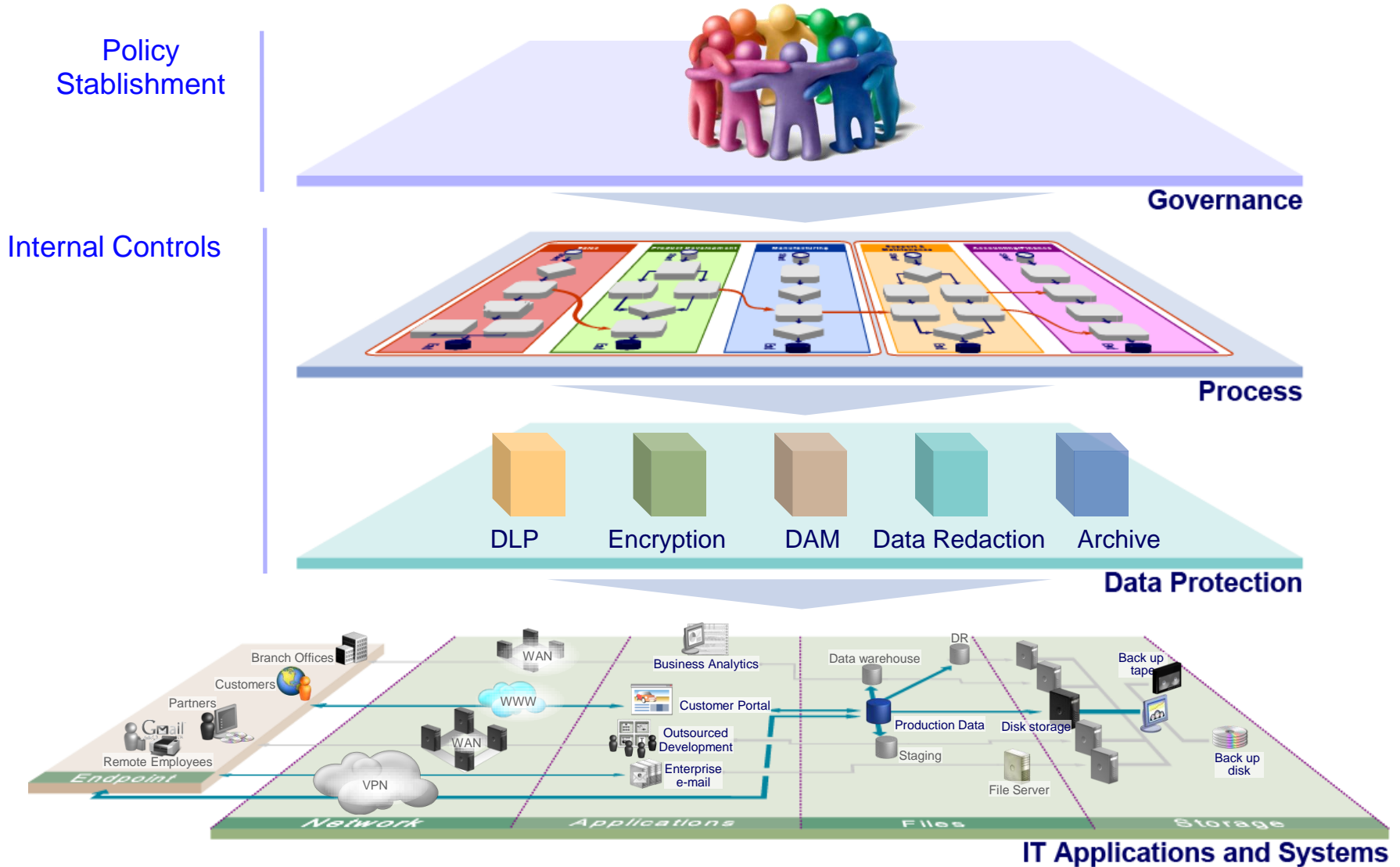
# Sensible data within an organization

Several data sources are used by business processes and application feed in diverse data bases



Today's organizations are virtual, global and dynamic

# Architecture



# Security's Relationship to Privacy

---

"You can have security without privacy, but you cannot have effective privacy without security."

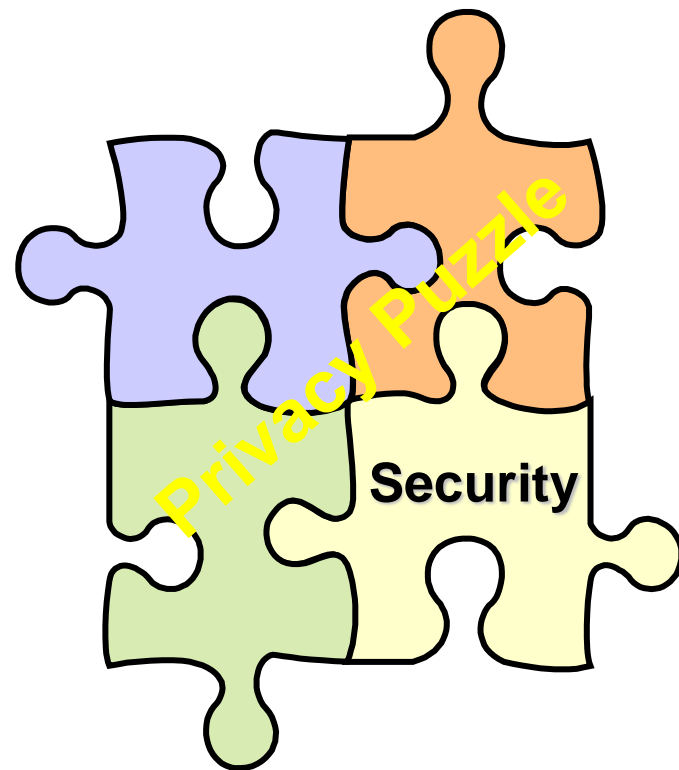
**Two primary components** of all privacy laws regulating PII include:

- **Usage** (the appropriate use of PII)
- **Security** or safeguarding (the protection of PII from loss and unauthorized access)

**Security** is about ensuring the **confidentiality, integrity, and availability of data** (including the systems, networks and filing cabinets that hold the data)

- **Confidentiality:** Access to data is limited to authorized parties
- **Integrity:** Assurance that the data is authentic and complete; changes to the data are restricted to authorized users
- **Availability:** Data should be accessible, as needed, by those who are authorized to access it

**Privacy laws are the primary drivers of security requirements and standards relating to the protection of PII**



# A Holistic Enterprise Privacy Program

---

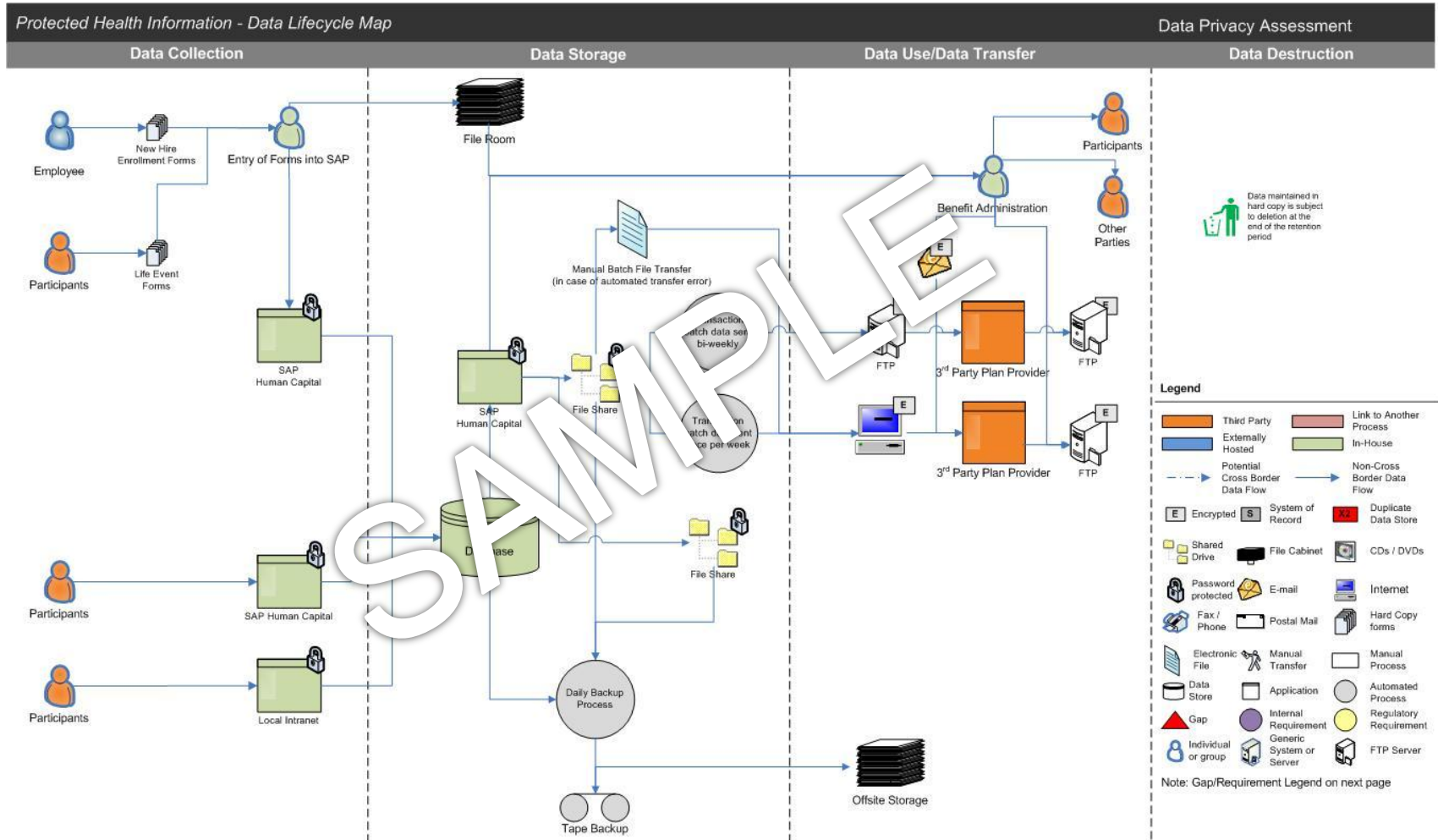


## Challenges

- Meeting client/employee concerns and perceptions
- Planning for a multi-regulatory environment
- Understanding global data flows
- Validating maps of personally identifiable information (PII)
- Managing the data lifecycle
- Defining metrics and effective reporting
- Creating compliant systems
- Value adoption throughout the enterprise

# Current State Assessment

To properly assess business processes for control and safeguard effectiveness at a manageable level, it is recommended to create detailed business process maps





# Privacy and Data Protection Trends

# Privacy and Data Protection Trends

---

- **Increased enforcement**
  - Enforcement activity drivers
  - Expansion of agencies and bodies that can enforce privacy legislation (e.g., HHS, FTC, AGs)
- **Increased liability**
  - Large fines (7 figures), consent decrees (20 year), criminal liability, class action lawsuits
- **Expanding requirements around breach notification**
  - Expansion of types of data elements that trigger breach requirements
  - Types of notification (e.g., data subject, regulatory agency, media)
  - Increased definition around notification obligations (e.g., number of records breached, time frames during which notification must be provided)
- **Increasing expectations around demonstrating privacy and security controls**
  - Formal security program, policies and procedures, training
  - Documented identity and access controls
  - Data protection tools (e.g., encryption, data leakage tools)
- **Increased number of privacy and data protection regulations**
- **Increased awareness of individuals who understand the value of obtaining inappropriate access to personal information**

# For further discussion please contact...

## Ivan Curiel

Attorney at Law

Deloitte Tijuana

+51 664 622 7878

[icuriel@deloittemx.com](mailto:icuriel@deloittemx.com)

## Antonio Silva

Director

Deloitte Tijuana

+52 664 622 7906

[antonsilva@deloittemx.com](mailto:antonsilva@deloittemx.com)

---

# Deloitte.

This presentation contains general information only and Deloitte is not, by means of this presentation, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This presentation is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor.

In addition, this article contains the results of a survey conducted by Deloitte. The information obtained during the survey was taken “as is” and was not validated or confirmed by Deloitte.

Deloitte, its affiliates, and related entities shall not be responsible for any loss sustained by any person who relies on this presentation.