Deloitte.

ISACA San Francisco Chapter

The 2007 Privacy Panel

Rena Mears, CISSP, CIPP, CPA, CISA
Partner, Deloitte & Touche LLP

March 23, 2007
San Francisco

What is Privacy and Why Now?

- **Definition of PII**
  - The definition is in the eye of the beholder (US, EU, APEC)
- **EU vs. US vs. everyone else**
  - Human right
  - Identity theft
  - Do no harm
- **Market drivers**
  - Globalization
  - Changing competitive landscape
  - Extended enterprise
  - Centralized architecture

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

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

Enterprise privacy and data protection risks

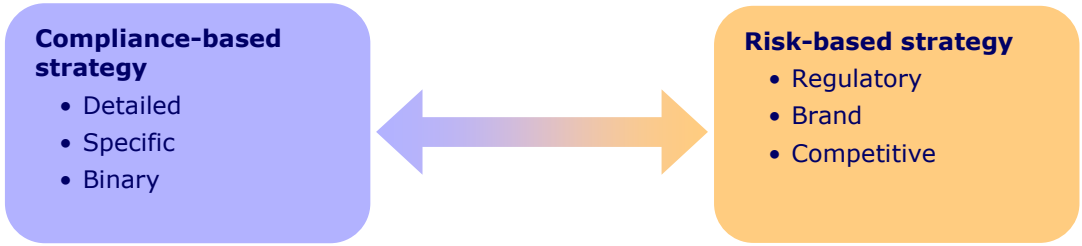
- **Regulatory**
  - International – EU
  - Industry – AICPA Taskforce
  - Breach notification – SB1386
    - 34 current state laws
- **Marketplace**
  - Brand
  - Competitive
- **Operational**
  - Third-party risk
  - Contractual
- **Financial**
  - Fines
  - Lawsuits/legal defense
  - Credit reporting costs
  - Stock price
  - Brand marketing

Managing and Mitigating the Risk

- **Risk-based approach**
  - Business process risk assessment
  - Rationalized requirements
- **Holistic program – Value Adoption**
  - Strategy
  - Policies, procedures, and guidelines
  - Data management and protection solutions
  - Training and awareness
  - Metrics, monitoring and reporting
- **Effective incident response**
- **Third party risk management**
  - Vendors and contractors
  - Outsourcing
  - Offshoring

Compliance vs. risk-based approach

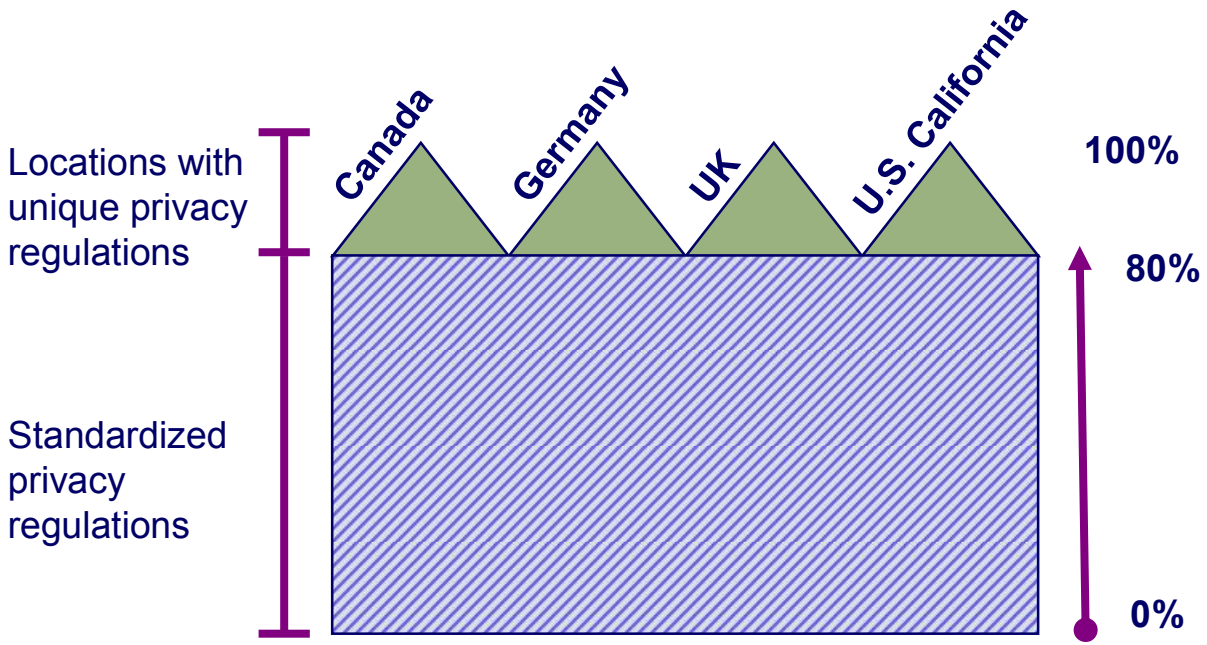
The approach to solving privacy-related issues ranges between adopting a compliance strategy to a risk-based strategy:



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

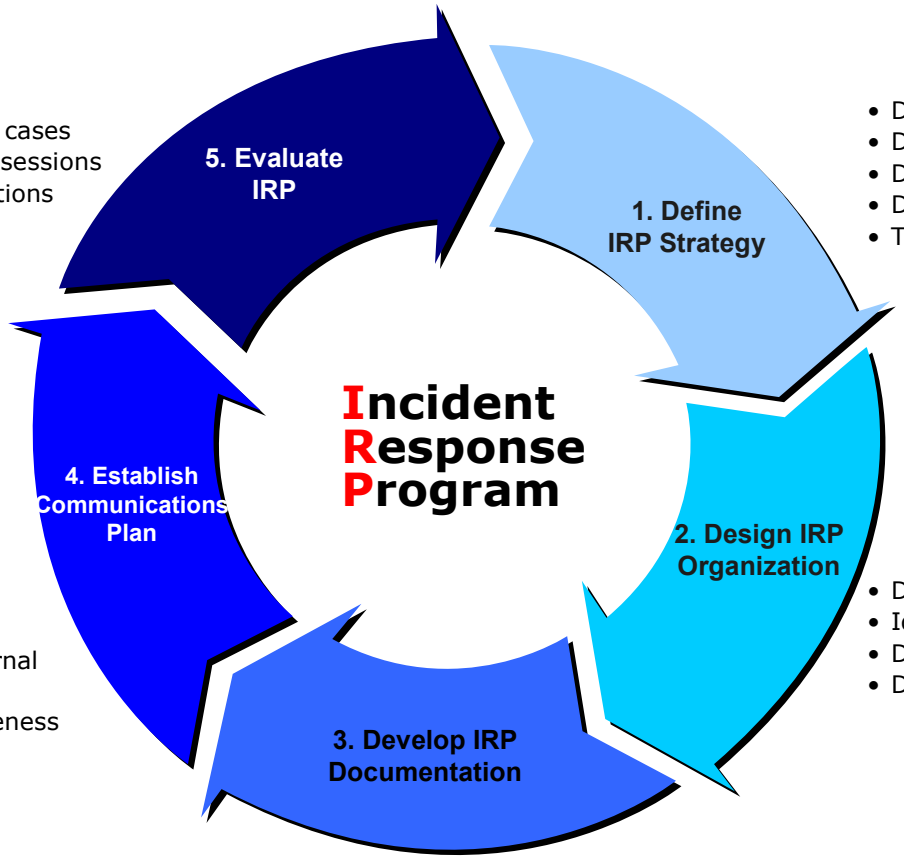
Risk-based and rationalized approach to privacy



- Identify where the highest risks exist and tackle the major, common issues
- Deal with local unique privacy requirements on a case-by-case basis

Holistic Program

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

Third Party Risk Management

Taking a risk-based approach to determine third party assessment approach and type assists to focus resources on business processes and third party relationships that pose the most potential risk to an organization

Lowest

Highest

Self Assessment

- Questionnaires, interviews
- Least cost
- Deal with low risk situations
- Staff availability can be an issue

Internal Audit

- Independent from group being audited but employed by company
- Operate under defined standards
- Reports can be very comprehensive
- Can be used for all risks levels depending on company tolerance
- No independent audit opinion for external use needed

Independent Assessment

- By qualified third party “auditor” or assessor
  - Performance of assessment
  - Performance of audit/examination
- The latter should be considered for significant risk areas
- More cost as move to audit

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 140 countries. With access to the deep intellectual capital of approximately 135,000 people worldwide, Deloitte delivers services in four professional areas, audit, tax, consulting and financial advisory services, and serves more than 80 percent 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 and Touche", "Deloitte Touche Tohmatsu" or other related names.

In the United States, Deloitte and Touche USA LLP is the U.S. member firm of Deloitte Touche Tohmatsu and services are provided by the subsidiaries of Deloitte and Touche USA LLP (Deloitte and Touche LLP, Deloitte Consulting LLP, Deloitte Financial Advisory Services LLP, Deloitte Tax LLP, and their subsidiaries), and not by Deloitte and 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 40,000 people in more than 90 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

Member of
Deloitte Touche Tohmatsu