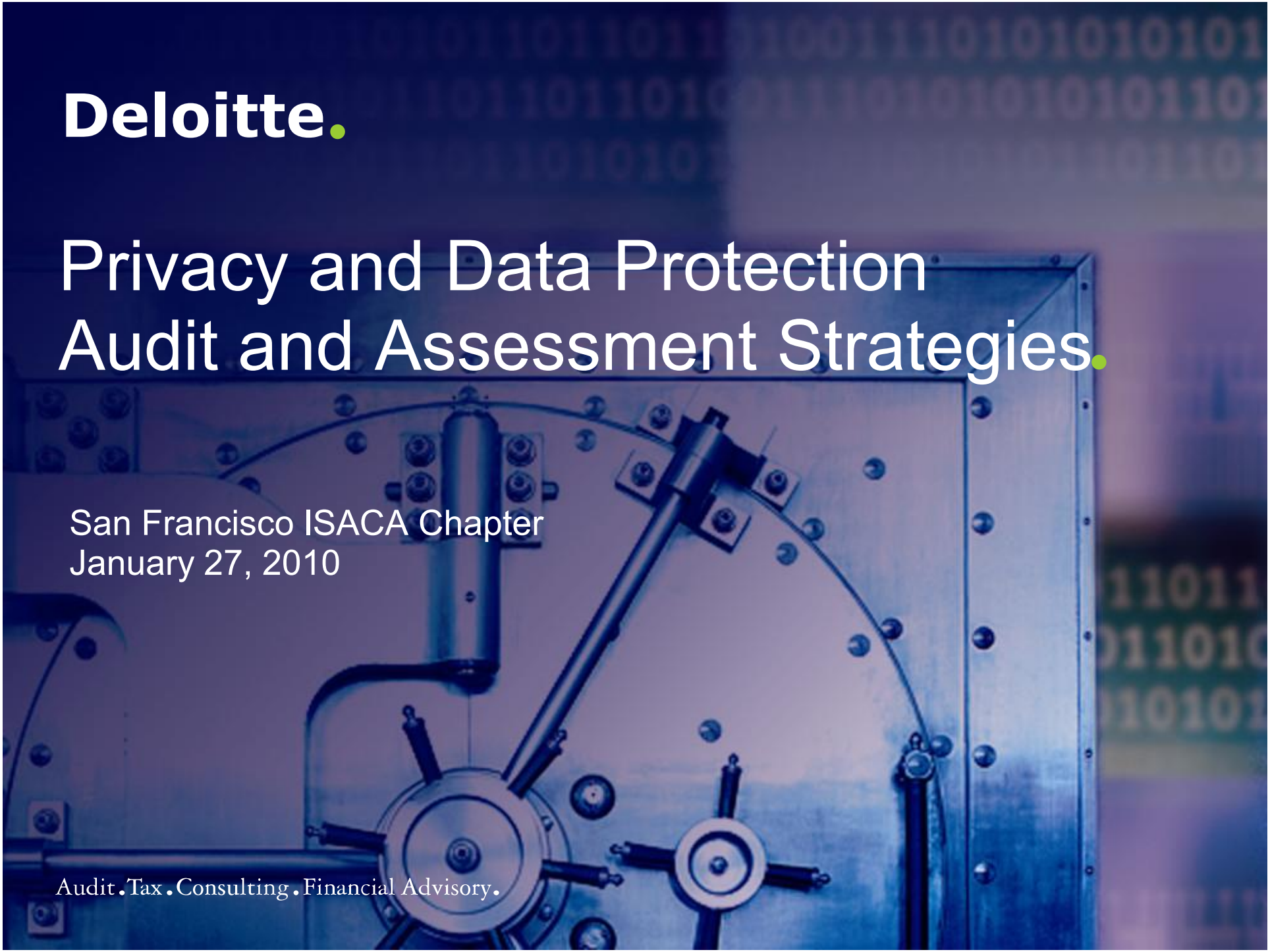


Deloitte.

Privacy and Data Protection Audit and Assessment Strategies.

San Francisco ISACA Chapter
January 27, 2010

Audit.Tax.Consulting.Financial Advisory.

Agenda

Introductions (Name, Organization, Role)

Topics and Drivers

General Types of Reviews

Understanding the Issues

Case Studies

Topics

What are the key drivers?

What are some of the emerging threats?

What are the different types of assessments and attestations?

Why might you use one type over another?

What does it typically take to perform these reviews?

What should you be addressing/thinking about?

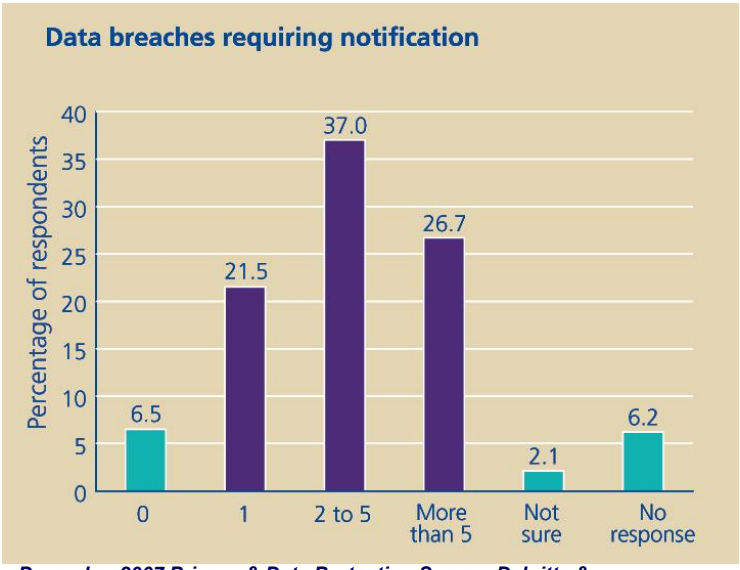
Breach Continues to be a Key Driver

- **In 2007, survey results showed more than 85% of organizations had at least one external data breach requiring notification**
- **Most respondents (66%) experienced between six and 20 internal incidents involving PII violations during the past 12 months**

December 2007 Privacy & Data Protection Survey, Deloitte & Ponemon Institute

- **In 2009, results from another survey showed 84% of companies experience more than one breach per year**
- **56% of breaches appear to be inside events**
- **Costs for responding to a breach grew to $202 / record**

Fourth Annual Report by The Ponemon Institute© & PGP Corporation, February 2009



December 2007 Privacy & Data Protection Survey, Deloitte & Ponemon Institute

Fourth Annual Report by The Ponemon Institute© & PGP Corporation, February 2009

Emerging Threats – Cyber Crime

The nature and sophistication of threats to information assets is evolving and traditional approaches to cyber security are not keeping pace

- Cyber criminals are targeting organizations and individuals with malware and anonymization techniques that can evade current security controls (e.g., using encryption technologies)
- Current perimeter-intrusion detection, signature-based malware, and anti-virus solutions are providing little defense and becoming obsolete
- Organizations tend to employ security-based, “wall-and—fortress” approaches to address the threat of cyber crime, but this is not enough to mitigate the risk

Organizations should understand how they are viewed by cyber criminals in terms of attack vectors, systems of interest, and process vulnerabilities so they can better protect themselves from attack

How to Help Mitigate the Risks: General Types of Reviews

Types of Assessments and Attestations

- Self- assessment (privacy office, information security, internal audit, compliance, business function)
  - Internal standard or requirements
  - External standards or requirements
    - Regulatory
    - PCI
    - GAPP
- Consulting based third-party assessment (Advisory)
  - Not an opinion (under standards by professional bodies like the AICPA)
  - Typically for the use only of the entity being assessed
- Attestations/Audits
  - Agreed-Upon Procedures
    - Limited audience
    - Not an opinion (the results of testing)
  - Audit
    - General audience
    - Auditable standards/requirements

AICPA Guidance

- ## Privacy Advisory Engagements

"Practitioners can provide a variety of advisory services to their clients, which include strategic, diagnostic, implementation, and sustaining/managing services using the Generally Accepted Privacy Principles criteria. These services could include, for example, advising clients on system weaknesses, assessing risk, and recommending a course of action using the Generally Accepted Privacy Principles criteria as a benchmark. "

- ## Agreed-Upon Procedures Engagements

"In an agreed-upon/specified procedures engagement, the practitioner performs specified procedures, agreed to by the parties, and reports his or her findings. The practitioner does not perform an audit or review of an assertion or subject matter or express an opinion or negative assurance about the assertion or subject matter. In this type of engagement, the practitioner's report is in the form of a description of procedures and findings. Generally Accepted Privacy Principles may be used in such engagements. This type of work would not lead to an assurance report, but rather to a report presenting the agreed-upon/specified procedures and the corresponding findings. Agreed-upon/specified procedures could be undertaken relative to a subset of an entity's system with reference to a subset of the Generally Accepted Privacy Principles.

Because users' needs may vary widely, the nature, timing, and extent of the agreed-upon/specified procedures may vary as well. Consequently, the parties to the report (agreed to/specified users and the client) assume responsibility for the sufficiency of the procedures since they best understand their own needs. The use of such a report is restricted to the specified parties who agreed upon the procedures."

See aicpa.org

AICPA Guidance

- ## Privacy Examination/Audit Engagements

"Relevant U.S. standards for attestation engagements are contained in the Statements on Standards for Attestation Services. Relevant Canadian standards for assurance engagements are contained in Section 5025 of the CICA Handbook. Privacy attestation/assurance engagements are defined within the context of these standards.

In an examination/audit engagement, the practitioner provides a high, though not absolute, level of assurance on a subject matter or assertion. With that objective, the practitioner develops examination/audit procedures that, in the practitioner's professional judgment, reduce the risk that the practitioner will reach an inappropriate conclusion to a low level.

A privacy assurance report ordinarily covers all 10 principles. All of their relevant criteria need to be met during the period covered by the report to issue an unqualified report.

The scope of the engagement can cover (1) either all personal information or only certain identified types of personal information, such as customer information or employee information, and (2) all business segments and locations for the entire entity or only certain identified segments of the business (retail operations, but not manufacturing operations or only operations originating on the entity's Web site) or geographic locations (such as only Canadian operations).

The scope of the engagement should cover all of the activities in the "information cycle" for the relevant personal information. These should include collection, use, retention, disclosure and destruction, de-identification or anonymization. Defining a segment that does not include this entire cycle could be misleading to the user of the practitioner's report."

See aicpa.org

AICPA Guidance

- ## Relationship between Generally Accepted Privacy Principles and the Trust Services Principles and Criteria

"Generally Accepted Privacy Principles are part of the AICPA/CICA Trust Services Principles and Criteria - a set of professional assurance and advisory services based on a common framework (i.e., a core set of principles and criteria). The Trust Services Principles and Criteria were developed by volunteer task forces under the auspices of the American Institute of Certified Public Accountants (AICPA) and the Canadian Institute of Chartered Accountants (CICA). The AICPA and the CICA are referred to in this document as "the Institutes." The other Trust Services Principles and Criteria are:

- **Security - The system is protected against unauthorized access (both physical and logical).**
- **Availability - The system is available for operation and use as committed or agreed.**
- **Processing Integrity - System processing is complete, accurate, timely, and authorized.**
- **Confidentiality - Information designated as confidential is protected as committed or agreed.**

These are discussed more fully at http://www.webtrust.org. "

See also aicpa.org

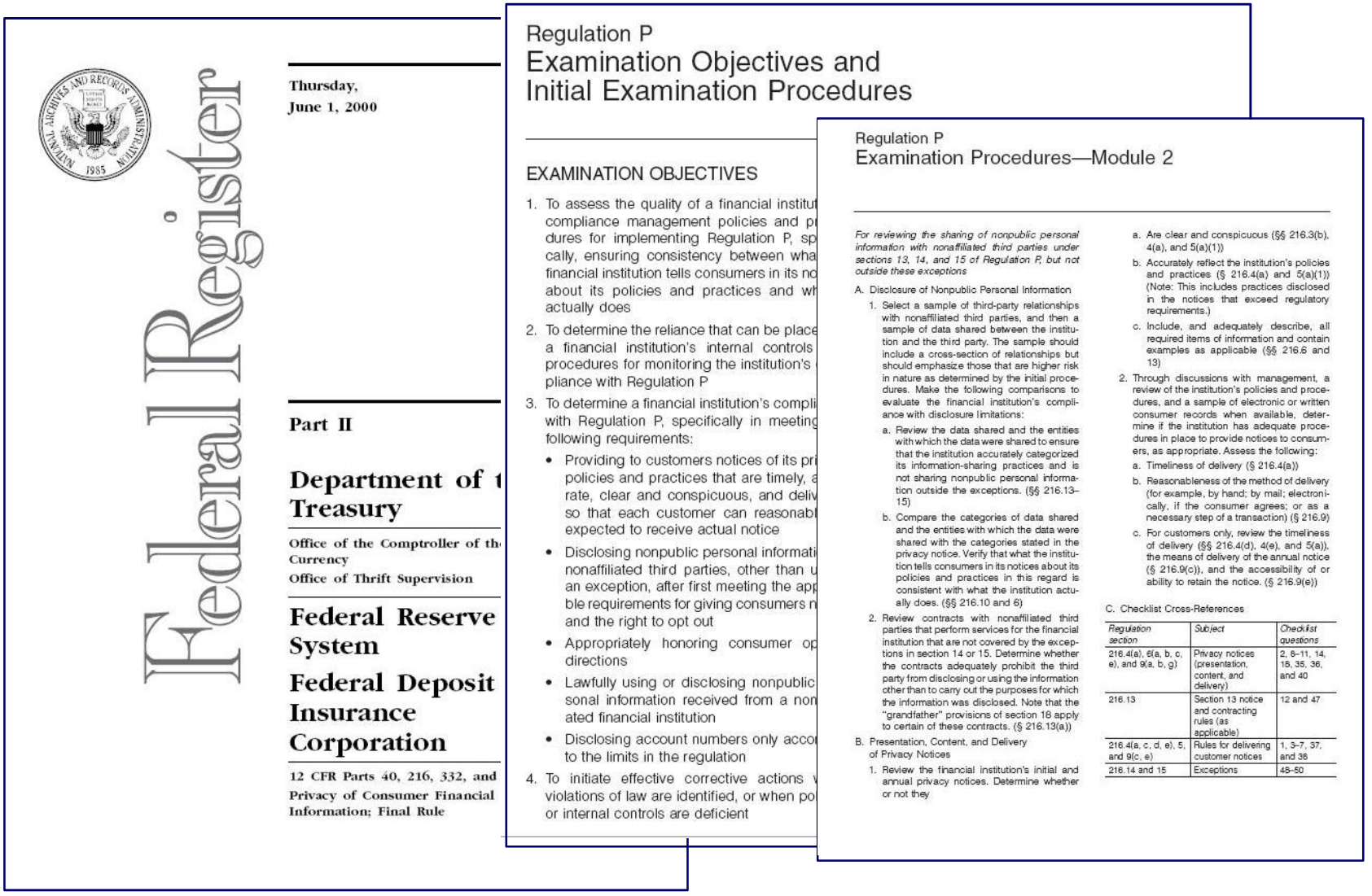
Generally Accepted Privacy Principles

- Part of the AICPA/CICA Trust Services Principles and Criteria
- A set of professional assurance and advisory services based on a common framework (i.e., a core set of principles and criteria).
- 10 privacy principles:
  - "Management: The entity defines, documents, communicates, and assigns accountability for its privacy policies and procedures."
  - "Notice: The entity provides notice about its privacy policies and procedures and identifies the purposes for which personal information is collected, used, retained, and disclosed."
  - "Choice and Consent: The entity describes the choices available to the individual and obtains implicit or explicit consent with respect to the collection, use, and disclosure of personal information."
  - "Collection: The entity collects personal information only for the purposes identified in the notice."
  - "Use and Retention: The entity limits the use of personal information to the purposes identified in the notice and for which the individual has provided implicit or explicit consent. The entity retains personal information for only as long as necessary to fulfill the stated purposes."
  - "Access: The entity provides individuals with access to their personal information for review and update."
  - "Disclosure**:** to Third Parties: The entity discloses personal information to third parties only for the purposes identified in the notice and with the implicit or explicit consent of the individual."
  - "Security: The entity protects personal information against unauthorized access (both physical and logical)."
  - "Quality: The entity maintains accurate, complete, and relevant personal information for the purposes identified in the notice."
  - "Monitoring and Enforcement: The entity monitors compliance with its privacy policies and procedures and has procedures to address privacy-related complaints and disputes."
- See: infotech.aicpa.org/Resources/Privacy/Generally+Accepted+Privacy+Principles

Example GAPP Principles

- Reference
- Management Criteria
- Illustrations and Explanations of Criteria
- Additional Considerations
- Need to tailor

Other Requirements



Federal Register

Thursday,
June 1, 2000

Part II

Department of t
Treasury

Office of the Comptroller of th
Currency
Office of Thrift Supervision

Federal Reserve
System

Federal Deposit
Insurance
Corporation

12 CFR Parts 40, 216, 332, and
Privacy of Consumer Financial
Information; Final Rule

Regulation P
Examination Objectives and
Initial Examination Procedures

EXAMINATION OBJECTIVES

1. To assess the quality of a financial institut
compliance management policies and p
dures for implementing Regulation P, sp
cally, ensuring consistency between wha
financial institution tells consumers in its nc
about its policies and practices and wh
actually does
2. To determine the reliance that can be place
a financial institution's internal controls
procedures for monitoring the institution's
pliance with Regulation P
3. To determine a financial institution's compli
with Regulation P, specifically in meetin
following requirements:
   - Providing to customers notices of its pri
policies and practices that are timely, a
rate, clear and conspicuous, and deliv
so that each customer can reasonabl
expected to receive actual notice
   - Disclosing nonpublic personal informati
nonaffiliated third parties, other than u
an exception, after first meeting the app
ble requirements for giving consumers n
and the right to opt out
   - Appropriately honoring consumer op
directions
   - Lawfully using or disclosing nonpublic
sonal information received from a non
ated financial institution
   - Disclosing account numbers only acco
to the limits in the regulation
4. To initiate effective corrective actions v
violations of law are identified, or when po
or internal controls are deficient

Regulation P
Examination Procedures—Module 2

For reviewing the sharing of nonpublic personal information with nonaffiliated third parties under sections 13, 14, and 15 of Regulation P, but not outside these exceptions

A. Disclosure of Nonpublic Personal Information
   1. Select a sample of third-party relationships with nonaffiliated third parties, and then a sample of data shared between the institution and the third party. The sample should include a cross-section of relationships but should emphasize those that are higher risk in nature as determined by the initial procedures. Make the following comparisons to evaluate the financial institution's compliance with disclosure limitations:
      a. Review the data shared and the entities with which the data were shared to ensure that the institution accurately categorized its information-sharing practices and is not sharing nonpublic personal information outside the exceptions. (§§ 216.13–15)
      b. Compare the categories of data shared and the entities with which the data were shared with the categories stated in the privacy notice. Verify that what the institution tells consumers in its notices about its policies and practices in this regard is consistent with what the institution actually does. (§§ 216.10 and 6)
   2. Review contracts with nonaffiliated third parties that perform services for the financial institution that are not covered by the exceptions in section 14 or 15. Determine whether the contracts adequately prohibit the third party from disclosing or using the information other than to carry out the purposes for which the information was disclosed. Note that the "grandfather" provisions of section 18 apply to certain of these contracts. (§ 216.13(a))

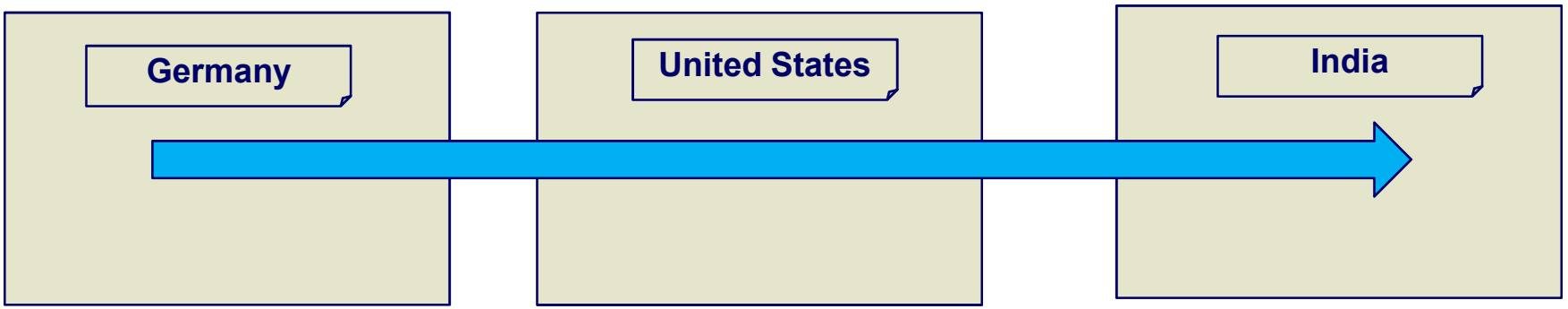
B. Presentation, Content, and Delivery of Privacy Notices
   1. Review the financial institution's initial and annual privacy notices. Determine whether or not they
      a. Are clear and conspicuous (§§ 216.3(b), 4(a), and 5(a)(1))
      b. Accurately reflect the institution's policies and practices (§ 216.4(a) and 5(a)(1)) (Note: This includes practices disclosed in the notices that exceed regulatory requirements.)
      c. Include, and adequately describe, all required items of information and contain examples as applicable (§§ 216.6 and 13)
   2. Through discussions with management, a review of the institution's policies and procedures, and a sample of electronic or written consumer records when available, determine if the institution has adequate procedures in place to provide notices to consumers, as appropriate. Assess the following:
      a. Timeliness of delivery (§ 216.4(a))
      b. Reasonableness of the method of delivery (for example, by hand; by mail; electronically, if the consumer agrees; or as a necessary step of a transaction) (§ 216.9)
      c. For customers only, review the timeliness of delivery (§§ 216.4(d), 4(e), and 5(a)), the means of delivery of the annual notice (§ 216.9(c)), and the accessibility of or ability to retain the notice. (§ 216.9(e))

C. Checklist Cross-References

Regulation section	*Subject*	*Checklist questions*
216.4(a), 6(a, b, c, e), and 9(a, b, g)	Privacy notices (presentation, content, and delivery)	2, 8–11, 14, 15, 35, 36, and 40
216.13	Section 13 notice and contracting rules (as applicable)	12 and 47
216.4(a, c, d, e), 5, and 9(c, e)	Rules for delivering customer notices	1, 3–7, 37, and 38
216.14 and 15	Exceptions	48–50

Other Requirements

- Examples of legal transfer mechanisms (EAA to US)
  - Consent
  - Safe Harbor
  - Model Contracts
  - Binding Corporate Rules

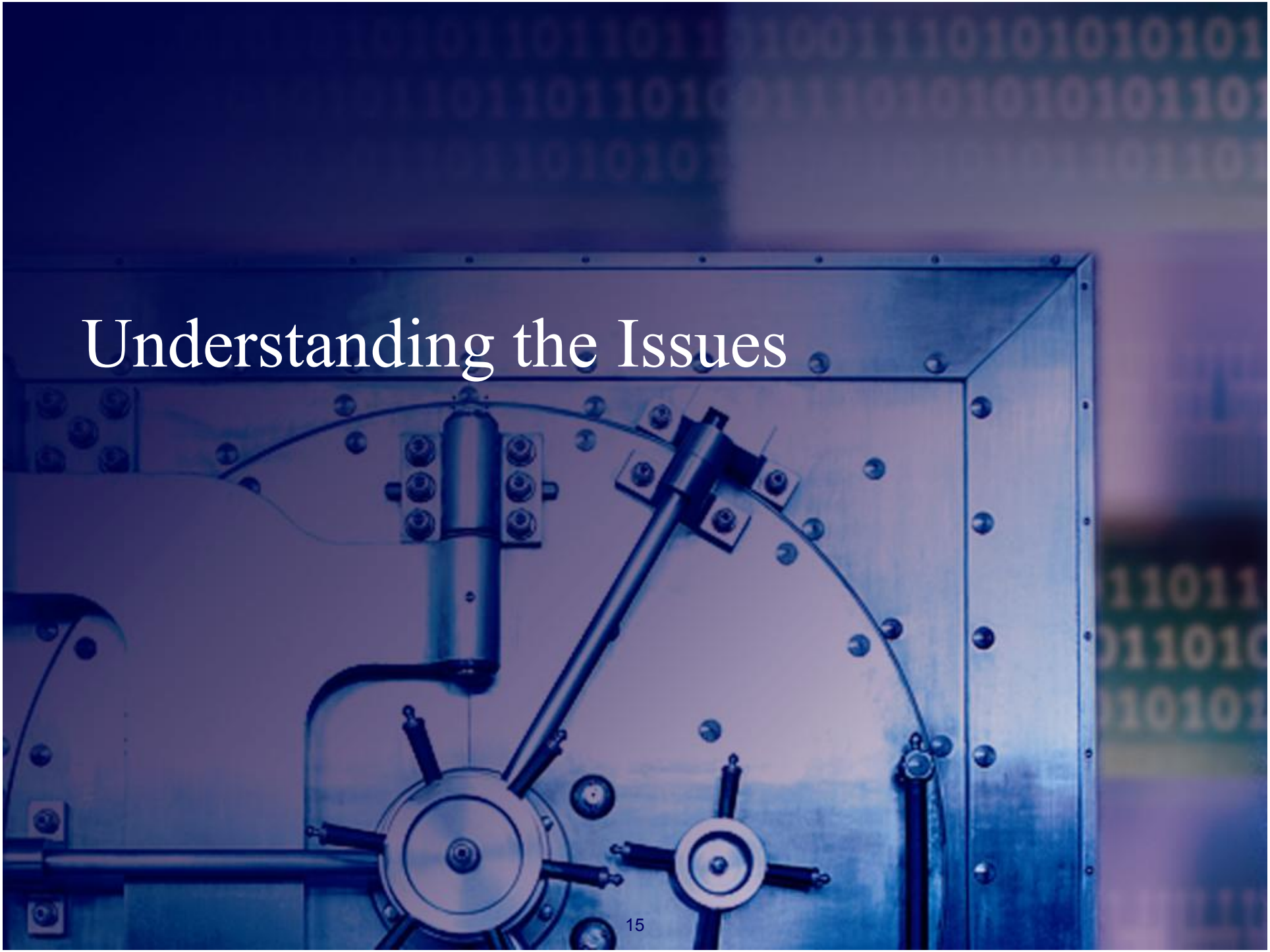


Other Requirements

- Unauthorized Access (California as an example)

Overview:	Requires prompt notification to CA residents in the event a business or agency knows or reasonably believes there has been a breach to computerized data that includes unencrypted personal information.
Who is Covered:	Any entity that conducts business in CA or that owns, licenses or maintains personal information of CA residents.
What is Covered:	Known or suspected acquisition of unencrypted PI information, defined as first name or first initial and last name in combination with one or more of the following: 1. Social Security Number 2. Drivers License Number or California ID Number 3. Account number with pin, access code or password 4. Medical information 5. Health insurance information
What is Required:	Requires prompt notification to CA residents if there is a known or suspected breach.
What are the Penalties:	Allows private rights of action.

Understanding the Issues



Understand the vocabulary

- Personally identifiable information
- Data Subject
- Controller
- Processor
- Processing
- Sensitive data
- Choice/Preference
- Access
- Integrity
- Opt-in/Opt-out
- Transfer
- On-ward transfer
- Secondary usage
- Unauthorized access
- Registration

How companies have gotten into trouble

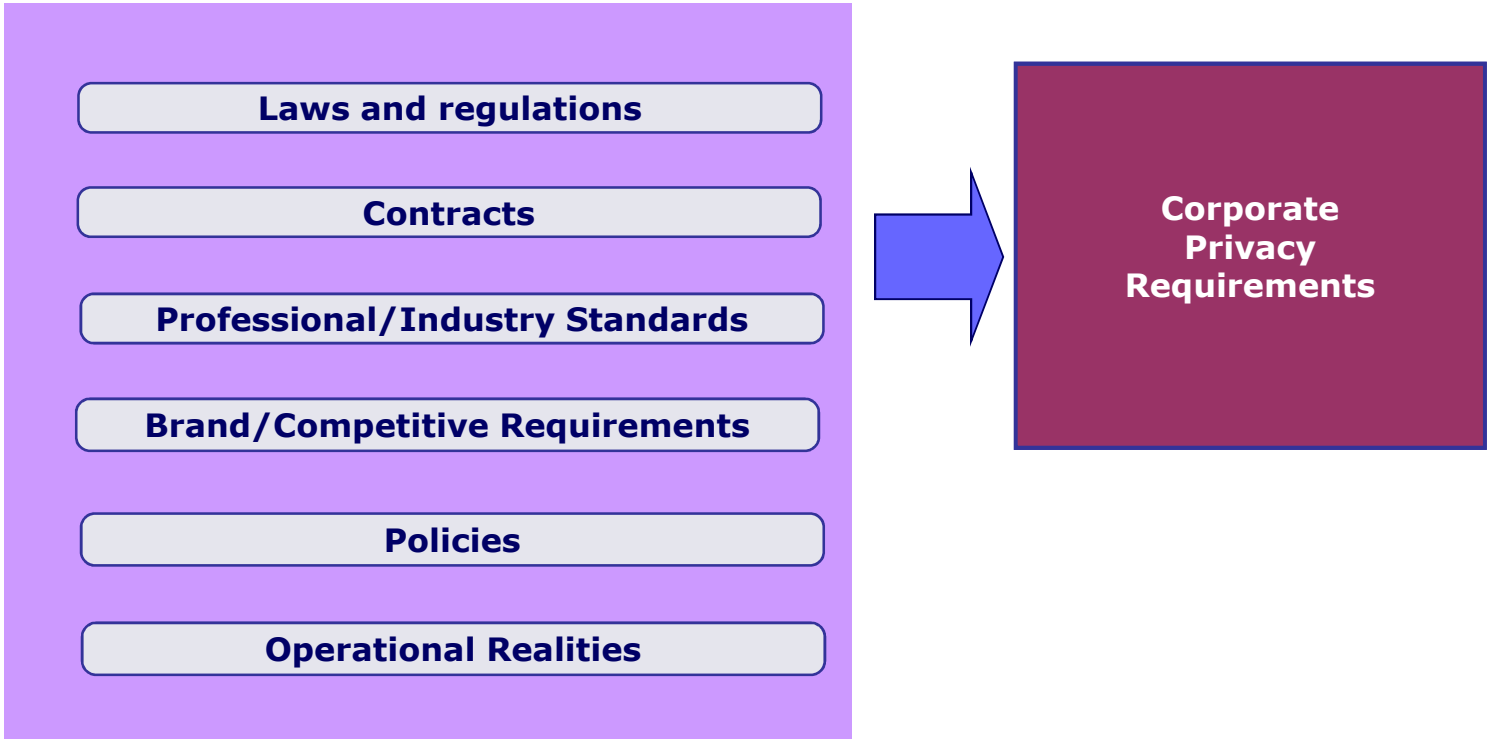
Common issues:

- Misrepresenting the collection purpose
- Non-disclosure of the means to collect PII (i.e., the use and/or duration of cookies, Web bugs, spyware, tracking technologies)
- Inadequate training
- Disclosing, sharing, or selling PII to third parties contrary to the organization's privacy policy
- Exporting PII
- Failure to register processing
- Misrepresenting the security protection of PII
- Data leakage

Many issues stem from:

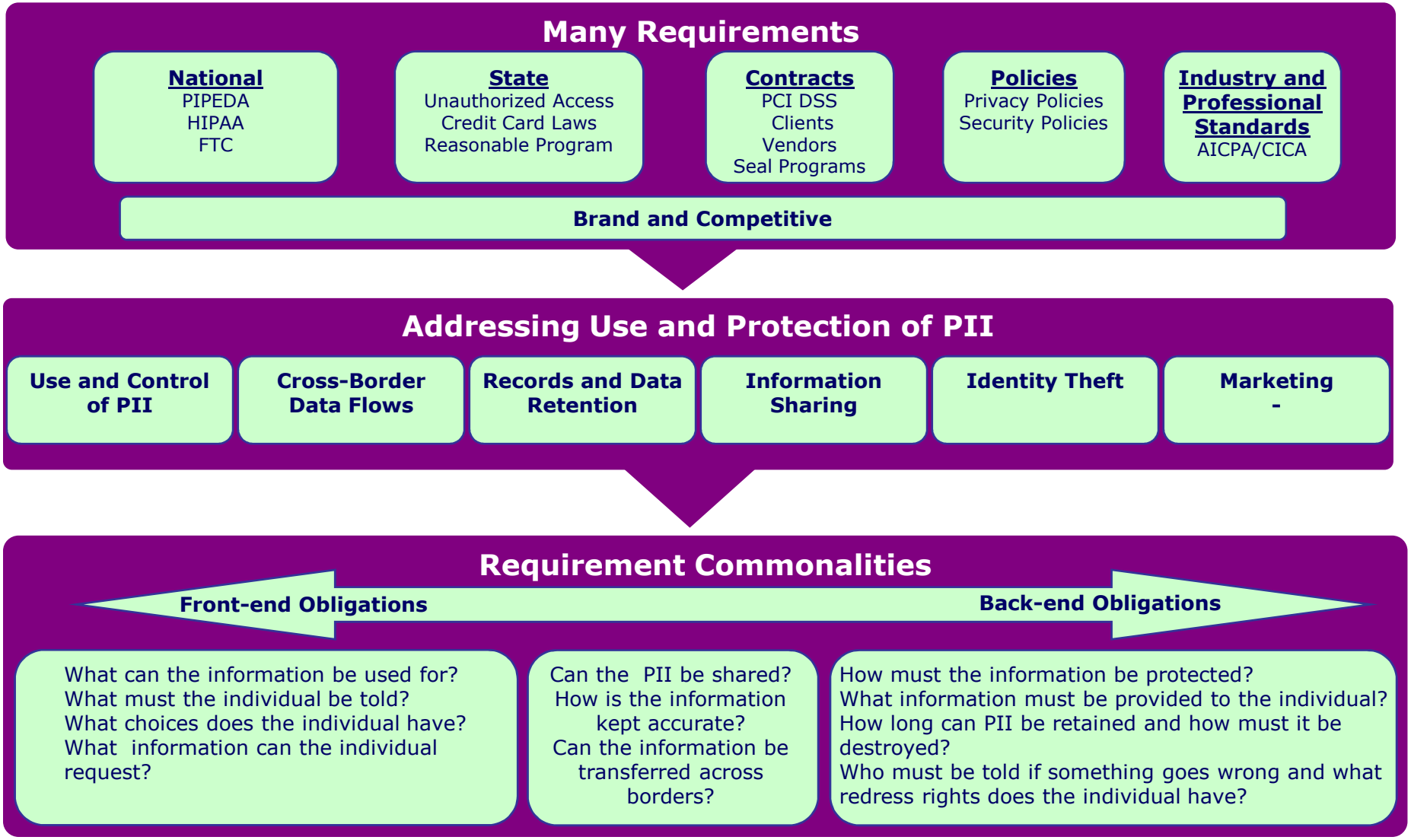
- A rush to policy
- A non-understanding of where the data is and what you do with it
- Non-coordination (or siloed approaches)

More than regulations – what are we trying to understand?



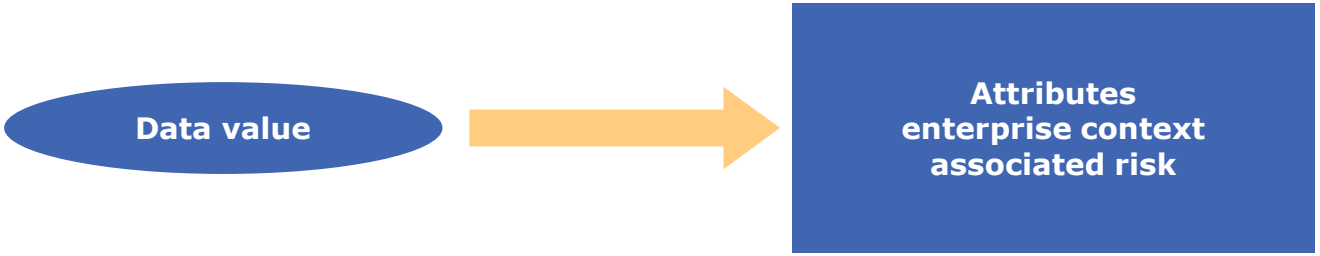
A purely regulatory focus can be problematic

What question are you trying to answer?

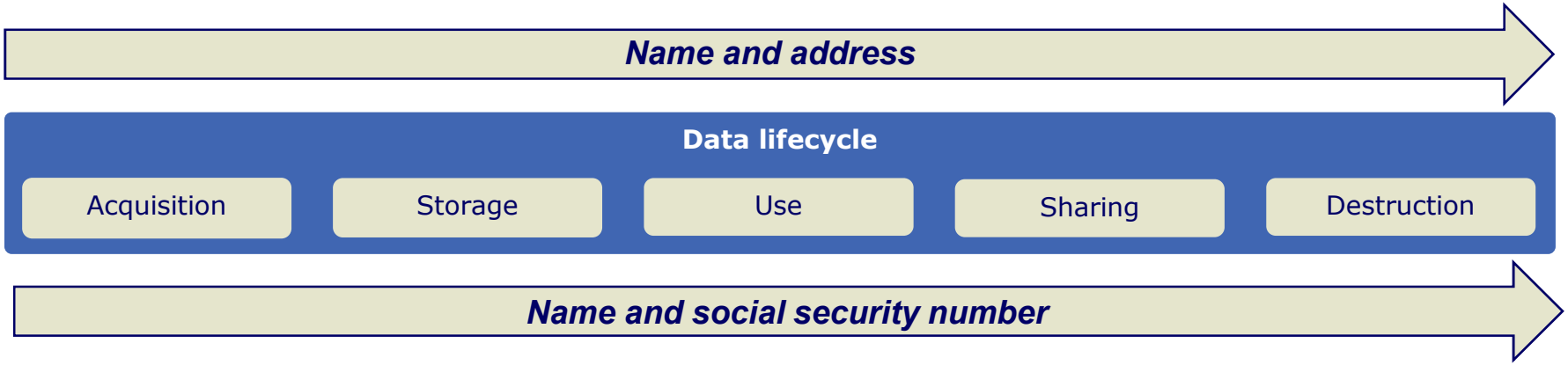


Data centric

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

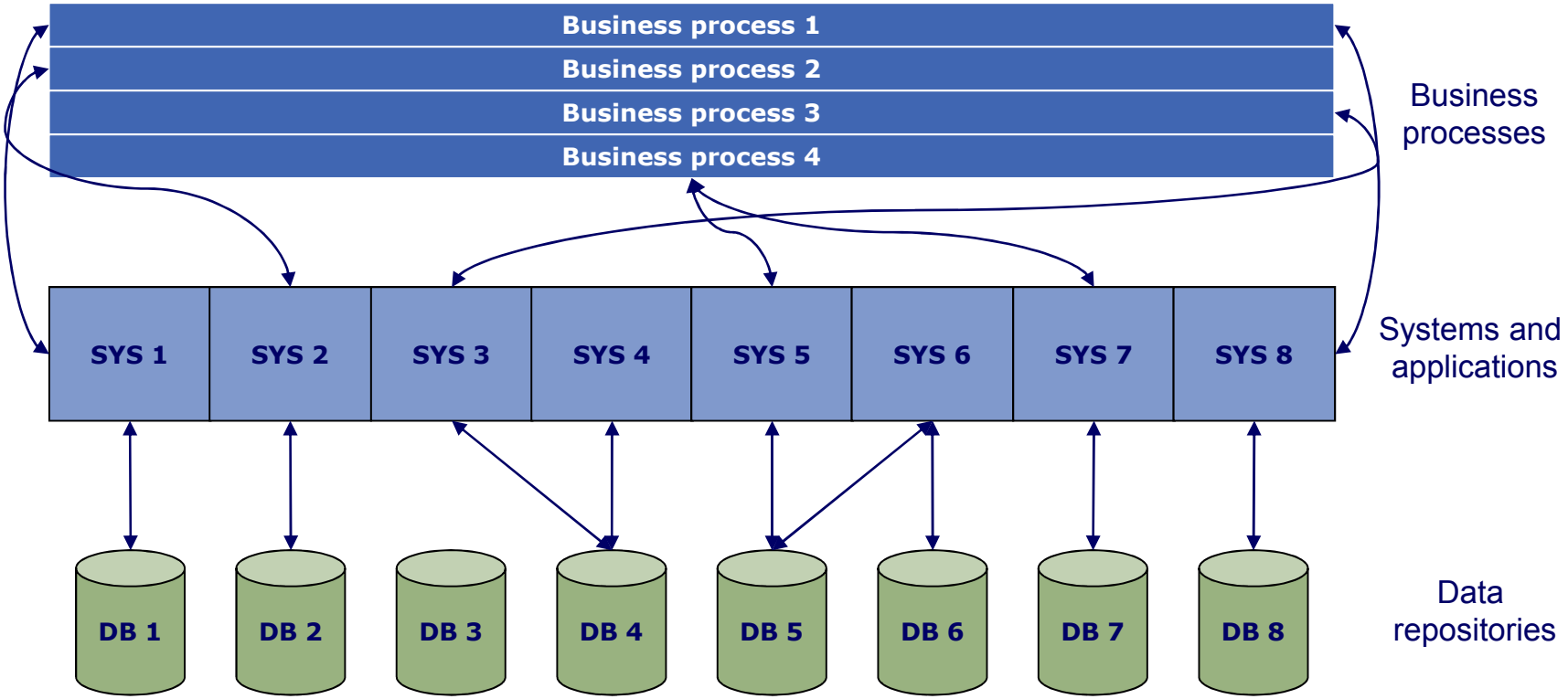


Compare the issues associated with two use cases over the lifecycle



Method of data analysis

Key is understanding the business processes, and then the supporting systems and associated data repositories that contain data.



Areas of focus

- Requirement adoption
- Deceptive and unfair practices
- Risk posed by unauthorized access laws
- Risk posed by cyber threats
- Special handling information (SSNs, Payment Data)
- Infrastructure change (ERP consolidation)
- Cross-border data flows
- Outsourcing/Third-parties
- Mergers and acquisitions

Case Studies

Case Study Themes

- Trying to do the right thing
- Connecting the dots
- Reducing the cost of procurement by moving off-shore and utilizing electronic payments
- Saving money through consolidation of ERP instances in the United States
- Just wanting what's due

Trying to do the right thing

A major pharmaceutical company needed to perform system maintenance work and take a server off-line that supported a marketing program. The marketing program was aimed at providing additional value to customers that used an anti-depressant drug. The company had a solid privacy program, a privacy officer, a policy assuring customers that they used and protected PII appropriated and adequately, and they provided a training program to make certain all employees were aware of the policy.

The IT professionals involved in the system maintenance work decided that the customers involved in the marketing program ought to know that the service would be unavailable for a period of time, and sent an email to all registered users of the drug. The problem was that everyone's address was included in the email header (a disclosure of all registered individuals taking the drug).

After investigations by multiple state and federal authorities, the entity entered into a "consent decree", that required (in addition to other consequences), outside oversight and independent review for 5 years.

- What would you like to know?
- What are the key issues (what are the attributes of this problem)?
- How would you assess an entity to understand whether this type of problem could occur?

Connecting the dots

A major company was experiencing low-level credit card fraud. Upon further investigation, they discovered that multiple systems and networks were found to be compromised with dormant or mutating forms of malware. The malware was designed to gather network information (system architecture, administrative credentials, etc.) and credit card data that subsequently communicated the information back to an unknown host.

- What would you like to know?
- What are the key issues (what are the attributes of this problem)?
- How would you assess an entity to understand whether this type of problem could occur?

Reducing the cost of procurement by moving off-shore and utilizing electronic payments

A B to B company embarked on an aggressive strategic effort to reduce the cost of its effort to support sales of parts and services to its customers. It moved operations into India and created a new on-line capability that supported electronic payments (all of which were built and supported by third-parties).

One day a client procurement officer noticed that camera equipment was purchased with his corporate credit card (the thief had the name, number and CVV2 code). After complaining to his bank, the source of the fraud was traced to the company. The company discovered a third party system maintenance worker stole the card data (but insisted they did not collect CVV2), confiscated his computer (which they owned and promptly re-imaged and re-circulated) and removed him from the site.

The card companies demanded a 3rd party forensic review which showed substantial non-compliance with the PCI DSS. Furthermore, it was discovered that unbeknownst to the company it did capture CVV2 data which was in a log file. In addition to having to notify all customers who purchased during the time the perpetrator was working with the company (1.5 years), the company was given the choice of becoming PCI DSS compliant (with a price tag of approximately $10m) or not accepting electronic payment – jeopardizing the strategic initiative.

- What would you like to know?
- What are the key issues (what are the attributes of this problem)?
- How would you assess an entity to understand whether this type of problem could occur?

Saving money through consolidation of ERP instances in the United States

A multi-national company had multiple instances of SAP (including substantial processing in Europe). It had a global privacy policy and local privacy policies in Europe. In order to reduce cost and simplify its operations, it embarked on a multi-year effort to consolidate those systems in the United States, with support personnel (help desk, development etc. located off-shore in India) – a $100m+ effort. A component of the information being transferred was HR data (including performance related information, payroll deductions to charitable entities like churches).

At almost the end of the project, a work council contacted a DPA to complain that personal information was going to be transferred contrary to the EU Data Protection Directive. The work council was concerned (in part) that the consolidation effort was going to result in reduced jobs. An investigation ensued and it was discovered that the legal mechanism to transfer information was inadequate (it was based on employee and customer consent) and that the company's registrations with authorities were inadequate.

The whole project was in doubt.

- What would you like to know?
- What are the key issues (what are the attributes of this problem)?
- How would you assess an entity to understand whether this type of problem could occur?

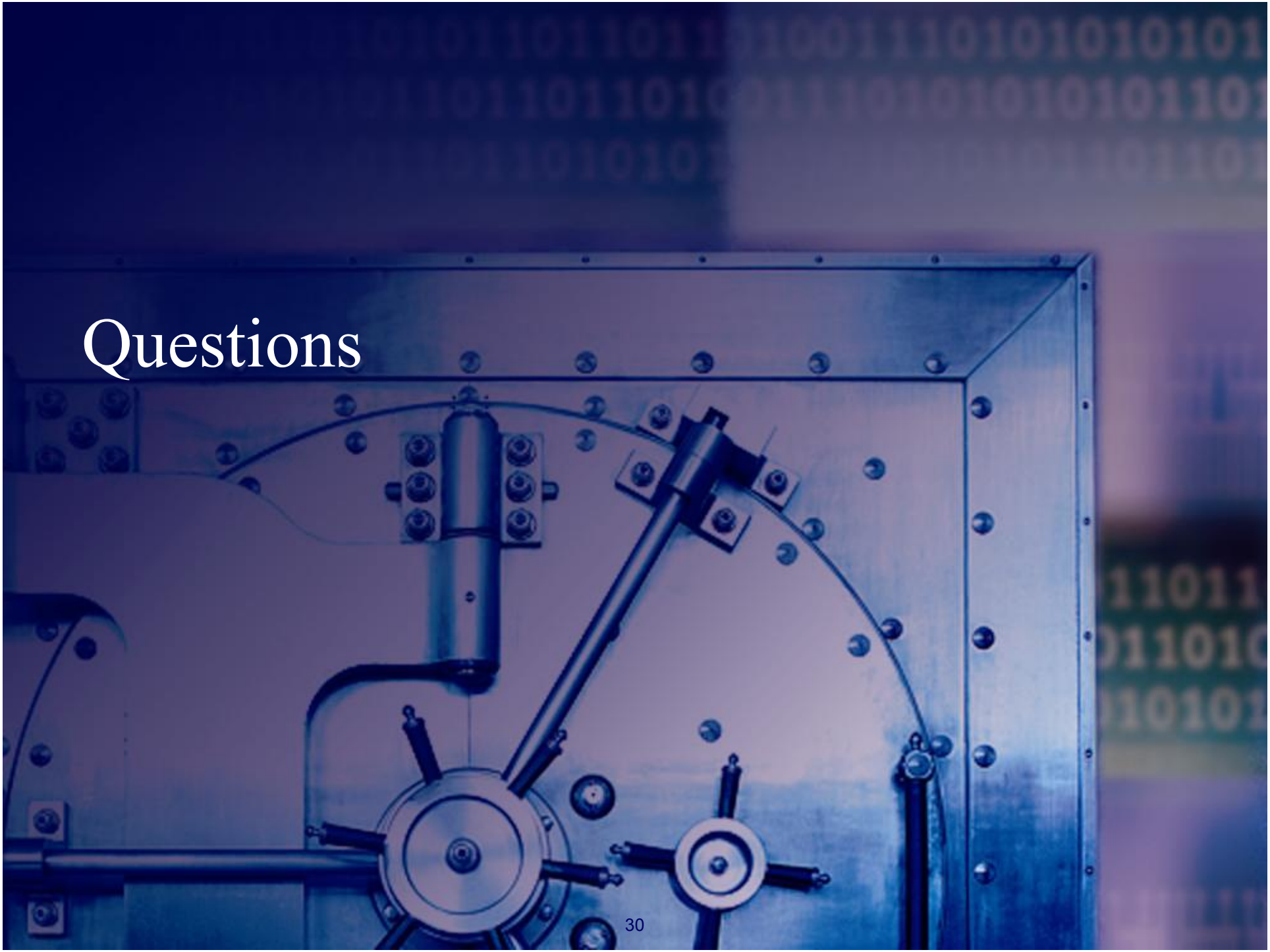
Just wanting what's due

A hospital sought to cut-costs by outsourcing transcription work. A doctor's notes were sent to a third-party who transcribed the information and sent it back to the hospital. What the hospital did not understand was that the third-party contracted with another vendor who sent the information to Pakistan (in fact, in a series of subcontracting relationships), where it was transcribed by individual contractors. One such contractor did not get paid and wanted her money. She threatened the hospital with posting patient names and information on the Internet (exposing a sample of the information), unless she got paid.

The story became public and received extensive news coverage. News outlets around the world identified the hospital in question, which resulted in enormous adverse publicity and regulatory issues.

- What would you like to know?
- What are the key issues (what are the attributes of this problem)?
- How would you assess an entity to understand whether this type of problem could occur?

Questions



Contact Information

Ken DeJarnette, Principal
Deloitte & Touche LLP
kdejarnette@deloitte.com
415-783-4316

John Morin, Manager
Deloitte & Touche LLP
jomorin@deloitte.com
415-783-6473

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 presentation contains the results of a survey conducted in part 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.