


# Conducting Personal Data Protection Reviews Based on International Laws

Michael Deeming, Assc. Director, Protiviti  
In-Depth Seminars – D31



# Objective

*At the completion of this presentation, you should have a greater understanding of International Data Privacy regulations and assessment. You will understand:*



Concepts of data privacy, and associated risks including those from emerging technologies i.e. BYOD, cloud computing



Overview of International Privacy landscape and Regulations



Contrast and comparison with select Privacy Regulations



Potential approach for a Data Privacy review

# What is Data Privacy and what can be done to evaluate it?

## Security

- Security is securing or protecting data assets. Typically viewed as the CIA triangle (Confidentiality, Integrity and Availability).

## Privacy

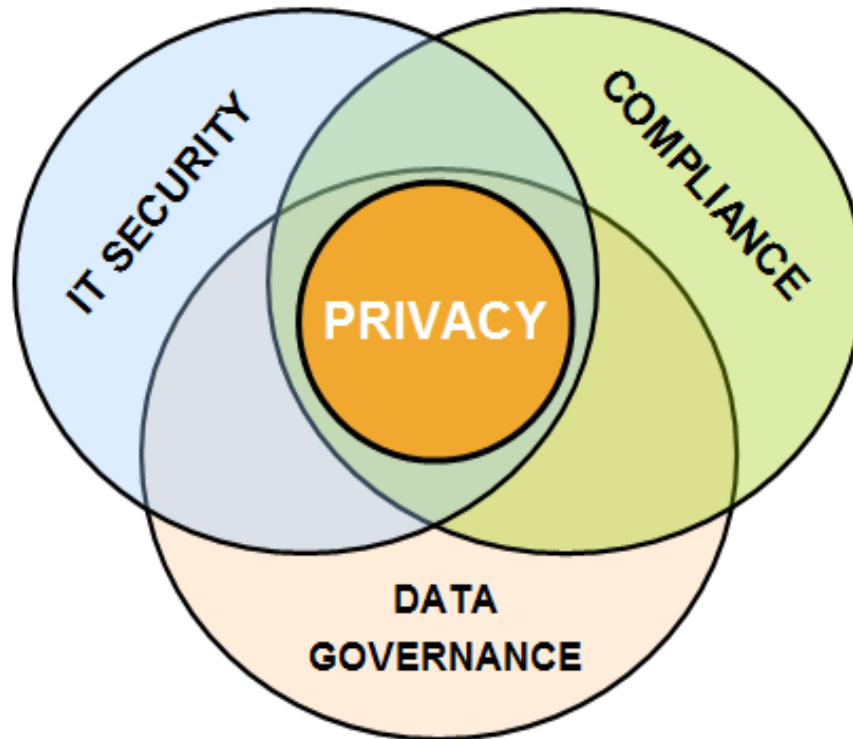
- Privacy is protecting the confidentiality of private data (personal information, proprietary data, etc.) of which Security is one element.

## Data Governance

- Data governance can be defined as the practices involved to effectively manage all classes of enterprise data from creation through disposal. These practices should reflect the requirements of a Privacy program.

# How do you classify “Privacy”?

*Is Privacy a security issue? Or a compliance issue? Or a data governance issue?*



# 1. Risks to Personal Data

# What are the Risks?

## THE TIMES Natural Resources

News | Opinion | **Business** | Money | Sport | Life | Arts | Puzzles | Papers



Yesterday's Shell results statement was appropriately scary

by Ian King, Business Editor's Commentator

Friday, November 1 6:55 PM

Welcome to your preview of The Times

Subscribe now

### Computer hackers add to ENRC's pile of problems



Juliet Samuel  
Last updated at 12:01AM, May 24 2013

ENRC has warned employees that its computer systems were hacked recently and that data could have been stolen.

The struggling Kazakh mining company, which is under investigation for fraud and corruption and is the subject of a takeover bid by its founding shareholders, sent out an e-mail to staff saying: "Whilst we cannot be certain that any particular personal data was accessed and used, we have decided to err on the side of caution and advise staff to take precautionary steps to protect against possible identity

ENRC has warned employees that its computer systems were hacked recently and that data could have been stolen.

Post a comment

Print

Share via

Facebook

Twitter

Google+

*Morning rush* *Adrenaline rush*

THE SUNDAY TIMES  
**DRIVING**

DRIVING.CO.UK

Behind the story:

Vast coal discovery off Cumbria coast 'could fire up British mining industry'

The industry could be reborn after the discovery of one to two billion tonnes of coking coal, a key ingredient...  
Last updated at May 24 2013

Post a comment



Tata Steel feels weight of Europe's recession


Tata Steel Europe employs more than half of its 33,000 workers in the UK, a legacy of Tata's takeover of the old... Last updated at May 24 2013

Post a comment

Profits for Bannan are wasted away



# What are the Risks?




Information Commissioner's Office

The UK's independent authority set up to **uphold information rights in the public interest**, promoting openness by public bodies and data privacy for individuals.

- Home
- For the public
- For organisations
- What we cover
- About the ICO
- News and events**
- Latest news**
- 2013**
- 2012
- 2011
- 2010
- Blog
- Current topics
- Events
- E-newsletter
- Press office
- Connect
- Enforcement

## Barclays Bank employee prosecuted for illegally accessing customer's account

### News release: 25 September 2013



A former Barclays Bank employee has been fined £3,360 after illegally accessing the details of a customer's account. In one case the employee, Jennifer Addo, found out the number of children the customer had and passed the details to the customer's then partner, who was a friend of Ms Addo.

Appearing at Croydon Magistrates Court today, 27-year-old Ms Addo was prosecuted under section 55 of the Data Protection Act and fined £2,990 for 23 offences and ordered to pay a £120 victim surcharge and £250 prosecution costs.

The bank was alerted to Ms Addo's activities when the customer contacted the bank to report that information from his account appeared to have been passed to his then partner. An investigation was launched by the bank that discovered Ms Addo had illegally accessed the customer's details on 22 occasions between 10 May 2011 and 8 August 2011. This was despite Barclays informing its staff that they should not access customers' accounts unless required.

When interviewed by her employer, Addo confirmed that she was aware that the complainant's details should not have been accessed, but still decided to

#### Latest news

- [Small businesses warned about importance of encryption](#)
- [Barclays Bank employee prosecuted for illegally accessing customer's account](#)
- [ICO carries global data protection enforcement resolution](#)
- [ICO appoints new non-executive members](#)
- [ICO responds to Michael Gove](#)

# What are the Risks?

[Subscribe/Manage Account](#) [Place An Ad](#) [LAT Store](#) [Jobs](#) [Cars](#) [Real Estate](#) [Rentals](#) [More Classifieds](#) [Custom Publishing](#)

---

# Los Angeles Times

LOCAL

U.S. WORLD BUSINESS SPORTS ENTERTAINMENT HEALTH LIVING TRAVEL OPINION

Search








L.A. NOW POLITICS CRIME EDUCATION O.C. WESTSIDE NEIGHBORHOODS ENVIRONMENT OBITUARIES

YOU ARE HERE: [LAT Home](#) → [Collections](#) → [News](#)

## UCLA hospitals to pay \$865,500 for breaches of celebrities' privacy

*Settlement with U.S. regulators also calls for UCLA to retrain staff and take steps to prevent future breaches. Some staff have already been fired for viewing the records of Farrah Fawcett, Michael Jackson and others.*

**July 08, 2011** | By Molly Hennessy-Fiske, Los Angeles Times

   Comments { 0 }  Recommend { 2 }  Tweet { 2 }  Share { 2 }  +1 { 0 }

UCLA Health System has agreed to pay \$865,500 as part of a settlement with federal regulators announced Thursday after two celebrity patients alleged that hospital employees broke the law and reviewed their medical records without authorization.

Federal and hospital officials declined to identify the celebrities involved. The complaints cover 2005 to 2009, a time during which hospital employees were repeatedly caught and fired for peeping at the medical records of dozens of celebrities, including Britney Spears, Farrah Fawcett and then-California First Lady Maria Shriver.



# What are the Risks?



Information Commissioner's Office

The UK's independent authority set up to **uphold information rights in the public interest**, promoting openness by public bodies and data privacy for individuals.



Home

For the public

For organisations

What we cover

About the ICO

News and events

Latest news

2013

2012

2011

2010

Blog

Current topics

Events

## ICO fines Glasgow City Council £150K

---

### News release: 7 June 2013



The Information Commissioner's Office (ICO) has issued Glasgow City Council with a [monetary penalty of £150,000](#) following the loss of two unencrypted laptops, one of which contained the personal information of 20,143 people.

The serious breach of the Data Protection Act comes after the council was previously issued with an enforcement notice three years ago, following a similar breach where an unencrypted memory stick containing personal data was lost.

In the latest incident, two unencrypted laptops were stolen from the council's offices on 28 May last year. The laptops were stolen from premises which were being refurbished and where complaints of theft and a lack of security had been made. One laptop had been locked away in its storage drawer and the key placed in the drawer where the second laptop was kept, but the

#### Latest news

[Small businesses warned about importance of encryption](#)

[Barclays Bank employee prosecuted for illegally accessing customer's account](#)

ICO carries global data

# What are the Risks?

The image is a screenshot of a BBC News Technology article. At the top is the BBC logo and a navigation bar with links for News, Sport, Weather, Capital, Culture, and Autos. Below this is a large red banner with the word 'NEWS' in white, followed by 'TECHNOLOGY' in a smaller font. A secondary navigation bar contains links for Home, UK, Africa, Asia, Europe, Latin America, Mid-East, US & Canada, Business, Health, and Sci/Environment. A large purple banner below the navigation bar reads 'CHOOSE FROM OVER 80 OPEN-ENROLLMENT OFFERINGS.' with a '> LEARN MORE' link. The article's date and time are '27 August 2013 Last updated at 11:29 GMT', and there are social media share icons for Facebook, Twitter, Email, and Print. The article title is 'Facebook to compensate users for sharing details on ads' by Joe Miller, BBC News. The main text states that approximately 614,000 Facebook users whose personal details appeared in ads on the site without their permission will each receive a \$15 (£9.65) payout. To the right of the text is a small image of a golf bag with a sign that says 'SALE FINAL REDUCTIONS! Bunker Mentality up to 50% OFF selected items in our SALE. 100% Great British Golf'.

**BBC** News Sport Weather Capital Culture Autos

## NEWS TECHNOLOGY

Home UK Africa Asia Europe Latin America Mid-East US & Canada Business Health Sci/Environment

**CHOOSE FROM OVER 80 OPEN-ENROLLMENT OFFERINGS.** > LEARN MORE

27 August 2013 Last updated at 11:29 GMT [Share](#) [f](#) [t](#) [e](#) [p](#)

### Facebook to compensate users for sharing details on ads

**By Joe Miller**  
BBC News

Approximately 614,000 Facebook users whose personal details appeared in ads on the site without their permission will each receive a \$15 (£9.65) payout.

**SALE FINAL REDUCTIONS!**  
Bunker Mentality up to 50% OFF selected items in our SALE. 100% Great British Golf

# What are the Risks?

FR EN ES



*"To protect personal data, support innovation, preserve individual liberties"*



Rechercher un article, fiche, démarche...



THE CNIL

DATA PROTECTION

PUBLICATIONS

TOPICS

Accueil > Home > News and events > News > Google : failure to comply before deadline set in the enforcement notice

ENGLISH

News



THE CNIL

DATA PROTECTION

PUBLICATIONS

TOPICS

## Google : failure to comply before deadline set in the enforcement notice

27 September 2013

On 20 June 2013, the CNIL's Chair had ordered Google to comply with the French data protection law within 3 months. On the last day of this period, Google responded to the CNIL. Google contests the reasoning of the CNIL and has not complied with the requests laid down in the enforcement notice

The formal enforcement notice of 20 June follows an analysis by European data protection authorities (united within the Article 29 Working Party) of the new privacy policy that Google implemented on 1 March 2012. The CNIL ordered Google to comply with the French data protection law within three months and in particular to:

- Define specified and explicit purposes;
- Inform users with regard to the purposes of the processing implemented;
- Define retention periods for the personal data processed;
- Not proceed, without legal basis, with the potentially unlimited combination of users' data;
- Fairly collect and process passive users' data ;
- Inform users and then obtain their consent in particular before storing cookies in their terminal.

# What are the Risks?





# What are the Risks?

MALAYSIA'S NO. 1 INVESTIGATIVE NEWSPAPER — WINNER OF THE MPI-PETRONAS BEST INVESTIGATIVE

Monday 25 OCTOBER 2013 PP423/11/201302/2011 www.malaymail.com.my

BeingFrank with Frankie D'Cruz

**HURTFUL 'BABY FOOD' MENACE**

>> pg6

**the malay mail** Est. 1994

*The Paper That Cares*

100,000 copies daily 40 sen for delivery per copy

FOLLOW US ON <http://www.facebook.com/malaymail> <http://www.twitter.com/malaymail>

## PERSONAL DATA FOR SALE

'Want to know more about Mukriz Mahathir or Opposition leader?' A database trader offered this information to our reporter who went undercover to check out a thriving but disturbing business. From RM1,700 to RM5k, for email addresses to credit card limits, no one is spared.

>> Report by SHAHRIM TAMRIN on pg2

## PRIVACY PIRATES

'The Malay Mail' probe uncovers shocking truth about whose hands your personal information is in

By SHAHRIM TAMRIN

— shahrimtamrin@mmmail.com.my —

**PETALING JAYA:** Many of us have received unwanted phone calls and text messages promoting goods and services.

So, it is only natural to wonder how our personal information could have been obtained by these callers with their sales pitches of free one-night stays at hotels and resorts, insurance products or fitness club memberships.

Even VIPs — the Tan Sri, Datuks, Yang Berhormat (Member of Parliament), Cabinet ministers, Royalty, high profile corporate leaders, celebrities and senior government officials — residing in high-end areas of the Klang Valley, are not spared.

The Malay Mail conducted a probe spanning three weeks into the issue and found personal data of individuals — whether rich and famous or just ordinary citizens — were being traded by unscrupulous database companies without regard to anybody's privacy.

After receiving numerous public complaints, our investigation found there were unanswered questions over the available protection for personal data and information

### PRICE RANGE

The personal databases offered to The Malay Mail were priced according to how they were sorted:

- **RM5,000:** 24,000 high-end records of individuals living in elite areas like Bukit Tunku, Country Heights, Damansara Heights, Bangsar, Mont Kiara, Sri Hartamas, Ampang, Bukit Antarabangsa, Damansara Utama, Mutiara Damansara and Taman Tun Dr Ismail (last updated April 2010)
- **RM1,200:** 16,136 records of individuals with a credit card limit of above RM30,000 (last updated Dec 2009)
- **RM1,800:** 69,000 credit card holders with a credit limit below RM10,000 (last updated Dec 2009)
- **RM1,500:** 160,000 Visa and Mastercard holders database (last updated Sept 2009)
- **RM1,700:** 760,000 email addresses of corporate salesmen and high achievers sorted by industry, company, profession, etc (last updated in April 2010)

security in the country.

It also uncovered worrying aspects related to the seemingly easy manner in which personal information was being sold or abused.

Even more mind-boggling was the discovery that personal information databases were being sold based on various categories, with one of the most popular being those based on an individual's income level.

With this database, VIPs and top company executives become fair game for telemarketing operations.

Such databases can be bought for as low as RM1,200 to RM5,000 for between 24,000 to 100,000 individual entries.

The information available in these databases are quite extensive and included the individual's name (with titles, where applicable), contact numbers (home and mobile), addresses and even MyKad numbers!

Posing as an interested buyer with a Penang-based telemarketing company, The Paper That Cares managed to get a sample database.

The database trader claimed he could provide further personal details if the potential buyer had specific requests.

"Do you want to know more about (Jelutong MP Datuk) Mukhriz Mahathir or an opposition leader?" he said.

"We can give you comprehensive database under different categories depending on your requirements."

During the probe, we were also offered a specific database of 100,000 female telecommunications customers (postpaid and prepaid users) throughout the country.

"We can provide you their ages, registered addresses, MyKad numbers and full names. The telco database is the latest you can get. It is updated on 24-hour basis," said the database trader.

When asked where such personal information was obtained, he said: "The high-end databases were mainly obtained from property developers while the credit card database is from financial institutions and market research agencies."

"As for telco records, we source it daily from various telecommunications providers and middle-men."

# Additional Breach Examples (Personal Data)

- October 2013: Adobe – Hacked
  - Names, other purchase information
  - 2.9 million customers
- April 2013: LivingSocial – Hacked
  - Name, Email Address, Date of Birth
  - 50 million customers
- March 2013: Evernote – Hacked
  - Usernames, Email Addresses
  - 50 million records affected
  - Public notification, password reset





# FTC Consent Orders Examples (Privacy)

- July 2013: HTC America
  - Weak security on phones
  - 20 years of reporting to FTC on external security audits
- February 2013: Path Inc
  - Collected more than privacy policy said
  - \$800,000 fine, 20 years of reporting to FTC on external security audits
- January 2012: UPromise
  - Insecure storage of customer information
  - Remediation, on external security audits
- Others: Twitter, Facebook, Google, MySpace



***It takes twenty years to build a reputation and five minutes to ruin it. If you think about that, you'll do things differently.***

***– Warren Buffett***

# Emerging Risks: Cloud Computing and Big Data



Jurisdiction: Sending, storing, processing in multiple jurisdictions.



Creation of new data streams and usage either by the organisation or the cloud information for purposes beyond those for which consent was originally given.



Security: Security of data while it resides in the cloud.



Data intrusion: Unauthorized access to data by an external party.



Misuse of processing data: The cloud provider might inappropriately access, manipulate or mine the data entrusted to them.



Preservance of data: What happens to the data at the end of the contract.

# Emerging Risks: BYOD



The device gets lost or stolen with access to company data and systems.



The device contracts a virus or has malware installed that can obtain company logins and data from that device.



The personal device user — however good his/her intentions are — can in effect be circumventing company security standards.



The company cannot control the use of the personal device should the employee allow children or friends to use the device.



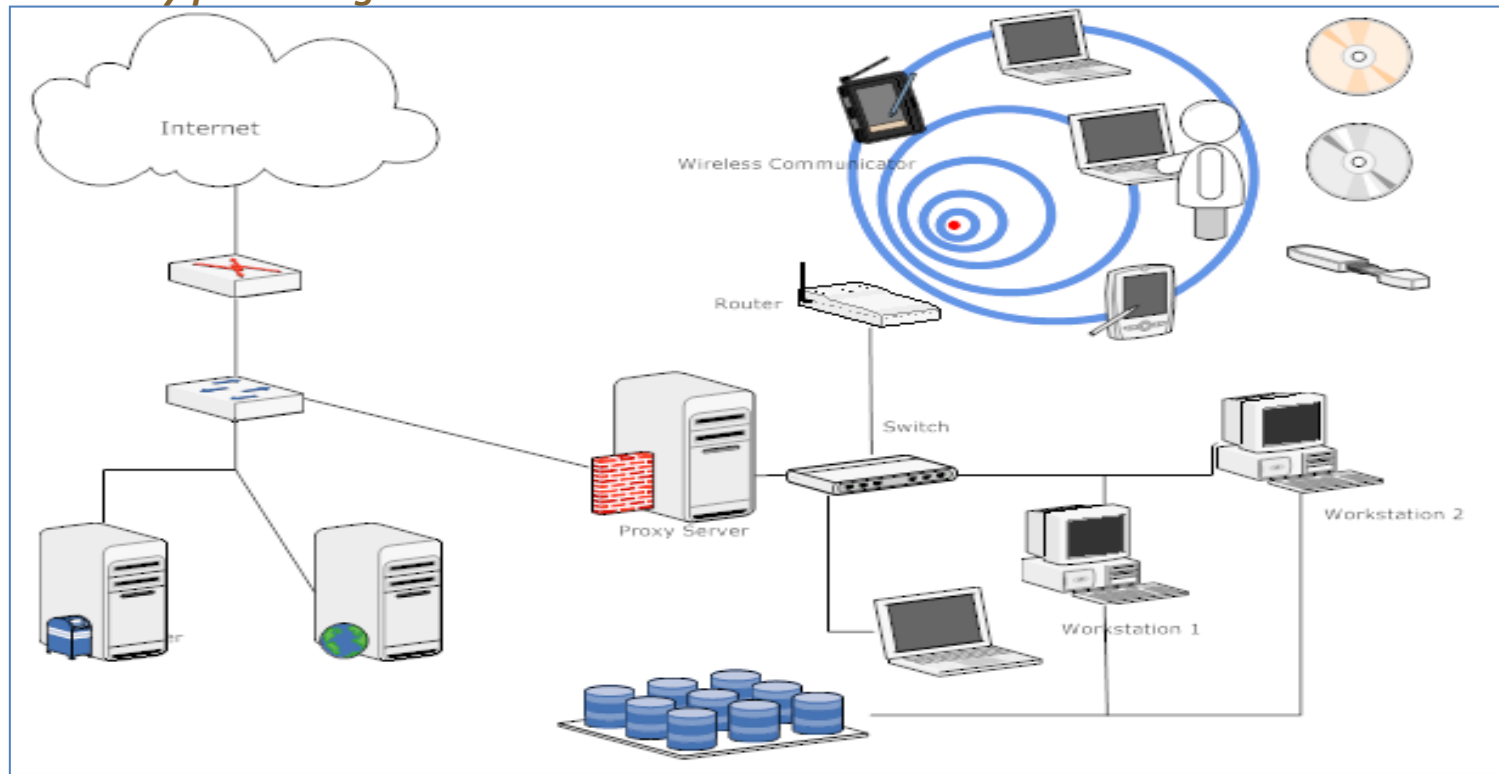
The employee may use the device to place files in personal applications in the cloud which may not be secure.



The employee plugs a mobile device into the USB port of his or her office computer thereby transmitting a virus to the office desktop.

# Data Privacy Technical Challenges

*Where is your data stored, who can access it, where are the network boundaries, and are my controls actually protecting the data?*



*Some 71 percent of [IT Security Professionals] said their organization does not have an accurate inventory of where personal data for employees and customers is stored.*

*- Source: [scmagazineus.com](http://scmagazineus.com)*

# Have a Good Story

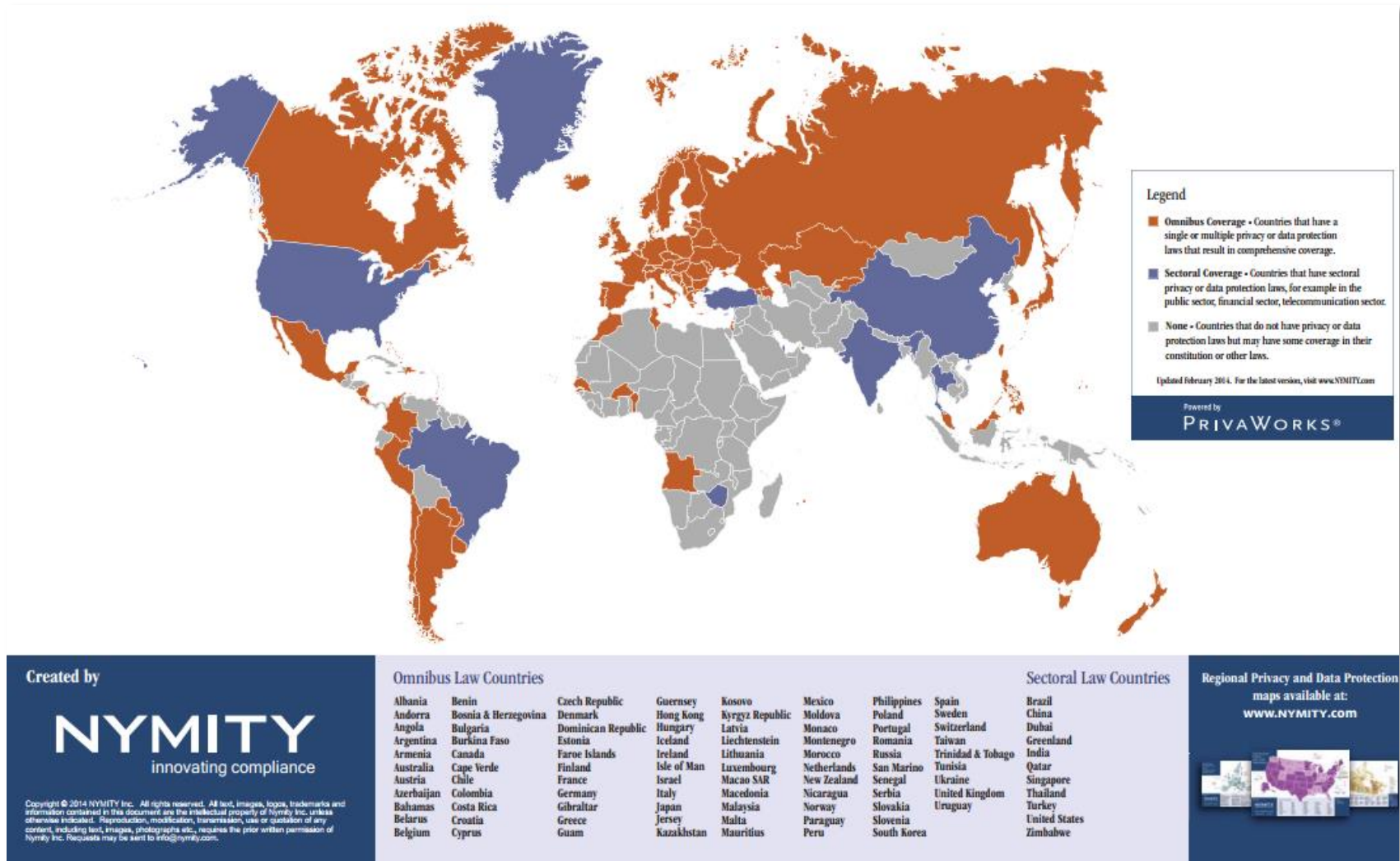
- ! *Could you confidently explain your security & privacy program to a reporter?*
- ! *Can you clearly demonstrate due care and due diligence?*
- ! *Good story vs. bad story*



## 2. Privacy Regulations



# Sectoral and Omnibus Privacy and Data Protection Laws



# International & Regional Instruments

- OECD Guidelines 1980
- Council of Europe Convention 1981
- European Directive 1995
- APEC Privacy Framework 2004
- Madrid Resolution 2009
- Proposed EU General Data Protection Regulation (issued on 25 January 2012)
- Singapore Personal Data Protection Act 2014
- India's Information Technology Act 2000



# OECD Guidelines 1980 (8 Principles)

- 1 Collection limitation
- 2 Data Quality
- 3 Purpose Specification
- 4 Use Limitation
- 5 Security
- 6 Openness
- 7 Individual Participation
- 8 Accountability



# APEC Privacy Framework 2004 (9 Principles)

- 1 Preventing harm
- 2 Notice
- 3 Collection Limitation
- 4 Uses of personal information
- 5 Choice
- 6 Integrity
- 7 Security safeguards
- 8 Access and correction
- 9 Accountability



# Madrid Resolution 2009 (6 Principles)

1 Lawfulness and fairness

2 Purpose specification

3 Proportionality

4 Data quality

5 Openness

6 Accountability



## European Directive 1995 (7 Principles for Safe Harbor)

- 1 Notice – explain purpose for PI collection and use
- 2 Consent – opt in/out for 3<sup>rd</sup> party disclosure
- 3 Onward transfer – 3<sup>rd</sup> party must apply notice and consent principles
- 4 Security – reasonable precautions to safeguard
- 5 Data Integrity – PI relevant and reliable for intended use
- 6 Access – reasonable access to PI and ability to amend
- 7 Accountability – available, affordable recourse to address disputes



# Proposed EU Data Protection Regulation



- One EU – Wide Data Protection Law (Regulation vs Directive)
- Penalties for breaches up to 100 000 000 EUR or up to 5% of the annual worldwide turnover of a company (up from 2% in the Commission's proposal)
- Mandatory data breach notification
- Explicit consent
- Right to be forgotten
- Right to obtain from the controller the rectification of personal data
- Right to restriction of processing
- Right to Erasure
- Data protection impact assessment [Mandatory in certain circumstances]



# Singapore Personal Data Protection Act (PDPA)

1

Today, organizations collect vast amounts of personal data, for use and collaboration with third party organizations to promote business development activities.

2

This trend in Asia is expected to grow exponentially as the processing and analysis of large amounts of personal data becomes more accessible as technology continues to advance.

3

In January 2013, the Singapore Parliament passed the Personal Data Protection Act (“PDPA”) designed to govern the collection, use and disclosure of personal data by organizations. Organizations were required to comply with PDPA since 2 July 2014.

4

By regulating the flow of personal data among organizations, the PDPA aims to strengthen and entrench Singapore’s competitiveness and position as a trusted, world-class hub for businesses.

5

The Bill is drafted to apply to all sectors in the economy and necessarily contains broad and general principles.

- *Provisions relating to the DNC (Do Not Call) registry became effective on 2 January 2014*
- *Data protection rules became effective on 2 July 2014.*

# Some of the US Data Protection Regulations

- The Federal Trade Commission Act (FTCA)
- The Gramm-Leach-Bliley Financial Services Modernization Act of 1999 (GLBA)
- The Fair Credit Reporting Act (FCRA)
- The Health insurance Portability and Accountability Act (HIPAA)
- The Children's Online Privacy Protection Act of 1998 (COPPA)
- Payment Card Industry Data Security Standards (PCI DSS)
- State Notification Laws:
  - California SB 1386/1798.81.5;
  - Massachusetts 201 CMR 17;
  - Colorado 6-1-176

# Work in Progress

## U.S Consumer Privacy Bill of Rights

- Individual Control
- Transparency
- Respect for context
- Security
- Access and Accuracy
- Focused Collection
- Accountability



# Personal Data Protection in India

**Information Technology Act 2000** contains some provisions on personal data protection, e.g., penalty for download, copy or extract of data from a computer without the permission of the owner (section 43), penalty for computer source code tempering (section 65), punishment for hacking (66), punishment for breach of confidentiality and privacy, unauthorized access to electronic record, etc. (section 72).

**The Information and Communication Technology (Amendment) Act, 2008** inserted section 43A which provides for punishment of body corporate for negligent handling of sensitive personal data by way of compensation up to 50 million Indian rupee (USD \$815,000).

**Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules 2011 (“Sensitive Personal Data Rules”)** was framed in 2011

‘Sensitive personal data or information of a person’ include (i) password; (ii) user details as provided at the time of registration or thereafter; (iii) information related to financial information such as Bank account/credit card/debit card/other payment instrument details of the users; (iv) Physiological and mental health condition; (v) Medical records and history; (vi) Biometric information; (vii) Information received by body corporate for processing, stored or processed under lawful contract or otherwise; (viii) Call data records.

# Obligations of Corporate Entities in India

- ➡ Publish privacy policy in the Website for handling and dealing personal information, mentioning the purpose of collection and usage of personal data.
- ➡ Personal information cannot be collected without consent of the data subject.
- ➡ Sensitive personal information cannot be collected or disclosed without prior permission.
- ➡ Transborder data transfer is allowed when it is legally necessary or with the consent of the data subject.
- ➡ Must take *Reasonable Security Practices and Procedures* containing managerial, technical, operational and physical security control measures. In case of any information security breach, such body corporate must show that such security control measures were taken.



### 3. Comparison of Regulatory Requirements by Country

# Regulatory Requirements in International Jurisdictions

	European Union [1995 Data Protection Directive]	United States of America	Malaysia Personal Data Protection Act 2010	Singapore Personal Data Protection Act 2012	Australia Privacy Act 1988	South Africa Protection of Personal Information Act 2013	Chile Personal Data Protection Law [No. 19628 of 2012]	Columbia Personal Data Protection Law [No. 15811 of 2012]
<b>Data Protection Principles</b>	√	√	√	√	√	√	No information available	No information available
<b>Rights of Data Subjects</b>	√	√	√	√	√	√	√	√
<b>Special enforcement entity</b>	√	√	√	√	√	√	√	√
<b>Exemption to public agency</b>	x	x	√	√	X	X	No information available	No information available

# Regulatory Requirements in International Jurisdictions

	European Union [1995 Data Protection Directive]	United States of America	Malaysia Personal Data Protection Act 2010	Singapore Personal Data Protection Act 2012	Australia Privacy Act 1988	South Africa Protection of Personal Information Act 2013	Chile Personal Data Protection Law [No. 19628 of 2012]	Columbia Personal Data Protection Law [No. 15811 of 2012]
<b>Civil and criminal remedies</b>	√	√	√*	√	√	√	√	√
<b>Mandatory reporting of breach to Regulator</b>	x	X [in some States]	X	X	X	√	X	X
<b>Differentiate personal data &amp; sensitive data</b>	√	√ [In some Laws]	√	X	√	√	√	√
<b>Organization must designate someone to take charge</b>	x	x	X	√	X	√	X	X

*\*Malaysia provides only for criminal penalties.*

# Regulatory Requirements in International Jurisdictions

	European Union [1995 Data Protection Directive]	United States of America	Malaysia Personal Data Protection Act 2010	Singapore Personal Data Protection Act 2012	Australia Privacy Act 1988	South Africa Protection of Personal Information Act 2013	Chile Personal Data Protection Law [No. 19628 of 2012]	Columbia Personal Data Protection Law [No. 15811 of 2012]
<b>Registration</b>	x	x	√	X	X	X	No information available	No information available
<b>Class action</b>	√	√	X	X	√	√	No information available	No information available
<b>Enforcement Authority can impose financial penalty</b>	√	√	X	√	√	X	√	√
<b>Do Not Call Registry</b>	X [In Some countries]	√	X	√	√ [In separate law]	X	X	X

# Do Not Call Register: A Comparison

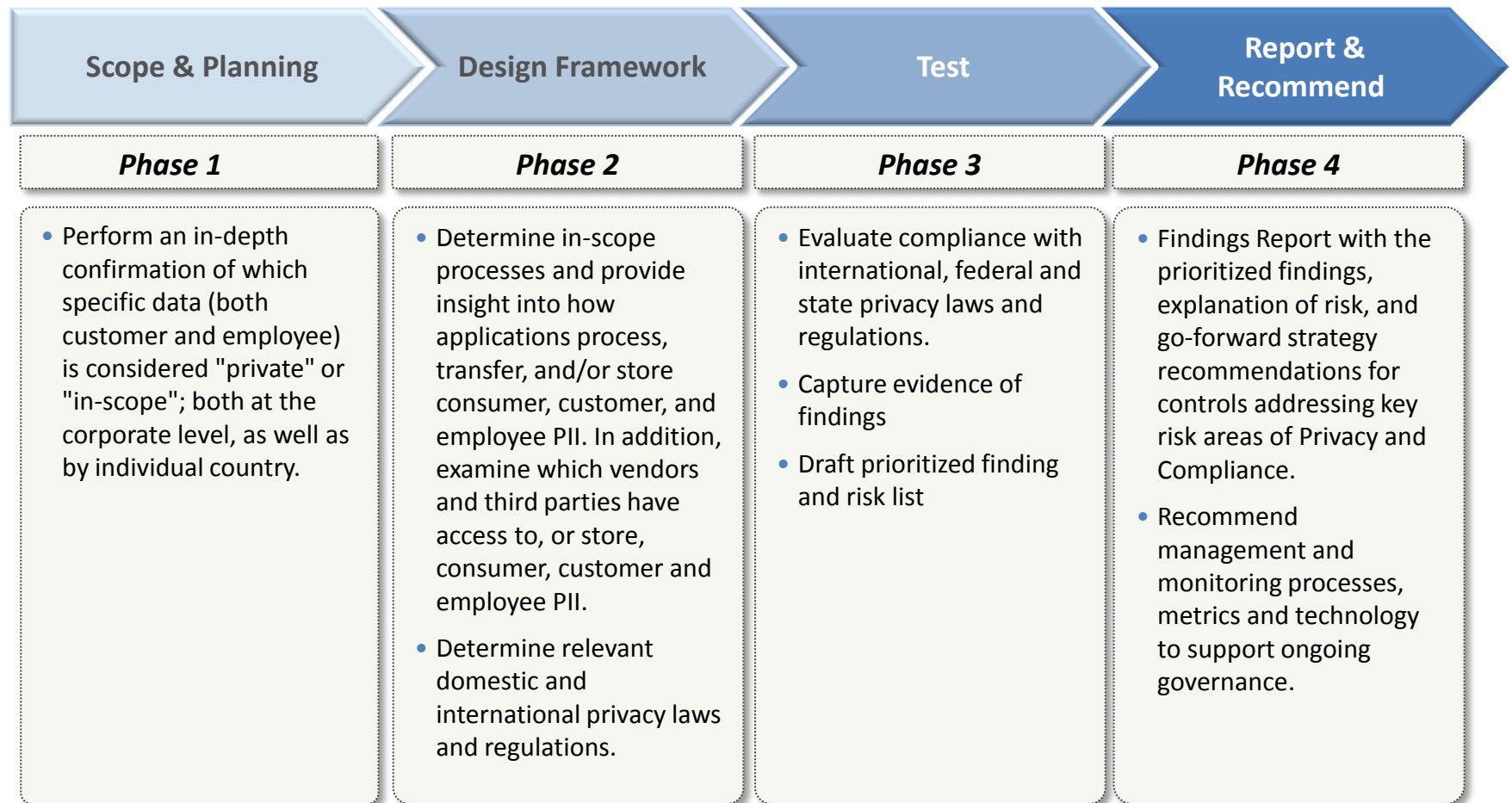
	Australia	Canada	India	Spain	UK	US	Singapore
<b>Register</b>	National Do Not Call Register	National Do Not Contact List	National Do Not Call Register	Listas Robinson	Telephone Preference Service	National Do Not Call Registry	National Do Not Call Register
<b>Year</b>	2006	2005	2007	2003	2003	2003	2013
<b>Regulator</b>	Australian Communications and Media Authority	Canadian Radio-television and Telecommunications Commission	Telecom Regulatory Authority of India	Federation of Electronic Commerce and Direct Marketing	Information Commissioner's Office	Federal Trade Commission	Personal Data Protection Commission
<b>Coverage</b>	<ul style="list-style-type: none"> <li>• Residential</li> <li>• Mobiles</li> <li>• VOIP</li> <li>• Business (from 2010)</li> <li>• Fax (from 2010)</li> </ul>	<ul style="list-style-type: none"> <li>• Residential</li> <li>• Mobiles</li> <li>• VOIP</li> <li>• Fax</li> </ul>	<ul style="list-style-type: none"> <li>• Residential</li> <li>• Mobiles</li> </ul>	<ul style="list-style-type: none"> <li>• Residential</li> <li>• Business</li> <li>• Mobiles</li> <li>• Mail</li> <li>• Email</li> </ul>	<ul style="list-style-type: none"> <li>• Residential</li> <li>• Business</li> <li>• Mobiles</li> </ul>	<ul style="list-style-type: none"> <li>• Residential</li> <li>• Mobiles</li> </ul>	<ul style="list-style-type: none"> <li>• Residential</li> <li>• Message in sound</li> <li>• Text</li> <li>• Fax</li> <li>• [Not applicable in case of B2B]</li> </ul>
<b>Size (as of 2012)</b>	8.5 million	10.7 million	161.7 million	Not available	19 million	217 million	??
<b>Renewal</b>	3 years	5 years	Permanent	Permanent	Permanent	Permanent	??

## 4. Assessing Compliance



# Executing a Data Privacy Assessment

*This phased approach involves a combination of manual and automated audit techniques to evaluate process and IT controls, and considers integration with existing IT security programs.*



# Executing a Data Privacy Assessment

## Phase 1: Scoping and Planning

- Perform an in-depth confirmation of which specific data (both customer and employee) is considered "private" or "in-scope"; both at the corporate level, as well as by individual country.
- Develop a general understanding of the types of data that flow through the company and which data contains personally identifiable information ("PII").
- Finalize information gathering techniques for all locations.
- Determine specific documentation that is available and will be gathered.
- Initiate data mapping.
- Summarize the overall results in a Data Storage Report that highlights every location and device where in-scope (PII) data was identified.

# What is Personal Data?

- Personal Data/Personal Information/Personally Identifiable Information
- AICPA Definition - information that **is about, or can be related to**, an identifiable individual. Individuals, for this purpose, include prospective, current and former customers, employees and others with whom the entity has a relationship. Most information collected by an organization about an individual is likely to be considered personal information if it can be attributed to an identified individual.



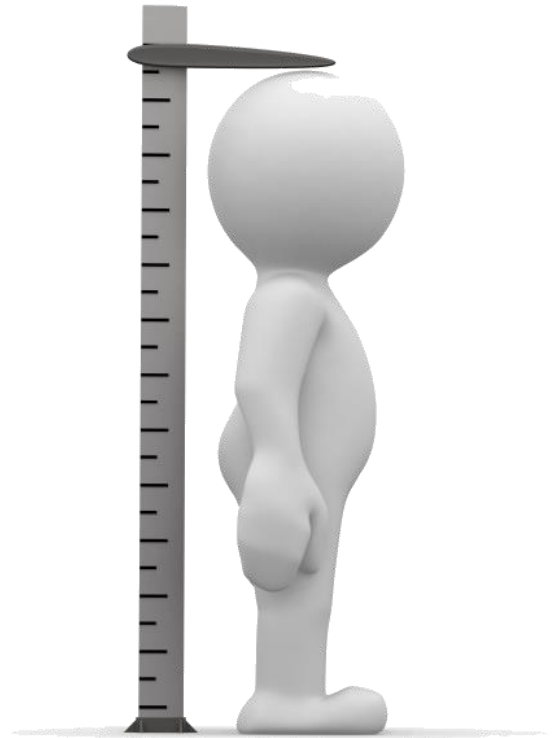
# Who is an Individual?

- Customers (prospective, current, former)
- Employees (job candidates, current, former)
- Contractors
- Vendors
- Stockholders
- Website Visitors
- YOU



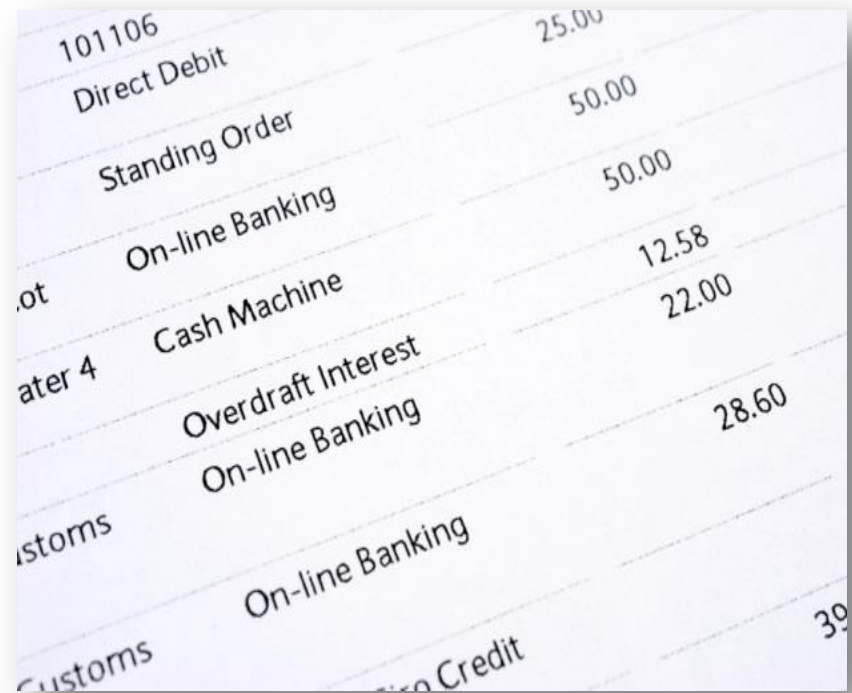
# Personal Information: Who They Are

- Name
- Mailing Address
- Phone Number
- Email Address
- Physical Characteristics
- Social Security Number
- Driver's License/ID number
- Passport number
- Credit/debit card number
- Bank account number
- IP Address, Login name, screen name
- Biometrics



# Personal Information: What They Have Done

- Purchases
- Financial Transactions
- Paychecks
- Communications
- Browsing History



Transaction	Amount
101106 Direct Debit	25.00
Standing Order	50.00
On-line Banking	50.00
Cash Machine	12.58
Overdraft Interest	22.00
On-line Banking	28.60
Credit	39.00

# Potentially Sensitive Personal Information

- Political affiliation
- Race or ethnicity
- Religious beliefs
- Union membership
- Sexual orientation
- Financial information
- Health condition or medical-related
- Criminal History
- Employment History
- Insurance Policy Number
- Education
- Password/Security Question Answer
- Signature





# Inventory What You Know

## *Data at Rest*

- **Electronic File Storage (network & hard drives)**
  - Excel/Word Documents
  - Desktop Databases
  - Downloaded Data (e.g., Text Files)
- **Business Applications**
  - POS (Bank, ID, SSN)
  - Documentum
  - Legal
  - Records Management Database
  - Research Repository or Testing Environment?
  - Other Corporate Apps/Databases (TBD)
- **Other Electronic File Storage**
  - Backup Tapes
  - CDR/DVD disks from third parties (manual interfaces)
- **Paper Files and Reports**
  - Unsecured storage of personal information (paper)
- **Third Party Applications/Environment**
  - Payroll Outsourcing (e.g., ADP)

## *Data in Motion*

- **Email**
  - Corporate Email
  - Web Email (personal)?
  - Third Party Email (e.g., sent to ABC)
- **Interfaces**
  - To/From Applications/Providers
- **Remote Access (Authorized)**
- **Unauthorized Access**
  - Virus, spy-ware
  - Hacking (Internal/External)
- **Network & Security Infrastructure**

## *Data in Use*

- **Laptops**
  - Disconnects from corporate network
  - More susceptible to theft
  - Tends to connect to internet in unfriendly locations (e.g., while traveling)
- **Storage Devices**
  - e.g., USB Keychain, disks, cd/dvd, tapes

# Discover What You Don't Know

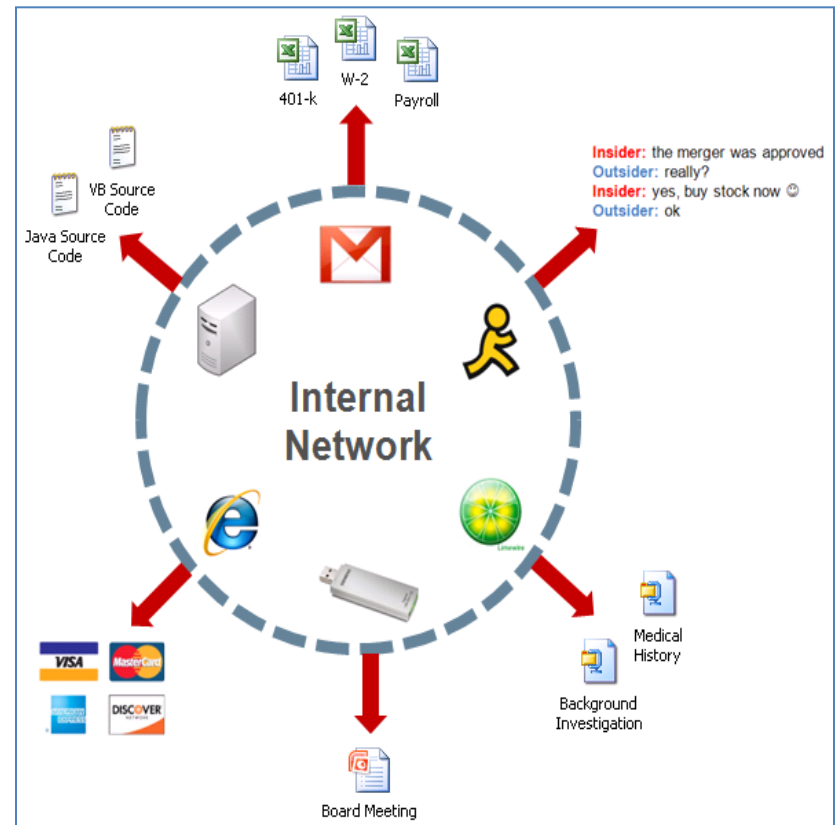
- Identify **departments** that handle sensitive data
  - Human Resources (Payroll, Benefits, Compensation)
  - Accounting
  - Finance
  - Legal
- Identify **key processes** that include the handling of sensitive data
  - Background Check
  - New Hire Process
  - Wage Garnishments
  - Payroll Processing
  - Benefits Enrollment
  - Direct Deposit Enrollment for Expense Reimbursement
  - Updating Bank Information
- Identify processes involving transfer of data to a **third-party** vendor
  - Payroll
  - Benefits

# Assess Data Leakage

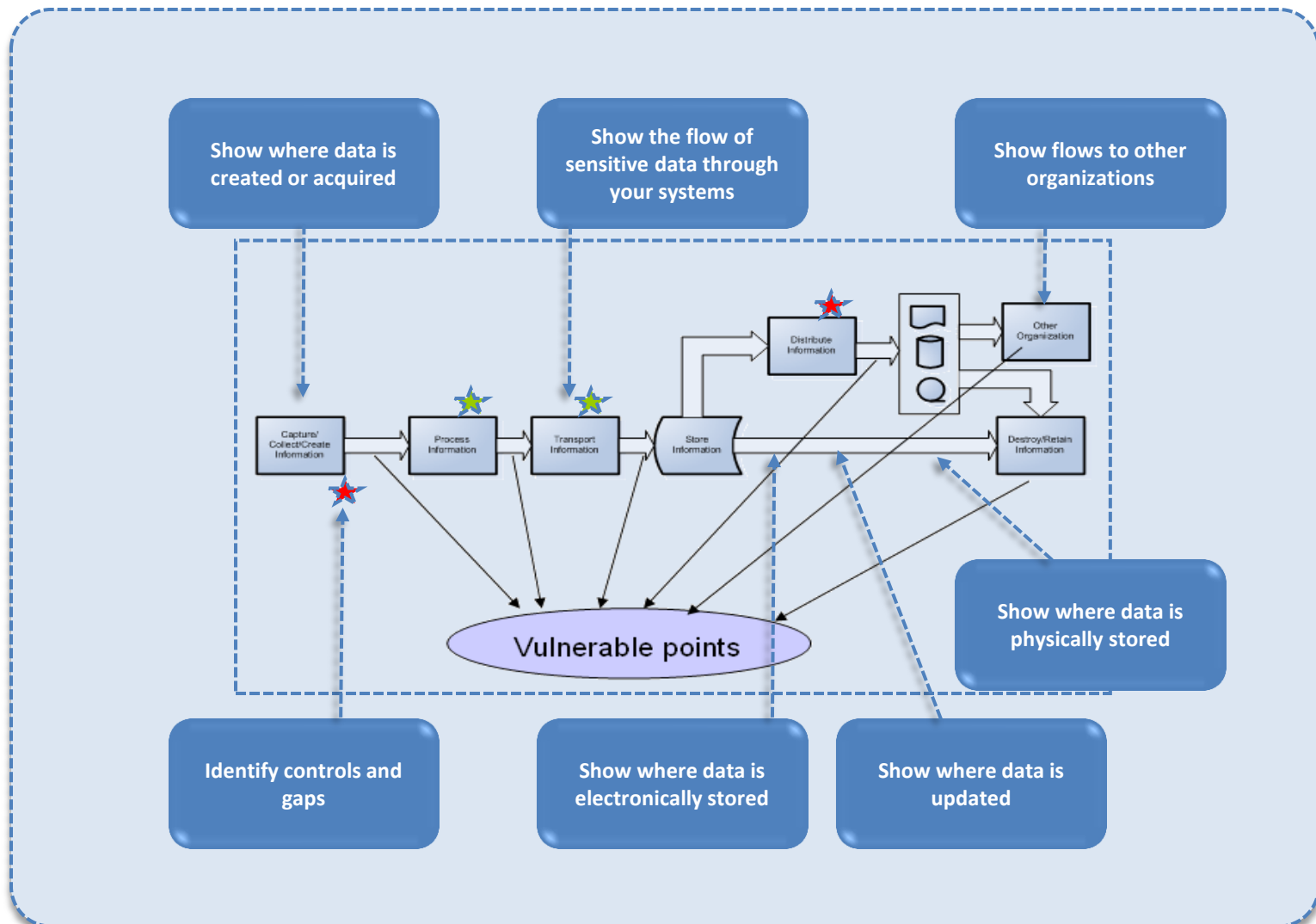
*Email, chat, instant messaging, and other collaboration technologies have introduced more opportunities for the exposure of sensitive information to the outside world.*

## Approach:

- Utilize a data monitoring application to identify potential instances where sensitive information is distributed outside of the in-scope environment
- Identify the specific business processes inadvertently exposing sensitive data through unknowing employees or non-secure technologies



# Data Privacy Assessment - Scoping



# Data Privacy Assessment - Scoping

## Sample Data Map Survey Tool

The screenshot displays the Intuit QuickBase interface for a 'Data Map Survey' application. The left pane shows the 'Add Data Map Survey' form, and the right pane shows the 'List All' report.

**Form Fields:**

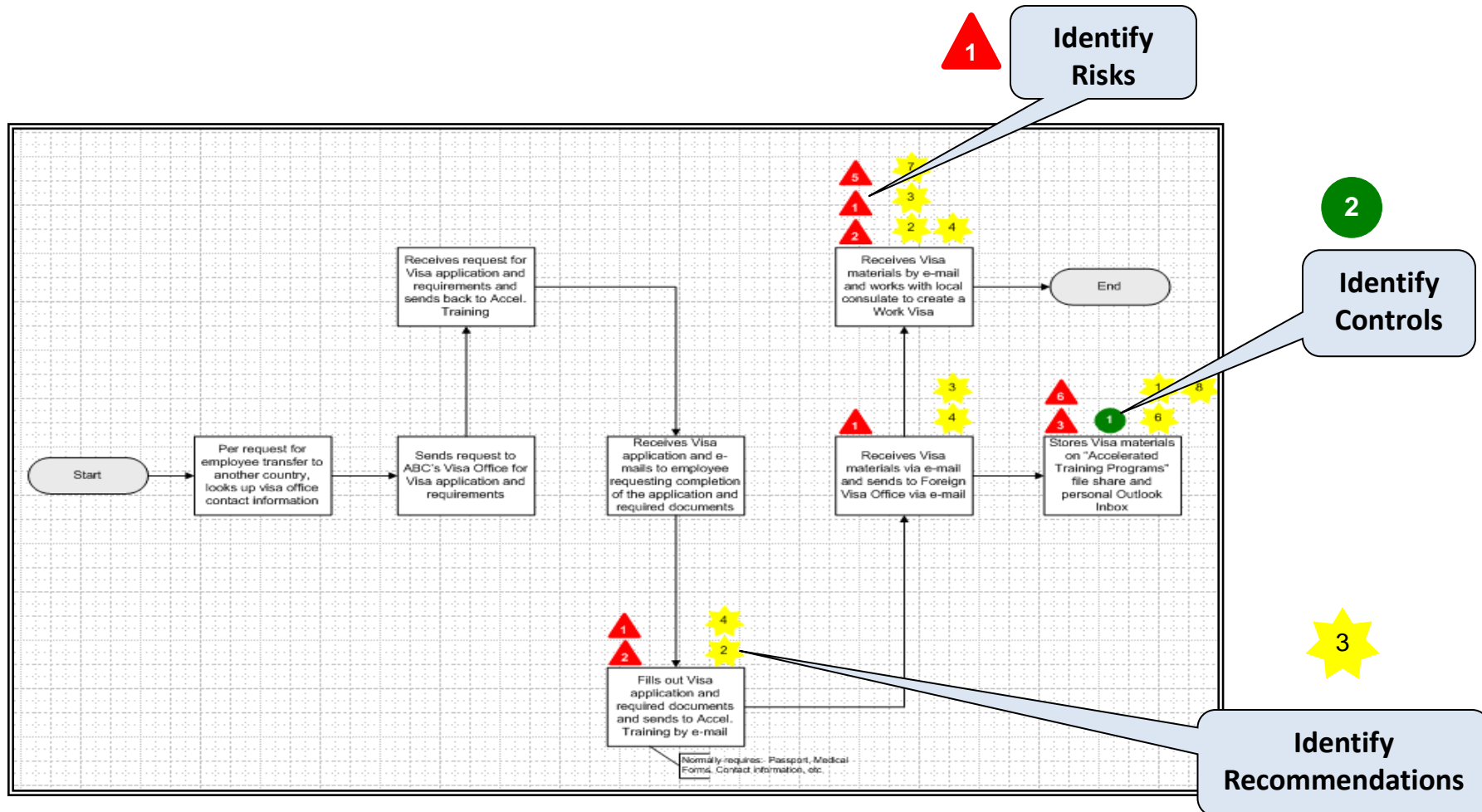
- Name: Jane Smith
- Email: jane.smith@smithworks.com
- Data Type: Data Type 1
- Why is this information collected?: In order to process customer orders for widgets.
- How is this information collected?: Using paper forms that are subsequently hand-keyed into the AS/400 application.
- Where is the information stored locally? On the network?: In file cabinets in accounting as well as the AS/400.
- Who is the data owner?: Mary Lee
- How long is the information kept?: 7 years
- What is the process for erasing or destroying data?: A third party shredding company comes onsite once per month to shred boxes outside their defined retention period. A nightly batch job on the AS/400 deletes data that exceeds retention requirements.

**Report Table:**

1 Data Map Survey Response										All
	Name	Email	Data Type	Why is this information collected?	How is this information collected?	Where is the information stored locally? On the network?	Who is the data owner?	How long is the information kept?	What is the process for erasing or destroying data?	
	Jane Smith	jane.smith@smithworks.com	Data Type 1	In order to process customer orders for widgets.	Using paper forms that are subsequently hand-keyed into the AS/400 application.	In file cabinets in accounting as well as the AS/400.	Mary Lee	7 years	A third party shredding company comes onsite once per month to shred boxes outside their defined retention period. A nightly batch job on the AS/400 deletes data that exceeds retention requirements.	

# Data Privacy Assessment - Scoping

## Sample Data Flow Diagram



# Executing a Data Privacy Assessment

## Phase 2: Design Framework

- Determine in-scope processes and provide insight into how applications process, transfer, and/or store consumer, customer, and employee PII. In addition, examine which vendors and third parties have access to, or store, consumer, customer and employee PII.
- Determine relevant domestic and international privacy laws and regulations.
- Using the AICPA's Generally Accepted Privacy Principles (GAPP) as a baseline, design a framework that involves the 10 Principles, incorporating the specific regulatory requirements identified above.
- With regards to the information security components of the engagement, establish the desired standard by which to benchmark the identified gaps (e.g., COBIT, ISO, NIST, etc.) in alignment with Component 8 of the GAPP framework.



# Data Privacy Assessment – Design Framework

- *Map data elements collected, processed and stored along with business purpose.*
- *Align data elements against regulations and other drivers.*

Category	Element	Graham Leach Bliley Act	Fair Credit Reporting Act	Health Insurance Portability and Accountability	Driver's Privacy Act	Federal Trade Commission Act	The Privacy Act of 1974	The Children's Online Privacy Protection Act	Family Educational Rights and Privacy Act
Names	First Name	X	X	X	X	X	X	X	X
	Middle Name	X	X	X	X	X	X	X	X
	Last Name	X	X	X	X	X	X	X	X
	Initials	X	X	X	X	X	X	X	X
	Aliases	X	X	X	X	X	X	X	
	Mother's Maiden Name	X	X		X	X	X	X	
Personal Likeness	Biometric Data	X		X			X		
	Photograph			X	X				
	Birth Date	X	X	X	X	X	X	X	X
	Gender								
	Race								
	Height			X	X				
	Weight			X	X				
	Eye Color			X	X				
	Hair Color			X	X				
	Blood Type			X					
	Disability Information			X	X				
	Sexual Orientation								
	Marital Status	X	X		X	X	X		
	Digital Signature								
	DNA Profile			X					
	Family Information	X	X	X	X	X	X	X	
	Social Security Number	X	X	X	X	X	X		
	Political Party Affiliation								
	Religious Affiliation								
	Citizenship Records								
	Naturalization Records								
	Alien Registration Records								
Educational and Professional Background	Education History								X
	Employment History						X		
	Military Records						X		
	Certifications/Licenses Earned								X
	Salary History						X		
	Job Performance History						X		

Source: IMF

# Data Privacy Assessment – Design Framework

## *Generally Accepted Privacy Principles (GAPP)*

<b>1. Management</b> <ul style="list-style-type: none"><li>Privacy policies and procedures</li><li>Communication to internal personnel</li><li>Responsibility and accountability</li><li>Review and approval</li><li>Supporting resources and quality of personnel</li></ul>	<b>2. Notice</b> <ul style="list-style-type: none"><li>Communication to individuals of the entity's privacy policies and procedures</li><li>Provision of notice</li><li>Entities and activities covered</li><li>Clear and conspicuous</li></ul>	<b>3. Choice &amp; Consent</b> <ul style="list-style-type: none"><li>Communication to individuals of choices and opt-out rights</li><li>Consequences of denying or withdrawing consent</li><li>Implicit or explicit consent</li></ul>	<b>4. Collection</b> <ul style="list-style-type: none"><li>Types of personal information collected and methods of collection</li><li>Collection from third parties</li></ul>
<b>5. Use &amp; Retention</b> <ul style="list-style-type: none"><li>Use, retention and disposal</li></ul>	<b>6. Access</b> <ul style="list-style-type: none"><li>Confirmation of an individual's identity</li><li>Updating or correcting personal information</li><li>Escalation of complaints and disputes</li></ul>	<b>7. Disclosure to Third Parties</b> <ul style="list-style-type: none"><li>Communication to third parties</li><li>Disclosure and protection of personal information that is shared</li><li>Response to misuse</li></ul>	<b>8. Security</b> <ul style="list-style-type: none"><li>Information security program</li><li>Logical and physical access controls</li><li>Environmental safeguards</li><li>Transmitted personal information</li><li>Testing security safeguards</li></ul>
	<b>9. Quality</b> <ul style="list-style-type: none"><li>Systems and procedures that maintain accurate and complete records</li><li>Relevance of personal information</li></ul>	<b>10. Monitoring &amp; Enforcement</b> <ul style="list-style-type: none"><li>Complaint process</li><li>Dispute resolution and recourse</li><li>Compliance review</li><li>Instances of noncompliance</li></ul>	

# Information Security Evaluation

## *Key tools:*

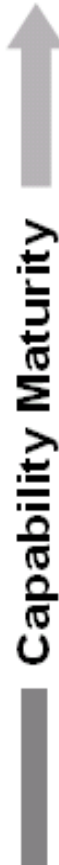
### ▶ **ISO17799/27001:** a security standard with 11 domains

- Security Policy
- Access control
- Security Organization
- Information Systems Acquisition
- Asset management
- Incident Management
- HR Security
- Business continuity
- Physical and Environmental
- Compliance
- Communications and Operations

### ▶ **Capability Maturity Model (CMM):** model to represent process maturity on a 5 tiered scale:

- Initial, Repeatable, Defined, Managed, Optimizing

# Use Capability Model to Evaluate



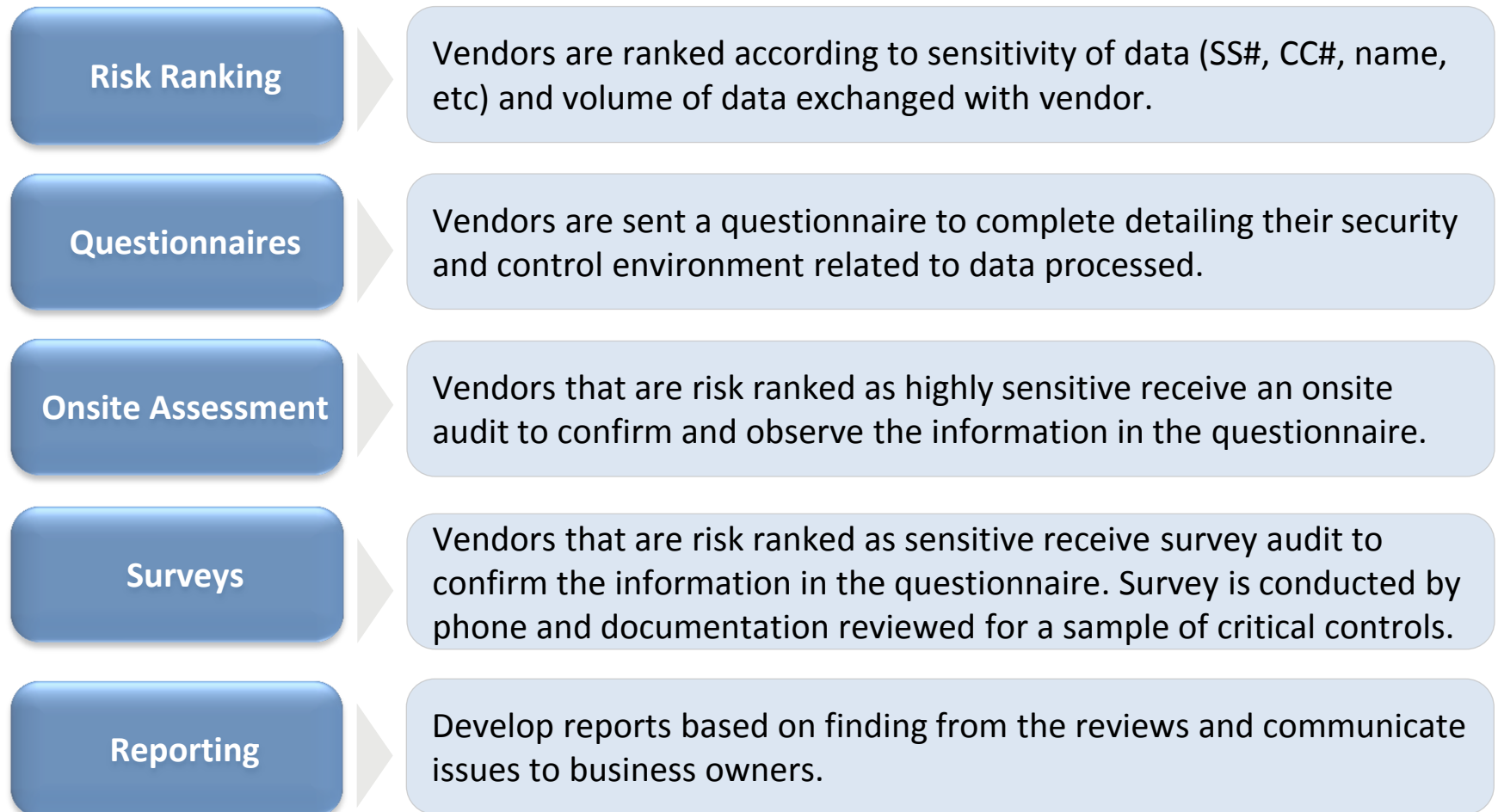
Capability Level	Capability Description
5. Optimizing	<b>CONTINUOUS IMPROVEMENT</b> Continuously improving controls enterprise-wide
4. Managed	<b>QUANTITATIVE</b> Risks managed quantitatively enterprise-wide "Chain of accountability"
3. Defined	<b>QUALITATIVE/QUANTITATIVE</b> Policies, process and standards defined and institutionalized -- "Chain of certification"
2. Repeatable	<b>INTUITIVE</b> Process established and repeating; reliance on people continues -- Controls documentation lacking
1. Initial	<b>AD HOC/CHAOTIC</b> Control is not a priority -- Unstable environment leads to dependency on heroics

# Sample Test Plan

Process Name	Privacy Objective	Control Ref#	Risk	Control Description	Control Type	Control Type	Test Steps	Maturity Levels
Customer Notice	Notice	3.1, 3.2, 9.3, 9.6, 9.7	Inappropriate collection of personal data	The entity's privacy policies address providing notice to individuals.	Preventive	Hybrid	1. Discuss if there is an existing agreement, guideline, or a set of required procedures followed to formally inform the client of Personal Data collection and usage. Are there evaluations performed with the clients on alternatives to the collection of Personal Data (e.g. working at client place instead of collecting the information)? Is the client aware of such alternatives? 2. Understand if there were an existing form and procedure to inform the client or seek client approval before Personal Data is collected or used.	Ad-Hoc maturity level observation: Notice policies and procedures exist informally. Repeatable maturity level observation: Notice provisions exist in privacy policies and procedures but may not cover all aspects and are not fully documented. Defined maturity level observation: Notice provisions in privacy policies cover all relevant aspects and are fully documented.
Customer Access and Complaint Resolution	Access	5.1, 5.2, 9.6, 9.7	Access not given to individuals in order to review and update his/her personal information	Individuals are informed about how they may obtain access to their personal information to review, update and correct that information.	Preventive	Manual	1. Are there documented procedures on how individuals may obtain access to their personal information to review, update and correct the information? 2. Is there evidence of consistent communication informing individuals of these procedures? 3. Are there processes in place to update communications to individuals when changes occurs to access policies and procedures? 4. Is there training and awareness for staff on these procedures?	Ad-Hoc maturity level observation: Individuals may be informed about how they may obtain access to their personal information; however, communications are inconsistent, sporadic and undocumented. Repeatable maturity level observation: Individuals are usually informed about procedures available to them to access their personal information, but this communication process may not cover all aspects and is not fully documented. Update and correction options may not be uniformly communicated. Defined maturity level observation: Individuals are usually informed about procedures available to them to access their personal information, but this communication process may not cover all aspects and is not fully documented. Update and correction options may not be uniformly
Training and Awareness	Access	5.1, 5.2, 5.3, 9.6, 9.7	Access given to individuals in order to review and update their personal information	Individuals are able to determine whether the entity maintains personal information about them and, upon request, may obtain access to their	Preventive	Manual	1. Are there formal documented procedures in place to allow individuals to search for and access their personal information? 2. Have employees been trained	Ad-Hoc maturity level observation: The entity has informal procedures granting individuals access to their information; however, such procedures are not be documented and may not be consistently applied. Repeatable maturity level observation: Some

# Testing Approach

## *Overview of a typical Vendor review process:*



# Executing a Data Privacy Assessment

## Phase 3: Test

- Identify and confirm the applicable standards prior to assessment.
- Assess each in-scope process and provide insight into compliance with applicable privacy standards (e.g., state or country specific privacy laws).
- As necessary, conduct site visits to evaluate the processes and expected control activities that should be operating at in-scope locations.
- Ensure the right questions are addressed and the necessary data elements are collected.
- Consolidate both the specific PII and information security related observations across all of the in-scope locations based on the gaps.



# Testing Approach

*Once there is a customized approach based on the GAPP framework, assess compliance with the applicable data privacy, direct marketing, anti-spam legislation and regulations.*

## **Management**

*What are the risks regarding personal data protection?*

- Roles and Responsibilities
- Risk Assessment

## **Data Privacy**

*Is the organization in compliance with all applicable privacy laws and regulations?*

- Collection and Usage of Personal Data
- Notice, Consent, and Quality
- Knowledge Sharing

## **Information Security**

*Is personal data protected?*

- Access Rights
- Authentication
- Storage
- Transmission
- Backups
- Systems Security
- Network Security
- Information Disposal
- Application Development and Management

## **Physical Security**

*Is personal data physically secure?*

- Physical Security
- Walkthroughs

## **Incident Response**

*Is the organization prepared in the event that a breach occurs?*

- Security Breach Response and Reporting

## **Training and Awareness**

*Is the organization aware of our information protection requirements?*

- Initial Training
- Ongoing Training and Awareness

## **Vendor Management**

*Do business partners securely protect our personal data?*

- Vendor Compliance
- Vendor Agreement and Signoff

*This exercise should focus on where the control design may be weak or nonexistent and will seek to identify improvement opportunities.*

# Data Privacy Assessment Examples

## *GAPP Framework #3 Choice and Consent*

Risk	Examples	Company XYZ Illustrations
No descriptions on the choices available to the individuals nor obtain consent with respect to the collection, use, and disclosure of personal information.	Explicit consent is not consistently obtained prior to collection of sensitive personal information. The retention of personal information is irregular and inconsistent.	<p>HR Policy details that prior to employment with Company XYZ, employment offer packs are prepared to potential candidates for acceptance. Personal information obtained for employment purposes would be consented upon candidate acceptance of offer packs.</p> <p>The Records and Document Management Policy details guidelines for data retention as set out in Appendix 1.</p> <p>For example, the Company XYZ HSEC policy outlines the data management policies governing protection of personal data, including medical and health records:</p> <ul style="list-style-type: none"><li>• policies exist around communication of personal data "personal data will not be communicated to third parties without the employee's explicit written consent."</li><li>• policies exist for data collection and record keeping and storage.</li></ul>

# Data Privacy Assessment Examples

## *GAPP Framework #4 Collection*

Risk	Examples	Company XYZ Illustrations
Inappropriate collection of personal data.	The identification of personal information is irregular, incomplete, inconsistent, and potentially out of date. Personal information is not adequately addressed in the entity's privacy and related security policies and procedures. Personal information may not be differentiated from other information.	<p>The Human Resources - Data Management Policy states:</p> <ul style="list-style-type: none"><li>• Update the master data record in ERP with the required new hire details prior to the employee commencement date and maintain the effective date of any change, including termination.</li><li>• Maintain current and complete personnel records in ERP for all employees and agency contractors.</li></ul> <p>Company XYZ HSEC policy outlines the data management policies governing protection of personal data, including medical and health records.:</p> <ul style="list-style-type: none"><li>• Formal procedures are defined for communication of personal data "personal data will not be communicated to third parties without the employee's explicit written consent."</li><li>• Also, policies exist for data collection, record keeping and storage.</li></ul>

# Data Privacy Assessment Examples

## *GAPP Framework #6 Access*

Risk	Examples	Company XYZ Illustrations
Access for individuals to review and update their personal information is not available.	Users may have incorrect personal information.	<p>User access at Company XYZ is restricted by security roles. Users are provided access as defined by their role which provides the ability to update their account profile and personal information.</p> <p>Also, the Company XYZ Change Management Policy requires that employee master file changes are validated and reviewed and that changes have corresponding source documents providing instructions to make the change. Requests to update personal information are supported by the end user's authorization.</p>

# Data Privacy Assessment Examples

## *GAPP Framework #8 Security*

Risk	Examples	Company XYZ Illustrations
Inadequate safeguarding of IT infrastructure - servers, applications, internet protocol (IP), networks of the company can lead to phishing attacks, data loss and theft.	<p>Personal information is being transmitted via unsecure transmission methods. Employees either do not have the tools necessary, or are unaware of their existence to facilitate secure communication with third parties.</p> <p>Internal/Database vulnerabilities are not scanned regularly leading to loss/misuse of data.</p>	<p>Company XYZ Information Management Policy sets forth many guidelines for securing data and infrastructure, including:</p> <ul style="list-style-type: none"><li>• Information Security Risk Management</li><li>• Physical and Environment Security</li><li>• Storage and Exchange of Information</li><li>• Access Control - End User and Third Party</li></ul>

# Data Privacy Assessment Examples

## *GAPP Framework #8 Security*

Risk	Examples	Company XYZ Illustrations
Authorized users may be granted access to incompatible duties.	Users may have unnecessary or inappropriate access to sensitive data such as personnel records and financial information.	<p>User Access Management is a key part of Company XYZ's SOX Compliance requirements. Key SOX controls around user access includes:</p> <ul style="list-style-type: none"><li>• Quarterly reviews of access.</li><li>• HR administration (onboarding, movements, terminations) and designation of appropriate GJGs.</li><li>• Use of SAP GRC 10.0 - ARA for user access assignment</li><li>• Privileged Access reviews.</li></ul> <p>Additionally, the IT Security Policy details access control requirements for end user access including:</p> <ul style="list-style-type: none"><li>• Grant end-users the minimum level of access privileges required to perform their job function and to prevent segregation of duties conflicts.</li></ul>

# Data Privacy Assessment Examples

## *GAPP Framework #8 Security*

Risk	Examples	Company XYZ Illustrations
Lack of inventory controls on devices and software's in the company can cause numerous security breaches.	Company devices and applications may not be adequately secured, resulting in data leak or being available to outside sources. Networks are not secured to prevent unauthorised intrusion.	<p>The IT Security Policy and the Information Management policy sets forth many guidelines for securing data and infrastructure, including:</p> <ul style="list-style-type: none"><li>• Information Security Risk Management</li><li>• Physical and Environment Security</li><li>• Storage and Exchange of Information</li><li>• Access Control - End User and Third Party</li></ul> <p>In addition, the Information Management - Services policy provides details regarding employees obligations to conform to Company XYZ requirements for use of company devices and applications.</p>



# Data Privacy Assessment Examples

## *GAPP Framework #10 Monitoring & Enforcement*

Risk	Examples	Company XYZ Illustrations
Lack of monitoring and compliance with the company's policies and procedures.	The entity has implemented documented policies and procedures covering all relevant aspects to monitor its privacy controls. Selection of controls to be monitored and frequency with which they are monitored are based on a risk assessment.	<p>Yearly SOX audits are mandated and performed on user Access management, Information Systems Security, and Human Resources Management.</p> <p>In addition, Company XYZ Internal Audit perform testing of Human Resources controls automated controls configured in the ERP - which checks to limit user access to sensitive functions. Manual testing and risk assessments are also performed by Internal Audit teams.</p>

# GAPP Framework CMM

GAPP 73 Criteria	Criteria Description	MATURITY LEVELS				
		Ad Hoc	Repeatable	Defined	Managed	Optimized
<b>Management (14 Criteria)</b>	<b>The entity defines, documents, communicates, and assigns accountability for its privacy policies and procedures.</b>					
Privacy Policies (1.1.0)	The entity defines and documents its privacy policies with respect to notice; choice and consent; collection; use, retention and disposal; access; disclosure to third parties; security for privacy; quality; and monitoring and enforcement.	Some aspects of privacy policies exist informally.	Privacy policies exist but may not be complete, and are not fully documented.	Policies are defined for: notice, choice and consent; collection; use, retention and disposal; access; disclosure; security for privacy; quality; and monitoring and enforcement.	Compliance with privacy policies is monitored and the results of such monitoring are used to reinforce key privacy messages.	Management monitors compliance with policies and procedures concerning personal information. Issues of noncompliance are identified and remedial action taken to ensure compliance in a timely fashion.
Communication to Internal Personnel (1.1.1)	Privacy policies and the consequences of non compliance with such policies are communicated, at least annually, to the entity's internal personnel responsible for collecting, using, retaining and disclosing personal information. Changes in privacy policies are communicated to such personnel shortly after the changes are approved.	Employees may be informed about the entity's privacy policies; however, communications are inconsistent, sporadic and undocumented.	Employees are provided guidance on the entity's privacy policies and procedures through various means; however, formal policies, where they exist, are not complete.	The entity has a process in place to communicate privacy policies and procedures to employees through initial awareness and training sessions and an ongoing communications program.	Privacy policies and the consequences of noncompliance are communicated at least annually; understanding is monitored and assessed.	Changes and improvements to messaging and communications techniques are made in response to periodic assessments and feedback. Changes in privacy policies are communicated to personnel shortly after the changes are approved.
<b>Management (14 Criteria) cont.</b>	<b>The entity defines, documents, communicates, and assigns accountability for its privacy policies and procedures.</b>					
Responsibility and Accountability for Policies (1.1.2)	Responsibility and account ability are assigned to a person or group for developing, documenting, implementing, enforcing, monitoring and updating the entity's privacy policies. The names of such person or group and their responsibilities are communicated to internal personnel.	Management is becoming aware of privacy issues but has not yet identified a key sponsor or assigned responsibility. Privacy issues are addressed reactively.	Management under stands the risks, requirements (including legal, regulatory and industry) and their responsibilities with respect to privacy. There is an understanding that appropriate privacy management is important and needs to be considered.	Defined roles and responsibilities have been developed and assigned to various individuals / groups within the entity and employees are aware of those assignments. The approach to developing privacy policies and procedures is formalized and documented.	Management monitors the assignment of roles and responsibilities to ensure they are being performed, that the appropriate information and materials are developed and that those responsible are communicating effectively. Privacy initiatives have senior management support.	The entity (such as a committee of the board of directors) regularly monitors the processes and assignments of those responsible for privacy and analyzes the progress to determine its effectiveness. Where required, changes and improvements are made in a timely and effective fashion.
Review and Approval (1.2.1)	Privacy policies and procedures, and changes thereto, are reviewed and approved by management.	Reviews are informal and not undertaken on a consistent basis.	Management undertakes periodic review of privacy policies and procedures; however, little guidance has been developed for such reviews.	Management follows a defined process that requires their review and approval of privacy policies and procedures.	The entity has supplemented management review and approval with periodic reviews by both internal and external privacy specialists.	Management's review and approval of privacy policies also include periodic assessments of the privacy program to ensure all changes are warranted, made and approved; if necessary, the approval process will be revised.
Consistency of Privacy Policies and Procedures with Laws and Regulations (1.2.2)	Policies and procedures are reviewed and compared to the requirements of applicable laws and regulations at least annually and when ever changes to such laws and regulations are made. Privacy policies and	Reviews and comparisons with applicable laws and regulations are per formed inconsistently and are incomplete.	Privacy policies and procedures have been reviewed to ensure their compliance with applicable laws and regulations; however, documented guidance is not provided.	A process has been implemented that requires privacy policies to be periodically reviewed and maintained to reflect changes in privacy legislation and regulations; however, there is no proactive review of	Changes to privacy legislation and regulations are reviewed by management and changes are made to the entity's privacy policies and procedures as required. Management may subscribe to a	Management assesses the degree to which changes to legislation are reflected in their privacy policies and made in a timely and effective fashion.

# Executing a Data Privacy Assessment

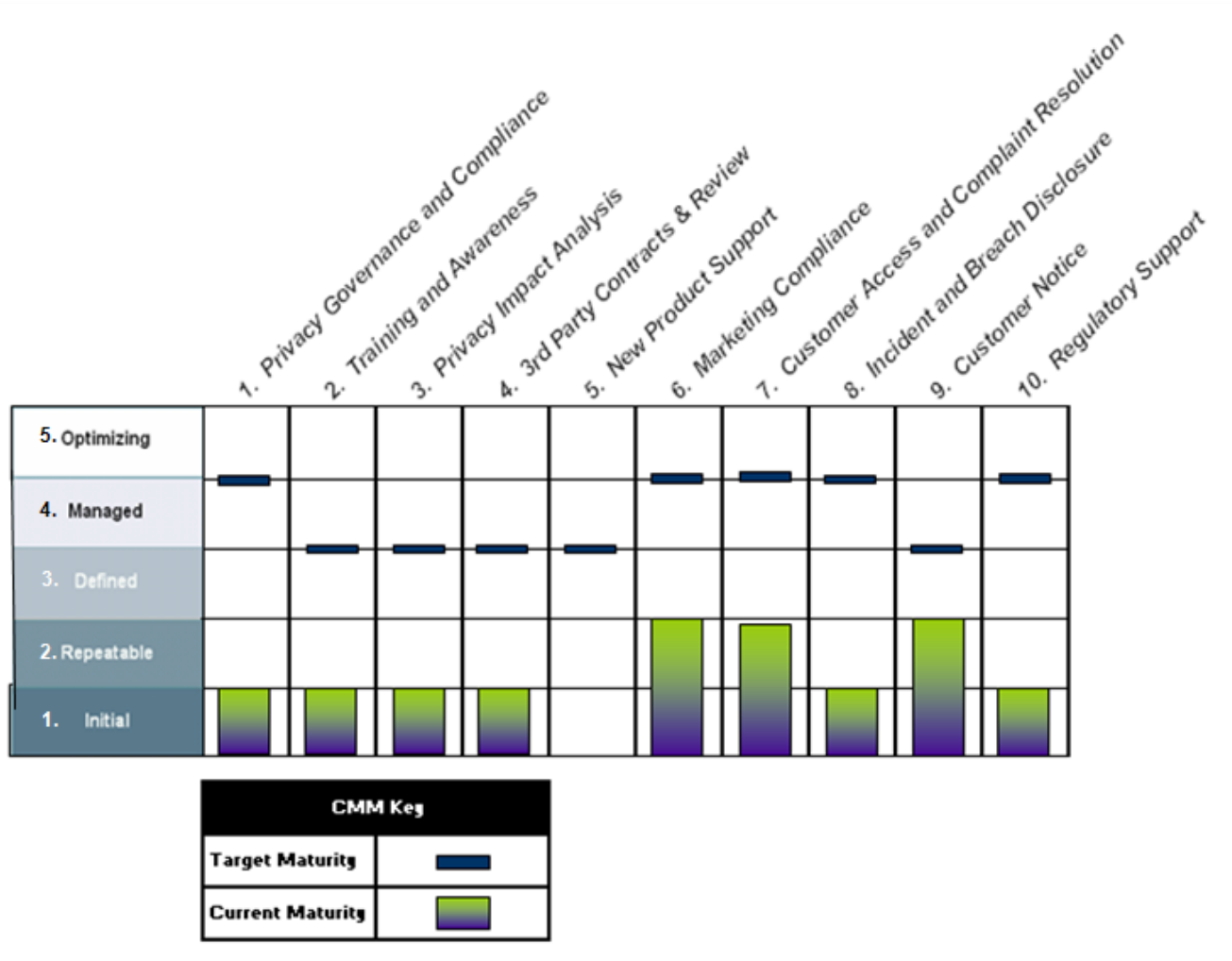
## Phase 4: Report & Recommend

- Complete the documentation of the Gap Assessment (both Privacy/PII and Information Security), organize and catalog all supporting materials including all interviewees, locations visited and documents reviewed.
- Consider remediation recommendations for all gaps with a prioritized approach based on level of risk, estimated cost of implementation, and estimated time to implement. To ensure feasibility, discuss corresponding variables (risk, cost, timing) which are consistent with strategic plan and objectives.
- Finalize those deliverables developed during Phases 1 - 3 and present results to management.
- Knowledge Transfer throughout the assessment.

# Privacy Process Assessment Example

Area	Summary
<b>1. Privacy Governance &amp; Compliance</b>	Policies are issued and compliance with policy is measured. The organization is structured in such a way to support policy development, dissemination and compliance into the organization. The data protection system assures data privacy - personal data protection objectives are defined, known and committed to by the entire organization Data protection issues are prevented and adequately addressed.
<b>2. Training &amp; Awareness</b>	The team receives periodic training for privacy issues. Training is tailored by country such that local requirements are met. Policy and its impact is widely known and implemented.
<b>3. Privacy Impact Analysis (PIA)</b>	A process exists to measure the risk of Personally Identifiable Information (PII) to the organization. PIAs are completed for all new applications and when significant changes occur. A central repository of systems and their PIAs is maintained.
<b>4. 3<sup>rd</sup> Party Access and Agreements</b>	3 <sup>rd</sup> parties where company shares data understands their responsibilities. Legal agreements share common language about data sharing and protection when handling company data. Compliance is periodically verified.
<b>5. New Product Support</b>	Resources exist to support new product development teams to understand and build into their systems and process the necessary and mandated privacy protections.
<b>6. Marketing Compliance</b>	Customers are given effective opt-in and opt-out alternatives in accordance with local rules and regulations that are tracked and maintained in order to respect the customer's right to privacy and right to not receive unsolicited communications.
<b>7. Customer Access &amp; Complaint Resolution</b>	Customers are given access to their data and can complain if they feel company is engaging in unfair data collection and retention practices. Company has a response process where Customer complaints are adequately resolved.
<b>8. Incident Response &amp; Breach Disclosure</b>	This service provides incident response and breach disclosure to company. If an event should occur the procedures for response and communication/escalation is available.
<b>9. Customer Notice</b>	In accordance with local rules and regulations, Customers are notified in a clear and concise manner about how company uses data and assured that company will not use their data for any other purpose than for which it has been collected.
<b>10. Regulatory Support</b>	This service provides a focal point for privacy related regulatory issues. Regulatory privacy audits, inquiry focal point and legal interpretation.

# Assessment of Current Capability



## 5. Summary of Key Lessons

# Privacy Questions Auditors Ask\*

## List of Top 10

- 1 What privacy laws and regulations impact the organization?
- 2 What type of personal information does the organization collect?
- 3 Does the organization have privacy policies and procedures with respect to collection, use, retention, destruction and disclosure of personal information?
- 4 Does the organization have responsibility and accountability assigned for managing a privacy program?
- 5 Does the organization know where all personal information is stored?
- 6 How is personal information protected?
- 7 Is any personal information collected by the organization disclosed to third parties?
- 8 Are employees properly trained in handling privacy issues and concerns?
- 9 Does the organization have adequate resources to develop, implement and maintain an effective privacy program?
- 10 Does the organization complete a periodic assessment to ensure that privacy policies and procedures are being followed?

*\*IIA Global Technology Audit Guide 5 – Managing and Auditing Privacy Risks*



# Typical Mistakes Organizations Make

- Not understanding the risk and cost
- Not funding Information Security
  - What is the value of the information you hold?
  - Do you have more or less manpower than your attackers?
- Information Security reporting to IT Operations
- Trying to do no more than anyone else
- Not having third party validation



***No one else spends on security.***

# Conclusions – Controls to Limit Risks

- Adopt internal privacy policies and practices, post a privacy notice that accurately reflects these policies and practices and comply with them
- Limit personal information kept
  - Don't collect what you don't need
  - Get rid of/depersonalize/anonymize information as soon as you can
  - Track how many records you have
- Encryption of sensitive information
  - File/record encryption
  - Laptop/personal device encryption
- Isolate sensitive systems on network/restrict access
- Two-factor (password + token) remote access
- Block “uncategorized” websites (if not known good, block)
- Breach detection/monitoring
- Incident Response – have plan that considers breach laws

