PIAs, Practice Reviews and Audits

From Privacy Risk Management to Privacy Governance

Alec Campbell

Objective

- *Describe a privacy management process characterized by:*
  - *Increased reliance on policies, standards and review processes*
  - *Reduced reliance on traditional point-in-time PIAs*
  - *Increased reliance on 'compliance checklists' and practice reviews*
  - *Shift from privacy risk management to privacy governance*

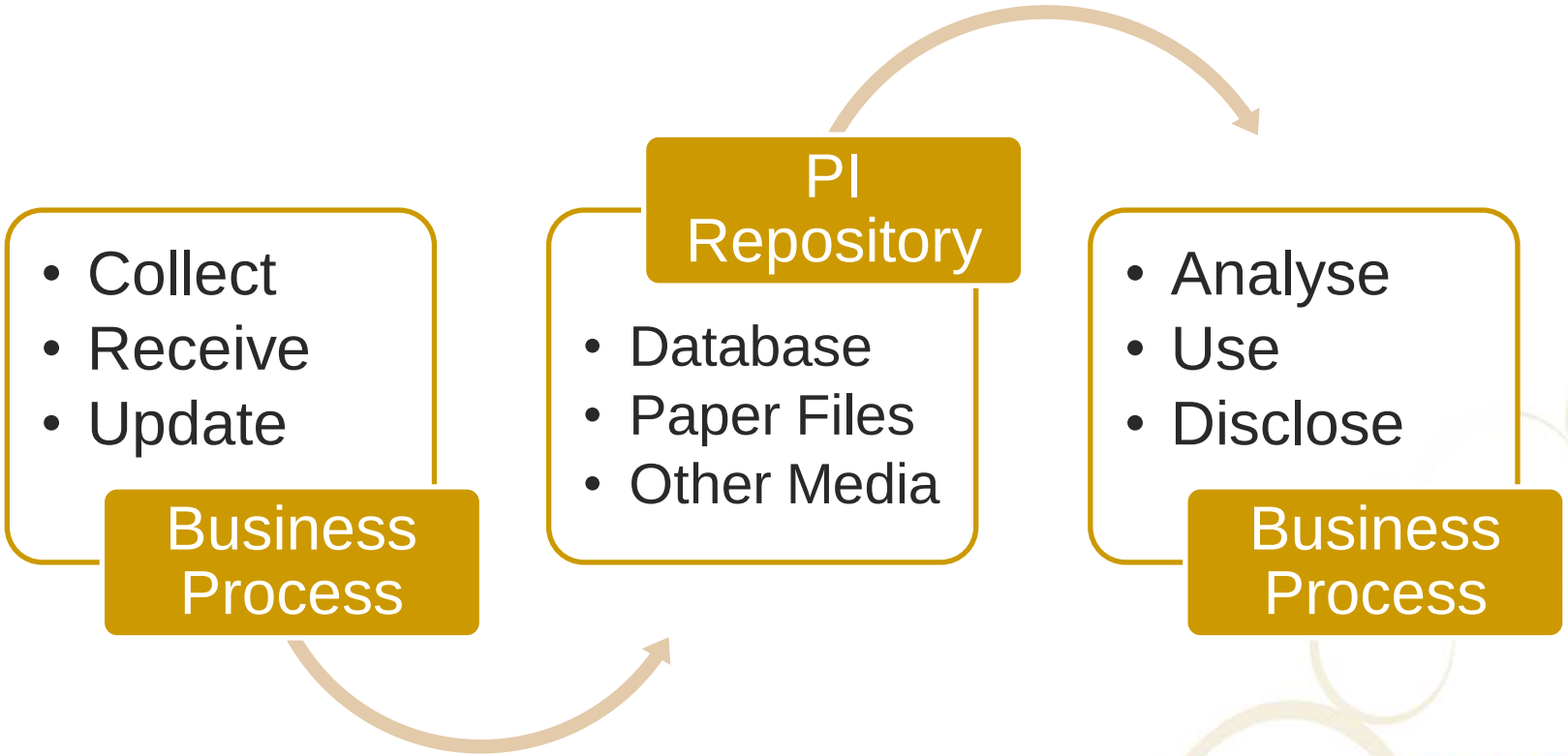
Agenda

- *PI repositories and business processes*
- *PIAs today*
- *Alternative PIA approaches*
  - *Multi-stage PIAs, checklists and automation*
- *Implementation in a privacy governance context*

Definitions

- *Personal information (PI)*
  - *Any recorded information about an identifiable individual.*
- *PI repositories and business processes (RBPs)*
  - **Repository***: A body of stored personal information in any form, but usually either a set of paper files or a database containing PI*
  - **Business process***: A set of inter-related actions intended to satisfy a business need, which supports or is supported by one or more PI repositories*
- *Privacy impact assessment (PIA)*
  - *Formal, recorded assessment of privacy risk and measures*

PI Repositories and Business Processes (RPBs)



Privacy Impact Assessments

- *Salient Characteristics*
  - *Currently the most common privacy risk management tool*
  - *In use since the late 1990s*
  - *Effective if done properly, but*
    - *Usually project-specific*
    - *Usually undertaken only at the start of the project*
    - *Rarely replicated or updated*
    - *Point in time*
    - *Labour- and expertise-intensive (costly)*
    - *No standardized methodology*

An Alternative Approach to PIAs

- *Two-stage PIA*
  - *Compliance checklist*
    - *Multiple choice*
    - *Completed by knowledgeable RBP manager in a day or less*
    - *Assesses compliance with specific aspects of applicable legislation, policy & privacy design standards*
    - *Reviewed by privacy officer*
    - *Universal; required for all new or changed RBP's*
  - *Comprehensive PIA*
    - *Similar to traditional PIA but does not duplicate checklist content*
    - *Undertaken only if indicated by checklist & PO review*

An Alternative Approach to PIAs: Privacy Checklist Examples

- *Govt of Alberta – semi-automated online checklist*
  - *Available to employees only*
- *Bell Canada – spreadsheet checklist with risk metrics*
  - *Memorial University (http://www.mun.ca/iapp/resources)*
- *Agiliance – privacy risk management software*
  - *http://www.agiliance.com/solutions/privacy.html*

From Risk Management to Governance

- *Enterprise PIA to establish baseline*
- *Privacy and security policies & procedures to establish enterprise direction*
- *Privacy & security design standards for PI RBP's*
- *Staged processes to assess all new PI RBP's*
- *Regular privacy practice reviews to ensure ongoing compliance with legislation, policy and design standards*
- *Periodic external privacy and security audits of selected RBP's*

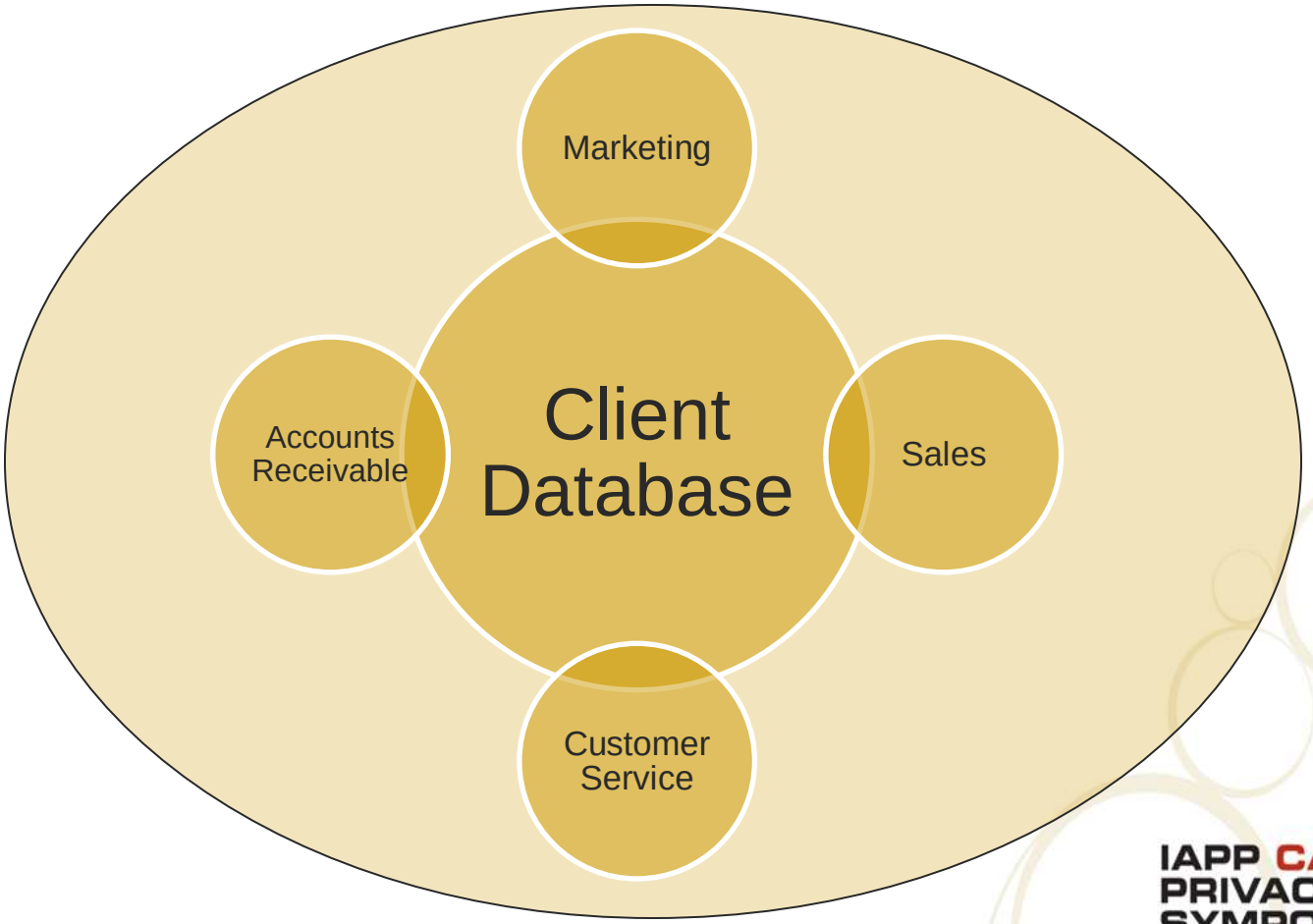
Phase 1: Developing the Compliance Checklist

- *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*
- *Multiple choice except for basic description items*
- *Based on legislation, privacy policy and privacy design standards, in that order.*
- *Include objective measures to trigger a comprehensive PIA*
- *Revise as necessary after the enterprise PIA*

Phase 2: Enterprise PIA

- *Privacy checklists for all RBPs*
  - *Comprehensive PIAs of RBPs only if indicated by risk thresholds; conducted separately from enterprise PIA*
- *At enterprise level, review:*
  - *Privacy & security policies & procedures*
  - *Privacy provisions in contracts & agreements*
  - *Privacy design standards*
    - *Features required of RBPs for privacy compliance*
  - *Security standards*
- *Fill the gaps as necessary*
  - *Including compliance checklist revisions*

Focus on PI Repositories and Business Processes (RBPs)



Phase 3: Privacy Compliance Checklists

- *Required of all new or changed data repositories and business processes, whether or not they are expected to involve PI*
- *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*

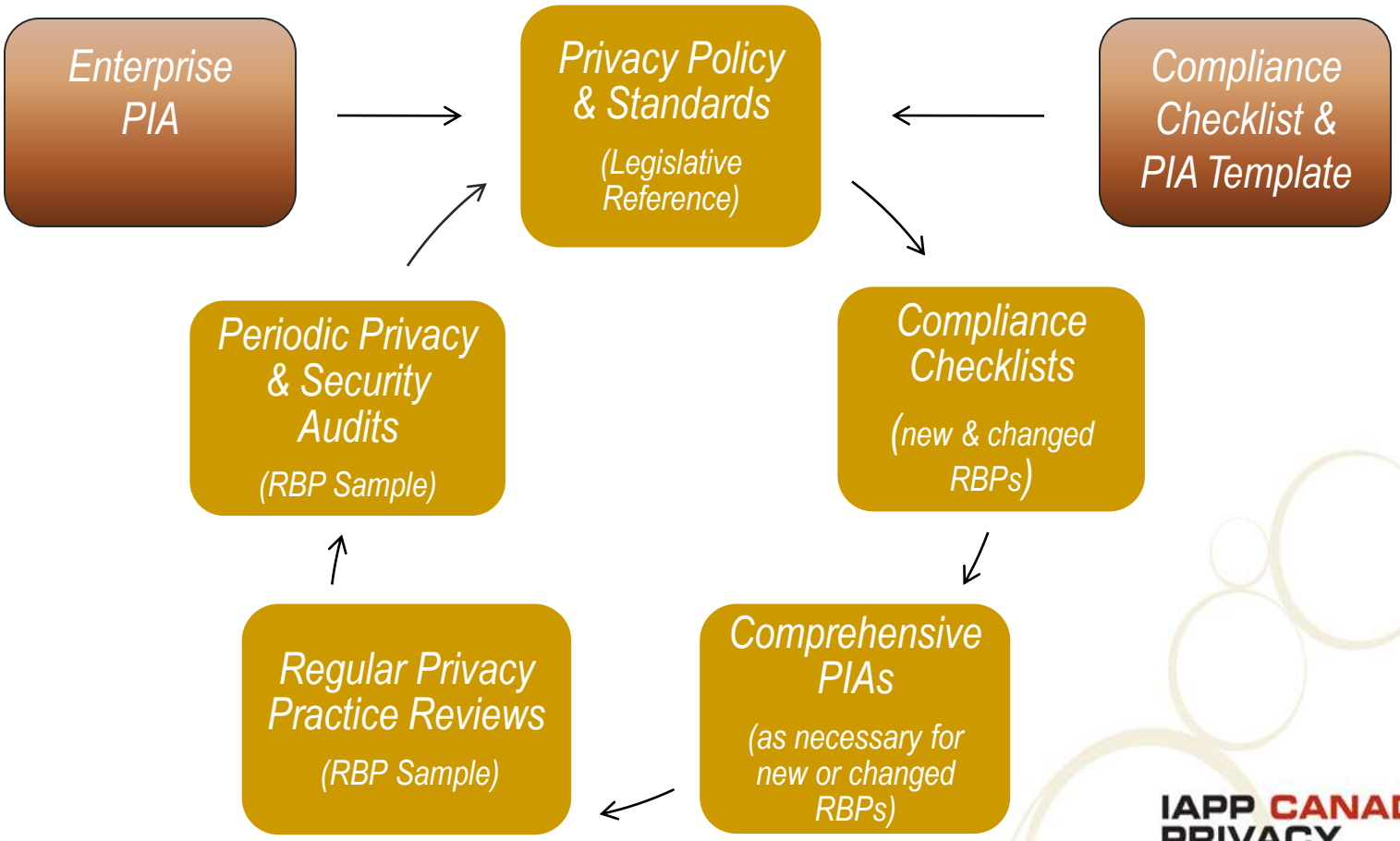
Phase 4: Privacy Practice Reviews

- *Uses compliance checklist, but completed by privacy officer*
- *Done in consultation with RBP staff*
- *Do a sample of RBPs each year*
- *Ideally, every RBP would have a compliance review every year or two, depending on the number of RBPs.*

Phase 5: Privacy and Security Audits

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

Privacy Governance Cycle



Questions?

Alec Campbell

President, Excela Associates Inc.

Edmonton, AB, Canada

alec@excela.info

780-945-0123

www.excela.ca