



Privacy Impact Assessments (PIA) Tools and Tips

MGS Access and Privacy Conference

Session E5 - September 14, 2006

Toronto, Ontario



Welcome

- ◆ Eric Lawton

Senior Policy Advisor

Ministry of Government Services

eric.lawton@mgs.gov.on.ca

- ◆ Peter Hope-Tindall

Chief Privacy Architect

dataPrivacy Partners Inc.

peter@hope-tindall.net



Schedule

1:00 – 1:20	Introduction to PIA's
1:20 – 1:40	PIA How-to
1:40 – 1:55	Introduce fictional Case Study
1:55 – 2:30	Work on 1 st Deliverable
2:30 – 2:45	Break
2:45 – 3:15	Report to Group
3:15 – 3:40	Work on 2 nd Deliverable
3:40 – 4:00	Privacy Challenge Questions



Introduction to PIA's

What is a PIA?

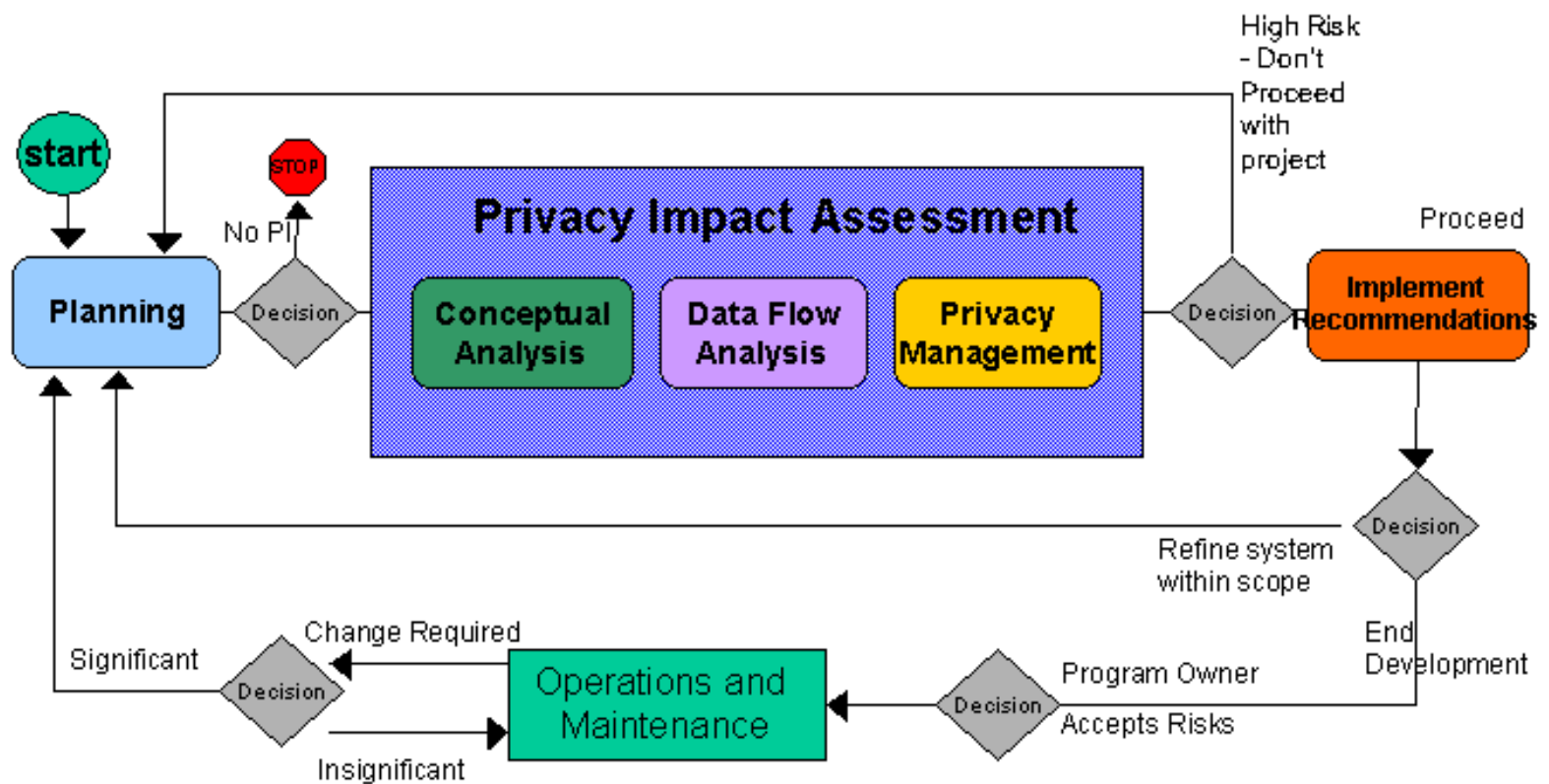
- ◆ A PIA is a due diligence exercise where organizations:
 - Describe a project
 - Show information flows
 - Establish legal authority to collect, use and disclose personal information
 - Analyse privacy risks and stakeholder concerns
 - Document mitigation strategies

Characteristics of a PIA

- ◆ Ideally, it should be:
 - Non-technical
 - Analyse risks
 - Given to decision-makers, stakeholders
- ◆ Use Proper Methodology
 - Ministries, agencies (FIPPA/MFIPPA Institutions) use Ontario MGS PIA Guidelines
 - Health Custodians use OIPC PHIPA PIA Guidelines
- ◆ Customization of format is acceptable
- ◆ Length depends on complexity of project



PIA Process





Elements of a PIA

- Executive Summary
- Introduction
- Project Background (including Environmental Scan)
- Description of Personal Information
- Privacy Analysis (legal compliance, FIPs)
- Privacy Management
- Signatures



Why do a PIA

- ◆ Confirms legal authority to collect, use and disclose personal information
- ◆ Ethical - respond to Fair Information Practices
- ◆ Risk mitigation – the best tool to identify privacy risks and document countermeasures
- ◆ Marketing/communications – key messages, update notifications, Privacy Statements
- ◆ Saves times and money – avoid re-design, project cancellation
- ◆ Sometimes you have to!



Legislation

- ◆ **Freedom of Information and Protection of Privacy Act (FIPPA)**
 - Mandatory for OPS institutions
- ◆ **Personal Health Information Protection Act (PHIPA)**
 - Mandatory where PHI is present
- ◆ **Programs Statutes**
 - Authority to collect, use and disclose PI
- ◆ **Personal Information Protection and Electronic Documents Act (PIPEDA)**
 - Federal statute, does not apply to FIPPA institutions
 - Applies to “commercial activities” in Ontario



Triggers – When a PIA is Required

- ◆ Creation or modification of database
- ◆ Major changes to existing programs
- ◆ New program involving c./u./d. of PI
- ◆ New service delivery structures and partnerships
- ◆ Multi-program service delivery integration
- ◆ Identification & Authentication schemes

...any proposal or policy that will result in substantial change to the collection, use, disclosure, or retention of personal information

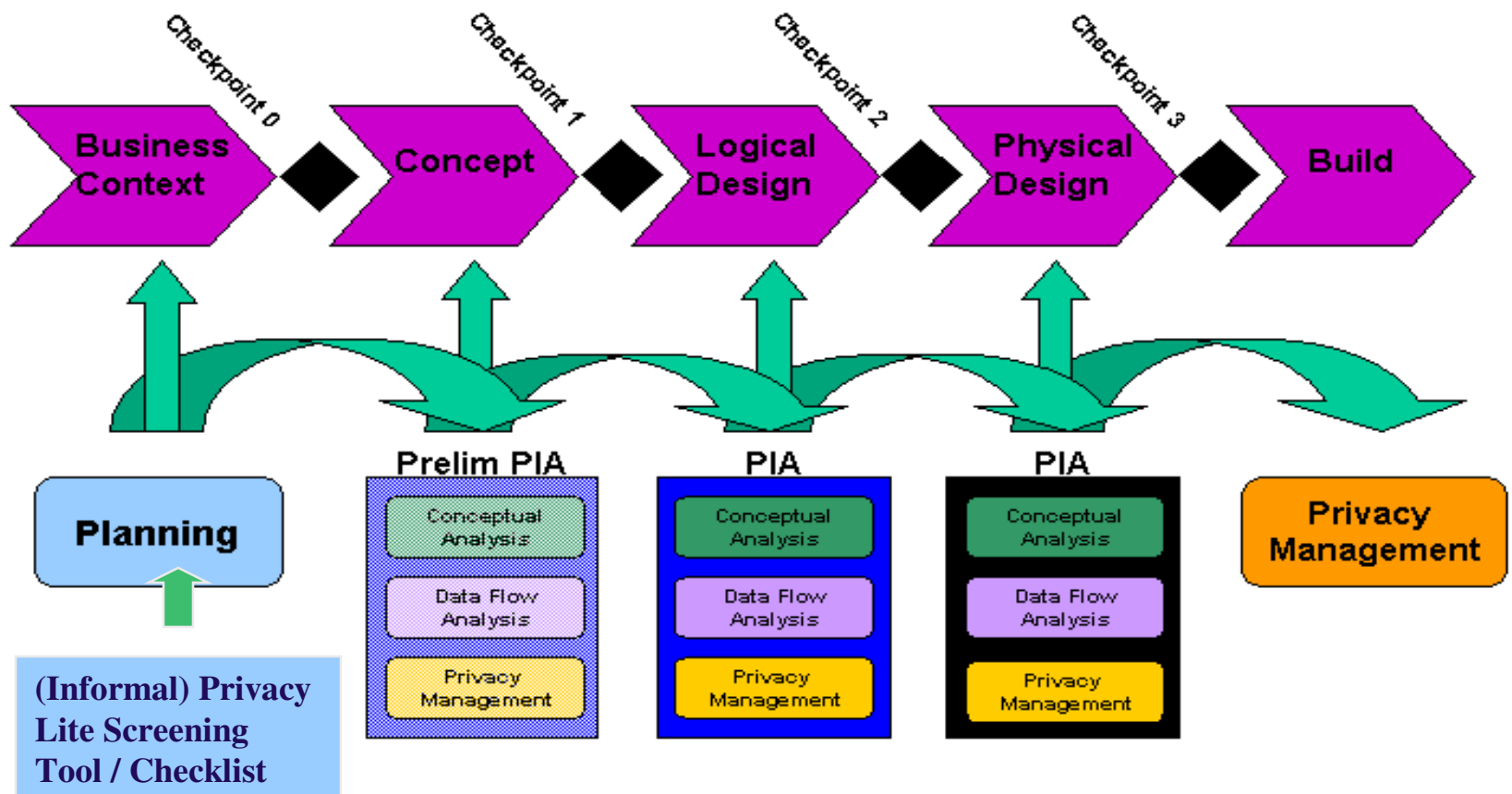


Timing

- ◆ When to start writing a PIA?
 - Not too early → when business requirements are set
 - Not too late → can still change course if necessary
- ◆ Privacy should be considered when developing business requirements (esp. uses & discl. of PI)
- ◆ Start early
 - PIA simply becomes a matter of documenting the privacy design decisions.

Build PIA into existing business process

Progressive Elaboration





Common PIA Challenges

- ◆ Lack of underpinning documentation;
 - Existing system design, MOU's, contracts, authorization from program statute
- ◆ New system built before considering privacy impacts;
- ◆ Project not well-defined (scope);
- ◆ PIA seen as roadblock to approval;
- ◆ Narrow focus – PIA emphasizes executive direction, benefits, not potential risks/impacts;
- ◆ Vendor pushing private-sector solution.



Multi-party PIA's

- ◆ Easier if one party takes the lead
 - Others can simply confirm PIA or explain differences
 - Consider complexities of different privacy requirements/laws
 - Allow time for multiple approvals
- ◆ Communication & transparency is key



Amendments/Addendums

- ◆ Don't worry – PIA's are not written in stone;
- ◆ Amend if needed;
- ◆ Existing PIA must be easily available – you may not be able to capture all the details of the long-term vision of the project in the addendum;
- ◆ Accuracy is the goal



Ontario Privacy Commissioner Review

- ◆ Not mandatory
- ◆ Good risk mitigation strategy
- ◆ No guarantees, not binding
- ◆ Timing may be tricky, but manageable
 - Give OIPC a head's up
 - Present early findings
 - For complex projects – invite participation
 - Follow-up once PIA is submitted
- ◆ Share OIPC comments with other reviewers
- ◆ PIA will be the 3rd place IPC looks after breach (after what %* &# happened and what did you do?)