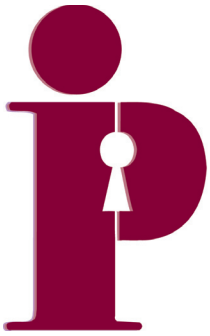
Privacy Risk Management

Building privacy protection into a Risk Management Framework to ensure that privacy risks are managed, *by default*



Information and Privacy Commissioner
Ontario, Canada

April 2010

Acknowledgements

The Information & Privacy Commissioner of Ontario, Canada wishes to acknowledge and thank Monica Merrifield, Vice President Risk Intelligence, YMCA of Greater Toronto; Fariba Anderson, Vice President IT Lottery, OLG; Dan Ruch, Chief Operating Officer, Ruch & Associates Inc.; and Jeff Kirke, Strategic Advisor to the Commissioner, for co-authoring this paper; and Niver Rubenyan of Sun Life Assurance Company of Canada, for her helpful contribution.

Information and Privacy Commissioner, Ontario, Canada

2 Bloor Street East
Suite 1400
Toronto, Ontario
M4W 1A8
Canada

416-326-3333
1-800-387-0073
Fax: 416-325-9195
TTY (Teletypewriter): 416-325-7539
Website: www.ipc.on.ca
Privacy by Design: www.privacybydesign.ca

Table of Contents

Foreword

In September, 2008, I delivered a presentation entitled, "*Minimize Risk – Maximize Protection and Gain a Competitive Advantage: Privacy is Good for Business,*" at the 33rd Annual RIMS Canada Conference in Toronto. My message – that the protection of personal information, embedded from the outset into an organization's technology, could be used to positively differentiate one organization from another, was well-received. Many participants approached me following my remarks to express their interest in better understanding the relationship between privacy and risk management. It seemed as though the idea of "privacy risk" had not yet come to the fore.

Encouraged by the suggestion of several attendees that we should develop a paper to further explore the issues and opportunities associated with integrating the two disciplines, I assembled a working group of privacy and risk management professionals in early 2009.

Early on, it became apparent that my concept of *Privacy by Design*, something I developed back in the '90s, complemented the various risk management frameworks that were frequently employed. Focussed on preventing privacy risks, *Privacy by Design* compels business leaders and developers to build privacy protection into, not just their technology, but also their business processes, physical design and networked infrastructure. In essence, it helps organizations to operate in a mode of what I call "default" privacy protection.

This paper is intended to open a dialogue. An introductory piece, it is targeted at risk management professionals and assumes a working knowledge of the fundamentals of that discipline. Identifying the growing significance of "privacy risk," it describes the manner in which *Privacy by Design* may be integrated within an organization's existing risk management process. In my experience, those who successfully embed privacy into their day-to-day operations are also delighted to discover that they've gained a sustainable competitive advantage.

Ann Cavoukian, Ph.D.
Information & Privacy Commissioner
Ontario, Canada

Introduction

The idea that privacy – an individual's right to control the collection, use and disclosure of information about him or herself – may present risk, seems to be a new one to many. That it should be a novel concept to those responsible for managing risk, however, needs to be addressed. Personal information is an asset, the value of which is protected and enhanced by a suite of security practices and business processes. Like other operational risks, those related to the protection of personal information benefit from the scrutiny of a formal risk management discipline.

Issues of privacy are associated with the management of Personal Information (PI), which describes much of the data collected by an organization regarding its employees, prospects and customers. Its hallmark is that it can be linked to an identifiable individual, either directly or indirectly. While all PI is to be respected, some elements are considered especially sensitive (i.e. financial information, health records, etc…), warranting special care and therefore, presenting added risk.

The cost of a data breach can be staggering. A survey of US. companies in 2009 yielded an average cost of $204 per compromised record; one breach of 100,000 records cost $31M to resolve.[1] Importantly, individuals also bear significant costs. In addition to contending with real financial damages, those made aware of a breach may also choose to purchase services to help protect themselves against future harm. Lifetime harm (the risk of which cannot easily be transferred through any form of insurance) may also arise, as in the case of compromised biometrics – after all, one has only a single set of fingerprints for life.

Personal Information Drives Privacy Risk:

Privacy risks and opportunities arise because of gaps between the sensitivity and/or quantity of personal information and how it is managed. A coin laundromat, for example, handles little personal information and so, need not dedicate substantial resources to privacy. The same cannot be said, however, of a doctor's office which manages both a high volume of, as well as some of the most sensitive information, that can be collected – one's health information. Information sensitivity and stakeholder expectations are critical barometers in determining an appropriate degree of diligence with respect to the protection of personal information.

The potential for irreparable harm, a function of the type of personal information compromised, demands an approach to risk management that can best be characterized as proactive. In fact, effective management of privacy risks or, as we call it, Privacy Risk Management (PRM) is preventative in nature – well-executed, it endeavours to eliminate privacy risk *before* the breach. This is accomplished by ensuring that privacy-protective measures are built into technology and processes – so that they become an organization's *default* mode of operation.

This approach to privacy – proactive, focussed on embedded protections, ever-present as the default – is called *Privacy by Design*[2] – a concept that was developed back in the '90s by Dr. Ann Cavoukian, the Information & Privacy Commissioner of Ontario, Canada. Noting that

1 http://searchsecurity.techtarget.com/news/article/0,289142,sid14_gci1379486,00.html#

2 *Privacy by Design* is more fully explained in Appendix 1 and, "Privacy by Design – The 7 Foundational Principles," The Information & Privacy Commissioner of Ontario, 2009. http://www.ipc.on.ca/images/Resources/7foundationalprinciples.pdf.

the increasing complexity and interconnectedness of information technologies posed a threat to privacy that regulation and legislation alone could no longer effectively safeguard against, Dr. Cavoukian pioneered the notion of privacy as a design feature – making it a default. A significant feature of her approach is its positive-sum or "win-win" nature – meaning that by embedding privacy from the outset, other business requirements, such as security and risk management, can be met without compromise.

Integrating a forward-looking approach to privacy, like *Privacy by Design* (*PbD)*, benefits an organization in several respects. Importantly, as an approach, it is complementary to virtually all risk management disciplines[3], which greatly simplifies implementation. It can also prove to be a cost-saving measure. Generally speaking, it is less expensive to build a feature (like privacy) into a system from the outset than it is to go back after the fact and attempt to "bolt it on" in response to legislation or industry best practices.

This paper introduces the concept of Privacy Risk Management (PRM). It begins by examining characteristics indicative of an organization's privacy and risk management maturity. While PRM offers benefits to any organization, not all will possess the prerequisites to fully implement it. Using a "roadmap," this section may provide insight into the steps that organizations can follow to optimize their approach to PRM.

Before examining the impact of privacy on the risk management process, consideration is given to the role of a Privacy Risk Management Practitioner. As with other forms of risk, everyone within an organization is responsible for protecting privacy. PRM Practitioners fulfill the role of privacy change agent and process custodian.

Finally, using the ISO 31000 Risk Management Framework, the impact of leveraging *PbD* is considered. Employing both *PbD* and ones established risk management process, organizations command a powerful process which will help to mitigate or eliminate a variety of privacy risks.

Risk is inherent in any pursuit which seeks to create value. Successful organizations, regardless of size, industry or structure, grow because they continually seek ways to embrace new opportunities and to manage risk – ***both*** need to be done effectively. Depending on the organization and the volume of personal information in its care, privacy risk may warrant special attention. In a very real sense, the choice that executive leadership must make is whether they're inclined to, "Pay now; or pay *more* later."

When is an organization ready to implement Privacy Risk Management?

Regardless of the size, structure or nature of an organization, its management of personal information unavoidably gives rise to risk. Such risk warrants adoption of a Privacy Risk Management (PRM) framework.

3 In this paper, we consider the integration of *PbD* and the ISO 31000 Risk Management – Framework.

Successful PRM depends upon an organization's approach to both the privacy and risk management disciplines. In fact, commitment to robust privacy and risk management programs on the part of senior leadership is at least as important as an organization's maturity with respect to either.

Task maturity, or the institutional ability to perform particular duties, is a useful method to gauge an organization's approach to privacy as well as their preparedness and capacity to respond to various risks. Appendix 2 presents a chart which may be used to roughly assess the pertinent dimensions of privacy and risk management task maturity. Taken as prerequisites, the attributes identified in the Appendix must each be practiced at a sufficiently advanced level to enable successful PRM implementation. Organizations which do not demonstrate this range of task maturity are encouraged to first focus on creating a "Culture of Privacy"[4] and/or adopt a risk management discipline.

As with traditional risk management, organizations which successfully launch a PRM discipline discover that it creates value through attention to "rewarded risk." It has been noted that,

> "In enterprises where risk management capabilities are not fully developed, unrewarded risk often represents the full extent of their risk management activities. Unrewarded risk gets its name from the fact that there is no premium to be gained for taking certain kinds of risks (for example, risks affecting operations, integrity of financial statements, and compliance with laws and regulations).
>
> Conversely, rewarded risk focuses on value creation; it involves managing risks to future growth, including putting capital at risk and making profitable bets. In rewarded risk-taking, a company receives a premium for taking and managing risks - and receiving approval in the marketplace - associated with new products, markets, business models, alliances, and acquisitions."[5]

Organizational Orientations

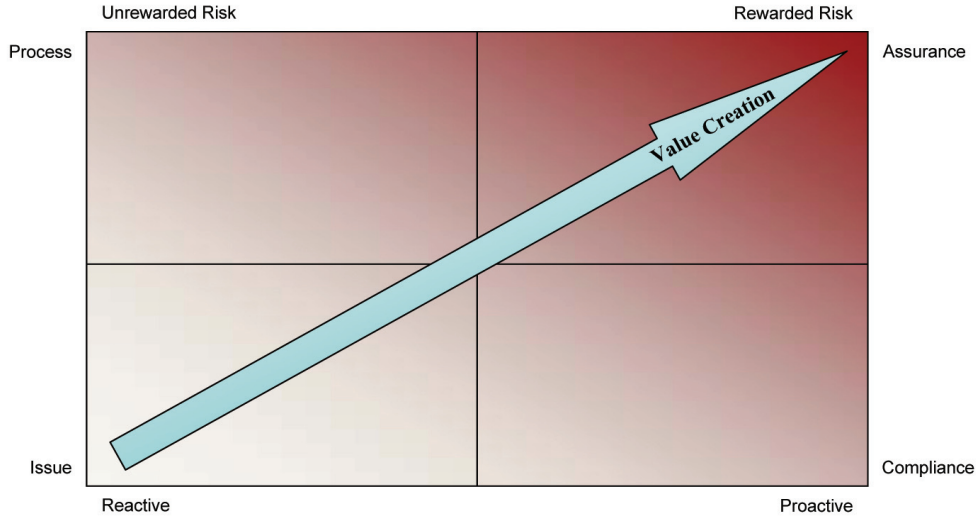


Figure 1. Organizational orientation leading to value creation

4 Privacy and Boards of Directors: What You Don't Know *Can* Hurt You," The Information & Privacy Commissioner of Ontario, 2007.

5 "The Risk Intelligent Enterprise – ERM Done Right," Deloitte Centre for Risk Intelligence.

The impact of privacy and risk management task maturity, as well as the benefits associated with PRM may be reflected in a matrix (Figure 1). Value creation, previously described as the benefit of attention to rewarded risk is also associated with the relatively mature practices of a focus on process rather than on individual issues as well as one on privacy assurance rather than simply on compliance. Above all, superior performance in each of these attributes accrues to organizations which demonstrate a key *PbD* trait – they are proactive rather than reactive.

What is the role of the Privacy Risk Management Practitioner?

Effective Privacy Risk Management Practitioners fulfill two fundamental roles: Change Agent and Process Custodian.

Privacy as a Catalyst for Broadening Risk Management Strategy

In 2002, the risk manager at the YMCA of Greater Toronto began 'integrative risk' activity when she spotted and embraced the opportunity to champion privacy.

Approaching 'privacy' as both a strategic and an operational risk flowing through the entire organization, the Risk Manager began cross-functional activity, working alongside program and process owners, to ensure readiness for changes in privacy law and to enhance the YMCA's commitment to privacy.

Privacy successes strengthened internal relationships, creating natural leverage for the risk manager to embark on an enterprise-wide risk management strategy, broadening the focus beyond traditional insurance and hazard risks.

1. **Change Agent** – Assuming the role of PRM Practitioner, the risk manager or other technical expert embarks on a strategic journey by taking the first steps in embedding privacy within the risk management process. In so doing, the PRM Practitioner helps to raise privacy risk consciousness within an organization. As observed in the 2006 RIMS Annual Survey of Risk:

> "Strategic risk management today means leading, not merely responding to events or demands from senior management. It means pushing to play a role in managing every aspect of the evolving risk environment, becoming a change agent rather than merely a caretaker of the 'traditional' risk management areas (of insurance and hazard risks)."[6]

2. **Process Custodian** – As with other types of risk, everyone in an organization has a role to play in managing privacy risk. The risk manager is especially well-equipped and ideally-positioned to take on the role of PRM Practitioner working alongside others involved in managing privacy risk including an organization's executive, business unit managers and support functions.

Figure 2 highlights the role of the PRM Practitioner as well as other functional roles and resource groups involved in managing privacy risk. Although smaller organizations may not assign an individual to each of the roles, identified, the responsibilities and contributions described below will nonetheless exist as part of other roles or may be outsourced, depending on the nature of the business.

6 *The Changing Face of Risk Management, Marsh / RIMS Annual Survey of Risk, 2006.*

PRM Practitioners may be members of an organization's IT, compliance, internal audit, privacy or risk management teams. Given the importance of embedding the discipline of managing privacy risk within an organization's existing risk management processes, however, they may find a more natural home in the risk management area.

Functional Role	Responsibility	Contribution
Leadership (Board, CEO, Founder)	Governance / Culture	Foster culture of privacy; establish risk appetite; and describe policies clarifying expectations.
Senior Privacy Executive	Accountability	Formal responsibility for privacy issues; ensure privacy is embedded in organizational processes. Role may be held by a Chief Privacy Officer, VP of IT, or CFO, among others.
PRM Practitioner (risk manager or other technical expert)	Process Management	Custodian of PRM process; provide guidance on process implementation; ensure privacy is included in organization-wide risk assessment; and offer insights on treatment options for emerging privacy risks.
Business Unit Managers	Risk and Control Owners	Identify and treat privacy risks and ensure continuous improvement. These managers represent an organization's operational leadership.
IT / Corporate Security	System Security	Maintain information system structure and integrity, including both logical and physical security.
Marketing and Sales	Brand / Reputation	Create products, services and programs with an eye to responsible use of personal information.
Customer Service / Quality Management	Monitoring	Monitor trends in privacy issues, providing an early warning for needed enhancements to increase organizational commitment to privacy.
Legal / Compliance / Internal Audit	Compliance/Assurance	Verify that privacy assessment and treatment processes are effective.

Figure 2. Roles and contributions associated with the PRM process.

Beyond their department affiliation, successful PRM Practitioners will generally demonstrate the following characteristics:

- **Process-Oriented** – The implementation of PRM programs demands business process engineering skills. Methodical and possessing a clear, end-to-end vision of business operations, they will assist in the development of privacy-protective processes throughout the organization.
- **Organizationally Astute** – Practitioners must avoid the urge to claim territory. As some tension between functional areas may arise while engaging in cross-functional activity, PRM Practitioners should focus on how they can complement what others are already doing. They must create and sustain the 'buy-in' that is key to fostering a culture of privacy and realizing the benefits that flow from effective PRM.
- **Effective Communicator** – The PRM Practitioner is not a 'superman'. They manage through a blend of technical expertise and, more importantly, moral suasion.

Successful PRM Practitioners evaluate and synthesize both internal and externally-oriented information. They demonstrate both reflective and integrative thinking. Other important skills and attributes include: project management; a strong knowledge of the business; and an ability to build relationships especially with business risk and control owners. Above all, being a facilitator, seeking opportunities to create synergies to enhance privacy performance in a manner that benefits an organization, is the clearest path to achieving and sustaining high performance.

What is the Privacy Risk Management Model?

While the impact of some privacy risks may prove to be especially potent, fortunately, there is nothing particularly unusual about managing the risks and opportunities arising from issues related to privacy. In fact, relatively mature organizations which have institutionalized risk management will discover, in many respects, they can manage it as another area of risk – similar to those posed by technology, economic factors or the environment.

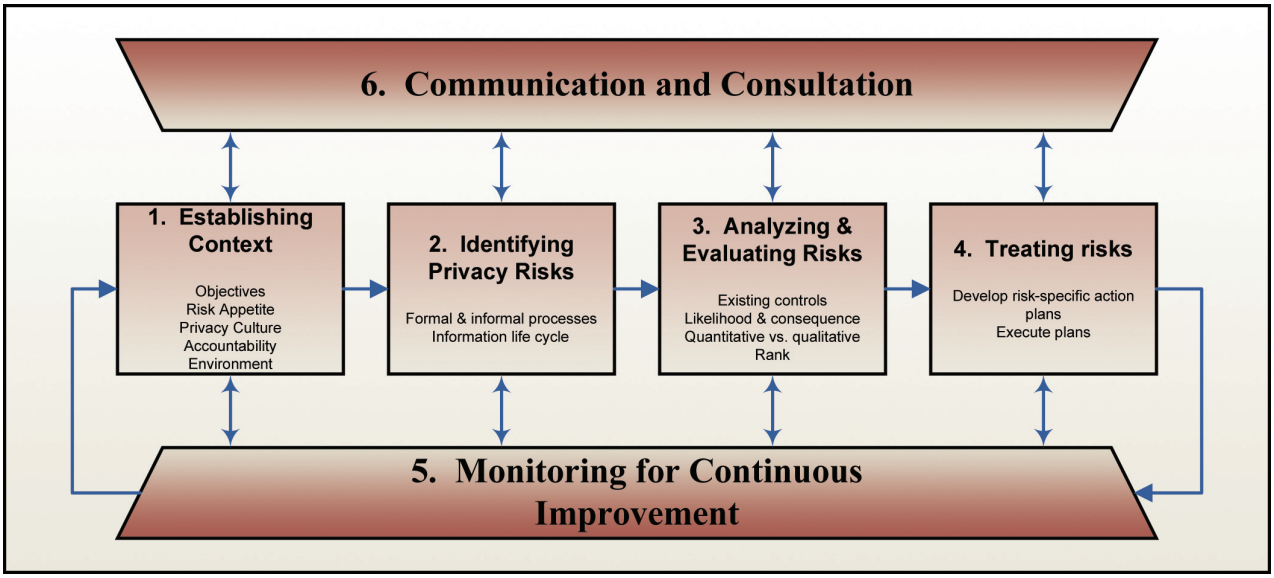


Figure 3. Sample Privacy Risk Management Framework.

Privacy by Design, which can (and should) inform the development of every policy or process dealing with personal information, is compatible with virtually any risk management regime – in this paper, we build on the framework described in ISO 31000 (refer to Figure 3). To ensure that privacy risks are successfully mitigated, it is important to make certain that the principles of *PbD* (Appendix 1) are not only embedded in an organization's risk management system, but also, in all of its programs and processes dealing with personal information.

Embedding privacy into the design of everything that comes in contact with stakeholder personal information ensures that it becomes an organization's default mode of operation, which is the ultimate goal. With privacy treated as a default, individuals no longer need to be cognizant of whether or how their information will be protected. Even if they do nothing, their privacy will remain intact.

Using the ISO framework as a guide and informed by the principles of *Privacy by Design*, we will now consider an approach to implementing Privacy Risk Management.

1. Establishing Context

Whether the organization is a small startup, a non-profit, a government agency, or a "Fortune 500" company – for most, the need to manage personal information[7] (PI) is more than just a compliance concern. Organizations which institutionalize a culture of privacy are best positioned to protect their stakeholders from the implications of privacy risks.

The management of PI and its attendant risks takes place within an organization's broad strategic and general risk management environment. It is critical to fully appreciate the external and internal contexts which affect privacy to better understand how privacy risks will be managed. Establishing context is a prerequisite in undertaking a strategic approach to, and setting the scope for, Privacy Risk Management. Scanning and assessing factors from an organization's external context that can affect privacy risk may include consideration of social, legal, technological, competitive environment, drivers and trends in privacy issues, perceptions and expectations of external stakeholders regarding privacy, to name a few factors.

When evaluating the internal context, an organization's governance structure, operational and strategic objectives, roles and accountabilities, policies, information systems and data flows, decision-making processes, relationships with and perceptions of internal stakeholders, as well as the organization's culture are among the elements to be considered. It is through its culture in fact that an organization can explicitly and implicitly demonstrate its accountability for safeguarding individuals' personal information.

PI must be managed in the same manner as any other high-value corporate asset, through documented operating practices, roles, responsibilities, structure and ultimately rewards and consequences. Relatively mature organizations will describe this in their "Code of Conduct" – itself a key dimension of successful PRM programs.

Once the context is established, design and implementation of a framework for managing risks may follow. Effective organizations expand the discipline of risk management from a functional perspective to one which is fully integrated within operations through proactive identification of major risks including privacy, effective treatment, and continuous monitoring and review of outcomes. Furthermore, as a key component of good risk management as well as *Privacy by Design*, accountability and transparency are assured through effective communication with stakeholders.

Senior leadership – individuals or Boards of Directors, depending on the organization – is critical in nurturing the integration of privacy, *PbD* and risk management. It is worth noting that this approach is not dependent on organization size or revenue. Practising PRM, any organization is able to effectively address privacy risks. Leaders have a fiduciary responsibility to protect and safeguard an individual's personal information – to do otherwise is, ultimately, bad for business.

In summary, successful organizations integrate the PRM program within their governance framework (Figure 4) and create a culture of accountability for privacy risks. Leaders exercise executive accountability and direct resources to manage demands for protection of individual personal information in accordance with risks and rewards.

7 Refer to Appendix 3 for an overview of personal information.

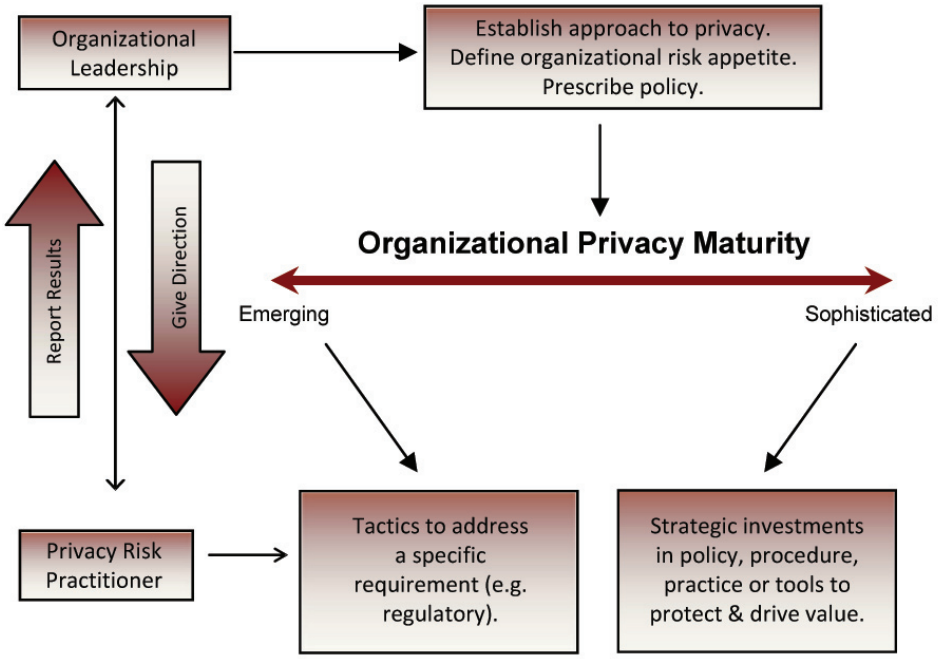


Figure 4. The Privacy Risk Management and Governance Framework.

2. Identifying Privacy Risks

Effectively protecting personal information requires identification of potential privacy risks so that they may be eliminated or, at the very least, mitigated. Within a relatively mature organization, this is accomplished using a combination of both formal and informal processes. Identification and protection of PI is the responsibility of everyone within an organization, regardless of their role or title. In a positive-sum manner, employees who are mindful of privacy, in addition to their designated role, provide improved protection for an organization's customers and employees by identifying privacy risks proactively.

Privacy risks are primarily operational risks, and are defined as those with a chance of causing direct or indirect loss resulting from: inadequate or failed internal processes and systems; issues related to staff; and, external events. They also include risks related to a company's outsourced service providers, an area that is often overlooked until it is too late.

In addition to traditional risk identification processes, such as Privacy Impact Assessments (PIAs) and privacy audits, there are many other techniques that can be leveraged to identify privacy risks. Organizations may engage in some, or all of the following, depending on their requirements:

1. **Developing a Culture of Privacy Protection** – Embedding privacy into the culture of an organization – creates an incredibly valuable mechanism for identifying privacy risk. Such a culture encourages staff to be more forward thinking and engaged. Through early identification of potential privacy risks, a more privacy-protective environment is established.

2. **Listening to Employee and Business Partner Feedback** – The mature organization's ongoing privacy training and regular communication with staff and business partners offers an opportunity to discover areas of concern. Listening to the questions; participating in the discussions; and, probing for feedback during such sessions may yield insight into potential privacy risks that might not otherwise surface through more conventional techniques.

3. **Enhancing Security Measures** – Effective security is essential for organizations to protect privacy and, like *PbD*, will address information technology, business processes and physical resources. Mature organizations consistently continue to strengthen security by focusing on finding gaps and weaknesses which, in turn, often pose privacy risks. Working closely with the firm's security group provides an opportunity to create real value regarding the protection of personal information.

4. **Following the Flow of Your Organization's Information** – Most organizations collect, use and store personal information; not all do a good job of destroying it at the end of its useful life. Fully documenting it (i.e. what PI is collected and created, who interacts with it, when, where, why, and by what means?), using a model like the Information Life Cycle (Figure 5), is an important step in identifying potential privacy risks. The model is useful because it ensures that all states of personal information are considered (e.g. handwritten applications; e-mails; the content of shared folders, USB drives, computers and file cabinets; etc…) – from cradle to grave.

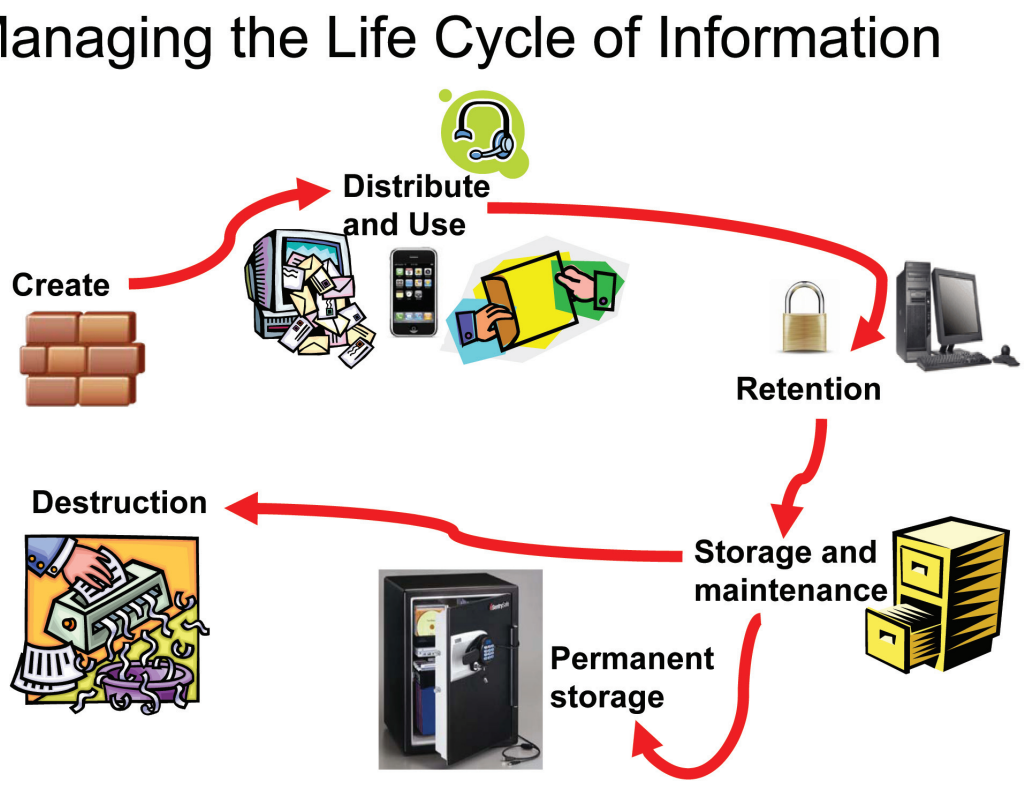


Figure 5 - The Information Life Cycle

Conducting a complete inventory of PI across the organization is an excellent starting point. Too many, however, focus on only the "official record" as their main concern. Operational complexity often demands that staff create and, therefore, manage copies of information in various formats in multiple departments and, possibly, in other organizations (i.e. third party service providers). For example, PI, originally collected on paper, is entered into a customer record system, which is accessible by staff in various departments, who may also create more paper and electronic copies of the same personal information. Each instance of personal information within an organization, regardless of the medium on which it is stored, must be protected.

5. **Examining the Key Business Processes** - Paying particular attention to specific areas in an organization and focusing on business processes which use PI provides a targeted approach to identifying privacy risks. Sales, Marketing and Customer Service departments are customer-facing and typically manage business processes with significant quantities of personal information.

6. **Embedding a Formal Change Management Program** – A Change Management program is a process to consider the organizational impact of proposed changes (i.e. strategic or tactical). It is often comprised of a multidisciplinary or cross-functional team whose objective is to identify potential privacy risks *before* the changes take place, thereby ensuring a robust implementation. (e.g. new or a replacement system, new markets, etc.).

7. **Reviewing Third Party Processes** – Many organizations outsource a wide variety of work to third parties. Customer, prospect and/or employee personal information may be transferred, processed and stored off-site. Privacy risks can become even more complex when the outsourced information crosses borders. ***Organizations cannot outsource their accountability to protect personal information***. For that reason, it is important to work closely with third parties to ensure they manage the information in a manner consistent with the organization's policies. In some cases, third parties may outsource activities to yet another company (i.e. 4th or 5th parties) making it critical that organizations be fully aware of how their information will be used and to ensure that potential privacy risks are identified early.

8. **Performing Self-Assessments** – The use of Privacy Audits and Privacy Impact Assessments provides an opportunity to delve deeply into specific projects or functional areas to identify potential privacy risks. Frequently, organizations can become complacent with PIAs and may either complete them by rote, simply filing (rather than acting upon) them or conducting them too late. To be effective, they need to be done before the project is underway and revisited throughout.

   Self-assessment review programs such as Risk Control Self Assessments (RCSAs) are becoming more common in organizations as a mechanism to identify risks and issues. Leveraging these provides another opportunity for organizations to reflect on privacy risks from the bottom-up.

9. **Establishing Privacy Committees –** Organizations can utilize Privacy Committees as a technique to identify and review privacy risks at a senior level. They should be comprised of cross-functional representation including executives from Operations, Marketing, Legal, Audit, Compliance, Security, and Risk Management who will discuss business needs and consider changes through a privacy lens.

10. **Engaging Internal Audit –** Internal Audits are conducted on an independent basis to examine operations within an organization. Areas of high risk are reviewed with management and reported to the Audit Committee. Embedding privacy risk elements into existing internal audit plans and programs is a strong mechanism helping to identify privacy risks within an organization.

    In addition to the techniques listed above to identify privacy risks, in Appendix 4, we have identified 50 business areas that organizations should consider as they undertake their privacy risk identification exercise.

3. Analyzing & Evaluating Risks

As important as it is to identify each of the risks faced by an organization, it must be acknowledged that few will possess resources sufficient to manage all of them effectively. It is, therefore, necessary to perform "risk triage" – ranking each of the identified risks (according to the organization's policies) and separating the minor (possibly "acceptable") risks from the major ones. Further, the process of analysis and evaluation may yield insight into appropriate treatment strategies. Not all risks warrant the same degree of attention, however. Well-established risk management processes, tools and deliverables may be applied to analyze privacy risks and evaluate which require active treatment and which need only be monitored.

As with traditional risk assessment, determining the inherent risk of a privacy event is the starting point - that is, the likelihood of a privacy event occurring multiplied by its potential impact. Next, each privacy risk must be considered within the context of an organization's existing technological, process and physical controls. The level of risk remaining after internal controls are applied, known as *residual risk*, is the focus of the PRM Practitioners as they evaluate and rank risks. Those with the greatest residual risk, naturally, are identified as the highest priority and lay first claim to the resources necessary to mitigate or eliminate them. On the other hand, where there is only a small gap between a privacy event and controls, it is less likely to be encountered and therefore, may only warrant the modest investment of monitoring.

In addition to the traditional sources of information used to analyze risks, PRM Practitioners should also avail themselves of relevant case judgements, interpretations and guidance published by privacy authorities.

Identified risks may be subject to one or more of the following forms of analysis:

1. **Qualitative Analysis –** using words and descriptive scales to quickly assess the relative magnitude of identified risks. Extremely flexible, it is often used when numerical data doesn't exist or is inadequate for the task. The Office of the Privacy Commissioner of Canada offers an example of the qualitative approach in its "PIPEDA Self-Assessment Tool."[8]

8 *PIPEDA Self-Assessment Tool*, Office of the Privacy Commissioner of Canada. http://www.priv.gc.ca/information/pub/ar-vr/pipeda_sa_tool_200807_e.cfm.

2. **Semi-Quantitative Analysis** – associates a numeric score with points on an otherwise descriptive scale (e.g. "1" = Rare; "5" = Almost Certain). While yielding a more structured ranking of risks than qualitative analysis, the numeric values *should not* be relied upon to compare relative risks (i.e. the impact of one risk vs. another). This approach is used by the American Institute of Certified Public Accountants and the Canadian Institute of Chartered Accountants (AICPA/CICA) in their "Privacy Risk Assessment Tool" which measures an organization's performance against the Generally Accepted Privacy Principles (GAPP).[9]

3. **Quantitative Analysis** – relies upon actual numeric values to communicate specific consequences (expressed in monetary, technical or human terms) and probabilities of outcomes. Such an approach is generally complex to undertake, requiring research and development of organization-specific models. It is generally only applied to evaluate the most significant potential risks. Because the desired degree of precision can be difficult to achieve, a sensitivity analysis may be employed to test the impact of differing considerations.

Evaluation is a process of comparing, for each identified risk, its assessed level of residual risk (determined through one or more of the techniques of analysis) against previously established criteria. Regardless of the form the analysis takes, the output is typically described in either a table or a "heat map" (both will be familiar to the risk manager). Either will help the PRM Practitioner to better understand where to target available resources.

Privacy opportunities or, potential market differentiators, represent an organization's chance to leverage its robust and proactive management of personal information. They should be subjected to a similar process of analysis and evaluation.

Despite the temptation to ignore seemingly trivial risks and opportunities, all those identified, regardless of their assessed severity and probability should be listed or plotted. Since even the most innocuous risk might grow into something significant given the right conditions, monitoring is particularly important.

4. Treating Risks

Having identified and assessed privacy risks, we need to determine how to address or treat them.

Mature organizations will recognize that the most effective risk treatment is the one undertaken *before* the risk is realized. That is why *Privacy by Design* is such an important concept for PRM Practitioners. Practicing *PbD* compels an organization to focus on making privacy the default mode of operation by building it into IT systems, processes and places of business.

Traditional treatment options, drawn from the risk management discipline, include a variety of techniques to mitigate risks and enhance opportunities. They range from *risk avoidance* by limiting, for example, the amount and type of data collected (also known as data minimization), to *risk reduction* by minimizing privacy risk using data protection controls and other preventative

9 "*Generally Accepted Privacy Principles*," AICPA/CICA, 2009. http://www.cica.ca/service-and-products/privacy/gen-accepted-privacy-principles/item10677.pdf.

measures, to *risk transfer* by making use of third party remedies, like purchasing internet liability insurance, for example.

Treatment strategies, some of which may be proactively employed as a matter of policy and others, which may be used alone or in combination to tackle privacy risks, include the following:

- Ensuring compliance with privacy laws, industry best practices, and following Fair Information Practices[10] to limit collection, use, disclosure and retention of personal information;
- Establishing oversight and accountability for privacy within each program and process area to help foster a top-down / bottom-up privacy culture;
- Developing, implementing and maintaining a privacy policy and practices to clarify personal information management requirements for employees and outsourced functions;
- Establishing complaint and feedback mechanisms to address privacy concerns;
- Monitoring protection performance, through audits or assessments – to incorporate privacy as part of ongoing quality assurance activity, identifying gaps and needed enhancements;
- Developing response protocols to ensure appropriate escalation and management in case of a major privacy incident or breach;
- Performing Privacy Impact Assessments and Information Life Cycle Audits to uncover vulnerabilities in specific projects;
- Using up-to-date encryption techniques to ensure that personal information is appropriately secured when stored on portable electronic devices;[11]
- Providing ongoing awareness through training, regular employee communications and debrief discussions following a privacy incident;
- Reviewing privacy incidents, analyzing trends and incorporating insights to enhance processes and systems through re-engineering;
- Accessing external expertise and resources available from privacy professionals throughout the world.[12]

As with technology and processes which reflect the principles of *PbD*, the most effective strategies to address privacy risk also focus on prevention. Borrowing from the above 'menu' of treatment techniques, what follows are a number of practical strategies that are particularly effective in mitigating privacy risk and creating value.

---

10 An overview of various evolutions of the Fair Information Principles can be found at: http://www.privacyrights.org/ar/fairinfo.htm.

11 *Encrypting Personal Health Information on Mobile Devices,* The Information & Privacy Commissioner of Ontario, 2007. http://www.ipc.on.ca/images/Resources/up-4fact_12_e.pdf.

12 For example, www.ipc.on.ca and www.privcom.gc.ca

1. Ensuring Compliance:

Compliance with applicable privacy laws, including information access requirements, is a key component of corporate governance and accountability, and vital to protect an organization's reputation and goodwill in the community. A privacy policy, the essential elements of which describe, in an easy to understand manner, how the organization will satisfy the Fair Information Principles[13, 14], is an important first step.

Having a good privacy policy and practices and, more importantly, effectively disseminating them to all employees and customers clarifies expectations. It reduces the risk of non-compliance with legislation (and its attendant liabilities), as well as affording a competitive advantage through satisfaction of the privacy expectations of customers. Given that privacy flows throughout the entire organization, well-crafted practices will bring consistency to the workplace regardless of the product, service or process area.

Once developed and implemented, organizations should periodically review and update privacy policies to ensure ongoing relevancy. Various tools and guides exist online which provide a framework for such a review. The American Institute of Certified Public Accountants' and the Canadian Institute of Chartered Accountants' (AICPA/CICA) Generally Accepted Privacy Principles (GAPP)[15], represents a thorough treatment of the area.

Particular attention to policy and practices will provide end-to-end life cycle protection of the organization's personal information assets. As well, such an approach also helps to demonstrate a high degree of visibility and transparency. Exceeding compliance requirements from the outset (i.e. practicing *PbD* – focussing on assurance) may elevate an organization's approach from mere compliance to practicing privacy as a competitive advantage or differentiator.

2. Responding to Privacy Incidents or Breaches:

A privacy breach occurs when PI is collected, retained, used or disclosed inappropriately. Information may be lost, stolen or inadvertently disclosed through human error. While organizations must strive to prevent such an event, the wide range of potential challenges mean that mature organizations will prepare for the inevitability of a breach. In so doing, they are ready to instantly execute (because time is of the essence) on two priorities:

1. **Containment** – identify the scope of the potential breach and take steps to contain it.
2. **Notification** – identify whose privacy was breached and, barring exceptional circumstances, notify those individuals accordingly.[16]

---

13 *Why Web sites need Privacy Policies,* The Information & Privacy Commissioner of Ontario, 1999. http://www.ipc.on.ca/images/Resources/web-priv.pdf

14 "*Your Privacy Responsibilities,*" The Office of the Information and Privacy Commissioner of Canada, 2009. http://www.priv.gc.ca/information/guide_e.pdf.

15 For additional information on GAPP, visit www.infotech.aicpa.org/resources/privacy/Generally+Accepted+Privacy+Principles/

16 *What to do if a privacy breach occurs: Guidelines for government organizations,* The Office of the Information & Privacy Commissioner of Ontario, 2006. http://www.ipc.on.ca/images/Resources/priv-breach-e.pdf

We know that up to 80 per cent of an organization's value comes from intangible assets such as brand equity and goodwill. Following a regimen of prevention and rapid response in the case of a breach are essential to minimize the risk of adverse media attention or negative impact on brand reputation.

3. Re-engineering:

Once an organization has identified a process that has resulted in an actual or potential privacy breach, the use of re-engineering should be utilized. Business process re-engineering is a technique that studies existing processes, seeking opportunities for improvement. Examples include streamlining to eliminate duplication or non value-added steps, adding or enhancing controls, or reducing processing costs. Processes which may result in privacy breaches should be examined carefully for re-engineering opportunities to reduce the risk of the loss, theft or inappropriate disclosure of PI.

4. Risk Transfer:

For many types of risk, transfer through use of third parties is a viable option. For privacy risks, however, use of a third party service provider (i.e. outsourcing) does not eliminate risk for the organization. Generally, the organization that collects the personal information remains accountable and is responsible for it, whether it is under their "roof" or that of a service provider. Accountability cannot be outsourced. Organizations should review the privacy practices of third parties they contract with, and incorporate privacy protection requirements and restrictions within agreements and perform privacy audits, where appropriate.

5. Monitoring for Continuous Improvement

Monitoring is an essential step in the PRM process. It helps organizations determine whether chosen strategies have achieved desired outcomes. Like most complex risks, privacy risks continuously evolve and monitoring will also uncover the need to revisit or introduce new strategies to address evolving technology, as well as legal and public expectations.

Mitigating Patron Privacy Risk Through Process Monitoring

As part of OLG's (Ontario Lottery and Gaming Corporation) program of "Responsible Gaming," individuals may participate in a service called "Voluntary Self-Exclusion." Participants gain a variety of protections; including the safeguard of being escorted from a facility should they be discovered on the premises. To aid in identification, each person provides a picture and other personal information.

As the number of subscribed patrons began to grow over time, OLG, through a process of continuous monitoring, discerned that their hard-copy-oriented practice of maintaining self-exclusion information failed to provide the desired level of accuracy. Following the principles of PbD, OLG developed (with researchers from the University of Toronto and assistance from the Office of the Information & Privacy Commissioner) a sophisticated, electronic, facial recognition system that, by design, will protect personal information with a leading-edge biometric encryption technology. OLG's innovative and industry-leading solution seeks to improve patron protection as well as the privacy of their personal information.

Monitoring trends in privacy incidents and complaints, and taking the time to review lessons learned, also enhances an organization's privacy protection efforts. Focusing on key questions like 'what went wrong?' and 'why?' will help drive privacy protection and process improvements where needed.

Early warning and other forms of monitoring are not only good governance; they are assurance activities which protect and enhance value for the organization.

6. Communication and Consultation

Ongoing communication with internal and external stakeholders is essential to achieving a high level of performance in managing privacy risk.

The ISO 31000 Standard defines the communication and consultation step in the risk management process as the "continual and iterative processes that an organization conducts to provide, share or obtain information and to engage in dialogue with stakeholders regarding the management of risk".[17]

Within the privacy context, an organization needs to look far and wide for issues and solutions to enhance its privacy performance. Establishing methods to communicate with staff about changes in privacy policy or safeguarding enhancements, providing management and Board reporting on effectiveness of privacy measures, establishing a response plan for communicating in the event of a privacy breach, or creating mechanisms for providing feedback and consultation on privacy issues are all good examples of privacy risk reporting and consulting. Together, these mechanisms offer a variety of information sources and privacy insights that may be consolidated in an overall status report or semi-annual risk review.

Conclusion

Privacy Risk Management is a critical dimension of an organization's existing risk management discipline. Managed in a fashion similar to conventional risks, privacy risks may be further mitigated by employing the principles of *Privacy by Design*. By embedding privacy within all of their personal information-related processes and practices, organizations can help to ensure that privacy risks will be managed, by default.

Organizations with moderate to advanced privacy and risk management capabilities are poised to begin to practice Privacy Risk Management. By embedding privacy into their existing risk management framework, they will be able to manage risks associated with the protection of personal information, in much the same fashion as any other business risk. Utilizing PRM, performance and value is enhanced through the execution of processes rather than ad hoc efforts.

Privacy Risk Management Practitioners are much more than simply "Process Custodians." They are also "Agents of Change" – advancing the banner of privacy within an organization, in general,

17 ISO 31000 Risk Management – Principles and Guidelines, November 2009.

and the risk management function, in particular. While they are critical in ensuring efficient PRM operations, the role itself is one that can be fulfilled by management associated with any of several different functions – depending on the organizational structure. To be truly successful, however, they require executive visibility and support.

The PRM Model described in this paper was based on the ISO 31000 Standard and serves as an example of the natural synergy between *Privacy by Design* and a popular Risk Management Framework. Others offer similar natural synergy.

Risk and privacy professionals need to work together to develop practices to manage the opportunities and risks posed by the management of personal information. There are undeniable competitive advantages within many industries to be realized by the organization perceived by customers to be the "best" at protecting personal information. It is, however, probably even more important to effectively manage personal information because of the risks. The potential for significant damage to the organization and irreversible harm to the individual is simply too great to be dismissed.

Appendix 1:

The 7 Foundational Principles of *Privacy by Design*:

1. ***Proactive*** not Reactive; ***Preventative*** not Remedial

The *Privacy by Design* (PbD) approach is characterized by proactive rather than reactive measures. It anticipates and prevents privacy invasive events *before* they happen. PbD does not wait for privacy risks to materialize, nor does it offer remedies for resolving privacy infractions once they have occurred — it aims to *prevent* them from occurring. In short, *Privacy by Design* comes before-the-fact, not after.

2. Privacy as the ***Default***

We can all be certain of one thing — the default rules! *Privacy by Design* seeks to deliver the maximum degree of privacy by ensuring that personal data are automatically protected in any given IT system or business practice. If an individual does nothing, their privacy still remains intact. No action is required on the part of the individual to protect their privacy — it is built into the system, *by default*.

3. Privacy ***Embedded*** into Design

Privacy by Design is embedded into the design and architecture of IT systems and business practices. It is not bolted on as an add-on, after the fact. The result is that privacy becomes an essential component of the core functionality being delivered. Privacy is integral to the system, without diminishing functionality.

4. Full Functionality – Positive-Sum, not Zero-Sum

Privacy by Design seeks to accommodate all legitimate interests and objectives in a positive-sum "win-win" manner, not through a dated, zero-sum approach, where unnecessary trade-offs are made. *Privacy by Design* avoids the pretense of false dichotomies, such as privacy ***vs.*** security, demonstrating that it ***is*** possible to have both.

5. End-to-End Lifecycle Protection

Privacy by Design, having been embedded into the system prior to the first element of information being collected, extends securely throughout the entire lifecycle of the data involved, from start to finish. This ensures that at the end of the process, all data are securely destroyed, in a timely fashion. Thus, *Privacy by Design* ensures cradle to grave, lifecycle management of information, end-to-end.

6. Visibility and Transparency

Privacy by Design seeks to assure all stakeholders that whatever the business practice or technology involved, it is in fact, operating according to the stated promises and objectives, subject to independent verification. Its component parts and operations remain visible and transparent, to users and providers alike. Remember, trust but verify.

7. Respect for User Privacy

Above all, *Privacy by Design* requires architects and operators to keep the interests of the individual uppermost by offering such measures as strong privacy defaults, appropriate notice, and empowering user-friendly options. Keep it user-centric.

Appendix 2:

Dimensions of Privacy & Risk Management Task Maturity:

Maturity	1 Ad Hoc	2 Initial	3 Repeatable	4 Managed	5 Leadership
Governance	Little senior management attention to privacy - issues are managed as they arise.	Privacy legislation and regulations are adopted as surrogates for policy.	Privacy policies and processes are established. The organization may introduce and begin to enforce a "Code of Conduct."	Operational impacts of privacy policies are monitored and continuously improved. The organization's "risk appetite" begins to be defined by senior management.	Senior management fosters a culture of privacy that encompasses the entire organization. Privacy regarded as a competitive advantage.
Accountability	No individual or organizational accountability for privacy and associated risks.	Situational accountability for privacy assigned to an individual or team.	Formal responsibility for issues of privacy added to those of an existing function - there may be some proactive consideration of privacy risks.	Privacy function separately identified as part of senior management - responsibilities are policy-oriented; privacy issues owned by business units.	Privacy routinely considered by all employees having been embedded in organizational processes through "Privacy by Design."
Approach to personal information management	Fragmented, undisciplined approach to personal information management.	Adoption of information life cycle principles - personal information sources and uses identified and inventoried.	Personal information management processes developed and implemented.	Personal information management processes are continuously monitored and improved.	Personal information management processes benchmarked against best of breed exemplars.
Relationship with Risk Management function	None.	Situational - as demanded by the specific risk to be mitigated.	Emerging - increasing awareness of privacy risks, though not rigourously managed; frequently identified serendipitously.	Active - privacy is identified as a risk area; privacy risk criteria and controls are developed and monitored to ensure optimum performance.	Considerations of privacy risk are fully integrated within the organization's (enterprise) risk management function.
Privacy Programs	Few, if any - some personal information may be secured.	More robust information security.	Situational adoption of programs such as online privacy polices and consent to foster customer trust & enhance reputation. Introduction of Privacy Impact Assessments.	"Privacy by Design" is introduced - considerations of privacy protection are embedded in new projects. Increased focus on risks posed by "business partners" (3rd parties).	Resilient processes anticipate reaction to crises and opportunities - escalation processes are well-defined - execution is swift and decisive.

Appendix 3:

Personal Information:

"Personal information"[18] means 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 where it appears with other personal information relating to the individual or where the disclosure of the name would reveal other personal information about the individual;

This list of examples of personal information is not exhaustive.

To qualify as personal information, the information must be about the individual in a personal capacity. As a general rule, information associated with an individual in a professional, official or business capacity may not be considered to be "about" the individual.

Even if information relates to an individual in a professional, official or business capacity, it may still qualify as personal information if the information reveals something of a personal nature about the individual.

Finally, to qualify as personal information, it must be reasonable to expect that an individual may be identified if the information is disclosed.

18 Freedom of Information and Protection of Privacy Act, R.S.O. 1990, c. F.31.

Appendix 4:

50 Areas to Identify Privacy Risks:

1. Administrative Security Safeguards
2. Application Development
3. Awareness & Training
4. Behavioral Advertising
5. Breach Response
6. Call (voice) Recordings
7. Conducting Background Checks (employees, volunteers, contractors)
8. Conducting Credit Checks
9. Conducting Employee Investigations
10. Cross-border Transfers
11. Customer Authentication Process
12. Customer Service Operations e.g. Call Centres
13. Data Governance
14. Data Leakage Protection
15. Debt Collection (including third party collection firms)
16. Disclosure to Authorities
17. Do-Not-Call and Telemarketing
18. E-mail Marketing
19. Employee Authentication
20. Employees Working Remotely (e.g. at home)
21. Encryption
22. Fraud Discovery and Monitoring
23. Handling Access Requests
24. Handling Employee Health Information
25. IT Monitoring

26. Lawful Disclosures
27. Legal & e-Discovery
28. Marketing using Fax
29. Online Communities and Collaboration
30. Online Marketing
31. Personal Information Handling Policies
32. Physical Security Safeguards
33. Privacy Audits
34. Privacy Complaints Process
35. Privacy Governance and Oversight
36. Privacy Impact Assessments
37. Privacy Laws and Regulations
38. Privacy Notice
39. Records Destruction
40. Records Retention
41. Safeguarding Data
42. Secondary Marketing
43. Security Audit
44. Social Networking Sites
45. Technical Security Safeguards
46. Telemarketing
47. Third Parties
48. Vendor Management
49. Video Monitoring
50. Video Surveillance

Information and Privacy Commissioner of Ontario
2 Bloor Street East, Suite 1400
Toronto, Ontario
Canada M4W 1A8
Telephone: (416) 326-3333
Fax: (416) 325-9195
E-mail: info@ipc.on.ca
Website: www.ipc.on.ca
Privacy by Design: www.privacybydesign.ca

OLG
4120 Yonge Street
Suite 500
Toronto, Ontario
M2P 2B8
Telephone: (416) 224-1772
Website: www.olg.ca

YMCA of Greater Toronto
42 Charles Street East
Toronto, Ontario
M4Y 1T4
Telephone: (416) 928-9622 or 1-800-223-8024
Fax: (416) 928-2030
Website: www.ymcatoronto.org

April 2010

Information and Privacy Commissioner, Ontario, Canada