Deloitte.
德勤

Privacy By Design:
"Privacy smart from the start".

13 June 2012

Peter Koo
Partner, Enterprise Risk Services
Deloitte Touche Tohmatsu

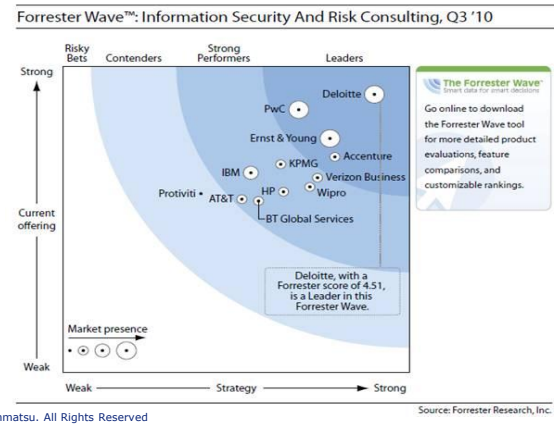
Agenda

1. About Deloitte
2. Privacy Incidents Around the World
3. Privacy Smart from the Start
4. Some Key Privacy Considerations in Design
5. Tools for Privacy Governance
6. Final Thoughts
7. Q & A

Global Leadership in Security and Risk Consulting

"In Forrester's 75-criteria evaluation of information security and risk consulting service providers, we found that Deloitte led the pack because of its maniacal customer focus and deep technical expertise."

Deloitte is the top-ranked Information Security and Risk Consulting firm in Forrester Research's latest report, Information Security and Risk Consulting Wave Q3 2010. The report highlights our strong client focus, technical expertise, and extensive service offerings which set us apart from others in the risk and security consultancy space.



Privacy and Data Loss Incidents

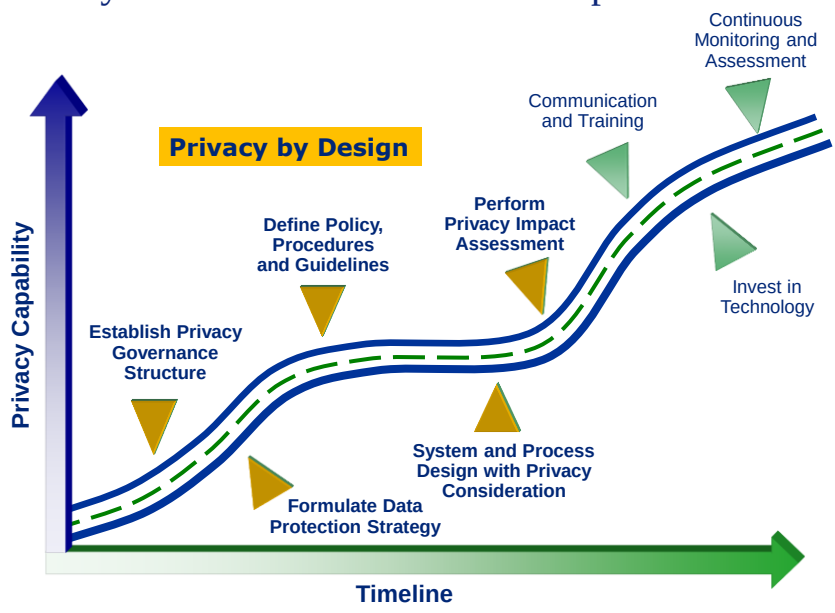
The Seven Foundational Principles

1. ***Proactive*** not Reactive; ***Preventative*** not Remedial
2. Privacy as the ***Default Setting***
3. Privacy ***Embedded*** into Design
4. Full Functionality - ***Positive-Sum***, not Zero-Sum
5. End-to-End Security - ***Full Lifecycle Protection***
6. ***Visibility*** and ***Transparency*** - Keep it ***Open***
7. ***Respect*** for User Privacy - Keep it ***User-Centric***

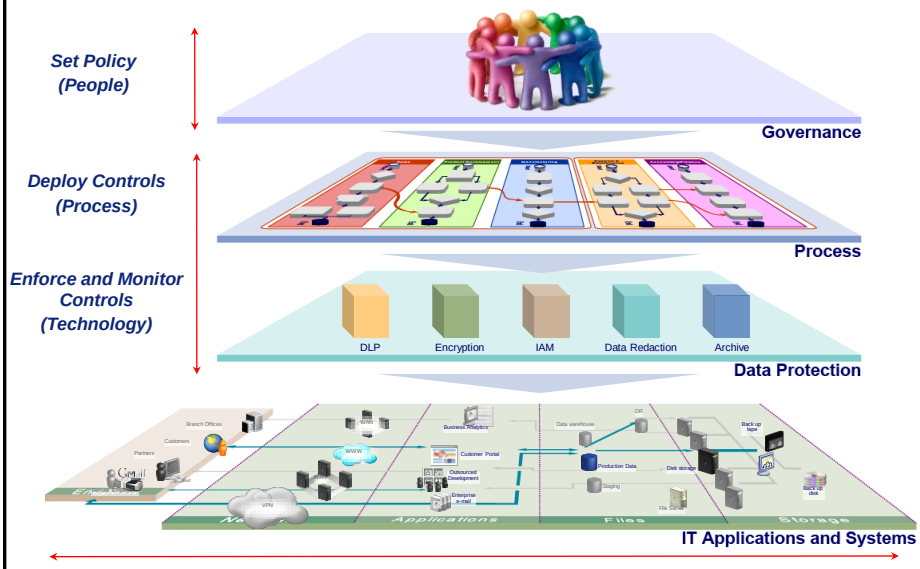
www.ipc.on.ca/images/Resources/7foundationalprinciples.pdf

Privacy Smart from the Start

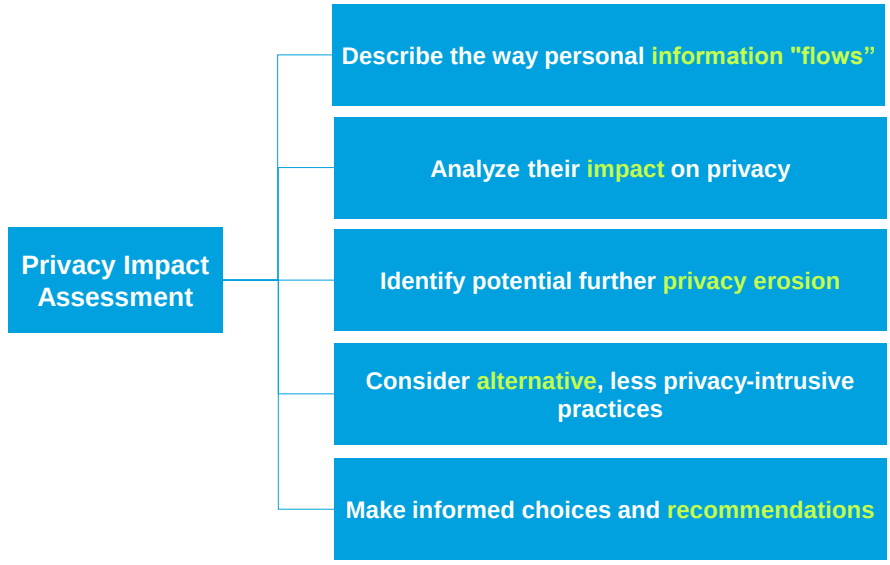
Privacy and Data Protection Roadmap



Implementing the Privacy Protection Framework: Combined top down, bottom up, side-ways..

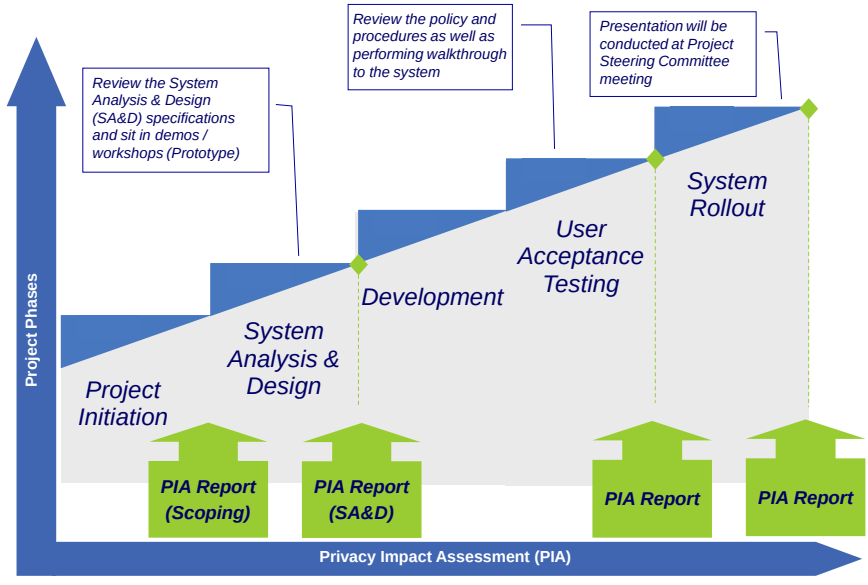


What Does a Privacy Impact Assessment (PIA) Do?



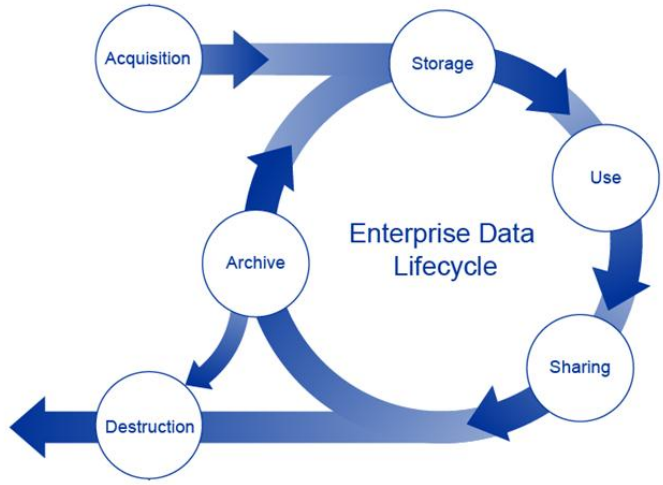
Source: Australia Office of the Privacy Commissioner

PIA in Process and System Design



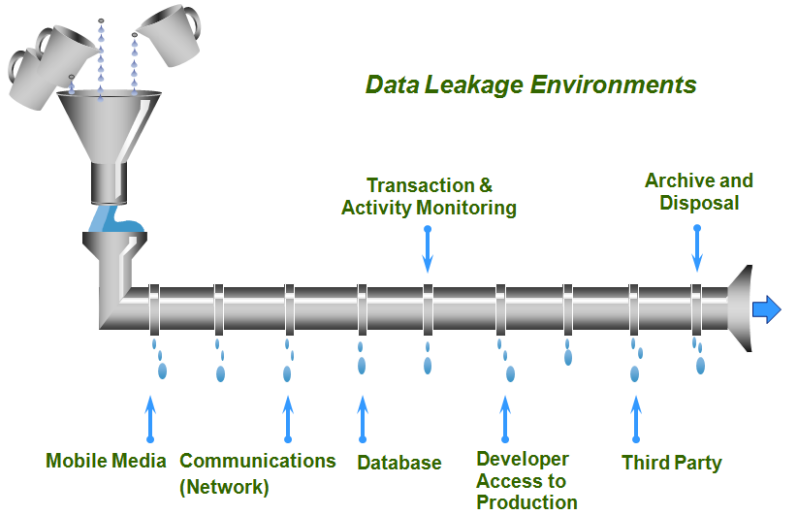
Data Management Life Cycle

The intrinsic and contextual value of data and associated ownership risk vary throughout the data life cycle and throughout the value chain of health plans



Data Leakage Happens

In business, well-intentioned employees simply getting their jobs done may inadvertently put information at risk, sometimes resulting in data leakage.

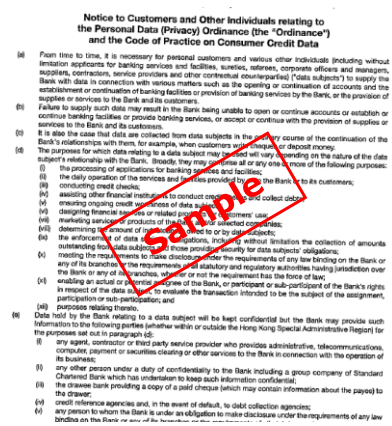


Some Key Privacy Considerations in Design

Collection and Use of Personal Data

Personal Information Collection Statement (PICS)

- Font size?
- Clarity of wordings?
- Understandable?
- Buried the PICS into the T&C?
- "Bundled Consent" for Direct Marketing?



Notice to Customers and Other Individuals relating to the Personal Data (Privacy) Ordinance (the "Ordinance") and the Code of Practice on Consumer Credit Data

(a) From time to time, it is necessary for personal customers and various other individuals (including without limitation applicants for banking services and facilities, sureties, referees, corporate officers and managers, suppliers, contractors, service providers and other contractual counterparties) ("data subjects") to supply the Bank with data in connection with various matters such as the opening or continuation of accounts and the establishment or continuation of banking facilities or provision of banking services by the Bank, or the provision of supplies or services to the Bank and its customers.

(b) Failure to supply such data may result in the Bank being unable to open or continue accounts or establish or continue banking facilities or provide banking services, or accept or continue with the provision of supplies or services to the Bank and its customers.

(c) It is also the case that data are collected from data subjects in the ordinary course of the continuation of the Bank's relationships with them, for example, when customers write cheques, or deposit money.

(d) The purposes for which data relating to a data subject may be used will vary depending on the nature of the data subject's relationship with the Bank. Broadly, they may comprise all or any one or more of the following purposes:

(i) the processing of applications for banking services and facilities;
(ii) the daily operation of the services and facilities provided by the Bank to its customers;
(iii) conducting credit checks;
(iv) assisting other financial institutions to conduct credit checks and collect debts;
(v) ensuring ongoing credit worthiness of data subjects;
(vi) designing financial services or related products for customers' use;
(vii) marketing services or products of the Bank and/or selected companies;
(viii) determining the amount of indebtedness owed to or by data subjects;
(ix) the enforcement of data subjects' obligations, including without limitation the collection of amounts outstanding from data subjects and those providing security for data subjects' obligations;
(x) meeting the requirements to make disclosure under the requirements of any law binding on the Bank or any of its branches or the requirements of any statutory and regulatory authorities having jurisdiction over the Bank or any of its branches, whether or not the requirement has the force of law;
(xi) enabling an actual or potential assignee of the Bank, or participant or sub-participant of the Bank's rights in respect of the data subject, to evaluate the transaction intended to be the subject of the assignment, participation or sub-participation; and
(xii) purposes relating thereto.

(e) Data held by the Bank relating to a data subject will be kept confidential but the Bank may provide such information to the following parties (whether within or outside the Hong Kong Special Administrative Region) for the purposes set out in paragraph (d):

(i) any agent, contractor or third party service provider who provides administrative, telecommunications, computer, payment or securities clearing or other services to the Bank in connection with the operation of its business;
(ii) any other person under a duty of confidentiality to the Bank including a group company of Standard Chartered Bank which has undertaken to keep such information confidential;
(iii) the drawee bank providing a copy of a paid cheque (which may contain information about the payee) to the drawer;
(iv) credit reference agencies and, in the event of default, to debt collection agencies;
(v) any person to whom the Bank is under an obligation to make disclosure under the requirements of any law binding on the Bank or any of its branches or

Ref: Guidance on the Collection and Use of Personal Data in Direct Marketing, Office of the Privacy Commissioner for Personal Data, Hong Kong

Sharing of Personal Data to Third Parties

Data Sharing

- **Clarity of Use of Personal Data?**
  (e.g. any purposes relating thereto)
- **Clarity of third parties?**
  (e.g. other business partners)

"4. The purposes for which data relating to a customer may be used are as follows : ... (vii) researching, designing financial services or related products for customers' use (viii) marketing services or products of the Group and/or selected companies ; (xv) purposes relating thereto.

5. Data held by the Group relating to a customer will be kept confidential but the Group may provide such information to the following parties for the purposes set out in paragraph 4 :-
(i) any agent, contractor, claim adjuster or third party service provider who provides administrative, telecommunications, computer, payment or securities clearing or other services to the Group in connection with the operation of its business; ... (vii) any insurance company or agent, broker, merchant or other business partners of the Group ...

Sample

Ref: Administrative Appeal No. 38 of 2009

Direct Marketing Materials

Direct Marketing Options

- Default setting for receiving marketing materials?

Sample

☐ Do not receive the "new issue" annoucements
If you tick this box you will not receive announcements about new issues of Free Software Magazine being out The content of this field is kept private and will not be shown publicly.

☐ Do not receive the newsletter (fortnightly)
If you tick this, you will never receive the FSM newsletter. The content of this field is kept private and will not be shown publicly.

- Any option for customers to unsubscribe marketing materials?

Sample

This promotional e-mail provides information on SAP's products and services that may be of interest to you. If you would prefer not to receive such e-mails from SAP in the future, please click on the Unsubscribe link.

Ref: Reference: Guidance on the Collection and Use of Personal Data in Direct Marketing, Office of the Privacy Commissioner for Personal Data, Hong Kong

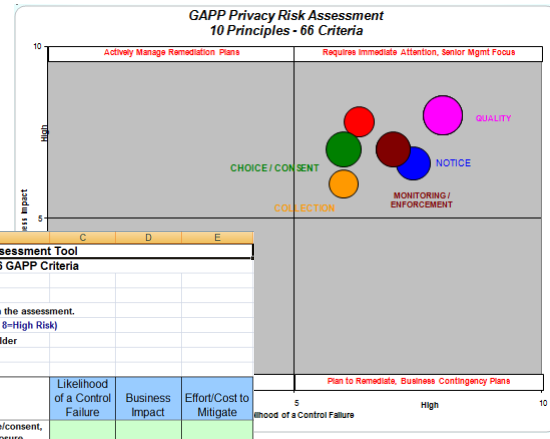
Tools for Privacy Governance

Tools for Privacy Governance

Different tools can be adopted at different levels of the organization to assist in strengthening personal data privacy protection.

Organizational Structure	Relevant Tools
Strategic and Board Level	Privacy Governance Framework / Risk Assessment
Entity Level	Governance Risk and Compliance (GRC)
Business Process Level	Role Based Access Control
Technology and Infrastructure Level	Identity and Access Management (IAM)

AICPA / CICA Privacy Risk Assessment Tool

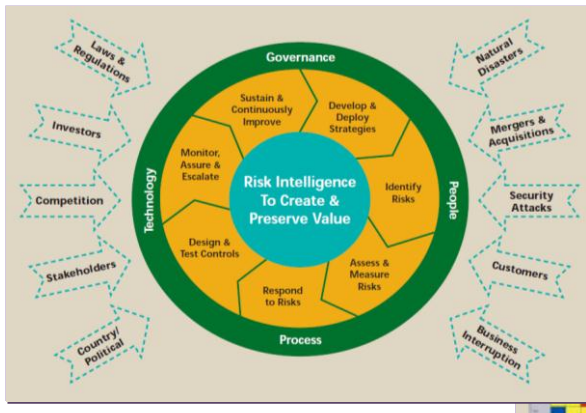


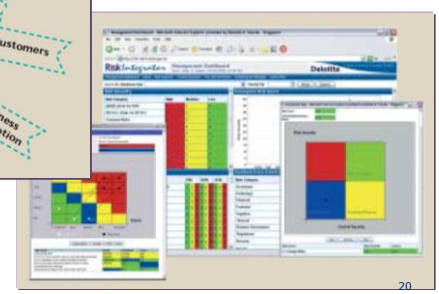
	A	B	C	D	E
		AICPA/CICA Privacy Risk Assessment Tool			
		Scoring Input Template for 66 GAPP Criteria			
	Instructions:				
	1. Use a separate Scoring Input Template for each person participating in the assessment.				
	2. Enter a risk score for each GAPP criteria. (2=Low Risk, 5=Medium Risk, 8=High Risk)				
	3. Copy the completed Scoring Input Template into the AICPA Privacy Folder				
	GAPP - 66 Criteria	**Criteria Description**	Likelihood of a Control Failure	Business Impact	Effort/Cost to Mitigate
	Privacy Policies (1.1.0)	Policies are defined for: notice, choice/consent, collection, use/retention, access, disclosure, security, quality, and monitoring and enforcement.			
	Communications to Internal Personnel (1.1.1)	Privacy policies are communicated at least annually to internal personnel responsible for collecting, using, retaining, and disclosing personal information. Changes in policy are communicated shortly after the changes are approved.			
	Responsibility and Accountability for Policies (1.1.2)	Responsibility is assigned to a person or group for documenting, implementing, enforcing, monitoring, and updating privacy policies.			
	Review and Approval (1.2.1)	Privacy policies and changes thereto are			

Scoring Input Template | Scoring Input Help | Scoring Guidance

Governance Risk and Compliance

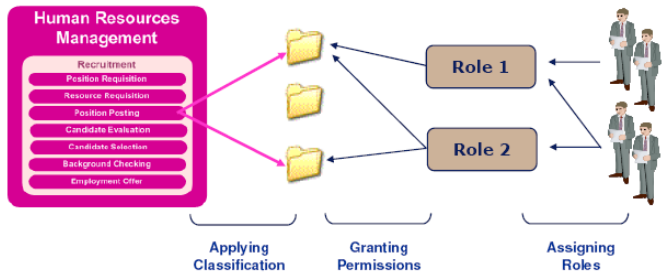
GRC can help you to understand and manage risks across the enterprise and at the business unit as well as risk areas such as strategy, regulatory and operations.





Role Based Access Control

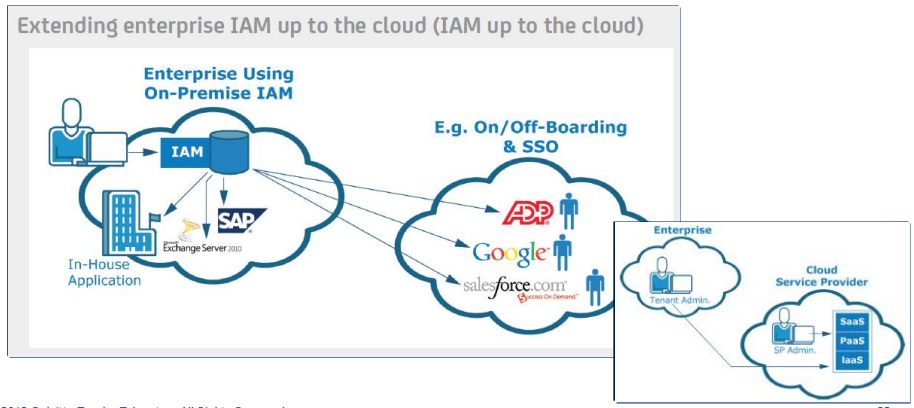
- A role-based access control (RBAC) model is to provide access to roles that create or consume information in the course of a business activity.
- The role is assigned permissions at the business activity level to define the relationship with an information class and related information assets.
- RBAC may be accomplished either through functional capabilities in a business system or through application of metadata and business description rules.



Identity and Access Management

The following IAM functions should be applied or extended to cloud-deployed systems:

- Privileged user management/root user control
- Identity management and role management
- Access management/single sign-on (SSO)
- Log management



Final Thoughts

Key Takeaways…

1. Privacy has become part of our daily life
2. **People, Process and Technology** are the keys to a successful privacy framework
3. **Privacy = key components on both business and IT strategies**
4. **Privacy Assessment** and **Continuous Monitoring** minimizes the privacy risk in system development
5. Protecting data privacy is everyone's responsibility **(Awareness)**
6. **Consult, Consult and Consult**……..

Q&A

Our Contacts

Deloitte Touche Tohmatsu
35/F One Pacific Place
88 Queensway
Hong Kong

Tel: 2852-1600
Fax: 2541-7392

Peter Koo
Partner
Enterprise Risk Services

Tel: 2852-6507
E-mail: petkoo@deloitte.com.hk

Maverick Tam
Director
Enterprise Risk Services

Tel: 2852-5810
E-mail: mtam@deloitte.com.hk

Should you require further information, please feel free to contact us or go to our web site at *www.deloitte.com*


Deloitte.
德勤