



# Risk Management for Privacy Governance Models



## Beyond PIAs

Alec Campbell  
Excela Associates Inc.

*PIPA Conference 2010  
Getting Through the Privacy Jungle*

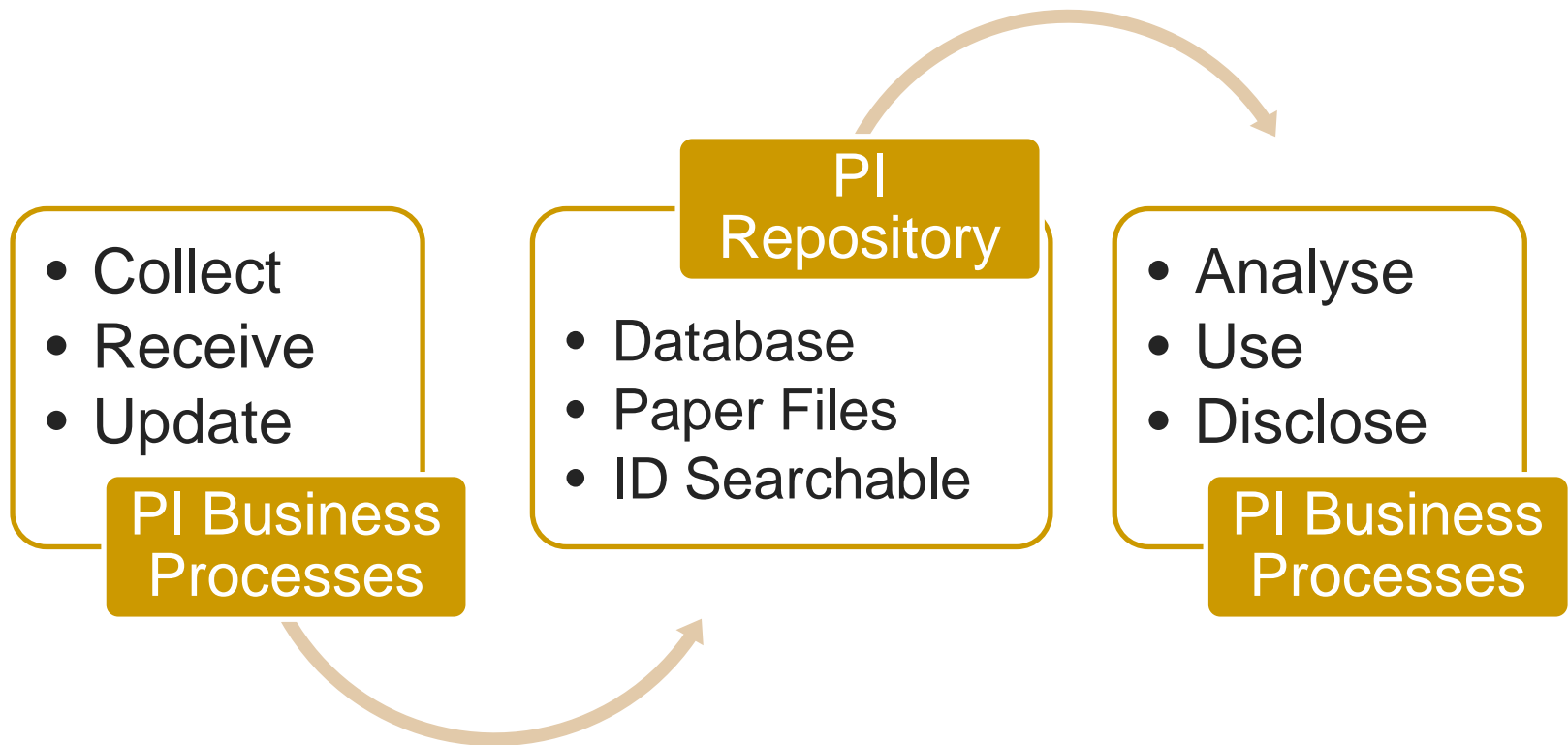
# Objective

- *Describe a privacy risk management process characterized by:*
  - *Increased reliance on policies, design standards and review processes*
  - *Reduced reliance on traditional point-in-time PIAs*
  - *Uses 'compliance checklists' and practice reviews*
  - *Shift from project-based privacy measures to enterprise-wide privacy governance, especially for IT functions*

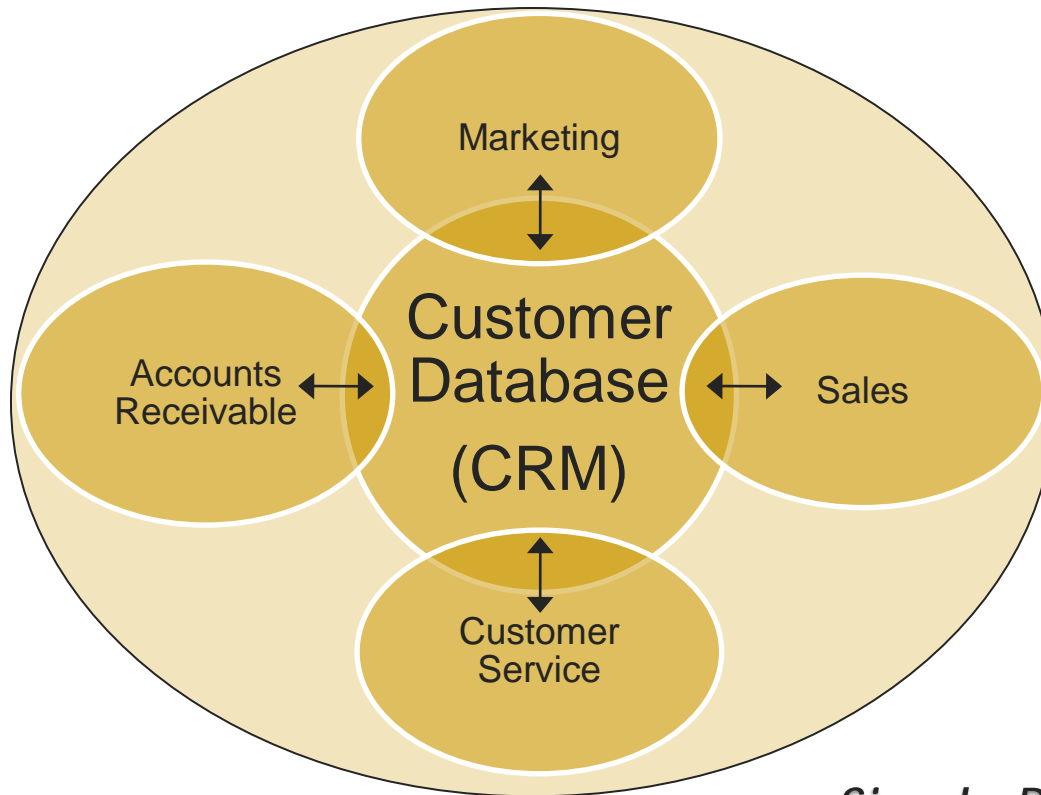
# Definitions

- *Personal Information (PI)*
  - *Any information specifically concerning one or more identifiable individuals, regardless of legislative definitions*
- *PI Standards*
  - *Consistent, enforceable policy, procedures and IT design standards governing the management of PI across the enterprise*
- *Privacy Governance*
  - *Enterprise-wide management of PI based on PI standards*
- *PI Cluster*
  - *A PI repository and its associated business processes*
    - **PI Repository:** *A body of stored personal information in any form, but usually a set of paper files or a database, searchable by one or more personal identifiers*
    - **PI Business Process:** *A set of inter-related procedures intended to satisfy a business need and associated with one or more PI repositories*

# PI Cluster Processes



# PI Cluster Elements



*Simple PI Cluster Example:*  
Single Repository and  
Associated Business Processes

# Privacy Impact Assessments

## ■ *Salient Characteristics*

- *In use since the late 1990s*
- *Currently the most common privacy risk management tool*
- *Effective if done properly, but have disadvantages*
  - *Costly: labour- and expertise-intensive*
  - *Usually project-specific*
  - *Do not scale well from the project to the enterprise level*
  - *Usually undertaken at the start of the project*
  - *Rarely replicated or updated, often out of date*
  - *Often employ no standardized methodology*
  - *Mostly text, making metrics and comparisons difficult*

# Tomorrow: *Beyond PIAs - Compliance Monitoring*

- *Multi-stage review process – concentrates greatest effort on greatest risk*
  - *Comprehensive PIA only when indicated by checklist*
    - *Confirms and mitigates problems, does not identify them*
- *Provides basic risk assessment for ALL projects*
  - *Compliance checklists easy enough to be mandatory*
- *Ongoing process – not just point in time*
  - *Supplement checklists & PIAs with privacy practice reviews and audits*

# Beyond PIAs: Compliance Monitoring

## ■ *Implementation:*

- *PI Standards*
  - *Privacy policies, procedures to establish enterprise privacy 'culture'*
  - *Privacy (& security) design standards for IT applications and systems*
- *Enterprise privacy review to establish baseline (optional)*
- *Compliance checklists to assess all PI Clusters and new projects*
- *Regular privacy practice reviews to ensure ongoing compliance with PI Standards or for known problem areas (e.g., following a minor breach)*
- *Periodic external privacy audits of selected PI Clusters, or for known problem areas (e.g., following a major breach)*



# Phase 1: *Develop PI Standards*

## *Privacy Policy*

- *Mandatory privacy practices, internal to the enterprise*
  - *NOT a communications instrument*
- *Separate from security policy (but dependent on it)*
  - *Privacy confused with security, especially in IT*
- *Suggested elements:*
  - *Address each CSA Model Code privacy principle*
  - *State executive commitment to privacy*
  - *State major exceptions to policy (legal requirements, etc.)*

# Phase 1: *Develop PI Standards*

## *Privacy Design Standards*

- *Privacy feature specifications for:*
  - *IT Applications*
  - *IT services & service providers (including cloud services)*
    - *Link to contractual provisions*
  - *PI Clusters*
    - *PI repositories*
    - *Business processes*
- *Cross reference or embed security requirements*

# Phase 2: *Develop the Compliance Checklist*

- *Paper checklists are a last resort. Distributable electronic questionnaires (such as spreadsheets) are better. Online questionnaires or applications are best.*
  - *ISSUES: Ease of completion, ease of aggregation, risk metrics, support for enterprise performance measures, automated response features (to suggest mitigation measures)*
- *Multiple choice except for basic description items*
- *Based on PI standards and applicable legislation*
- *Include objective measures to trigger a comprehensive PIA*
- *Revise as necessary after the enterprise privacy review*
- *(PIA template out of scope for today)*

# Phase 2: Privacy Checklist Examples

- *Bell Canada – spreadsheet checklist with risk metrics*
  - *Memorial University (<http://www.mun.ca/iapp/resources>)*
  - *Government of Ontario*  
*(<http://www.accessandprivacy.gov.on.ca/english/pub/index.html>)*
- *Agiliance – privacy risk management software*
  - *<http://www.agiliance.com/solutions/privacy.html>*
- *Govt of Alberta – Privacy Planning Tool*
  - *Online checklist with semi-automated responses*
  - *Available to employees only*

# Phase 3: Enterprise Privacy Review

- *Optional but recommended*
- *Privacy checklists for all major PI Clusters*
  - *Comprehensive PIAs of PI Clusters only if indicated by risk thresholds; conducted separately from privacy review*
- *At enterprise level, review:*
  - *Privacy & security policies & procedures*
  - *Privacy provisions in contracts & agreements*
  - *Existing PI standards*
    - *Especially IT design standards (privacy architecture)*
    - *Features required of PI Clusters for privacy compliance*
  - *Security standards*
- *Fill the gaps as necessary*
  - *Including compliance checklist revisions*

# Phase 4: *Implement the Compliance Checklist*

- *Required of all new or changed data repositories and business processes, and other projects*
- *Completed by a knowledgeable project manager(s) or middle manager(s), NOT by the privacy officer*
  - *Accountability must rest with responsible business unit(s)*
- *Reviewed by the PO, who decides whether a comprehensive PIA is required*
  - *Decision supported by checklist metrics*

# Phase 5: Comprehensive PIA

- *Based on template*
- *If determined necessary by PO based on checklist results*
- *Focused on known areas of major privacy risk*

# Phase 6: Privacy Practice Reviews

- *Do a sample of PI Clusters each year*
- *Ideally, every PI Cluster would have a compliance review every year or two, depending on the number of PI Clusters.*
- *Non-PI Cluster practice reviews as necessary or indicated*
  - *E.g., breaches, otherwise identified privacy risks*
- *Uses compliance checklist, completed by privacy officer in consultation with PI Cluster staff*
  - *Checklist may be expanded for privacy reviews*
- *Comprehensive PIAs follow*
  - *If indicated by risk thresholds*

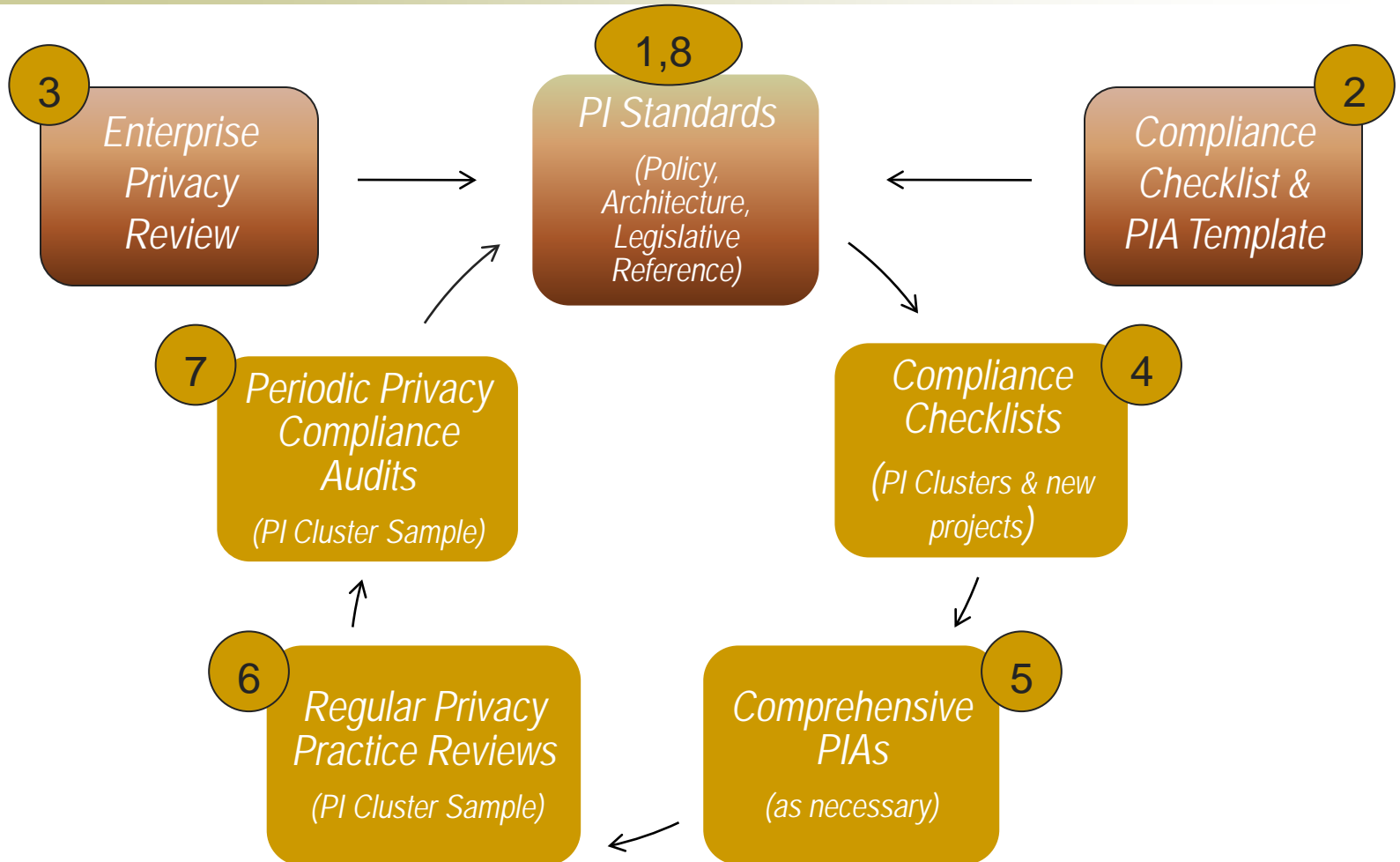
# Phase 7: Privacy Compliance Audits

- *Important to have periodic external assessment, especially where there are potential compliance or liability risks*
- *Select a sample of one or more critical or high risk PI Clusters*
- *Because of time and effort involved in an audit, not every PI Cluster will be audited in a large enterprise*
- *Should cover both privacy and information security*
- *Use established audit standards and qualified auditors*
  - *For privacy audit, GAPP is a good standard; several standards available for security audits*

# Phase 8: Revise PI Standards

- *Revise as necessary based on experience with other stages of process*
- *Training and awareness measures required whenever major changes are made*
- *Ensure all new employees and contractors are familiar with PI Standards.*

# Recap: PI Standards Compliance Monitoring



# Compliance Monitoring Advantages

## ■ Advantages

- *Based on consistent, enterprise PI standards*
- *Focused effort on high risk areas – PI Clusters*
- *Checklists are easy enough to make mandatory for all projects*
- *Ongoing process – not point in time*
- *Scalable project to enterprise via PI Standards and PI Cluster focus*
- *Better risk management than traditional PIAs*
- *Same or lower risk management costs after initial investment*

## ■ Disadvantages

- *Initial investment*
  - *Development of PI standards , compliance checklist, PIA template*
  - *Enterprise privacy review (optional)*

# Questions?

Alec Campbell  
President, Excela Associates Inc.  
Edmonton, AB, Canada

[alec@excela.ca](mailto:alec@excela.ca)

780-945-0123

[www.excela.ca](http://www.excela.ca)