PRIVACY IMPACT ASSESSMENT

A USER'S GUIDE

Information and Privacy Office
I&IT Strategy, Policy, Planning and Management Branch
Office of the Corporate Chief Strategist
Management Board Secretariat

June 2001

Ontario

CONTENTS

PART ONE – PRIVACY IMPACT ASSESSMENTS: AN OVERVIEW

WHAT IS A PRIVACY IMPACT ASSESSMENT?

A privacy impact assessment (PIA) is a process that helps to determine whether new technologies, information systems, and proposed programs or policies meet basic privacy requirements. It measures both technical compliance with privacy legislation -- such as the *Freedom of Information and Protection of Privacy Act* (FIPPA) or the *Municipal Freedom of Information and Protection of Privacy Act* (MFIPPA) and the broader privacy implications of a given proposal.

PRIVACY IMPACT ANALYSIS AT A GLANCE

The three components of the PIA process include:

Conceptual Analysis	***Data Flow Analysis***	***Follow-up Analysis***
Prepare a plain language description of the scope and business rationale of proposed initiative Identify in a preliminary way potential privacy issues and risks, and key stakeholders Provide a detailed description of essential aspects of the proposal, including a policy analysis of major issues Document the major flows of personal information Compile an environment issues scan to review how other jurisdictions handled a similar initiative Identify stakeholder issues and concerns Assessment of public reaction	Analyze data flows through business process diagrams , and identify specific personal data elements or clusters of data Assess proposal's compliance with FOI and privacy legislation, relevant program statutes, and broader conformity with general privacy principles Analyze risk based on the privacy analysis of the initiative, and identify possible solutions Review design options, and identify outstanding privacy issues/concerns that have not been addressed Prepare response for unresolved privacy issues	Review and analyze physical hardware and system design of proposed initiative to ensure compliance with privacy design requirements Provide a final review of the proposed initiative Conduct a privacy and risk analysis of any *new changes* to the proposed initiative relating to hardware and software design to ensure compliance with FOI and privacy legislation, relevant program statutes, and broader conformity with general privacy principles Prepare a communications plan

GOALS OF A PRIVACY IMPACT ASSESSMENT

The PIA process is designed to ensure that privacy is considered throughout the business redesign or project development cycle, and particularly at the conceptual stage, the final design approval and funding stage, the implementation and communications stage, and at the post-implementation audit or review stage.

The goals of a PIA include:

- ✓ Providing senior executives and the government with the tools necessary to make fully- informed policy and system design and/or procurement decisions based on an understanding of privacy risk and of the options available for mitigating that risk;

- ✓ Ensuring accountability for privacy issues is clearly incorporated into the role of project managers and sponsors;

- ✓ Ensuring that there is a consistent format and structured process for analysing both technical and legal compliance with FIPPA and MFIPPA, relevant program statutes, MBC Directives, and internationally accepted fair information practices;

- ✓ Ensuring that the protection of privacy is included in the core criteria for business or I&IT projects, and for subsidiary project activities, to reduce the potential for subsequent project termination or retrofitting systems for privacy compliance;

- ✓ Providing basic documentation on the flow of personal information for common use and review by policy and program design staff, systems analysts, and security analysts, and as the basis for:

  - < Consultations with the Information and Privacy Commissioner, and other stakeholder groups,
  - < public announcements,
  - < adequate notice and consent statements for clients, legislative amendments, contract specifications and penalties, partnership agreements, and monitoring and enforcement mechanisms,
  - < post-implementation verification and periodic reviews and audits;

- ✓ Preventing the inadvertent development of personal information management systems that may be characterized or criticized as facilitating surveillance; and

- ✓ Dentifying remedial steps necessary to improve privacy protection in pre-existing programs or systems.

WHEN IS A PRIVACY IMPACT ASSESSMENT NEEDED?

MANAGEMENT BOARD REQUIREMENTS

The new guidelines for the annual *Information and Information Technology (I&IT) Plans* submitted to Management Board Secretariat (MBS) indicate that a PIA may be required where proposals and submissions may affect client privacy. A PIA will now normally be required as part of any Management Board of Cabinet (MBC) submission seeking approval to begin the detailed design phase or to request funding approval for product acquisition or system development work.

It is the responsibility of sponsoring ministries to identify projects that may affect client privacy. This guide has been prepared to assist ministries in identifying such projects and in completing the required *Privacy Impact Assessment* (PIA). Further assistance and support is available through MBS's Information and Privacy Office.

IDENTIFYING INITIATIVES THAT REQUIRE A PRIVACY IMPACT ASSESSMENT

Not all proposals involve a substantive change to the collection, use, or disclosure of personal information. Those that do, however, must be accompanied by a PIA for approval. Examples of initiatives that are likely to require a PIA include those involving:

- ✓ ***Creation or modification of databases*** containing personal information, particularly where the information is sensitive and/or includes a significant number of people;
- ✓ ***Identification and authentication schemes***, especially proposals for multi-purpose identifiers or those that make use of biometrics;
- ✓ ***Constraining or eliminating existing opportunities for anonymity or pseudonymity*** through program or service channel redesign in a given program area or service delivery context; and
- ✓ ***The use of smart cards*** .

Sponsoring ministries should be aware that as systems become more complex, the probability of unexpected cause and effect relationships increases, so that proposals that appear to involve minor technical enhancements for customer convenience and governmental efficiency may, in fact, represent significant privacy risks.

Some common scenarios are outlined below, along with guidelines for determining whether a PIA may be required in each instance. Ministries should consider the full scope of a proposal's implications government-wide or in an "enterprise" context (as defined in the *Enterprise Information and Information Technology Architecture Principles*), as it may effect the overall advisability of the project, or highlight the importance of certain aspects of the business or systems design. Consideration should also be given to the flow of personal information beyond the program, to payment clearing agents and financial institutions, and any legislation applying to those entities.

COMMON SCENARIOS

Minor Changes to Existing Programs
Generally, proposals involving minor changes to the scope of program information requirements -- such as the collection of additional eligibility data as authorised by statute and reflected in revised notices or consents, or data matching agreements developed in accordance with the *MBS Directive on Computer Matching of Personal Information* -- would not require a PIA.

Major Changes to Existing Programs
Proposals that entail major increases in the scope of collection, use and disclosure of personal information, through program integration, broadening of target populations, a significant shift toward indirect collection of personal information, or the expansion of data collection for new eligibility criteria or program administration functions, for example, should be accompanied by a PIA.

If the current program does not involve potentially contentious privacy issues, a PIA would be required only for those elements of the program or project that are being changed. Thus, it would likely not be necessary to map the data flow for the entire system, or to perform a privacy analysis for all the categories of personal information collected, through the relationship between the current program and the proposed changes may need to be examined.

New Programs
In general, proposals for new programs that involve significant collection, use, or disclosure of personal information should be accompanied by a PIA.

New Delivery Structures and Partnerships

Limited Out-Sourcing

The specific details of out-sourcing arrangements will determine whether a PIA is required. Sponsors should consult with the Information and Privacy Office for assistance in determining if a PIA is needed.

If an out-sourcing arrangement provides that personal information collected for the program will not be linked to non-program personal information or used for non-program purposes, that the government will retain control of and accountability for the personal information, and that appropriate security and compliance verification measures will be implemented, a PIA will not likely be required.

Delivery Channel(s) Management

If an out-sourcing arrangement delegates operational decision-making power regarding delivery channels and customer service systems, a PIA is required.

Multi-Program Front End Delivery Integration

Where a proposal for integrated program delivery involves the integration of personal information collected for distinct legislative programs, a PIA is required. Co-location of program delivery, which includes shared IT&I infrastructures but not services -- such as common client indexes or files, or common customer billing or benefit payments systems -- does not require a PIA.

DEVOLUTION

A PIA is not required where functions are devolved to an agency or municipal entity that is or will be scheduled under FIPPA, or where the ministry retains accountability for the personal information collected.

Other proposed devolution's may require a PIA; sponsors should consult with the Information and Privacy Office.

CHANGES IN TECHNOLOGY

Maintenance

Routine system maintenance such as minor software upgrades or patches, or replacement of equipment that does not materially change information management functions or system security does not require a PIA.

Upgrades

Minor upgrades which have no impact on the way in which personal information is managed do not require a PIA.

Major upgrades to systems and operating systems that change the functionality of information management, access protocols, records indexes or security features, however, should be accompanied by a PIA. Where such upgrades are not accompanied by program design and delivery changes, the PIA will normally be limited to identifying the risks, improvements, countermeasures and net privacy effects of the proposed upgrades.

Additional Systems Linkages

Proposals that involve linking separate program databases, or creating files that index or point to the personal information of individuals on such databases, require a PIA. Where data matches are undertaken in accordance with the Directive on Data Matching, a PIA is not required.

Enhanced Accessibility

Changes that effect how and where program administrators, customers or third parties access personal information require a PIA. Examples of such changes would include putting new or additional customer data on the Internet or on other media such as CD-ROMs, on virtual private networks, or at kiosks.

Ministries should note that the *MBS Directive on Managing, Distributing and Pricing Government Information (Intellectual Property)* requires that a PIA be included with any request to Publications Ontario to sell or license a personal information database. In addition, providing other program areas or governments with network access to customer databases may require a PIA. Ministries operating personal information databases accessible by municipalities or other entities must complete a PIA before allowing them to change access systems.

EIA Initiatives and Common/Strategic Products

Enterprise Information and Information Technology Architecture (EIA) initiatives, including out-sourced transaction subsystems, card systems, and common applications products for the collection, transmission, or storage of personal information, require a PIA. If vendors or products have already been selected, a PIA must still be completed prior to pilot trials and project implementation. Privacy risks identified through the privacy impact assessment process that cannot be minimised or eliminated must be calculated as part of the overall cost of the proposal.

PREPARING FOR A PRIVACY IMPACT ASSESSMENT

THE TIMING OF THE PRIVACY IMPACT ASSESSMENT

Informed decision making and the ability to design system architecture, which address actual or potential privacy concerns, are dependent, on early identification of privacy issues. An understanding of the kinds of questions that will arise in the context of the privacy impact assessment, as well as where risks may lie, should therefore be incorporated into the early phases of the project and system development life cycles.

While the completion of a full and detailed PIA may only be possible at later stages in the system development and acquisition phase, the PIA is best approached as an evolving document, which will grow increasingly, detailed over time.

RESOURCE REQUIREMENTS

The scope and volume of resources needed to complete a PIA will depend on a number of factors, including what stage the project or proposal is at, and the scope of the proposed changes to or new uses of personal information. Policy, technical, and legal staff will normally participate in the completion of the PIA.

In general, it will be most efficient to begin the PIA process at the start of the *conceptual stage* of the initiative, as some components of the PIA will, in any event, be completed as part of the normal policy development process. In addition, early consideration of privacy issues should prevent unnecessary effort being expended on the development of options that are incompatible with key privacy-related business and technology design decisions.

ASSIGNING RESPONSIBILITY FOR THE PRIVACY IMPACT ASSESSMENT

While accountability for compliance with privacy requirements ultimately rests with the "head" of a public body (normally the Minister), sponsors may find it useful to designate a senior level project team member as the privacy lead or project privacy manager (PPM). The PPM should have a clear mandate to participate in or review the project design decisions against the criteria of the PIA, and provides ongoing advice and feedback to the senior project management team.

THE RANGE OF SKILLS THAT MAY BE USEFUL

The PPM may need to draw upon a wide range of skill sets from internal or external resources that are to be assigned to the project. Such skills would likely include:

Policy Development skills	***Operational Program and Business Design skills***	***Technology and Systems expertise***	***Risk and Compliance Analysis skills***	***Procedural and Legal skills***	***Access to Information and Privacy expertise***
Relating to business-specific policy experience, broad strategic policy and planning skills, and stakeholder impact analysis and consultation skills.	Relating to those associated with examination of proposals for the operational flow of the business, and analyse the feasibility, practicality, efficiency of the program and of public/private partnerships.	Relating to the design, attributes and operations of mainframe and legacy systems, networking products, new Internet tools, system security, and front-end customer interface systems including, counter/staff terminal entry, unattended computer/kiosk, Automated Voice response, attended voice/call centres, remote access, smart cards, card read/write devices at the customer interface level, financial/ transaction settlement systems, and biometric tools.	Relating to those associated with comprehensive financial and due diligence audits, and the emerging specialities related to audits of computer system vulnerabilities.	Relating to program authority for Out-Sourcing, program or agent collection and use of personal information, jurisdiction of institutional oversight mechanisms, statutory, regulatory and contractual options, and potential statutory or code conflicts where multiple statutes or jurisdictions are involved.	Relating to the FIPPA/MFIPPA, privacy provisions in relevant program statutes, national and international privacy standards, privacy enhancing technologies, and current privacy developments.

PART TWO – UNDERSTANDING PRIVACY

WHAT IS PRIVACY?

Privacy encompasses a number of inter-related values, rights, and interests unique to individuals. It is generally considered to have at least four dimensions:

- ✓ ***Privacy of the person***: refers to the integrity of an individual's body, and spans issues such as compulsory immunization, blood transfusions, or sampling of body fluids or tissue.
- ✓ ***Privacy of personal behavior***: refers to the right of privacy relating to such matters as sexual preferences and habits, political activities and religious practices.
- ✓ ***Privacy of personal communications***: the right to communicate with others without routine monitoring.
- ✓ ***Privacy of personal data***: also called information privacy, this refers to the right to determine when, how and to what extent you will share personal information about yourself.

This PIA methodology is principally concerned with the privacy of personal data, or information privacy, as it is generally the most relevant in the context of government proposals for new or revised service delivery projects. Where a ministry proposes a course of action that may have implications for other types of privacy, such as privacy of the person, the PIA will continue to be relevant, but will require additional questions and analysis focussing on the particular risks raised by the proposal. Sponsoring ministries are encouraged to seek assistance from the Information and Privacy Office in these cases.

An important aspect of information privacy is freedom from surveillance. Surveillance is the systematic investigation or monitoring of an individual's activities or communications. Its primary purpose is to collect information about that individual, their activities, or their associates.

The government's specific legal obligations to protect the privacy of personal information are outlined in the FIPPA/MFIPPA. In some instances, additional requirements may form part of program statutes.

Under the *FIPPA*, personal information is recorded information about an identifiable individual, including:

(a) information relating to the race, national or ethnic origin, colour, religion, age, sex, sexual orientation or marital or family status of the individual;

(b) information relating to the education or the medical, psychiatric, psychological, criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved;

(c) any identifying number, symbol or other particular assigned to the individual;

(d) the address, telephone number, fingerprints or blood type of the individual;

(e) the personal opinions or views of the individual except if they relate to another individual;

(f) correspondence sent to an institution by the individual that is implicitly or explicitly of a private or confidential nature, and replies to that correspondence that would reveal the contents of the original correspondence,

(g) the views or opinions of another individual about the individual; and

(h) the individual's name if it appears with other personal information relating to the individual or where disclosure of the name would reveal other personal information about the individual.

Personal information must be about an identifiable individual, however an individual's name need not be attached to the information to qualify as personal information. A physical description or a photograph of a person attached to other personal information about that person is personal information even where no name is given. An individual's name on its own is not personal information. To be personal information within the meaning of the Act, the name must be associated with other personal information.

In addition to obligations to protect personal information under FIPPA/MFIPPA, and relevant program statutes, ministries contemplating proposals likely to effect privacy should be aware of general standards for privacy – such as the Canadian Standards Association's *Model for the Protections of Personal Information* (CSA Standard) – which may influence public opinion, and of how similar proposals in other jurisdictions have been received. Such considerations may well be key to appropriately identifying the privacy risks associated with the proposal.

ASSESSING PRIVACY RISK IN GOVERNMENT SERVICE DELIVERY

THE CHALLENGE OF ELECTRONIC SERVICE DELIVERY

Just as the private sector has begun to invest in electronic commerce as a way of bringing consumers better service, more choice and better prices, governments have begun to look to electronic service delivery (ESD) as a way of interacting with the public more rapidly, more efficiently, and more responsively.

Citizens, while welcoming client-driven, interactive, integrated information and services from government, have some concerns about privacy and security in electronic contexts. Studies show that 86% of Canadians are very concerned about giving out personal information on the Internet, and 91% of Canadians are concerned about giving out credit card information online.

Experience suggests that citizens will not participate in electronic transactions where privacy and security concerns have not been appropriately addressed. In some jurisdictions, public outcry about privacy has resulted in programs having to be withdrawn or substantially redesigned at a significant cost. As we design and implement ESD systems, then, we must be sensitive to the concerns that may arise as a result of computerised information systems that can monitor, track, or observe individuals without their knowledge or consent. These features may contribute to a lack of public confidence, and must be addressed as a critical element of achieving truly client-driven electronic service delivery. Well-designed ESD systems can enhance both personal privacy and information security, minimizing risk while providing better and more efficient service.

PERSPECTIVES ON RISK

The risk of a proposal meeting with public concern about privacy is present wherever the collection, use, or disclosure is at issue.

The risks associated with failing to consider the privacy implications of a given proposal can take many forms, and may include, for example:

- ✓ ***Failure to comply*** with either the letter or the spirit of FIPPA/MFIPPA, or fair information principles more generally, resulting in criticism from the Information and Privacy Commissioner (IPC).
- ✓ ***Stimulating public outcry*** as a result of a perceived loss of privacy or a failure to meet expectations with regard to the protection of personal information;
- ✓ ***Loss of credibility or public confidence*** where the public feels that a proposed program or project has not adequately considered or addressed privacy concerns;
- ✓ ***Underestimating privacy requirements*** such that systems need to be redesigned or retrofitted late in the development stage at considerable expense.

To minimize risk, potential causes of concern should be addressed as early in the design process as possible, with reference to the *Enterprise Information and Information Technology Architecture Privacy Design Principles for Personal Information* (EIA Privacy Design Principles). Where risk cannot be mitigated through technical or policy instruments, such as effective system design or the use of privacy-enhancing technologies, sponsoring ministries should provide decision-makers with a full assessment of the risks and a strategy for responding to pubic concerns.

To successfully identify design or program features in a given initiative that may contribute to a lack of public confidence, and to appropriately anticipate public reaction to an initiative, the clients perspective on risk must be considered, as they will generally bear the consequences of privacy breaches.

Proposals may be subject to public criticism even where the requirements of FIPPA or MFIPPA have been met. Broader fair information principles, and the public expectations that flow from those principles and other relevant legislation, such as the federal government's *Personal Information Protection and Electronic Documents Act* (federal Act) must also be considered.

The federal Act regulates the collection, use, and disclosure of personal information in the private sector, based on the CSA Standard. Representatives from the public sector, industries (including transportation, telecommunications, information technology, insurance, health, and banking), consumer advocacy groups, unions and other general-interest groups developed the CSA Standard in the 1990s. It represents a consensus among all stakeholders, and is based on the Organisation for Economic Co-operation and Development's *Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data* (OECD Guidelines). It addresses two broad concerns: the way in which organisations collect, use, disclose and protect personal information; and the right of individuals to have access to personal information about themselves and to have the information corrected if necessary.

The federal Act responds to a number of pressures, including growing public concern about privacy, the need to provide the right framework to stimulate electronic commerce, and addressing the *European Union Data Protection Directive* (EU Directive). The EU Directive requires member states to block transfers of information to non-member states that do not offer "adequate" protection.

The scope of the federal Act is extensive, and it is likely to form the basis of public expectations of privacy. Significantly, the federal Act enshrines the notion that individuals should have the opportunity to consent to the collection, use, or disclosure of their personal information. In developing project proposals, ministries should be aware that the federal Act is likely to stimulate higher public expectations for consent-based privacy protection.

RISK MANAGEMENT: TOOLS FOR PROTECTING PRIVACY

Experience over time and across jurisdictions has shown that the most effective way to protect personal information is to use a combination of tools and strategies, which include the implementation of fair information practices, privacy-enhancing technologies, PIAs, standards, and public education.

FAIR INFORMATION PRACTICES

In 1980, the OECD developed privacy guidelines on the protection of privacy and transborder flows of personal information. Canada signed the OECD Guidelines in 1984. While there have been numerous developments in the protection of personal information since that time, the principles enshrined in the OECD Guidelines continue to serve as the foundation for most efforts to protect personal information around the world. The OECD Guidelines are based on fair information practices (FIPs). FIPs are basic principles for the collection, use, disclosure, retention and disposal of personal information.

While there are some variations, fair information principles normally include the following:

1. Ensuring public awareness and transparency (openness) of information policies and practices;
2. Establishing necessity and relevance of the information collected;
3. Building in finality (establishing the uses of the information in advance and eventually destroying it);
4. Identifying the person who has responsibility for protecting personal information within an organization;
5. Getting informed consent from the individual; and
6. Maintaining accuracy and completeness of records.

The international influence of the OECD Guidelines, and of FIPs more generally, has been significant, and is apparent in Ontario's FIPPA and MFIPPA legislation.

Decision-makers must recognize that, while changing service delivery mechanisms and the extensive use of new technologies may alter programs and information systems, FIPS continue to be relevant as a minimum standard for the protection of personal information. Program or project sponsors must ensure that adequate steps have been taken to protect personal information through adherence to such practices

PRIVACY-ENHANCING TECHNOLOGIES

In the last decade, a number of technologies have been specifically developed to be privacy-enhancing technologies (PETs). Such tools assist in protecting privacy, and often do so by providing genuine, untraceable anonymity.

PETs such as encryption, digital signatures, and anonymous electronic cash and service delivery systems, may protect personal information from unauthorized collection, use and disclosure. The effective incorporation of such technologies into basic program or system design can often alleviate pressures on privacy that result from program goals or efficiency requirements with little or no increase in cost.

A good example of practical use of PETs is pseudo-identification, which can authenticate individuals for the receipt of government services. It does so by allowing the authentication of people's eligibility rather than their identity. A pseudonymous record or transaction is one that cannot, in the normal course of events, be associated with a particular individual. Hence a transaction is pseudonymous in relation to a particular party if the transaction data contains no direct identifier for that party, and can only be related to them in the event that a very specific piece of additional data is associated with it. To be effective, pseudonymous mechanisms must involve legal, organizational and technical protections, such that the link between a transaction and an identifiable individual can be made only under appropriate circumstances.

Pseudonymity, and other PETs, can provide innovative ways of addressing fundamental issues in system design while protecting personal information. Used to their full potential, such technologies can provide more secure identification to reduce fraud; more secure networking to reduce losses from theft; and more secure payment systems which will dispense with the administrative costs of cash while permitting high levels of user anonymity and privacy protection. Applied in association with FIPs, PETs make it clear that cost savings and privacy protection need not be opposing values.

PRIVACY IMPACT ASSESSMENTS

PIAs help to determine whether new technologies, information systems, or proposed programs or policies meet basic privacy requirements. They provide a framework for identifying and reviewing privacy issues as they arise within particular contexts.

STANDARDS

Sector or activity-specific privacy standards, such as the *Electronic Service Delivery Privacy Standard*, that reflect the kinds of fair information principles embodied in the CSA Standard, can provide a vehicle for clearly articulating privacy expectations in a given context, and may be particularly useful where partnerships are involved.

PUBLIC AND/OR KEY STAKEHOLDER CONSULTATION

It may be appropriate to consult on major initiatives proposing new collections, uses, or disclosures of personal information, or on significant overhauls of existing programs. Depending on the type of initiative being proposed, or the level of complexity involved, ministries may find it useful to consult broadly with the public or narrowly with key stakeholders. It is assumed that ministries preparing to undertake such consultations will work with their communications branches in developing a communications strategy.

Focused, strategically-timed public discussions can assist program or system designers in anticipating broader public reactions to proposals that may have implications for the protection of personal information. Conducted early in the process, such consultations may help to eliminate options which meet with significant resistance.

In addition to public consultations, ministries may also wish to monitor public opinion on related topics that may be relevant to their proposals. Such monitoring may assist in anticipating public reaction, and should focus not only on privacy-related issues that may arise in the province, but also on public reaction to similar proposals in other jurisdictions. This will provide some sense of the environment into which the proposal will be received, and may be a good indicator of public expectations.

COMMON SOURCES OF RISK

Elements of program design, system characteristics, and/or the choice or design of delivery channels may contribute to risks to privacy and violations of fair information practices. Some of the more common sources of risk are summarized below.

It is important to note that the PIA is not designed to dictate specific courses of action, or to curtail the sponsoring ministry's range of options in terms of program design or technology options. The function of the PIA is simply to ensure that privacy risks associated with a given proposal are properly identified and addressed wherever possible, and that decision-makers have been informed of these risks and the options available for mitigating them.

PROGRAM CHARACTERISTICS

Risks to privacy may arise as a result of any of a number of program characteristics, including:

- ✓ ***Data profiling/data linkage***: combining unrelated personal information obtained from a variety of sources to create new information about individuals. Data linkage may be facilitated through the storing of personal information in centralized databases or by linking unrelated databases.

- ✓ ***Transaction monitoring***: tracking an individual's transactions with one or more programs. This usually results in the creation of new personal information describing an individual's overall experience with one or more programs.

- ✓ ***Identification of individuals***: ESD generally requires identification of individuals and authentication of that identity as a way of managing security risks. Surveillance risks exist where the use of common identifiers or identification systems facilitates data sharing, profiling, or transaction monitoring.

- ✓ ***Physical observation of individuals***: tracking the movement or location of individuals through the use of vehicle transponders, satellite locators, cameras, or mechanisms for recording individual use of kiosks.

- ✓ ***Publishing or re-distributing public databases containing personal information***: this might include publishing assessment rolls on the Internet or on compact disks, or publishing court records on the Internet. Electronic publishing frequently eliminates practical limits on the misuse of information, as it can be easily manipulated and used for purposes entirely unrelated to its intended use in manual form.

SYSTEM CHARACTERISTICS AND TECHNICAL ARCHITECTURE

The degree to which ESD programs preserve or erode privacy is generally determined by the architecture or design of the systems that support them, and by the technologies that drive those systems. Business and technology managers should review technical architecture to determine whether and how certain inherent functional characteristics may pose a risk to privacy. Common examples of such characteristics are summarized below.

Common (Network) Directory Services

Most systems seek to maximize ease of access for many users from any number of locations. A central list is maintained of individuals authorized to access the system and their privileges. Most central listing activity is automated, and is designed to collect similar listings from linked or related systems that make it possible to find someone with an ID, electronic address, or privileges within the connected systems. This function is known as common directory services.

Where common directory services list personal information about individuals as customers of government programs, privacy issues may arise. This is particularly relevant in self-service electronic program delivery models, or where a directory is shared or aggregated between programs such that data profiling or data matching may be facilitated.

Alternative Service Delivery

Alternative service delivery (ASD) may raise a number of issues with regard to the protection of personal information. In assessing ASD arrangements, it is important to keep key differences between public and private sector service delivery in mind:

1. *Government has demand powers, which the private sector does not generally have;*
2. *In most cases, there is the possibility of choice in consumer dealings with the private sector; and*
3. *The data being collected through these arrangements is, in many cases, more sensitive than data that would normally be collected by the private sector.*

Depending on the sensitivity of the data, relatively straightforward out-sourcing of IT services or program intake functions where personal information is collected and processed on behalf of a public body and subject to FIPPA may not raise significant privacy issues.

In many cases, however, ASD arrangements are relatively complex and so require more careful scrutiny. Examples of such arrangements would include:

- ✓ ***Merging*** previously isolated transaction systems into a common governmental window,

- ✓ ***Localizing*** data collection activities through a common private sector window for previously isolated program data collections systems, which may also include concurrent data collection for private sector transactions,

- ✓ ***Materially changing*** the status of personally identifiable information, organizational accountability, and oversight of the business by accepted mechanisms such as internal auditors, a Provincial Auditor, the IPC, or an Ombudsman.

Regardless of the specific details of the ASD arrangement, it is important that personal information continues to be protected when it passes into the hands of contractors and sub-contractors.

Service Monitoring

There is growing pressure for program areas to monitor service delivery in order to measure customer satisfaction and allocate resources. Careful system design can allow for monitoring with little or no privacy invasion. For example, Internet browser cookies and transaction logging systems can be designed and used to capture generic, non-identifiable or anonymized data which provides an adequate basis for service management without significant privacy risks. In such cases, a PIA will not generally be required.

Where service monitoring does involve the use of personally-identifiable data, however, a PIA will likely be necessary.

Delivery Channel Management

The shift toward new delivery channels can pose distinct challenges for security and privacy. Moving from systems based on personal interaction at a counter, or signed paper mail, to computer or kiosk-based transactions, automated voice response, call centres, or remote access systems, raises new issues with regard to client identification and authentication, and to the provision of notice or consent. Call centres, for example, may access program data for a range of programs, making data profiling both easier to perform and more difficult to detect. Sponsoring ministries may wish to preserve a range of access channels for service delivery, allowing customers to choose their preferred level of personal comfort, risk and convenience.

Wherever changes in delivery channels result in changes to how personal information is collected, used, or disclosed, a PIA will be required.

Data Warehousing and Data Marts

Data warehouses and data marts may, over time, provide a venue for limitless data matching and creation of new forms of personal information inconsistent with client expectations. By their nature, data warehouses and marts challenge or violate the basic privacy principles relating to limiting collection, disclosure, use, and obtaining consent for new uses. Thus, they entail a high degree of risk from a privacy perspective, and may well meet with public resistance. A PIA is required wherever data warehousing and/or data marts are being proposed.

Risks must be carefully measured against the expected benefits to be derived from the data warehouse. In proceeding with the PIA, sponsoring ministries should pay particular attention to any proposal to integrate personal data from separately legislated program databases or private sector databases.

The risks associated with data warehousing and data marts may be reduced in a number of ways, including:

- ✓ ***Using artificial intelligence (AI) products*** to research trends within a single program database as an alternative to data warehousing;

- ✓ ***Anonymizing the data***, thereby limiting potential threats to identification and privacy loss to a small number of individuals managing the data stripping or ID conversions;

- ✓ ***Soliciting voluntary individual consent*** for inclusion in the data warehouse. This approach may limit the size and cost of the data warehouse while providing sufficient strategic information;

- ✓ ***Providing value-added information services*** to interested parties instead of allowing direct access to identifiable data;

- ✓ ***Ensuring the custodianship and control*** of identifiable data remains subject to FIPPA, and that such data are subject to frequent formal independent audits for compliance with project privacy and security standards.

Where such strategies are employed, the scope of the PIA will be significantly reduced.

PART THREE – DOING THE PRIVACY IMPACT ASSESSMENT

AN OVERVIEW OF THE PROCESS

A *Privacy Impact Assessment* (PIA) is a process that helps to determine whether new technologies, information systems, and proposed programs or policies meet basic privacy requirements. It also measures both technical compliance with privacy legislation, such as the *Freedom of Information and Protection of Privacy Act* (FIPPA) or the *Municipal Freedom of Information and Protection of Privacy Act* (MFIPPA), and the broader privacy implications of a given proposal. The PIA is also intended to help policy writers and decision-makers manage potential privacy risks.

The three components of the PIA process include:

Conceptual Analysis	***Data Flow Analysis***	***Follow-up Analysis***
Prepare a plain language description of the scope and business rationale of proposed initiative Identify in a preliminary way potential privacy issues and risks, and key stakeholders Provide a detailed description of essential aspects of the proposal, including a policy analysis of major issues Document the major flows of personal information Compile an environment issues scan to review how other jurisdictions handled a similar initiative Identify stakeholder issues and concerns Assessment of public reaction	Analyze data flows through business process diagrams , and identify specific personal data elements or clusters of data Assess proposal's compliance with FOI and privacy legislation, relevant program statutes, and broader conformity with general privacy principles Analyze risk based on the privacy analysis of the initiative, and identify possible solutions Review design options, and identify outstanding privacy issues/concerns that have not been addressed Prepare response for unresolved privacy issues	Review and analyze physical hardware and system design of proposed initiative to ensure compliance with privacy design requirements Provide a final review of the proposed initiative Conduct a privacy and risk analysis of any *new changes* to the proposed initiative relating to hardware and software design to ensure compliance with FOI and privacy legislation, relevant program statutes, and broader conformity with general privacy principles Prepare a communications plan

The end result of the PIA process is documented assurance that all privacy issues have been appropriately identified and either adequately addressed or, in the case of outstanding privacy issues, brought forward to senior management for further direction.

The ability to provide such assurances is largely dependent on the extent to which all-relevant factors and potential privacy issues have been considered. Sponsoring ministries should, therefore, ensure that they take into account the following four key areas as they work through this process:

PEOPLE	*PROCESS*	*ENVIRONMENT*	*TECHNOLOGY*
Consider ongoing management, privacy training programs, general organizational awareness of privacy and security issues, the level of knowledge required to perform specific functions, the availability of manuals and other forms of guidance, and mechanisms for communicating privacy and security policies.	Consider what information is collected, why and how it is collected, how privacy and security are ensured operationally, and what mechanisms are in place to provide individual access to information.	Consider the physical space where information is stored, physical security measures, the availability of secure document disposal facilities, and processes for secure disposal of old information technology (e.g., personal computers, legacy servers, etc.) that may hold personal information.	Consider system design characteristics, data security and integrity measures, access controls, and audit trails .

Where to Begin – AN OVERVIEW OF THE PROCESS

While a complete PIA will include multiple components (e.g., proposal description and rationale, the data map, the privacy analysis, risk analysis, etc.) different components of the PIA may be useful to project managers and system designers at various stages in the decision-making process.

For example, if a project is at the *Conceptual Analysis*, it is important for decision-makers to identify the privacy issues that may arise, and the options available for avoiding or addressing those issues. In this case, it would be more useful to begin with a general analysis of the issues and risks that may arise in relation to a given initiative. By contrast, where decisions are being made about system design, it might be more useful to develop a data flow diagram in order to understand the implications of different design choices.

Early work on the PIA enables early identification of major issues, allowing project managers and system designers to examine business process and technology options to reduce or eliminate privacy-related issues as the project moves forward. Wherever the process begins, the PIA should be updated at each major project development milestone so that there is no need for a major re-documentation when final approvals for detailed design and implementation are sought. Outlined below is a detailed description of the three components of the PIA process beginning with the *Conceptual Analysis*.

CONCEPTUAL ANALYSIS

The *Conceptual Analysis* is intended to provide a detailed description of the essential aspects of the proposal (e.g., scope, business rationale, etc.) and an environmental issues scan, and identify significant privacy issues and potential risks so that decision-makers have a comprehensive understanding of the potential privacy implications that

the proposal may generate. For example, a proposal to create a new database (or modify an existing database) that contains particularly sensitive information would require a fairly detailed conceptual analysis to ensure that key issues and risks, stakeholder concerns and input related to such a proposal are thoroughly identified and addressed.

At this stage in the PIA process the overall level of analysis of the proposal and the information provided will be less detailed than that which is provided at the *Data Flow Analysis*. At the next stage in the assessment process, project managers will be expected to provide more detailed information regarding data flow diagrams, privacy analysis and risk analysis. However, the key objective of the *Conceptual Analysis* is to establish for decision-makers a general understanding of what the proposed initiative intends to do, and what privacy and stakeholder issues may generally emerge as a result of the proposed initiative.

The conceptual analysis may include a number of features. The first is the identification and description of the business initiative that is being proposed, including high-level information regarding the initiative's scope and rationale, and describe how the initiative fits into the broader business planning cycle of the sponsoring ministry and the government.

The second is a detailed description of the essential aspects of the proposal that includes a comprehensive policy analysis of the proposal's major issues. For example, this description might include an examination of the business case and rationale for using personal information. In some cases an initiative may be able to achieve its business function by using anonymous data instead of personally identifiable information. The analysis of the proposal's essential aspects might also examine whether or not the initiative will introduce new technology options. If so, the technology should be analysed to ensure that it does not unintentionally introduce new privacy risks.

The third feature, a high level documentation of major flows of personal information, is an integral part of the PIA process. Before a thorough privacy analysis of a proposal can occur (see Part Four – PIA Tool Kit for specific analysis questions), the flows of personal information need to be identified and documented.

An initiative's activities can be described from an information management perspective as a series of processes consisting of:

- ✓ Information collection (data inputs);
- ✓ Transaction processing involving the application of rules, validations and decision-making;
- ✓ The provision of a product or service in terms of a decision, benefit, or licence (output); and
- ✓ Transactional data recording the above events. These may be temporary records such as system logs, paper forms used prior to input, and data records or subject files in any media.

The fourth feature of the *Conceptual Analysis* is an environmental issues scan to review how other jurisdictions have handled a similar initiative. Reviewing the experiences of others will assist project managers in identifying the key privacy concerns and risks of a given proposal. It may also reveal how another jurisdiction solved a specific privacy challenge.

The fifth feature is the identification of stakeholder issues and concerns. This stakeholder impact analysis can assist program managers and decision-makers in anticipating broader reactions to proposals that may have implications for the protection of personal information. Stakeholders include anyone or group who has an interest or concern, or who may be effected by the proposed initiative. It is important that stakeholder views are properly documented and addressed whenever possible. Conducted early in the process, such analysis can help to eliminate hardware, software and/or system design options which may meet with significant stakeholder resistance.

The final feature of the *Conceptual Analysis* is an assessment of the public reaction towards the proposed initiative regarding its implications for the protection of their personal information. The risk of a proposal meeting with public concern about privacy is present wherever the collection, use or disclosure of personal information is at issue. Assessing the public's reaction toward a proposal can assist decision-makers in anticipating broader public reactions, and help identify what steps need to be taken to improve overall acceptance.

The risks associated with failing to consider the privacy implications of a given proposal can take many forms. For example, if a proposal fails to comply with either the letter or the spirit of FIPPA/MFIPPA, or fair information principles more generally, it may receive public criticism from the Information and Privacy Commissioner (IPC). This criticism may then stimulate public outcry about a perceived loss of privacy or failure to meet expectations about the protection of personal information.

Depending on the type of initiative being proposed or the level of complexity involved, ministries may find it useful to consult broadly with the public or narrowly with key stakeholders. It is assumed that ministries preparing to undertake such consultations

will work with their communications branches in developing a communications strategy.

In addition to public consultations, ministries may also wish to monitor public opinion on related topics that may be relevant to their proposals. Such monitoring may assist in anticipating public reaction, and should focus not only on privacy-related issues that may arise in the province, but also on public reaction to similar proposals in other jurisdictions. This will provide a sense of the environment into which the proposal will be received, and may be a good indicator of public expectations. Conducting public assessment early in the process may help to eliminate options which meet with significant resistance.

DATA FLOW ANALYSIS

The *Data Flow Analysis* provides comprehensive documentation of data flows through business process diagrams, identifies specific personal data elements or clusters of data, assesses the proposal's compliance with FOI and privacy legislation, relevant program statutes and broader conformity with general privacy principles, and identifies potential privacy risks to provide solutions. This component of the PIA process should also review design options, and identify outstanding privacy issues/concerns that have not been addressed, and prepare response for unresolved privacy issues.

This stage may have three features. The first is to analyze data flows through business process diagrams that illustrate the major components of the proposal including specific personal data elements or clusters of data. This stage in the PIA process involves a detailed analysis of data flows by elaborating on the business process diagram.

The documentation of data flows involves a two-part process. The first is the preparation of a business process diagram. At a minimum, the diagram should identify at a general level the major components of the business process and how personal information is collected, used, disclosed, and retained through this process.

The business process diagram may be prepared using any of a number of methodologies. In choosing an approach, ministries should consider the nature and complexity of the proposed project. Some possible approaches to mapping the business process would include *flow charts*, *structured analysis* and/or *object-oriented analysis* (see Part Four – PIA Tool Kit)

While the business process diagram documents the high-level flow of personal information, it does not provide an adequate level of detail for a comprehensive privacy impact assessment. Thus, the second part of the documentation process involves a more detailed analysis of data flows that builds on the business process diagram. The framework and key questions for the privacy analysis can be found in Part Four – PIA Tool Kit.

The second feature is an assessment of the proposal's compliance with FOI and privacy legislation, relevant program statutes, and broader conformity with general privacy principles through a structured privacy analysis.

As a process, a PIA is designed to provide evidence of compliance with privacy principles. The privacy analysis contributes to this goal by taking project managers and system designers through a series of key questions (see Part Four – PIA Tool Kit for specific analysis questions) that identify how personal information is collected, used, and disclosed, and interrogate a proposal's technical compliance with legislation and general privacy requirements. Additional questions assist in anticipating how the public is likely to react to key issues associated with the proposal. The goal, therefore, is not simply to ascertain that legislation and privacy requirements have been met, but also to flesh out and bring to the attention of decision-makers broader privacy issues that may raise public concerns.

Not all questions in the analysis section will be relevant to every proposal. By the same token, the questions listed may not reflect all the considerations that will be important in a given context, particularly where program statutes may outline particular requirements with regard to privacy, or where there is evidence (e.g., from other jurisdictions) that public concern may focus on a particular element of a proposal. Consequently, this section can and should be modified where necessary to ensure that all relevant questions have been considered. Questions should not, however, be focused solely on strict technical compliance with legislative requirements, but should also attempt to identify areas of potential public concern.

The final feature of the *Data Flow Analysis* is to undertake a risk analysis based on the conclusions generated by the privacy analysis, and when possible provide solutions to address these risks. In those few cases when a solution to privacy concerns are not *fully* resolved, a legitimate rationale should be provided for why the concerns where not addressed, and brought forward to senior management for further direction

FOLLOW-UP ANALYSIS

The *Follow-up Analysis* is intended to provide a review and analysis of the proposed initiative's physical hardware and system design to ensure that what is eventually built complies with basic privacy design requirements.

Although the substantive data flow analysis and privacy analysis will have already taken place during the *Conceptual Analysis* and *Data Flow Analysis* this stage provides further opportunity to identify any circumstances where privacy may be a at risk in the initiative from a physical design and implementation perspective.

Analysis of the proposed initiatives' physical components may reference the *Enterprise Information and Information Technology Architecture Privacy Design Principles* (EIA Privacy Design Principles). The *EIA Privacy Design Principles* represent an assessment and compliance framework that is based on both the statutory requirements in FIPPA/MFFIPA and the ten fair information practices in the *CSA Model Privacy Code*. The Ontario government specifically developed these principles to support the design and implementation of initiatives that will meet basis privacy requirements such as compliance with provincial FOI and privacy legislation and general privacy principles.

By designing initiatives with *privacy design principles* built in at the out set ensures that the initiative that will be eventually built conforms to basic privacy requirements such as allowing individuals to make informed decisions regarding the purposes for which their personal information is collected and disclosed). Therefore, the analysis of the initiative's physical hardware and system design is critical step in the privacy assessment and compliance process. Consequently, the *Follow-up Analysis* is intended to provide a final opportunity for project managers and system designers to review whether or not hardware, software and system design issues and concerns related to the proposed initiative have been thoroughly identified and addressed.

In some cases new changes to a proposal may require further privacy and risk analysis. The analysis of new changes ensures compliance with FOI and privacy legislation and relevant program statutes, and broader conformity with general privacy principles. At this stage, the privacy and risk analysis should focus specifically on the new changes and not the entire project. This is analysis should assess the potential impact of the new changes, provide a detailed rationale for why the changes where made, and if necessary indicate what solutions are being proposed to address and mitigate potentials privacy concerns.

A communications plan should be developed in preparation for the implementation of the proposed business initiative. This particularly important if privacy issues or concerns were identified during the PIA process. In such cases the communications plan should include messaging that specifically addresses what issues or concerns were identified and how they have been resolved. In those few cases when privacy concerns were not *fully* resolved, a legitimate rationale should be prepared for why privacy concerns where not addressed.

PART FOUR – PIA TOOL KIT

DOCUMENTING THE DATA FLOW – STEP ONE

A business activity can be described from an information management perspective as a series of processes consisting of:

- ✓ Information collection (data inputs);
- ✓ Transaction processing involving the application of rules, validations and decision-making;
- ✓ The provision of a product or service in terms of a decision, benefit, or licence (output); and
- ✓ Transactional data recording the above events. These may be in the form of temporary records such as system logs, paper forms used prior to input, and data records or subject files in any media.

Step One involves a two-part process. The first is the preparation of a business process diagram. At a minimum, the diagram should identify, at a general level, the major components of the business process and how personal information is collected, used, disclosed, and retained through this process.

The business process diagram may be prepared using any of a number of methodologies. In choosing an approach, ministries should consider the nature and complexity of the proposed project. Some possible approaches to mapping the business process would include:

Flow Charts	***Structured Analysis***	***Object-oriented Analysis***
Are most useful for relatively simple applications. Flow charts provide a good general sense of program steps and data flows, along with an outline of the relationships among these elements and the progression between them	Identify major steps in a program and then breaks these steps down, according to function, until the project can be represented as a progression through a series of small steps. This is a good way of reducing very complex projects into manageable components	Combines the mapping of processes with the mapping of the data flows attached to those processes. It sets out the processes and the organization of these processes (i.e. the architecture), and specifies which data are being used and where in each process they are being used

While the business process diagram documents the high level flow of personal information, it does not provide an adequate level of detail for subsequent stages in the privacy impact assessment process, and particularly for the privacy analysis. Thus, the second part of the process involves a more detailed analysis of data flows that builds on the business process diagram. This analysis provides details of how personal information is collected, used, and disclosed based on a series of questions. The focus on the analysis is on those aspects of the information management life cycle that may have the greatest impact on determining whether the proposals successfully meet

privacy requirements. Obviously, the more detailed the business program is, the simpler the second stage will be.

The framework for this analysis can be found at Figure A.2.

GOALS OF STEP ONE

When step one is completed, an individual reviewing the diagram and data flow analysis will be able to identify and trace personal information from the point of collection to the point where all copies of the information are destroyed or permanently archived. While tracing the life cycle of the personal information, the reviewer would have an accurate description of all the stakeholders who accessed or used the information under specific conditions, and where copies of such records may exist.

A NOTE ON COMPLEX SYSTEMS

Where there are complex subsystems or information flows, as in a multi-ministry smart card initiative, for example, it may be more manageable to have multiple data flow analyses. In some systems, a hierarchy of data flow analyses might be required to accurately portray the flow of personal information during its life cycle through each responsible institution and its agents. Completion of the charts and analysis may require co-operation between organizations.

The final result should always be a charting of all the personal information collected, directly or indirectly, by or on behalf of an organization, illustrating the regular and irregular uses and disclosures of the information, and how it is stored.

THE DATA FLOW ANALYSIS

The first section A.1 of the analysis is the identification and description of the personal information. Normally this would be done in clusters of data elements which relate to the types of information used in delivery, collected on forms, indirectly collected or disclosed to other parties. Examples would be basic identification or biographical information, eligibility data, financial data, decision data, benefit or licence data.

The second section A.2 records all of the direct and indirect collection activities by program staff, other individuals and organizations relating to the above data element or cluster category.

Section A.3 documents the planned or regular disclosures of the data elements or cluster. It also identifies the custody of both program and transaction related records that contain personal identifiers. These forms of records are increasingly common in large systems using multiple business partners in the information life cycle.

Irregular disclosures are to be listed in section A.4.

If there are any other records that may be populated with the data elements or clusters not previously captured, they should be listed in section A.5, along with an explanation of who is responsible for the record, and what privacy protections apply.

Section A.1
Program/Initiative _____

Page ___ 0f _____

Data Elements/Category_____ **No ____ of _____**

Name_____

List and describe the personally identifiable data elements in the category:
1)
2)
3)
4)
5)
6)
7)
8)
9)
10)
11)
12)
13)
14)
15)
16)
17)
18)
19)
20)
21)
22)
23)
24)
25)

A.2 Information Collection			**If Not Directly Collected Is the Personal Information (PI) Indirectly Collect from:**						
Collection is performed by	**What is the statutory authority for the direct collection and/or indirect collection?**	**Is the PI Directly Collected from customer [Yes/No]**	**Publicly Accessible Governmental Databases Name(s)**	**Intra/Inter Governmental Information sharing agreements-name(s)**	**Private Sector information sharing agreements name(s)**	**Multi Program Data Marts/ Warehouses**	**Subscription to private sector data services - name**	**Other name**	**Itemize Customer PI disclosed in order to access 3rd party customer data records**
Dedicated Program Staff **Yes ❍ No ❍**									
Other OPS Staff e.g. staff of another program or ministry. **Yes ❍ No ❍**									
Dedicated Contractor e.g. a contractor who works solely for the program. **Yes ❍ No ❍**									
Generic Service Provider e.g. a contractor who works for multiple ministries or programs simultaneously. **Yes ❍ No ❍**									
Client Agent e.g. solicitor, trustee, physician, or other service provider. **Yes ❍ No ❍**									
Other **Yes ❍ No ❍**									

USE OF INFORMATION

Under s. 41 of FIPPA, an institution must not use personal information in its custody or under its control except:

1) where the person to whom the information relates has identified that information in particular and consented to its use;

2) for the purpose for which it was obtained or compiled or for a consistent purpose; or

3) for the purpose for which the information may be disclosed to the institution under section 42 or under section 32 of the Municipal Freedom of Information and Protection of Privacy Act.

Attach a description of the uses of personal information in the organization, indicating the authority for those uses.

A.3 **List Regular Business Transactions That Disclose or Give Access to Personally Identifiable Data Records to:**	**Yes**	**No**	**Limited Access**	**Full Access**	**Is a New PI Record Created as a result? Describe**	**Identify Custodian(s) of New PI Record Created**	**Is a Log of Access Transactions Created by One or Both Parties? If yes, identify Custodian(s).**	**What is the Authority for Disclosure under FIPPA?**
OPS program or systems staff								
OPS program auditors								
Other OPS Systems staff								
Other OPS Staff e.g. staff of another program or ministry								
Dedicated Contractor e.g. a contractor who works solely for the program								
Generic Service Provider e.g. a contractor who works for multiple ministries or programs simultaneously								
Client Agent e.g. solicitor, trustee, physician,								
Financial Institutions								
Financial Transaction Agents								
External Contract Auditors								

A.3 **List Regular Business Transactions That Disclose or Give Access to Personally Identifiable Data Records to:**	**Yes**	**No**	**Limited Access**	**Full Access**	**Is a New PI Record Created as a result? Describe**	**Identify Custodian(s) of New PI Record Created**	**Is a Log of Access Transactions Created by One or Both Parties? If yes, identify Custodian(s).**	**What is the Authority for Disclosure under FIPPA?**
By Legislative Mandate to Public or Private agencies - name								
Data Marts/ warehouses Other than when fully Anonymized								
By Information Sharing Agreement (ISA) to intra/inter governmental programs - name								
To the Public or For Sale to the Public or Commercial Interests								
By ISA to Non-governmental programs - name								

A.3 **List Regular Business Transactions That Disclose or Give Access to Personally Identifiable Data Records to:**	**Yes**	**No**	**Limited Access**	**Full Access**	**Is a New PI Record Created as a result? Describe**	**Identify Custodian(s) of New PI Record Created**	**Is a Log of Access Transactions Created by One or Both Parties? If yes, identify Custodian(s).**	**What is the Authority for Disclosure under FIPPA?**
To Client by Self Service in any media								
To Client via 3rd Party								
Client via Written Program request								
Other								

A.4 **Note *Irregular* Business Transactions that Disclose or Give Access to Personally Identifiable Records to:**	**Yes**	**No**	**Limited Access**	**Full Access**	**Is a New PI Record Created? Describe**	**Identify Custodian(s) of New PI Record Created**	**Is a Log of Access Transactions Created by One or Both Parties? If yes, identify Custodian(s).**	**What is the Authority for Disclosure Under FIPPA?**
Recognized Law Enforcement (excluding police) agents per FIPPA without a warrant or subpoena.								
Other public sector program investigators, by data sharing agreement, on request.								
Other Disclosures								

A.5 **Identify any other PI record database or log produced by business or system transactions that are not listed elsewhere and are not under direct program custody or control. Include temporary and permanent record collections.**	**Record and contents**	**Under control of**	**In the Custody of**	**Applicable privacy legislation and/or contractual privacy provisions**
e.g., financial settlements provider(s) transaction logs, temporary update data stored in system pending validation, call centre/help desk call logs, etc.				

THE PRIVACY ANALYSIS – STEP TWO

As a process, a PIA is designed to provide evidence of compliance with privacy principles. The privacy analysis, contributes to this goal by taking analysts through a series of key questions that interrogate a proposal's technical compliance with FIPPA and relevant program statutes. Additional questions aim at measuring broader conformity with general privacy principles and at anticipating likely public reaction to key issues associated with the proposal. The goal, then, is not simply to ascertain that FIPPA requirements have been met, but also to flesh out broader privacy issues that may raise public concerns, and so should be brought to the attention of decision-makers.

Not all questions in the analysis section will be relevant to every proposal. By the same token, the questions listed may not reflect all the considerations that will be important in a given context, particularly where program statutes may outline particular requirements with regard to privacy or where there is evidence (e.g., from other jurisdictions) that public concern may focus on a particular element of a proposal. This section, therefore, can and should be modified where necessary to ensure that all relevant questions have been considered. Questions should not, however, be focused solely on strict technical compliance with legislative requirements, but should attempt to identify areas of potential public concern.

Generally problem areas with privacy issues will in most cases be found to relate to those questions where the answer is in the "NO" column for each principle. A summary of privacy concerns for each of the 10 principles may be noted in the "NOTES" box provided and flagged for further analysis.

For each principle make a list of privacy design practices relevant for the project.

The principles and questions listed below are organized around the ten principles of the CSA Standard, which are:

- Accountability,
- Identifying Purposes,
- Limiting Collection,
- Consent,
- Limiting Use, Disclosure, and Retention,
- Accuracy,
- Safeguards,
- Openness,
- Individual Access, and
- Challenging Compliance

PRINCIPLE 1 – ACCOUNTABILITY

An organization is responsible for personal information under its control and shall designate an individual or individuals who are accountable for the organization's compliance with the following principles.

1.1
Accountability for the organization's compliance with the principles rests with the designated individual(s) (or, where the institution is subject to FIPPA, with the "head" as defined by the Act in s. 2 and in O. Reg. 460), even though other individuals within the organization may be responsible for the day-to-day collection and processing of personal information. In addition, other individuals within the organization may be delegated to act on behalf of the designated individual(s).

1.2
The identity of the individual(s) designated by the organization to oversee the organization's compliance with the principles shall be made known upon request.

1.3
An organization is responsible for personal information in its possession or custody, including information that has been transferred to a third party for processing. The organization should use contractual or other means to provide a comparable level of protection when the information is being processed by a third party.

FIPPA makes institutions accountable for the collection, use, disclosure and retention of personal information managed directly or on their behalf by other public or private sector partners. In programs that rely on partnerships, organizations may find it useful to develop program-specific privacy codes or standards that clearly articulate expectations and responsibilities, as in the *ESD Privacy Standard*.

1.4
The CSA Standard requires organizations to implement policies and practices to give effect to the principles, including:

- implementing procedures to protect personal information;
- establishing procedures to receive and respond to complaints and inquiries;
- training staff and communicating to staff information about the organizations policies and practices; and
- developing information to explain the organizations policies and procedures.

Some aspects of these requirements are captured under sections of FIPPA/MFIPPA, but in this area the requirements of the CSA Standard are, overall, more rigorous. Organizations working with private sector partners who are required by federal law to meet the Standard in an arrangement where FIPPA/MFIPPA do not apply should, however, consider these requirements.

DISCUSSION

While accountability for compliance with privacy requirements ultimately rests with the "head' of a public body (e.g., the Minister), organizations may find it useful to designate a Project Privacy Manager (PPM) who will be responsible for the management and coordination of information resources, policies and procedures, and for overseeing the completion of the PIA.

QUESTIONS FOR ANALYSIS

	YES	*NO*
Has responsibility for the PIA been assigned to a Project Privacy Manager or other individual(s)?	?	?
Where the custody or control of personal information will be transferred to other public or private sector partners as part of the project:		
Has the chain of accountability been documented, up to and including the Minister's ultimate accountability as the head under FIPPA?	?	?

Are the performance requirements of the accountable parties comprehensively specified in a measurable way, and subject to specific performance or compliance reviews?	?	?
Where public and private sector partners are not subject to FIPPA, have independent third-party audit mechanisms been incorporated into performance and partnership agreements such that public accountability is assured?	?	?
Where public and private sector partners are not subject to FIPPA, has the option to schedule them under FIPPA been fully evaluated and documented?	?	?
Will the ministry be provided with the results of regularly scheduled audits and compliance checks on the privacy practices of external partners and will those reports be made available to the program clients?	?	?
Have legal opinions been sought regarding:	?	?
1. Legislative authority to transfer ministry program delivery responsibilities to partners, including a consideration of the authority for partners to collect, use, disclose or retain personal information as necessary on behalf of ministries? and/or	?	?
2. Legislative authority to alter or limit in any material way the collection, use or disclosure of personal information as authorized by ministry program statutes and FIPPA for the purpose of delivering services through the partners? And/or	?	?
3. Legislative authority to set service standards and procedures for client authentication and the legal authority to collect and use personal information for authentication purposes? and/or	?	?
4. Legislative authority to amend or modify the delegation or designation of statutory program functions to the partners?	?	?
Has the organization retained the legal or contractual right to develop mechanisms to determine whether personal information collected on its behalf is disclosed to third parties for any purposes?	?	?
Does the organization have specific audit and enforcement mechanisms that oversee the collection, use and disclosure of personal information by public or private sector partners?	?	?

ANTICIPATING PUBLIC EXPECTATIONS

In the past, concerns have been raised about the implications of ASD for access to government information and the protection of personal information. Expressions of such concern can be found, for example, in the IPC's 1998 Annual Report, which comments on the privatization of Ontario Hydro, and changes to the *Safety and Consumer Statutes Administration Act* (1996) such that independent non-profit corporations will take over supervisory and inspection functions in a number of areas, including elevators, amusement rides and gasoline handling.

Other jurisdictions are also facing important challenges with regard to access to information and privacy in ASD. With this in mind, analysts should consider the following questions:

- Does the proposal entail a real or perceived decrease in public accountability (for example, through the use of private sector partners)?

- Has a strategy been developed for communicating to the public about measures that are in place to ensure appropriate accountability?

NOTES

PRINCIPLE 2 – IDENTIFYING PURPOSES

The purposes for which personal information is collected shall be identified by the organization at or before the time the information is collected.

2.1
The organization shall document the purposes for which personal information is collected in order to comply with the Openness principle and the Individual Access principle.

Under s. 39 of FIPPA, an organization collecting personal information must inform the individual to whom the information relates of:

- the legal authority for the collection;

- the principal purpose or purposes for which the personal information is intended to be used; and

- the title, business address and business telephone number of a public official who can answer the individual's questions about the collection.

This does not apply where the head may refuse to disclose the personal information under subsection 14 (1) or (2) (law enforcement).

2.2
Identifying the purposes for which personal information is collected at or before the time of collection allows organizations to determine the information they need to collect to fulfil these purposes. The Limiting Collection principle requires an organization to collect only that information necessary for the purposes that have been identified.

Identifying purposes enables organizations to focus their data collection on only that information which is necessary for the stated purposes, or to find alternatives to the collection of personal information. This is critical to effectively limiting collection. Since data collection and maintenance is expensive, “identifying purposes” is the first step in reducing operating costs throughout the information life cycle.

2.3
Organizations shall provide a statement of purposes (notice of collection, s. 39 (2)) to be made available through all mediums of delivery (i.e. paper forms, counter, phone, on-line, automated telephone or kiosk service) and shall identify the personal information to be collected, the authority for its collection, the principal purpose(s) for which it is collected, and the name, position, address and telephone number of a contact person.

In addition, s. 45 of FIPPA requires annual publication of an index (the Directory of Records) of all personal information banks setting forth, in respect of each personal information bank:

(a) its name and location;
(b) the legal authority for its establishment;
(c) the types of personal information maintained in it;
(d) how the personal information is used on a regular basis;
(e) to whom the personal information is disclosed on a regular basis;
(f) the categories of individuals about whom personal information is maintained; and
(g) the policies and practices applicable to the retention and disposal of the personal information.

Collection of information that is not personally identifiable, such as the automated collection of statistical transaction information, does not have to be described in the notice of collection or the personal information bank section of the Directory of Records.

2.4
When personal information that has been collected is to be used for a purpose not previously identified, or for a purpose not consistent with a previously identified purpose, the new purpose shall be identified prior to use. Unless the new purpose is permitted by law, the consent of the individual is required before information can be used for that purpose. (FIPPA, s. 41, s. 46)

Where personal information is used or disclosed for a purpose other than those identified, FIPPA requires that a record of the use or disclosure be appended to the record containing the personal information (s. 46).

2.5
Persons collecting personal information should be able to explain to individuals the purposes for which the information is being collected, as per FIPPA s. 39 (2).

2.6
This principle is linked closely to the Limiting Collection principle and the Limiting Use, Disclosure, and Retention principle.

DISCUSSION

Statements of purpose should be simple, and may imply certain consistent purposes. For example, a statement that customer financial information, such as a credit card number or cheque, is used for the purposes of processing payment for a good or service (such as a fishing license or provincial park reservation) would reasonably include disclosure to a collection agency in the event of non-payment.

Care must be taken to ensure that consistent purposes are reasonable and not contrived; a full disclosure of purposes is required.

QUESTIONS FOR ANALYSIS

	YES	***NO***
Has a clear relationship been established between the personal information to be collected and the program's functional and operational requirements?	?	?
Have all options to minimize the routine collection of personal information been considered?	?	?
Does the notice of collection contain the specific purposes, the legal authorities for collection, and the contact information for the official designated to respond to queries regarding the purposes of collection, or	?	?
Is there documentation regarding a waiver of notice, or is notice not required as per a specific FIPPA exception?	?	?
If there are secondary purposes that are not required to be included in the notice of collection (e.g. audit trail information, transaction validation, financial settlements), have these been documented elsewhere, such as in the Directory of Records, or attached to the record as per s. 46 of FIPPA?	?	?
Is client consent sought for secondary uses of personal information, such as service monitoring?	?	?
Is the notice of collection made available through all mediums of delivery (i.e. paper forms, counter, phone, automated telephone or kiosk service mediums) and does it identify:	?	?

< the personal information to be collected, < the authority for its collection, < the principal purpose(s) for which it is collected, < the name, position, address and telephone number of a contact person?		
Does the notice of collection clearly distinguish between personal information collected for program purposes and personal information collected by partners for other purposes? Alternatively, are separate notices provided?		

ANTICIPATING PUBLIC EXPECTATIONS

Are the purposes identified consistent with what public expectations are likely to be given the nature of the initiative?

See further questions under “Openness principle”.

NOTES

PRINCIPLE 3 – CONSENT

The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where otherwise permitted under FIPPA.

Note: In certain circumstances personal information can be collected, used or disclosed without the knowledge and consent of the individual. For example, legal, medical, or security reasons may make it impossible or impractical to seek consent. When information is being collected for the detection and prevention of fraud or for law enforcement, seeking the consent of the individual might defeat the purpose of collecting the information. Seeking an individual's consent may be impossible or inappropriate when the individual is a minor, seriously ill, or mentally incapacitated.

3.1
Where consent is required for the indirect collection of personal information and the subsequent use or disclosure of information, an organization should seek consent for the use or disclosure of the information at the time as it seeks consent for collection.

Consent for indirect collection should generally include:

- the identification of the personal information to be collected;
- the source from which the personal information may be collected; and
- the name of the institution that is to collect the personal information.

A record should be kept with the date and the details of the authorization.

3.2
The principle requires "knowledge and consent". Organizations shall make a reasonable effort to ensure that the individual is advised of the purposes for which the information will be used. To make the consent meaningful, the purposes must be stated in such a manner that the individual can reasonably understand how the information will be used or disclosed (FIPPA, s. 39 (2)). For example, if address information is to be used for the mailing of related literature, it would be important to distinguish between a business sending its own or related firms mailings from the address list in its possession, and the sale or release of that address list to other firms or generic direct marketing agencies. (See FIPPA s. 43)

3.3
An organization may not, as a condition of the supply of a product or service, require an individual to consent to the collection, use, or disclosure of information beyond that required to fulfil the explicitly specified and legitimate purposes such as those authorized by legislation (FIPPA, s. 38 (2)).

3.4
In obtaining consent, the reasonable expectations of the individual are relevant. For example, a public utility commission may disclose personal information to a debt collection agency to recover monies owed to the commission for utility bills in arrears. Such disclosures would reasonably be expected by persons who have not discharged their debts to the commission. On the other hand, an individual would not reasonably expect that personal information given to a health-care professional would be given to a company selling health-care products, unless consent were obtained. Consent shall not be obtained through deception.

Under sections 42(c), 43 FIPPA / s.32(c), 33 MFIPPA, personal information may be disclosed for the purpose(s) for which it was originally collected, or for a consistent purpose. A purpose is a consistent purpose only if the individual from whom the information was directly collected might reasonably have expected such a disclosure of the information. For further elaboration on this point, see Principle 5.

3.5
The way in which an organization seeks consent may vary, depending on the circumstances and the type of information collected. Some examples would be:

(a) an application form may be used to seek consent, collect information, and inform the individual of the use that will be made of the information. By completing and signing the form, the individual is giving consent to the collection and the specified uses;
(b) a checkoff box may be used to allow individuals to express their consent. Individuals who do not check the box are assumed not to consent;
(c) consent may be given orally when information is collected over the telephone; and
(d) consent may be given at the time that individuals use a product or service.

Generally, seeking written consent is preferable because it provides the best evidence that consent was given. A written consent should specify:

- the particular personal information to be used;
- how or for what purpose the information will be used;
- the date of the consent; and
- the institution to which the consent is given.

Where consent is obtained verbally, a notation should be made on the file and/or record indicating that verbal consent to use the personal information for a particular purpose was obtained, and recording the circumstances of the consent.

3.6
An individual may withdraw consent at any time, subject to legal or contractual restrictions and reasonable notice. The organization should inform the individual of the implications of such withdrawal and ensure information systems have the capacity to record and act upon the withdrawal of consent.

DISCUSSION

While authority for the use of personal information may flow from a number of sources, including program statutes and the consistent purposes rationale, consent is generally favoured as the underpinning of fair information practices.

Sometimes the purpose for which the information is collected is obvious. For example, an individual who inserts a long distance card into a telephone reasonably expects the telephone company to use the personal information for the purposes of billing the cardholder. This purpose so closely aligns with the data subject's expectations that consent is expressed by their act of inserting the card into the telephone.

Nonetheless, the individual has a right to know what the principle purposes of the collection are, or indeed that there are no other intended purposes for the information. The application which the individual completes in order to obtain the card should identify all the purposes. The list of purposes need not be so inclusive that individuals will not read or comprehend it.

While consent may be sought in various ways, organizations should be sensitive to public expectations when determining which method to employ. Experience in the private sector suggests that consumers are generally hostile to methods of seeking consent that rely on an opt-out, rather than an opt-in to positively indicate consent. In addition, the federal Act, which will apply broadly throughout the private sector, operates on the basis of consent. This is likely to have a significant influence on public expectations, and may result in mounting pressure for government programs to place a greater emphasis on consent.

QUESTIONS FOR ANALYSIS

	YES	***NO***
Does consent require a positive action by the customer, rather than being assumed as the default?	?	?
Is consent to indirectly collect, use, and disclose personal information clear and unambiguous?	?	?
Where personal information is collected indirectly from third parties, is consent obtained from the individual to whom the information pertains by either the organization collecting indirectly or the organization disclosing the information?	?	?
Does the proposal envision possible secondary uses for the personal information collected? If yes, does the authority for those uses flow from:	?	?

< consent?	?	?
< the consistent purpose rationale?	?	?
< other statutory authority?	?	?
Is consent sought for secondary uses of personal information, such as service enhancement, resource management or research?	?	?
Where necessary, are mechanisms in place to obtain consent for the use of personal information for purposes not previously identified? (See the *EIA Privacy Design Principles*)	?	?
Can a client's refusal to consent to the collection or use of personal information for a secondary purpose, unless required by law, be honoured without disrupting service?	?	?
Does refusal to consent to secondary uses of personal information by any service delivery partners effect the level of service provided to an individual with regard to authorized governmental transactions?	?	?

Are there standards in place for administering consent requirements that address:	?	?
1. Making the determination whether the customer has the capacity to give consent by reasons of age or capacity; and	?	?
2. Recognition of persons authorized to make decisions on behalf of an incapable person or minor.	?	?

ANTICIPATING PUBLIC EXPECTATIONS

Are the proposed consent provisions consistent with existing standards in comparable areas of the public or private sector?

Is the form of the consent being sought (e.g., opt-in or opt-out) likely to stimulate negative public reaction?

Has the opportunity for the data subject to participate knowledgeably in decisions affecting their personal information been maximized through the use of informed consent?

NOTES

PRINCIPLE 4 – LIMITING COLLECTION

The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means.

4.1
Organizations shall not collect personal information indiscriminately. Both the amount and the type of information collected must be limited to that which is necessary to fulfill the purposes identified. In addition, one of three conditions set out in s. 38 (2) of FIPPA must exist in order for personal information to be collected:

- The collection must be expressly authorized by statute;
- The information must be used for law enforcement purposes; or
- The information must be necessary for the proper administration of a lawfully authorized activity.

The authority to collect personal information is limited to the collection of *necessary* information.

4.2
Personal information must be collected by fair and lawful means. Organizations must not collect information by misleading or deceiving individuals about the purposes for which they are doing so.

4.3
Personal information must be collected directly from the individual to whom it relates unless FIPPA expressly permits indirect collection, as set out in s. 39.

An individual may consent to an indirect collection of his or her own personal information. The authorization must include:

- an identification of the personal information to be collected;
- the source from which personal information may be collected;
- the name of the institution that is to collect the personal information.

4.4
This principle is linked closely to the Identifying Purposes principle and the Consent principle.

DISCUSSION

Organizations should consider the business objectives of data collection and examine alternative means of achieving those objectives. In some cases, these can be satisfied without collecting personally identifiable information, thereby dispensing with additional administrative requirements to meet policy and legal obligations regarding privacy and security.

For example, where card readers are used by transportation companies instead of tokens, the basic information needed is whether the individual is authorized to make the trip. For planning purposes, it may be useful to know a vehicle's entrance and exit points and time of day of travel, but this does not necessitate collection of personally identifiable information about the individual cardholder. Collecting only the information necessary may limit the degree of privacy risk associated with a given initiative, and may also satisfy business efficiency goals.

QUESTIONS FOR ANALYSIS

	YES	***NO***
Is the collection of personal information:	?	?
1. Expressly authorized by a statute, or	?	?
2. Does it relate directly to and is it necessary for the proper administration of a lawfully authorized activity, or,	?	?
3. Is it exempt from notice under section 39(3) of FIPPA (law enforcement)?	?	?
Is personal information collected directly from the individual?	?	?

If no, is there indirect collection of personal information from third parties?	?	?
If so, has the individual to whom the information pertains consented to such collection, or is the collection:	?	?
1. Authorized by a statute, a treaty, or an agreement thereunder?	?	?
2. Authorized by the IPC?	?	?
3. From a report of a reporting agency under the Consumer Reporting Act?	?	?
4. Or is it for one of the following purposes:	?	?
‣ An honour or award ‣ Crown debt collection or payment ‣ Law enforcement ‣ Use in proceedings before a court, judicial or quasi-judicial tribunal.	? ? ? ?	? ? ? ?
Is personally identifiable information indirectly collected from other programs?	?	?
Is information used for planning, forecasting, or evaluation purposes anonymized?	?	?
Will customer activity be monitored (e.g. for the purposes of providing security and quality assurances)?	?	?
If yes, will personal information be used?	?	?
If yes, What is the authority for using the personal information: < consent < consistent purposes rationale < statutory authority < other (describe)	 ? ? ? ?	 ? ? ? ?
Is notice provided?	?	?
Is access to data restricted to accountable security staff?	?	?

Is the personal information used for any other purposes or disclosed to any other business units (other than law enforcement personnel)?	?	?
Does the monitoring conform with the *MBS Directive on Information and Information Technology Security*?	?	?

ANTICIPATING PUBLIC EXPECTATIONS

Does the program require the collection of personal information that clients are likely to consider highly sensitive? If so, what steps have been taken to ensure public confidence?

Often, the first step in effectively limiting collection is narrowly and precisely defining the statutory authority for collection. Relying heavily on the discretion of public officials to limit data collection, without appropriate statutory limitations, may prove difficult in the face of competing pressures to maximize data collection. With this in mind, is the statutory authority for collection as narrowly defined as possible?

NOTES

PRINCIPLE 5 – LIMITING USE, DISCLOSURE, AND RETENTION

Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Personal information shall be retained only as long as necessary for the fulfillment of those purposes.

5.1
Organizations using personal information for a new purpose shall document this purpose.

In order to comply with s. 41 of FIPPA, an institution must not use personal information in its custody or under its control except

(a) where the individual has consented, in writing, to the use of that particular information for a specified purpose;
(b) for the purpose for which it was obtained or compiled or for a consistent purpose;
(c) for a purpose for which it was disclosed under section 42 of the Act (where disclosure permitted). See Principle 3 on this point.

5.2
Organizations should develop guidelines and implement procedures with respect to the retention of personal information. These guidelines should include minimum and maximum retention periods. Personal information that has been used to make a decision about an individual shall be retained long enough to allow the individual access to the information after the decision has been made. An organization may be subject to legislative requirements with respect to retention periods.

Regulations under FIPPA (O. Reg. 460 s. 5) prescribe a general one-year minimum retention period for personal information following the last date of use of the information. Operational and legal considerations may require a longer retention period. In developing records retention guidelines, organizations should refer not only to FIPPA, but also to the *MBS Directive on the Management of Recorded Information and the Archives Act*.

5.3
Personal information that is no longer required to fulfill the identified purposes should be destroyed, erased, or made anonymous. Organizations should develop guidelines and implement procedures to govern the destruction of personal information.

Institutions subject to FIPPA may dispose of personal information only by (1) transferring it to the Archives of Ontario or (2) by destroying it in such a manner that the information cannot be reconstructed or retrieved. (O. Reg. 459 s. 2)

In addition, each institution must maintain a disposal record setting out what personal information has been destroyed or transferred to the Archives of Ontario and the date of that destruction or transfer. This disposal record must not contain personal information. (O. Reg. 459, s. 6)

5.4
Personal information must not be disclosed without proper authority. Under FIPPA, access to personal information within an organization should ordinarily be allowed only on a need-to-know basis (s. 42 (d)). Generally, this should be based upon a two-part test:

1) the employee must need access to the information in order to perform their duties; and

2) the access by the employee must be in support of a legitimate business function of the organization (i.e. they must not use their access privileges for personal reasons).

Under O. Reg. 460, s. 4 (2) the head of an organization is responsible for ensuring that only those individuals who need a record for the performance of their duties shall have access to it.

Disclosures outside the organization must be in accordance with section 42 of the Act (s. a-c, e-n).

5.5
This principle is closely linked to the Consent principle, the Identifying Purposes principle, and the Individual Access principle.

DISCUSSION

The principle of limiting use, disclosure and retention is particularly relevant in the context of data matching, profiling, and data warehousing. Such activities should be initiated only after the completion of a business case which includes its own privacy impact assessment, identification of the techniques which will be used to validate the result of the matching or profiling activity, and the method of notifying the individuals prior to taking action against them. The business case must be reviewed by the IPC in accordance with the *MBS Directive on Enhancing Privacy: Computer Matching of Personal Information*.

Another area in which the Limitation Principle may be relevant is with regard to public records. Public records are usually created by government agencies for some purpose which benefits society. For example, land title information is made public so that individuals can determine who the registered owner and lien holders are on a given property. Other records are public by custom, such as telephone directories.

New or additional uses of personal information which are not consistent with the context or purpose for which the record was initially made public may pose a major challenge. For example, the public would not expect land title information, including land value and the initial balance of the mortgage to be retrievable by the name of the owner. There is a public benefit is retrieving the information by property description; when the information is available by the name of the owner or mortgagor, the disclosure may become intrusive and, in some cases, may pose a threat to security.

Adopting new technologies to improve basic services creates opportunities for new uses, including revenue sources, which must be carefully analyzed in the context of fair information practices and privacy rights. Under FIPPA, the head of a public body is accountable for approving all consistent uses of public records. *The MBS Directive on Managing, Distributing, and Pricing Government Information (Intellectual Property)* provides guidance in these circumstances.

QUESTIONS FOR ANALYSIS

	YES	***NO***
Is personal Information used exclusively for the stated purposes and for uses that the average client would consider to be consistent with those purposes?	?	?
Are personal identifiers, such as the social insurance number, used for the purposes of linking across multiple databases?	?	?
Where data matching or profiling occurs, is it consistent with the stated purposes for which the personal information is collected?	?	?
Is there a record of use maintained for any use or disclosure not consistent with original stated purposes?	?	?
Is the record of use attached to the personal information record?	?	?
Is there any data matching between programs, ministries, and private sector partners which fall outside the purview of the *MBS Directive on Enhancing Privacy: Computer Matching of Personal Information*?	?	?
Where personal information is disclosed to an authorized data mart or data warehouse, does the head approve each new use, user, and matches?	?	?
1. Are such disclosures performed in consultation with the IPC and in compliance with *MBS Directive on Enhancing Privacy: Computer Matching of Personal Information*?	?	?
2. Is the individual to whom the information pertains informed of the disclosure?	?	?

ANTICIPATING PUBLIC EXPECTATIONS

Are the limitations on the use and disclosure of personal information set out in law or policy reinforced by the information and information technology architecture of the information systems?

NOTES

PRINCIPLE 6 – ACCURACY

Personal information shall be as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used.

6.1
The extent to which personal information shall be accurate, complete, and up-to-date will depend upon the use of the information, taking into account the interests of the individual. Information shall be sufficiently accurate, complete, and up-to-date to minimize the possibility that inappropriate information may be used to make a decision about the individual. (FIPPA s. 40 (2))

6.2
Section 40 (2) of FIPPA stipulates that the head of an institution shall take reasonable steps to ensure that personal information on the records of the institution is not used unless it is accurate and up to date. Organizations should note, however, that FIPPA does not require that personal information which is not being used be routinely updated.

By the same token, the CSA Standard holds that an organization should not routinely update personal information, unless such a process is necessary to fulfil the primary purposes for which the information was collected. When discrepancies are noted, the subject should be given the opportunity to correct or clarify discrepancies.

6.3
Personal information that is used on an ongoing basis, including information that is disclosed to third parties, should generally be accurate and up-to-date, unless limits to the requirement for accuracy are clearly set out.

QUESTIONS FOR ANALYSIS

	YES	*NO*
Does the record indicate the last update date?	?	?
Is a record kept of the source of the information used to make changes (e.g., paper or transaction records)?	?	?
Where applicable, is there a procedure, automatically or at the request of the individual, to provide notices of correction to third parties to whom personal information has been disclosed?	?	?
Are records kept regarding requests for a review for accuracy, corrections, or decisions not to correct?	?	?
Does the data subject have access to these records?	?	?
When an individual challenges the accuracy of a record, are they provided with information about the ministry contact person responsible for the records?	?	?
If the individual and the ministry program representative cannot reach agreement regarding the accuracy of the record(s), is the individual advised of his or her right to file a statement of disagreement?	?	?
Does the custodian of the record note the statement of disagreement on the record(s) in such a manner as to ensure that subsequent users who access the record(s) through any service channel are aware that the accuracy of the record(s) is disputed?	?	?

PRINCIPLE 7 – SAFEGUARDS

Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.

7.1
The security safeguards shall protect personal information against loss or theft, as well as unauthorized access, disclosure, copying, use or modification. Organizations shall protect personal information regardless of the format in which it is held. (O. Reg. 460 s. 4, and *MBS Directive on Information and Information Technology Security*.)

7.2
The nature of the safeguards will vary depending on the sensitivity of the information that has been collected, the amount, distribution, and format of the information, and the method of storage. More sensitive information should be safeguarded by a higher level of protection.

7.3
The methods of protection should include:

(a) physical measures, for example, locked filing cabinets and restricted access to offices;
(b) organizational measures, for example, security clearances and limiting access on a "need-to-know" basis; and
(c) technological measures, for example, the use of passwords, PKI, biometrics, and encryption.

7.4
Organizations shall make their employees aware of the importance of maintaining the confidentiality of personal information.

O. Reg. 460, s. 4 (1) states that every head shall ensure that reasonable measures to prevent unauthorized access to the records in his or her institution are defined, documented and put in place, taking into account the nature of the records to be protected.

7.5
Care shall be used in the disposal or destruction of personal information, to present unauthorized parties from gaining access to the information. (O. Reg. 459, s. 4 and 5 and the *MBS Information and Information Technology Security Directive*)

DISCUSSION

As information systems become larger and more complex, security risks increase and potential rewards for unauthorized access grow. These risks must be measured and evaluated in terms of the effect on public confidence, lost business days, costs of rebuilding the data, and the consequences to data subjects of corrupted data, public release, or covert use by unauthorized parties.

There are a variety of technological tools and system design techniques which may enhance both privacy and security. These may include strong encryption, technologies of anonymity or pseudo-anonymity, and digital signatures.

QUESTIONS FOR ANALYSIS

	YES	***NO***
Has there been an expert review of all the risks and the reasonableness or proportionality of countermeasures taken to secure against unauthorized or improper access, collection, use, disclosure, and disposal through all access channels?	?	?
Have security procedures for the collection, transmission, storage, and disposal of personal information, and access to it, been documented?	?	?
Have staff been trained in requirements for protecting personal information and are they aware of policies regarding breeches of security or confidentiality?	?	?
Are there controls in place over the process to grant authorization to add, change or delete personal information from records?	?	?
Is the system designed so that access and changes to personal information can be audited by date and user identification?	?	?

Are user accounts, access rights and security authorizations controlled and recorded by an accountable systems or records management process?	?	?
Are access rights only provided to users who actually require access for stated purposes of collection or consistent purposes?	?	?
Is user access to personal information limited to only that required to discharge the assigned functions?	?	?
Are the security measures commensurate with the sensitivity of the information recorded?	?	?
Are there contingency plans and mechanisms in place to identify security breaches or disclosures of personal information in error?	?	?
1. Are there mechanisms in place to communicate violations to stakeholders and to data subjects to mitigate collateral risks?	?	?
2. Are there mechanisms in place to advise appropriate ministry, corporate or other law enforcement authorities of security breaches?	?	?
Are there adequate ongoing resources budgeted for security upgrades, with specific measurable performance indicators in systems maintenance plans?	?	?

ANTICIPATING PUBLIC EXPECTATIONS

Have security risks been assessed from the point of view not only of the organization, but also of the client in terms of the potential impact of a security breach (e.g., is there potential for credit card numbers to be compromised)?

Where a particular delivery channel poses a high security risk, has an alternative been maintained?

NOTES

PRINCIPLE 8 – OPENNESS

An organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information.

8.1
Organizations shall be open about their policies and practices with respect to the management of personal information. Individuals should be able to acquire information about an organization's policies and practices without unreasonable effort. This information shall be made available in a form that is generally understandable. (FIPPA s. 31, 32, 45)

8.2
Organizations must make certain information available under FIPPA (s. 31, 32, 33, 34, 35, 36, 45). For the *Directory of Records*, for example, this information includes:

(a) the name/title and address of the person who is accountable for the organization's polices and practices and to whom complaints or inquiries can be forwarded;

(b) the means of gaining access to personal information held by the organization;

(c) a description of the type of personal information held by the organization, including a general account of its use;

(d) a copy of any brochures or other information that explain the organization's policies, standards, or codes; and

(e) what personal information is made available to related organizations (e.g. partners or subsidiaries).

8.3
An organization may make information on its policies and practices available in a variety of ways. The method chosen depends on the nature of its business and other considerations. For example, an organization may choose to make brochures available in its place of business, mail information to its customers, provide online access, or establish a toll-free telephone number.

QUESTIONS FOR ANALYSIS

	YES	*NO*
Do the *Directory of Records* and information management policies list all personal information banks collected under the control of legislation in government or 3rd party custody, including:	?	?
1. Where information is transferred to support indirect collection	?	?
2. The operation of shared or multi program data systems	?	?
3. Data marts or warehouses	?	?
4. Data transferred to a third party for business processing (e.g., credit and debit settlements)	?	?

ANTICIPATING PUBLIC EXPECTATIONS

Given that the minimum requirements for openness under FIPPA may not be adequate to meet public expectations or to ensure public confidence in a new program or initiative, the following questions might also be considered:

1. Have communications products and/or a communications plan been developed to fully explain information-processing practices so as to reassure the public, in some detail, about how their personal information will be protected?

2. Have opportunities for routine disclosure and active dissemination been fully explored, as recommended by the IPC? Routine disclosure occurs when access to a general record is granted on a routine basis as the result of a request. Active dissemination refers to the release of information without any request. For additional information, see *Routine Disclosure/Active Dissemination: A Joint Project of the Office of the Information and Privacy Commissioner/Ontario and The Freedom of Information and Privacy Branch, Management Board Secretariat*.

NOTES

PRINCIPLE 9 – INDIVIDUAL ACCESS

Upon request, an individual shall be informed of the existence, use, and disclosure of his or her personal information and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.

Note: In certain situations, an organization may not be able to provide access to all the personal information it holds about an individual. Exceptions to the access requirement should be limited and specific. The reasons for denying access should be provided to the individual upon request. Exceptions may include information that contains references to other individuals, information that cannot be disclosed for legal, security, or commercial proprietary reasons, and information that is subject to solicitor-client or litigation privilege.

Section 49 of FIPPA / s. 38 of MFIPPA set out the grounds for refusing to disclose personal information to the individual to whom it pertains. The grounds are enumerated in subsections 49(a) through (f) FIPPA/38(a) through (f) MFIPPA, and include those cases where disclosure:

- would constitute an unjustified invasion of another individual's personal privacy;
- would reveal a confidential source and the information relates to an evaluation or opinion compiled to determine suitability for employment or for the awarding of government contracts or other benefits;
- could reasonably be expected to prejudice the individual's mental or physical health; or
- could reasonably be expected to reveal information received in confidence.

9.1
Upon request, an organization shall inform an individual whether or not the organization holds personal information about the individual. Organizations are encouraged to indicate the source of this information. The organization shall allow the individual access to this information. In addition, the organization should provide an account of the use that has been made or is being made of this information and an account of the third parties to which it has been disclosed. (FIPPA s. 10, 31, 32, 35, 44-47)

9.2
An individual may be required to provide sufficient information to permit an organization to provide an account of the existence, use, and disclosure of personal information. The information provided shall only be used for this purpose.

9.3
In providing an account of third parties to which it has disclosed personal information about an individual, an organization should attempt to be as specific as possible. When it is not possible to provide a list of the organizations to which it has actually disclosed information about an individual, the organization should provide a list of organizations to which it may have disclosed information about the individual.

9.4
An organization shall respond to an individual's request within the time limits provided under FIPPA and may charge fees for access in accordance with the regulations (O. Reg. 460, s. 5.2, 5.3, 6, 6.1, 7, 8, 9). The requested information shall be provided or made available in a form that is generally understandable. For example, if the organization uses abbreviations or codes to record information, an explanation shall be provided.

9.5
When an individual successfully demonstrates the inaccuracy or incompleteness of personal information, the organization shall amend the information as required. Depending upon the nature of the information challenged, amendment involves the correction, deletion, or addition of information. Where appropriate, the amended information shall be transmitted to third parties having access to the information in question. (FIPPA s. 47)

9.6
When a challenge is not resolved to the satisfaction of the individual, the substance of the unresolved challenge should be recorded by the organization. When appropriate, the existence for the unresolved challenge should be transmitted to third parties having access to the information in question. (FIPPA s. 47)

DISCUSSION

Individuals sometimes disagree with the organization's interpretation of the information in their file. Where the organization is satisfied that the information is incorrect, it must correct the information in accordance with this principle. In those instances where the organization does not agree that the information is incorrect, the individual should be able to file a statement of disagreement which is displayed to authorized staff each time the contentious record is displayed.

QUESTIONS FOR ANALYSIS

	YES	***NO***
Is the system designed to ensure that access to all of the subject's data can be achieved with minimal disruption to operations?	?	?
Are the data subject's access rights assured for all the data sets of all the parties in the information life cycle, including private sector partners and subcontractors, 3rd parties provided subject information through profiling/matching?	?	?
Are all custodians aware of the right to access, formal or informal request procedures, mandatory advising of formal appeal procedures to data subjects, fees, and limits of their decision making authority?	?	?

ANTICIPATING PUBLIC EXPECTATIONS

In some cases, it will be both possible and desirable to provide routine access to personal information. For example, an individual may wish to verify the address a program has on file in order to confirm that it is up to date. Having such a request go through the formal freedom of information process adds unnecessary complexity and expense. Routine access should be provided wherever possible.

Have opportunities for providing routine access to personal information been fully explored? Is routine access supported through appropriate policies and operational procedures?

NOTES

PRINCIPLE 10 – CHALLENGING COMPLIANCE

An individual shall be able to address a challenge concerning compliance with the above principles to the designated individual or individuals accountable for the organization's compliance. *(FIPPA, Part IV)*

10.1
The individual accountable for an organization's compliance is discussed under principle one.

10.2
Organizations shall put procedures in place to receive and respond to complaints or inquiries about their policies and practices relating to the handling of personal information. The complaint process should be easily accessible and simple to use.

10.3
Organizations shall inform individuals who make inquiries or lodge complaints of the existence of relevant complaint mechanisms, such as internal processes and remedies available through the IPC's office. In addition, where government services are delivered through third parties, organizations should ensure that these parties notify individuals of the existence of such mechanisms where relevant. (See the *MBS Directive on Alternative Service Delivery Framework*)

DISCUSSION

Ministries are accountable under FIPPA for complaints regarding the collection, use, and disclosure of personal information under their control and on their behalf, and for responding to access requests within legislative time frames. In addition, individuals may complain to the IPC.

Ministries and partners should establish procedures to informally resolve customer complaints regarding personal information practices. Mechanisms should be put in place to ensure that partners co-operate fully with the responsible ministry and provide all necessary information to respond to a complaint or appeal.

QUESTIONS FOR ANALYSIS

	YES	*NO*
Complaint procedures are established including links to partnership agreements and staff role assignments.	?	?
A procedure has been established to log and periodically review complaints and their resolution with a view to establishing improved information management practices and standards.	?	?
Oversight and review mechanisms comparable to those ensuring the accountability of public sector bodies covered by FIPPA are being implemented.	?	?
Proportionate to the level of activities outside the direct supervision of ministry personnel, regular independent compliance audits of partner information practices and privacy requirements have been established as contractual deliverables.	?	?

ANTICIPATING PUBLIC EXPECTATIONS

While the emphasis in Principle 10 is on responding to specific complaints, organizations should also be aware of the risk of more generalized policy critiques. The Annual Report of the IPC, for example, may call public attention to certain design features that may undermine the protection of personal information. Such critiques often focus on the broad privacy implications of a given program or proposal, rather than simple technical compliance with FIPPA. Organizations must be sensitive to these risks when assessing the privacy implications of their proposals.

Questions which may help organizations to understand the sources of such risks would include:

1. Has a similar program been proposed or implemented in other jurisdictions (nationally or internationally) and, if so, how did watchdog agencies, the media, and the public react? What elements of the program, if any, caused the greatest public concern, and what measures have been put in place to pre-empt similar reactions in Ontario?

2. Have watchdog agencies, including privacy commissioners in other provinces, issued reports or opinions on issues that would be relevant to the proposal and, if so, have these been taken into account?

Where appropriate, have key internal or external stakeholders been provided with an opportunity to comment on the implications of the proposal for the protection of personal information?

NOTES

SUMMARIZING THE RESULTS – STEP THREE

At this stage in the process, organizations should have both a detailed account of the data flow within a program or proposed program, and an analysis of compliance with FIPPA and broader privacy principles. This should provide a solid basis for determining whether there are any outstanding privacy issues which should be addressed before or as the proposal moves forward.

Organizations should have identified and resolved technical compliance with the requirements of FIPPA through the PIA process. Therefore, any outstanding privacy issues which will form part of the summary document will relate to compliance with broader privacy principles and possible triggers of negative public reaction. An understanding of the environment in which the proposal is being made and of public expectations with regard to privacy must, therefore, figure prominently in the determination of what the outstanding issues are.

In summarizing their results, organizations should keep in mind that one of the key goals of the privacy impact assessment is to provide senior executives and the government with the tools necessary to make fully- informed policy and system design and/or procurement decisions based on an understanding of privacy risk and of the options available for mitigating that risk. When preparing the summary of the results of the PIA, then, analysts should seek to communicate clearly about risks or possible risks that have been identified through the PIA process, particularly where those risks have not been successfully addressed through system design or policy measures (i.e. *residual* risks).

While the format of the summary will be largely determined by the organization's needs, it should, at a minimum, convey the following information:

- ✓ ***Description of the proposal*** including programs and/or partners involved, objectives, timing and key milestones, resource requirements, public benefits, and pointers to more detailed information about the proposal;
- ✓ ***List of relevant legislation*** that may have a bearing on privacy requirements, including program statutes, and relevant policies, including any applicable Management Board Directives;
- ✓ ***Identification of specific privacy risks*** relevant to the proposal (see template below);
- ✓ ***Options*** that exist for addressing or mitigating those risks, along with the implications of each option;
- ✓ ***Analysis*** of whether other jurisdictions, either in Canada or internationally, have addressed similar risks and whether their approaches were successful;
- ✓ ***Identification of any residual risks*** that cannot be addressed through the proposed options and, where possible, an analysis of the likely implications of these residual risks in terms of public reaction and program success; and
- ✓ ***Proposed*** privacy communications strategy, if appropriate.

Privacy Risks Identification Template

Privacy Risk	Description	Addressed by	Not Addressed

PART FIVE – LINKAGES TO GOVERNMENT MANAGEMENT PROCESSES

In June 1998, Management Board of Cabinet (MBC) approved the recommendation from Management Board of Secretariat (MBS) that a completed PIA be required prior to approval of I&IT projects that involve changes in the management of personal information held by government programs.

In December 1999, the *Privacy Impact Assessment Guidelines* were approved and finalized, and are now being used to assess privacy implications in a number of I&IT projects (e.g., data warehousing, electronic service delivery, etc.) dealing with personal information within the government. Ministries are asked to self-identify, but Cluster CIOs have ultimate responsibility to identify new I&IT business proposals that may affect client privacy.

Co-operation and linkages across the government have been established to meet MBS direction with regards to *I&IT Business Planning* processes, *Enterprise Architecture* planning and the *Architecture Review Board* processes.

The *PIA Guidelines* may be used in early planning stages, or as part of consulting contract deliverables, but must be included in MBC submissions that involve changes in the management of personal information held by government programs.

This requirement ensures that the privacy of individuals is an integral component in the design of new service delivery, technology or information systems, not only at the beginning but also throughout the development and maintenance life cycle of these projects across the government. This approach is intended to preclude inappropriate investments in early strategies and development work, and the need to substantially revise such projects.

The PIA process takes project sponsors through a series of steps that assist them in confirming that their proposed initiatives meet basic privacy objectives, and promote fully informed policy decision-making and system design choices.

Architectural Review Board

Prior to receiving MBS approval of I&IT business projects, sponsoring ministries are required to have their initiatives reviewed by the *Architectural Review Board* (ARB). The ARB is a "gatekeeper" board and does not have priority or budgetary (resources) responsibilities. The ARB's primary function is to uphold quality assurance and standards with the criteria as noted within the scope of responsibility. The board's decisions are final for projects that are in compliance with the Enterprise Architecture.

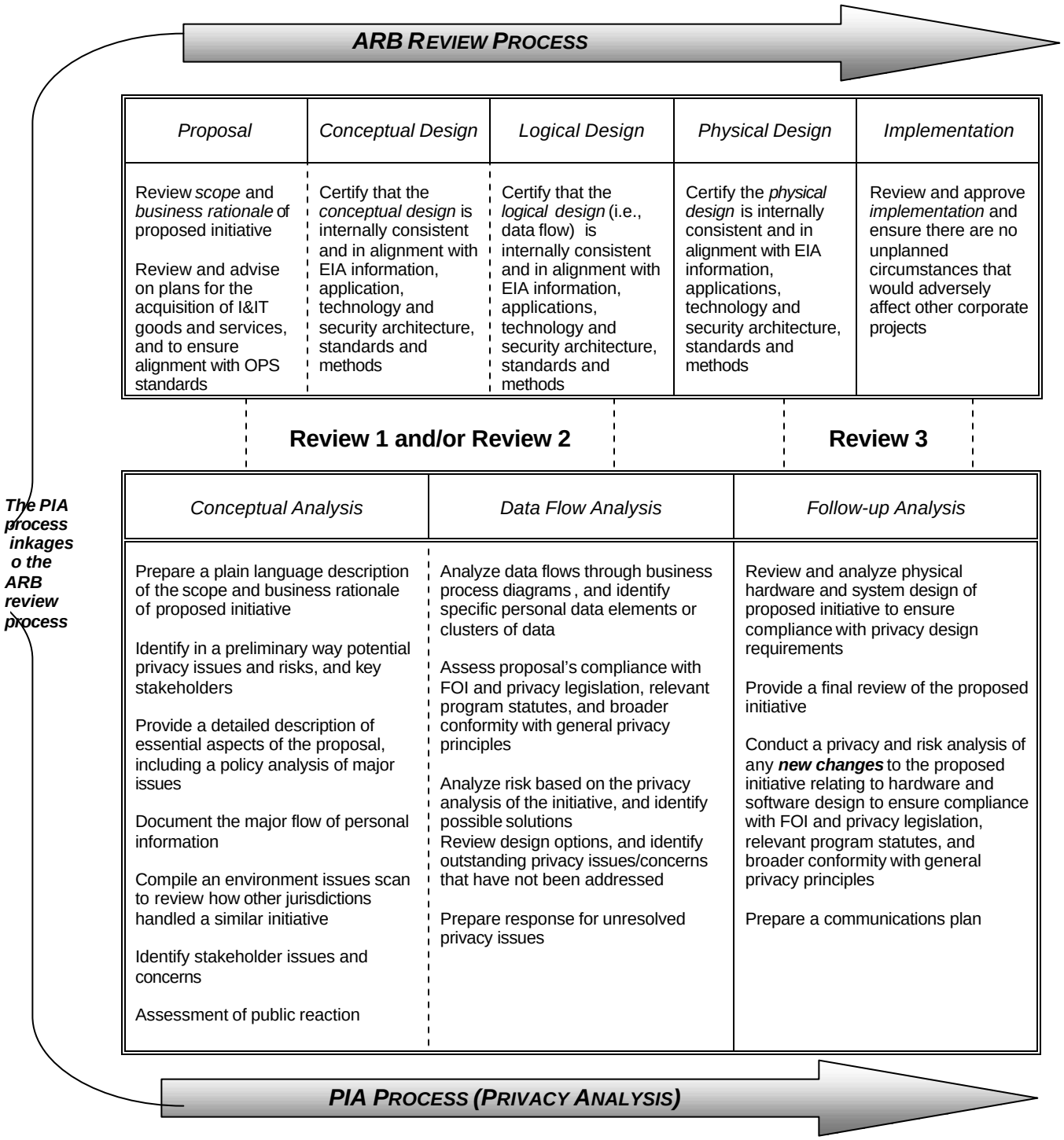
Projects will be asked to go to the *Information and Information Technology Executive Leadership Council* (IITELC) where they are enterprise-wide in scope (major milestones), non-compliant with the Enterprise Architecture or in the case where the ARB recommends changes are required to the project or the project needs to stop due to non-compliance. In addition, ARB discussions and decisions will be reported to IITELC on a monthly basis.

The ARB requires a PIA to be prepared for I&IT business projects that may affect client privacy as part of its review process to ensure that privacy issues and concerns are fully identified, documented and addressed. To assist ministries in preparation for the ARB review process, this section of the *PIA Guidelines* illustrates how the PIA structure is linked to the decision-making structure of the ARB processes.

This section also incorporates terminology and concepts that are consistent with the *Enterprise Information and Information Technology Architecture* (EIA) framework. The EIA framework is based on the *Zachman Framework*, and like the *PIA Guidelines* is a project management tool (and process) intended to assist project managers and system designers in their development of I&IT project that support the government as a whole.

The *Architectural Review Board and Privacy Impact Assessment Review Process* diagram outlined below is intended to guide project sponsors through the ARB review process. The table identifies what the different ARB stages are and explains what is required from a privacy impact assessment perspective. The table also lists the three ARB review steps that all I&IT projects are required to have before proceeding to final review stage.

ARCHITECTURAL REVIEW BOARD AND PRIVACY IMPACT ANALYSIS REVIEW PROCESS



RESOURCES AND GLOSSARY

PIA EVALUATION FORM

We are committed to continuous improvement of the PIA. In order to ensure that the PIA Guidelines meet the needs of the people working most closely with them, we would ask you to take a moment to fill in this evaluation form. Please feel free to copy the form for other members of your team.

Completed evaluation forms should be sent to:

Information and Privacy Office
Management Board Secretariat
77 Wellesley Street West, 8th Floor
Toronto, Ontario M7A 1N3

If the space provided for any of the answers is insufficient, please attach additional pages.

OVERALL ASSESSMENT

Did you find the PIA guidelines easy to work with? If not, please indicate which sections you found difficult and why.

Are there additional resources that you suggest be added to the Guidelines (e.g. web resources, reports, etc.)? If so, please detail.

Did you seek assistance from the Information and Privacy Office? If so, was it for a particular issue or for general guidance?

Would you have preferred to have had training prior to completing the PIA? If so, please indicate what areas you would have liked to be trained in, such as privacy policy issues, legislative requirements, privacy in systems design, etc.

PART ONE

Was the purpose of the PIA clear to you after reading Part One?

Did you have difficulty determining whether a PIA was required for your proposal?

Were you able to appropriately anticipate the resource requirements of the PIA based on the discussion in the Guidelines?

Identify the areas of expertise that you drew upon to complete the PIA (e.g. legal, technical, communications, system designers):

PART TWO

How would you rate your familiarity with privacy issues before beginning the PIA? Please circle one.

5- very familiar 4- familiar 3- somewhat familiar 2- not very familiar 1- not familiar

Did you find the discussion about privacy in this chapter to be at the appropriate level? If you found it either too basic or too complex, please indicate what kind of information you would like to see added or removed.

Did you feel that there was enough information provided about tools for protecting privacy, such as privacy-enhancing technologies?

PART THREE AND PART FOUR

Did you find that the three components of the PIA were useful in contributing to the end goal of the PIA?

Would you add, remove, expand, or retract any of the three components? Explain.

Did you experience any difficulty in documenting the data flow?

In general, did the Privacy Analysis questions cover areas relevant to your proposal?

Were there many questions that were not relevant to your project? If so, please indicate what these questions were about.

Did you add any questions? If so, please indicate what these questions were about.

Did you find the questions related to anticipating public reaction useful? Explain.

Were the instructions for preparing the risk management plan sufficiently clear?

Would you have preferred that a standard template for the risk management plan be provided?

Did the risk management plan meet the expectations of senior management in terms of the level of detail and the type of information provided? Explain.

ADDITIONAL COMMENTS

Are there any additional comments about any aspect of the PIA Guidelines that you would like to make?

Thank you for completing this evaluation; we appreciate your input.

Name

Ministry

If you would be willing to participate in a work group to review the PIA, please attach a business card or provide contact information in the space below.

GLOSSARY OF TERMS

Adequate notice – one or more statement(s) that fully describes to an individual, the purposes of collection, use, disclosure and retention of personally identifiable data to him or her.

Acquisition phase – a stage when system hardware and software is purchased or leased.

Alternative Service Delivery – practices that offer a substitute for the conventional methods of delivering government services.

Anonymizing the data – the act of removing personal identifiers from data i.e. converting personally identifiable information to aggregate data.

Application of rules – principles to which a computer program is required to conform while processing data or transactions.

Artificial intelligence (AI) – intelligence produced by human effort rather than originating naturally i.e. the result of computers and code developed by programmers used to store and manipulate large volumes of data from single or multiple programs.

Biometrics - a measurable, unique biological feature or personal trait used to recognize the identity or verify the claimed identity, of an individual.

Business process diagram – a course of action or a series of stages in for example manufacture or some other business operation describing the series of changes from start to finish for all business functions.

Client privacy – preventing unauthorized collection, use and disclosure of customer data by computerized or other means

Computer system vulnerabilities – an assessment of threats and risks e.g. unauthorised access, data loss or modification etc. based on the computer system environment and data sensitivity

Common (Network) Directory Services – a list of all internal system users (behind a firewall) including electronic routing information to deliver for example electronic mail.

Contract specifications and penalties – legal and binding agreements between contracting parties outlining the consequences for a breach of contract provisions

Consent statements for clients – notice to individuals regarding collection, use disclosure and retention of personal data including consequences of providing or withholding consent

Contractual – in the nature of a contract

Data flows – mapping the flow and manipulation of information within a system or between multiple systems that may or not use computer technology

Data inputs – data that is operated on by any process or system

Data profiling/data linkage – recording and collection of personally identifiable information that reveal personal manner and attitude

Data map – associate each element of a data set (input) with elements of the output data set in the context of computer processing and electronic transmission of data.

Data Warehousing and Data Marts – a federated data warehouse is a centralized repository for all electronic data. Data from different programs is intergated here. Users are not permitted to access federated warehouse data. Data from the warehouse is exported in whole or in part to data marts for access by users. (The role of the data warehouse and data mart can also be reversed i.e. whether data is imported or exported from a data warehouse to a data mart depends on the implementation strategy).

Delivery Channel Management – managing the medium used to access or deliver government services.

Devolution – delegation of power to local or regional administration

Directive on Enhancing Privacy: Computer Matching of Personal Information – mandatory rules for linking data between two or more data sets.

Due diligence audits – independent confirmation (by an auditor) demonstrating adequate care and effort applied to one's work.

Eligibility data – a collection of data fields and elements required to determine qualifications for a government program.

Enterprise Information and Information Technology Architecture Principles – are overarching goals and objectives that apply to all technology and systems at an enterprise wide level.

Expressly authorized by statute – distinctly shown as permitted by law.

Facilitating surveillance – making it easier to track or profile the experience of individuals across government programs

Identification and authentication schemes – the process of determining and verifying the identity of an individual.

Identification of individuals – in an electronic service delivery context this involves a registration process where physical and other attributes of identity claims are verified resulting in the issuance of electronic identity certificates. The electronic certificates are used to electronically authenticate individuals who wish to access government services or programs to determine eligibility etc.

Indirect collection of personal information – personally identifying information collected from sources other than directly from the data subject

Information management life cycle – includes the collection, use, disclosure and retention of recorded information

Information systems – the process of capturing, recording, storing and manipulation of data with or without the use of computer technology.

Irregular Business Transactions – not processed according to the usual rules or processing of unanticipated business requirements.

Legislative amendments – process of changes to written law or legal requirements

Localizing data collection activities through a common private sector window – assigning data collection across government programs to a particular place or organization.

Materially changing the status of personally identifiable information – arrangements that may alter the rules and accountability for managing personal information.

MBC Directives – mandatory requirements for all Ontario Government ministries

Merging previously isolated transaction systems into a common governmental window – in this case transactions would loose the character or identity of their sponsoring program or ministry e.g. multi-function electronic kiosks or service counters

Monitoring and enforcement mechanisms – tracking methods of compliance.

Multi-program front-end delivery integration - the act of combining parts of existing programs into a common process e.g. registration, common service counter etc.

Multi-purpose identifiers – a unique number or symbol assigned to an individual for use by more than one government program

Physical observation of individuals – creating a profile regarding the movement of individuals from data captured by electronic recording and monitoring devices e.g. cameras, vehicle transponders etc.

Privacy-enhancing technologies (PETs) – are those technologies that provide users with control in terms of collection, use and disclosure of his or her personal information such as encryption, digital signatures, and anonymous electronic cash and service delivery systems

Program integration – the act of combining parts of existing programs into a common process.

Pseudo-identification – purported or supposed identity i.e. not genuine identity

Pseudonymity – fictitious name assumed by the author

Publishing or re-distributing public databases containing personal information – the act or instance of making partial or entire content of a database publicly known

Relevant program statutes – regulatory environment for a government program

Retrofitting systems for privacy compliance – changes to system design and logic impacting the collection/capture, processing, storage and or transmission of data

Risk assessment – the process of quantifying the impact of implementing a particular idea, process, system or strategy

Service Monitoring – maintaining regular surveillance over electronic delivery of services using computer programs that record and track information about clients in order to manage or improve services.

Smart Cards – are cards that contain a computer processor i.e. the card may be a full computing device with (contact or wireless) networking capabilities. Smart cards have the capacity for computations, running software applications, data storage and interactions with other computing devices.

Soliciting voluntary individual consent – individuals acting on their own free will in giving permission to have their data collected and stored in a data warehouse

System development life cycles – start-to-finish timelines related to commencing a project through to system implementation.

System design – mapping functional requirements and program logic to automate capturing, storing, manipulating, retrieving and outputting data using computer technology.

Technical compliance – meeting requirements of a regulatory framework.

Transaction monitoring – maintaining regular surveillance over electronic interaction by individuals in their personal or official capacity.

Untraceable anonymity – where source of authorship can not be determined

Value-added information services – the increase in value of output data over input data that is processed by a computer relative to subjective interest of the end user.

RELATED LINKS

Enterprise Information and Information Technology Architecture Principles
http://intra.itpb.gov.on.ca/eia/home/index.htm

European Privacy Directive (full title)
http://europa.eu.int/eur-lex/en/lif/dat/1995/en_395L0046.html

Canadian Standards Association Model Privacy Code; see Schedule 1 of the *Personal Information Protection and Electronic Documents Act*
http://www.privcom.gc.ca/english/02_06_01_e.htm

Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (108/81)
http://europa.eu.int/comm/internal_market/en/media/dataprot/inter/con10881.htm

Information and Privacy Commissioner's 1998 Annual Report
Privatization of Ontario Hydro
http://www.ipc.on.ca/english/pubpres/ann_reps/ar-98/ar-98e.htm

Management Board Directive on Enhancing Privacy: Computer Matching of Personal Information
http://intra.cpb.gov.on.ca/html/Enhprivd.html

Management Board Directive on Managing, Distributing and Pricing Government Information (Intellectual Property)
http://intra.cpb.gov.on.ca/html/Govpubd.html

OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980)
http://www.oecd.org//dsti/sti/it/secur/prod/PRIV-EN.HTM

Routine Disclosure/Active Dissemination (RD/AD): A Joint Project of the Office of the Information and Privacy Commissioner/Ontario and The Freedom of Information and Privacy Branch, Management Board Secretariat)
http://www.ipc.on.ca/english/our_role/code/practices/numb22.htm

Safety and Consumer Statutes Administration Act, 1996 from Publications Ontario
http://209.195.107.57/

The Freedom of Information and Protection of Privacy Act, and *the Municipal Freedom of Information and Protection of Privacy Act*
http://www.gov.on.ca/MBS/english/fip/act/act.html

The Personal Information Protection and Electronic Documents Act
http://www.privcom.gc.ca/english/02_06_01_e.htm