Office of the Chief Information
and Privacy Officer

Privacy Impact Assessments
101: The Basics

Tracy Ann Kosa, Privacy Impact Assessment Specialist

Access and Privacy Workshop
Sharing New Perspectives
October 6-7, 2007

Objectives

- **To discuss and learn, as practitioners, about the PIA and how to make it work**
  - A PIA is part of a privacy program
  - A PIA isn't one person's job
  - A PIA should identify the story

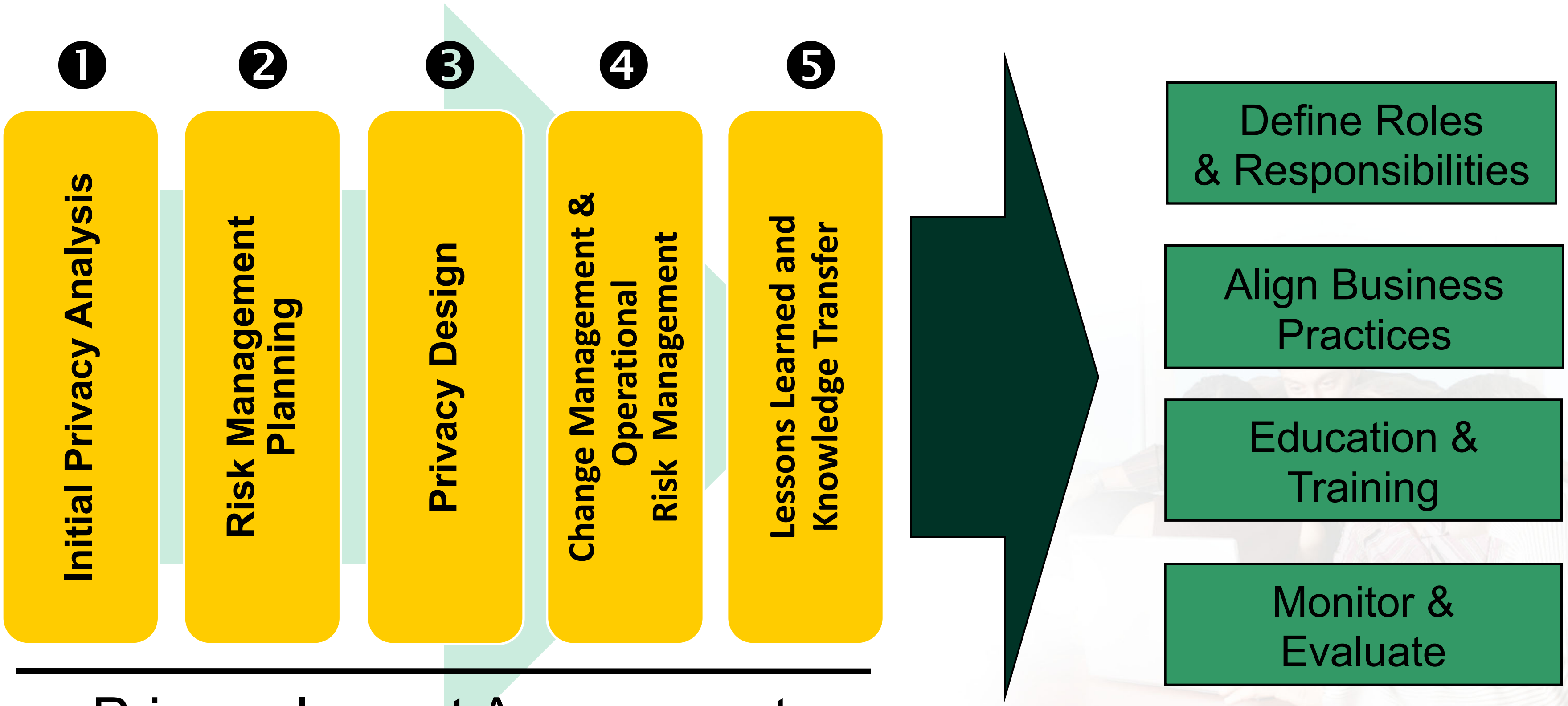
Overview

- Part 1: What is a PIA
- Part 2: How do you do a PIA

Privacy By Design

Program/System Under Development

Program/System Operational



Privacy Impact Assessment

How Did We Get Here

- **Why do you need to know what a PIA is?**
  - New job?
  - New project?
  - New responsibilities?

What Is A PIA

- A PIA is a tool for evaluating new systems for impacts on privacy of personal information
- The PIA determines whether basic privacy requirements have been met in (a) new technologies, (b) information systems, and / or (c) proposed programs
- A PIA measures technical compliance with privacy legislation
- A PIA identifies privacy compliance issues, risks, mitigation strategies and recommendations

What That Means

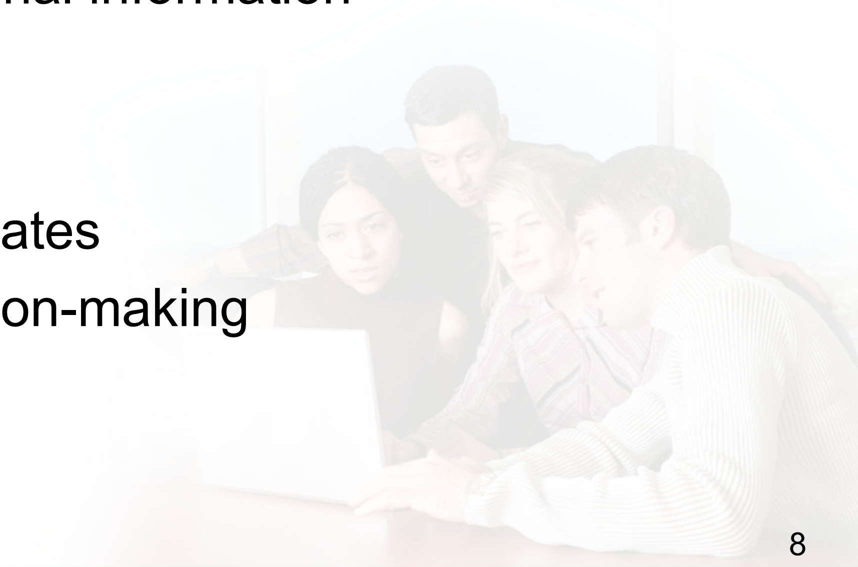
- A PIA is a Process

- A PIA is a Deliverable

PIA Outputs

- **Definition:**
  - The PIA **describes** business processes, technological components, personal information flows, and controls in a system that contains personal information

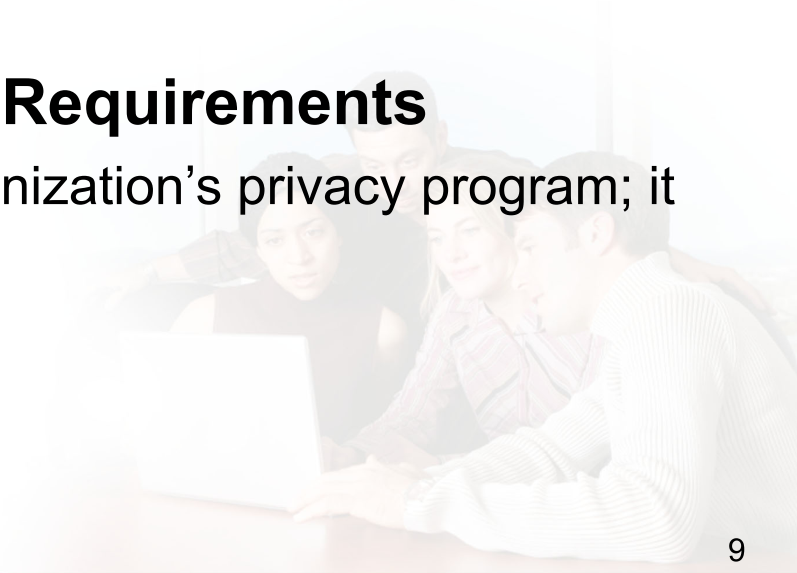
- **In other words, the PIA**
  - **Process** informs and educates
  - **Document** supports decision-making



A PIA Is Not

- **A Threat Risk Assessment (TRA)**
  - PIA and TRA can complement each other
  - Privacy = Data, Security = Infrastructure

- **The Sum Total of Privacy Requirements**
  - The PIA is the part of an organization’s privacy program; it tells the one story

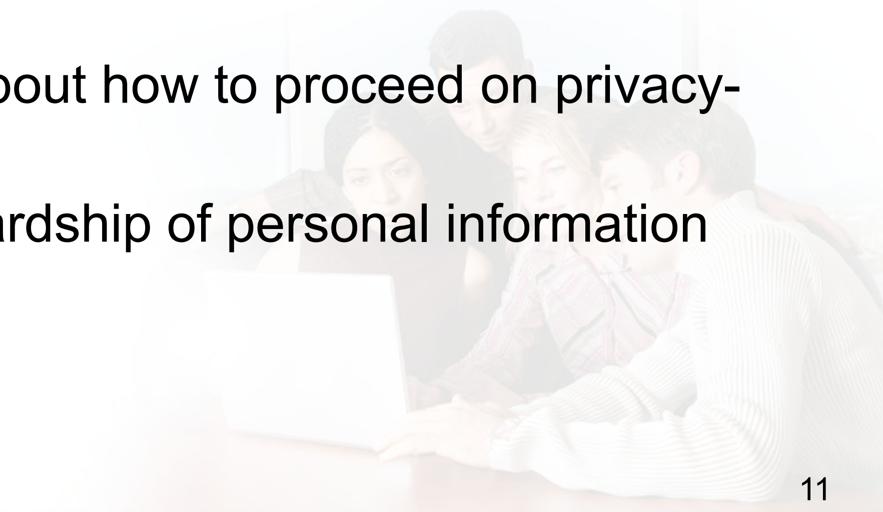


Why Do A PIA?

- **Privacy Legislation**
- **Corporate Directives**
  - I&IT Directive
  - I&IT Security Directive
  - Procurement Directive
- **Corporate Standards**
  - GO ITS 54 (SDLC)
  - GO ITS 23.1
  - Corporate Operating Policy on Internet Tracking Technologies
  - Electronic Service Delivery Privacy Standard
  - Threat / Risk Assessment Guidelines
- **Gateway Review Process**
- **Architecture Review Process**

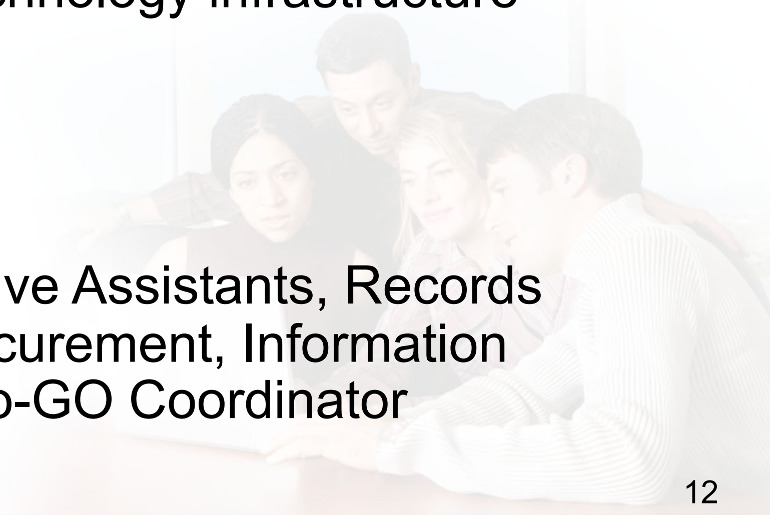
Why Do A PIA?

- **Practicing Good Privacy**
  - Documentation and evidence of what privacy compliance already exists
  - Identify privacy problems and potential issues before a breach or complaint
  - Inform the organization about how to proceed on privacy-related activities
  - Demonstrate active stewardship of personal information



Who Should Do A PIA?

- **The Ideal**
  - Total knowledge about the project being addressed
  - Comprehensive understanding of all privacy legislation, regulations and best practices
  - Complete understanding of technology infrastructure

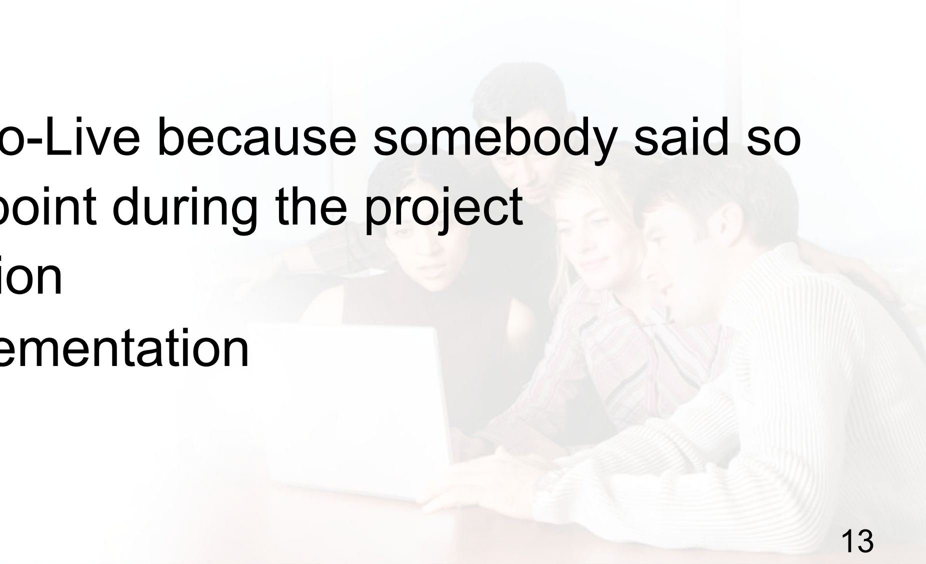


- **The Reality**
  - Us, and …
  - Project Managers, Administrative Assistants, Records Officers, Archivists, Legal, Procurement, Information Security, FOI Coordinator / Info-GO Coordinator

When Should A PIA Start and End?

- **The Ideal**
  - Start: PIA builds on privacy analysis which begins on Day 1
  - End: when the project closure activities are completed

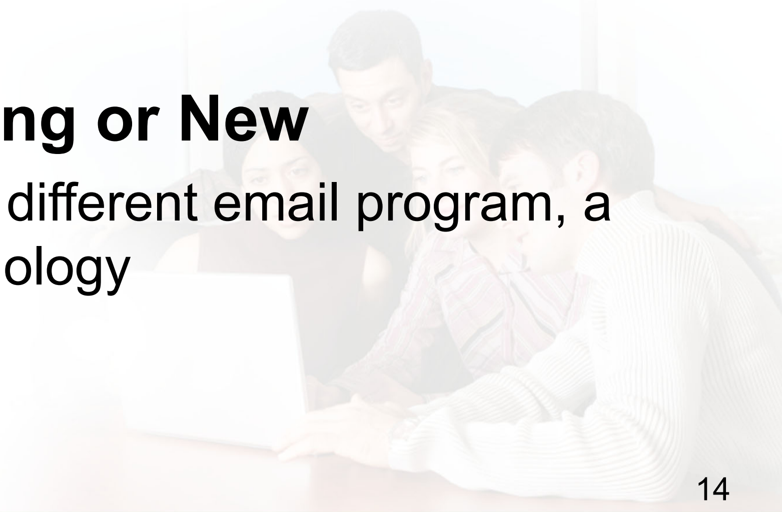
- **The Reality**
  - Start: 3 weeks before Go-Live because somebody said so
  - Start: At some random point during the project
  - Start: After implementation
  - Start: 5 years after implementation
  - End: 6 to 8 weeks later
  - End: Never



When Should A PIA Happen?

- **The Business Process is Changing or New**
  - When a feasibility document is completed
  - When a project charter is completed
  - When personal information processes are outsourced

- **The Technology is Changing or New**
  - A new hosting environment, a different email program, a new service provider for technology



5 Steps for a PIA

- Step 1: Define the Scope
- Step 2: Information Gathering
- Step 3: Report Writing
- Step 4: Review / Rewriting
- Step 5: Delivery

Step 1 of 5: Defining the Scope

- **Process**
  - Small, medium or large?
  - Amount of personal information affected / impacted / held

- **Document**
  - Assign ownership, responsibility and accountability within the program area
  - Identify (high-level) the technology

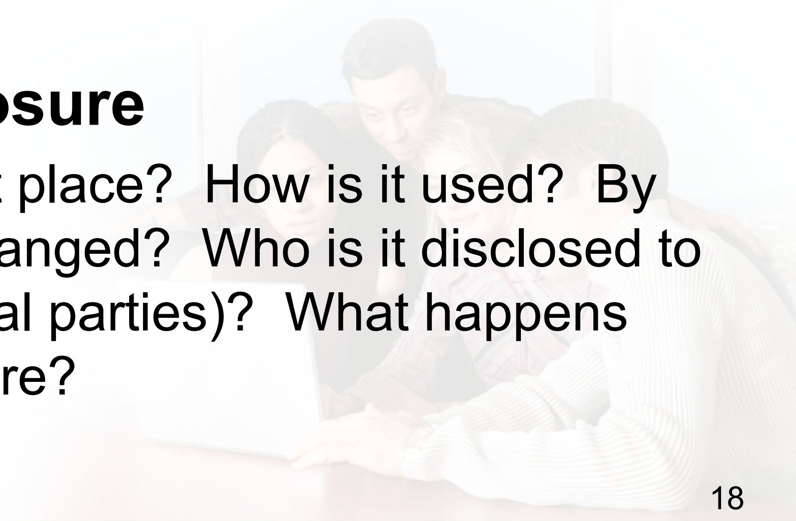
Accountabilities

- **Project Sponsor**
  - Accountable for project, including conducting PIA, approval of risk mitigation strategies and acceptance of residual risk
- **Chief Information Officer**
  - Accountable for identifying corporate IT risks and providing advice and guidance to Project Sponsor on the performance of appropriate privacy due diligence, and on potential consequences of accepting privacy risks.
- **Chief Information and Privacy Officer (OCIPO)**
  - Sets Practice Standards, provides tools and education
  - PIA Development Service (Centre of Excellence)

Step 2 of 5: Information Gathering

- **Follow the PI**
  - talk to everybody who works with PI relevant to the project including business and technology groups, support and administrative staff

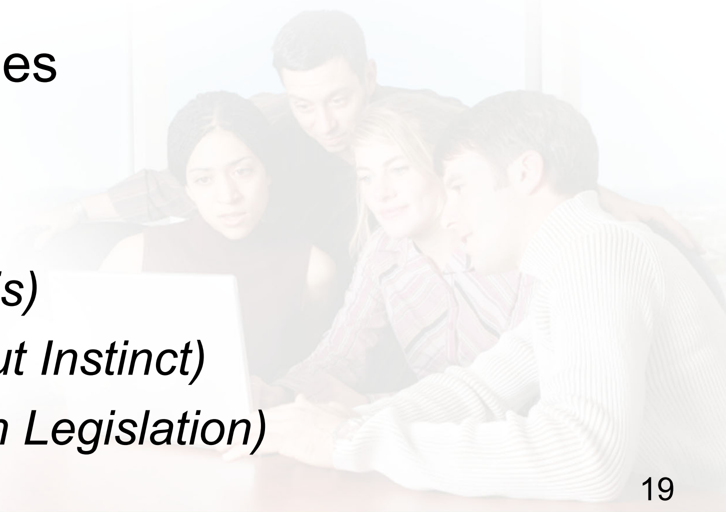
- **Collection, use and disclosure**
  - how did it get there in the first place? How is it used? By who? For what? Has this changed? Who is it disclosed to (including internal and external parties)? What happens when nobody needs it anymore?



Step 3 of 5: Report Writing

- **Depending on scope, allow time to pull together information gathering into a report format**

- **Standard Table of Contents:**
  - Description of Business Processes
  - Description of Technology
  - Privacy Analysis
    - *Findings (based on Gap Analysis)*
    - *Risk Management (based on Gut Instinct)*
    - *Design Requirements (based on Legislation)*



Step 4 of 5: Review / Rewriting

- Create hard timelines for program area to provide input, questions and commentary
- Section by section is easier then the whole document
- Allow time to re-write the PIA with an additional review cycle (not with the program area)

Step 5 of 5: Delivery

- Document, business and technology owner(s)
- See ‘Accountabilities’

Resources

- **For Privacy Requirements**
  - OCIPO’s PIA Compliance Checklist
- **For Privacy Advice**
  - OCIPO’s Access & Privacy Branch, (416) 212-7061
  - http://www.accessandprivacy.gov.on.ca/
- **For the PIA Deliverable:**
  - OCIPO’s PIA Centre of Excellence

Tracy Ann Kosa
Privacy Impact Assessment Specialist
PIA Development Service
Office of the Chief Information and Privacy Officer
Ministry of Government Services

(416) 212-1136
tracy.kosa@ontario.ca