

Privacy by Design Curriculum 2.0

Instructor Resources

MODULE TWO: APPLIED PRIVACY BY DESIGN

Presentation 4: Embedding Privacy in Organizational Culture, Policy, and Process



CONTENTS

Overview	2
Essential Reading	2
Learning Objectives	2
<i>Implementing Good Privacy Practices:</i>	
Overview of Presentation	3
Further Reading	5
Presentation Materials with Instructor Notes	6



Overview

When fully implemented, *Privacy by Design* touches every aspect of the organization. This section explores key steps in such an implementation, including creating a Culture of Privacy, developing privacy-protective policies, and supporting those policies with new or existing processes. It introduces the concept of Privacy Risk Management as an example of how existing processes can be leveraged in pursuit of better privacy practices.

Essential Reading

Information and Privacy Commissioner/ Ontario with Ontario Lottery and Gaming Corp. and YMCA, [Privacy Risk Management](http://www.privacybydesign.ca). www.privacybydesign.ca

Ann Cavoukian, Ph.D., Marty Abrams, & Scott Taylor, [Privacy by Design: Essential for Organizational Accountability and Strong Business Practices](http://www.ipc.on.ca). www.ipc.on.ca

Learning Objectives

Participants will develop an understanding of the scope of *Privacy by Design* within the organization, and how it applies not only to IT projects but also to management processes. They will be introduced to the idea of privacy as a core competency. They will also become familiar with the notion that privacy can and should be managed like other risks that are part of an organization's Risk Management discipline, and with tools that can help them to support the implementation of *Privacy by Design*.

Embedding Privacy in Organizational Culture, Policy, and Process:

Overview of Presentation

<i>Slide</i>	<i>Title</i>	<i>Theme</i>
4.1	The Privacy Payoff	Privacy fuels brand loyalty and yields competitive advantages
4.2	Reaping the Rewards	How can organizations reap the rewards of privacy?
4.3	Time to Re-Invent	Take advantage of the privacy opportunity.
4.4	Implement <i>Privacy by Design</i>	Reaping the rewards of privacy requires a full implementation of <i>PbD</i> , across the organization.
4.5	<i>PbD</i> inside the Organization	An overview of how privacy operates at the level of organizational culture, policies, and processes.
4.6	The First Step: Put Privacy into the Picture	Privacy must form a part of how organizations understand their external business environment.
4.7	Create a Culture of Privacy	Privacy has to start at the top.
4.8	Develop Strong Privacy Policies	Policies provide structure for institutionalizing privacy practices.
4.9	Use Processes	Processes support implementation of privacy policies.
4.1	Leverage Existing Processes	In mature organizations, privacy may be incorporated into existing management processes.
4.11	Example: Adding Privacy to the Risk Management Process	An example of how privacy may be incorporated into the risk management process.
4.12	Privacy Risk Management Maturity Model	Privacy risk management requires maturity in both the risk management and privacy areas.
4.13	Privacy Risk Management Framework	Based on ISO 31000:2009 Risk Management Framework.

Slide	Title	Theme
4.14	Working Through the Process	Working privacy into the framework.
4.15	Incorporating Privacy into Other Management Processes	Privacy may also be incorporated into other management processes in much the same way.
4.16	Tools	Processes can be supported by tools such as Privacy Impact Assessments, staff training, and certification programs.
4.17	The End Result: Privacy Embedded Throughout the Organization	Return to overview of how privacy operates at the level of organizational culture, policies, and processes.
4.18	Reaping the Rewards	Privacy fuels brand loyalty and yields competitive advantages.

Further Reading

C.K. Prahalad and Gary Hamel, The Core Competence of the Corporation. Harvard Business Review, 1990.

Ann Cavoukian, Ph.D., Information and Privacy Commissioner, Ontario, Canada with Terry McQuay, President, Nymity Inc., [A Pragmatic Approach to Privacy Risk Optimization](#). www.ipc.on.ca

Information and Privacy Commissioner, Ontario, Canada, [Privacy and Boards of Directors: What You Don't Know Can Hurt You](#). www.ipc.on.ca

Privacy Impact Assessments

Information and Privacy Commissioner, Ontario, Canada. [Privacy Diagnostic Tool](#). www.ipc.on.ca

Information and Privacy Commissioner, Ontario, Canada. [The New Federated Privacy Impact Assessment \(F-PIA\)](#). www.ipc.on.ca

Office of the Privacy Commissioner of Canada. [PIPEDA Self-Assessment Tool](#). www.priv.gc.ca

Information Commissioner/UK, [Privacy Impact Assessments: An International Study of their Application and Effects](#). www.ico.gov.uk

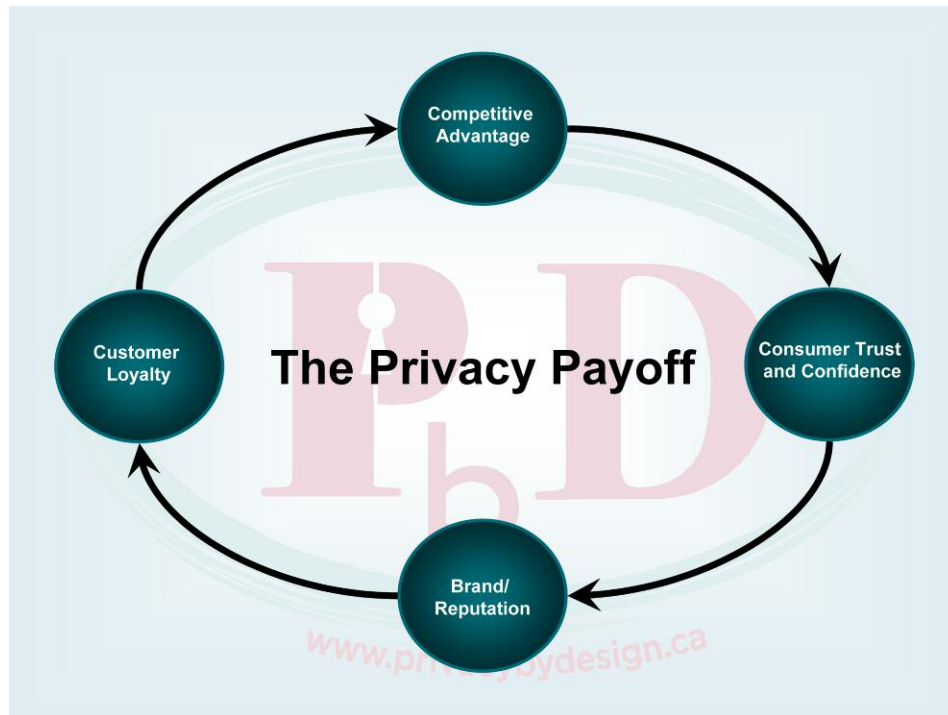
Information Commissioner/U.K., [PIA Handbook Version 2.0](#). www.ico.gov.uk

Office of the Privacy Commissioner/Australia, [Privacy Impact Assessment Guide](#). www.privacy.gov.au

Presentation Materials with Instructor Notes



Slide 1



Slide 2

As outlined in Module One, privacy matters to business because it matters to consumers.

The business case for privacy focuses, in essence, on gaining and keeping consumer trust, helping drive loyalty and repeat business, and avoiding customer “churn.”

The diagram above shows how the value proposition for privacy typically breaks down:

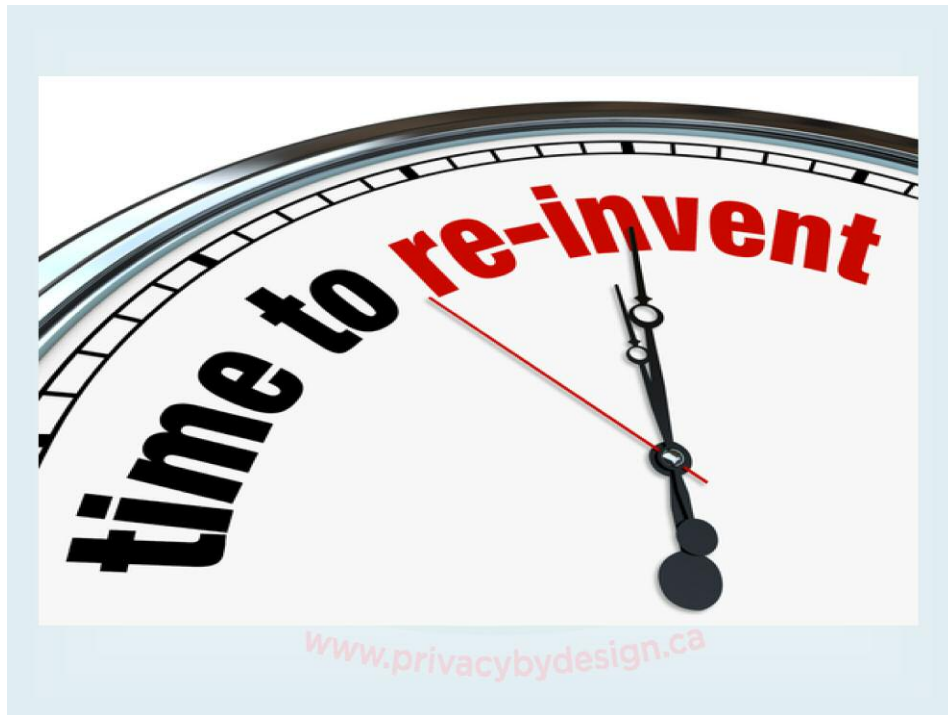
- Consumer trust is among the drivers of successful relationships with customers and enhances their lifetime value;
- Consumer trust hinges critically on the strength and credibility of an organization’s information privacy policies and practices;
- Positive experiences, and the absence of negative ones, reinforce trust in the brand; and
- Trusted brands attract customer loyalty, which drives strong customer relationships and creates sustained competitive advantages.



How can your organization reap the rewards of privacy?

Slide 3

How, then, can organizations position themselves to reap the rewards of good privacy practices?



Slide 4

Implement *Privacy by Design*

Develop strong privacy practices



Use privacy to gain a sustainable
competitive advantage



Build in long term customer value

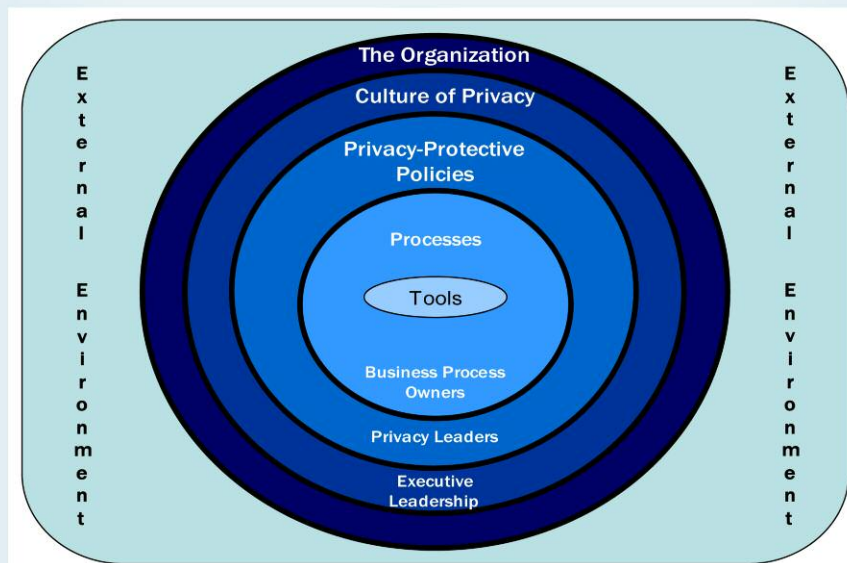
Slide 5

In order to seize the opportunities associated with privacy effectively, and gain a sustainable competitive advantage, organizations have to make privacy a core competency.

A core competency is something that a business does well, that provides customer benefits, and is hard for competitors to imitate. It can take various forms, including technical/subject matter know how, a reliable process, and/or close relationships with customers and suppliers. When a core competency yields a long term advantage to the company, it becomes a sustainable competitive advantage. (From C.K. Prahalad and Gary Hamel, *The Core Competence of the Corporation*, Harvard Business Review, 1990.)

Ultimately, the aim of a full implementation of *Privacy by Design*, at the organizational level, is to ensure that privacy is a core competency, and that good privacy practices pervade throughout the organization.

***PbD* inside the Organization**



Slide 6

In order to achieve this kind of benefit – to extract value from privacy practices and to minimize risks associated with the handling of personal information – privacy protection must become part of the fabric of how an organization thinks and operates, at every level.

When fully implemented, *Privacy by Design* touches every aspect of the organization.

This diagram shows a high-level view of the organization and its operating environment. Implementing *Privacy by Design* requires consideration of each of these domains, which are elaborated in the following slides.



Slide 7

Implementing *Privacy by Design* begins with the recognition that privacy must form a part of how organizations understand their business environment. This includes not only whatever regulatory requirements may apply, but also the shifting expectations of consumers with regard to privacy, what competitors are doing, and international developments in this area that may have an impact on the organization or its lines of business.

Successful organizations, regardless of size, industry, or structure, grow because they continually seek ways to exploit new opportunities and to manage the risks associated with every aspect of their environment, including privacy. **Both** need to be done effectively.

Risks associated with personal information include accidental disclosure, breach, and secondary use without consent. Organizations that fail to protect privacy risk hard and soft costs associated with:

- Legal liabilities, class action lawsuits;
- Loss of stakeholder confidence and trust;
- Diminished brand value and reputation damage;
- Loss of customers and competitive edge;
- Penalties and fines levied; and
- Costs of crisis management, damage control, review and retrofit of information systems, policies and procedures.

By contrast, those organizations that earn and keep consumer trust, thereby helping drive loyalty and repeat business, realize the competitive advantage associated with privacy.



Slide 8

The importance of privacy must be a message that comes from, and is sustained by, the top. It is here that the tone for the organization's operations are set, and where the opportunity exists to create a Culture of Privacy.

A Culture of Privacy enables sustained collective action by providing people with a similarity of approach, outlook, and priorities. It is what leads privacy to be woven into the fabric of day-to-day operations of the organization, at all levels.

At a minimum, a Culture of Privacy involves attempts to institutionalize Fair Information Practices. Forward-thinking organizations, however, will embrace the 7 Foundational Principles of *Privacy by Design*, which incorporate and extend Fair Information Practices. They make privacy protection an organization's default mode of operation.

Developing a Culture of Privacy helps an organization to move beyond simple legislative compliance. Thorough training, ongoing monitoring, auditing, and assessment are key components of a Culture of Privacy.

In an organization with a Culture of Privacy, employees are engaged, execute privacy plans, and provide regular report backs. These organizations treat privacy as a business issue and not simply a compliance one. They make privacy a part of their business strategy, and infuse it in their work plans.

Develop Strong Privacy Policies

***To provide structure for
embedding privacy
practices in day-to-day
activities***

www.privacybydesign.ca

Slide 9

Inevitably, a Culture of Privacy fosters the development of privacy-protective **policies**.

These policies articulate the organization's privacy posture, communicate it throughout the organization, and provide a governance structure for institutionalizing privacy practices throughout the organization.

Use Processes

***To guide implementation
of strong privacy policies***

www.privacybydesign.ca

Slide 10

Processes ensure that everyone within the organization, simply by following the steps, will fall within the bounds of a given policy.

Some processes may be specific to privacy, such as Privacy Impact Assessments. Others will be existing management processes to which privacy can be added....

Leverage Existing Processes

- In mature organizations, privacy can be incorporated into existing processes such as:
 - *Product development*
 - *Financial approvals*
 - *IT development and maintenance*
 - *Human resources management*
 - *Risk management*

www.privacybydesign.ca

Slide 11

Mature organizations may already have a number of management processes in place, some of which may lend themselves to the incorporation of privacy considerations.

Such processes may include product development processes, financial approvals processes, and risk management. In the following slides, we demonstrate how the principles of *Privacy by Design* can be incorporated into the risk management discipline.

Example:

Adding Privacy to the Risk Management Process

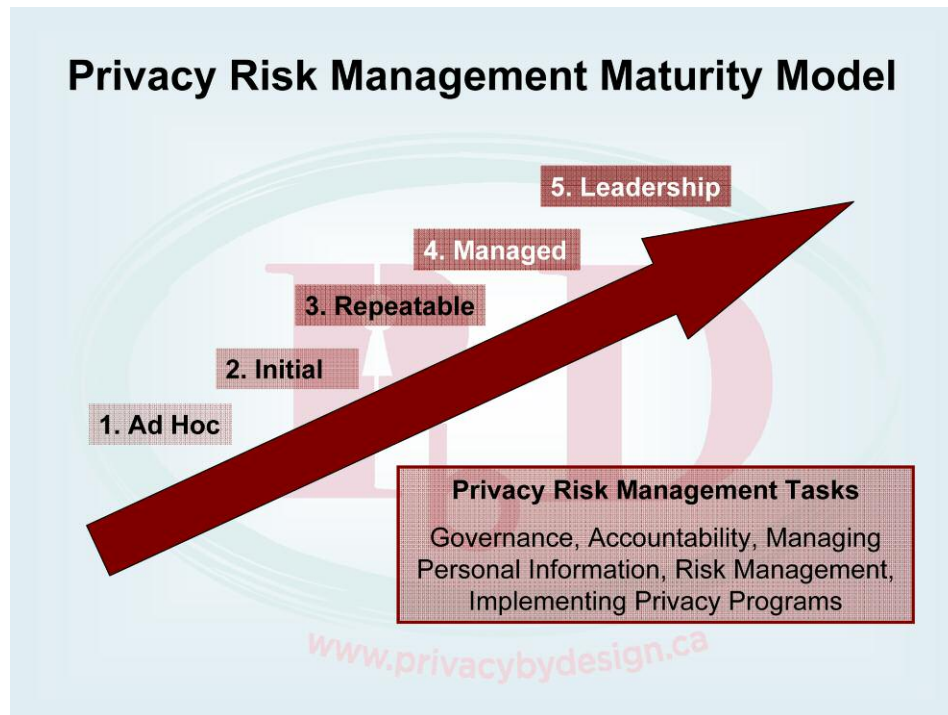
**Risk Management Discipline
+ *Privacy by Design* Principles**

Privacy Risk Management

www.privacybydesign.ca

Slide 12

Privacy Risk Management (PRM) is a concept developed by Dr. Ann Cavoukian, the Ontario Information and Privacy Commissioner (Canada). It basically takes the concept of *Privacy by Design* and applies it to the discipline of risk management.



Slide 13

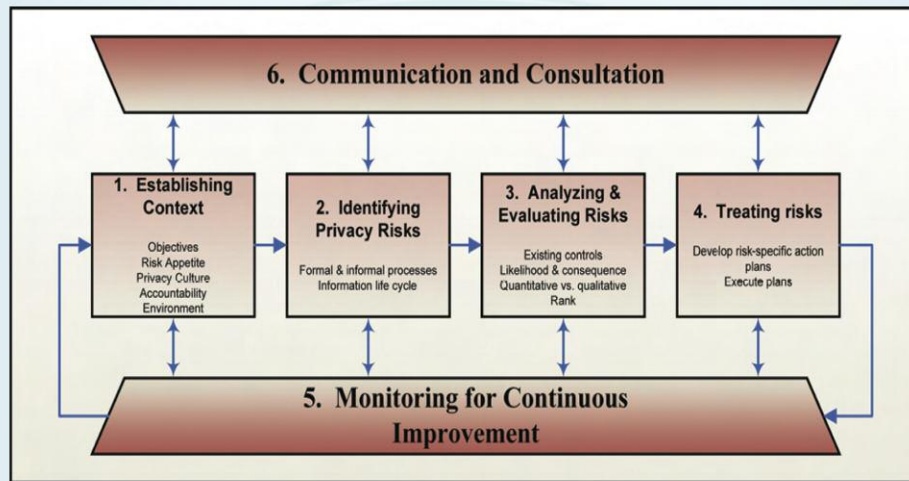
Successful PRM depends on an organization's approach to both the privacy and risk management disciplines. Senior-level commitment to robust privacy and risk management programs, and an organization's maturity with respect to both, are key.

Task maturity, or the institutional ability to perform particular duties, in a predictable fashion, is a useful method to gauge an organization's approach to privacy as well as their preparedness and capacity to respond to various risks.

The chart above is a simplified representation of a Privacy Risk Management Task Maturity Matrix that is used to roughly assess the pertinent dimensions of privacy and risk management task maturity. Taken as prerequisites, the attributes identified must each be practiced at a sufficiently advanced level to enable successful Privacy Risk Management implementation.

In other words, organizations that do not have a mature risk management or privacy process are probably not ready to implement Privacy Risk Management.

Privacy Risk Management Framework



Based on ISO 31000:2009 - Risk Management -- Principles and Guidelines

Slide 14

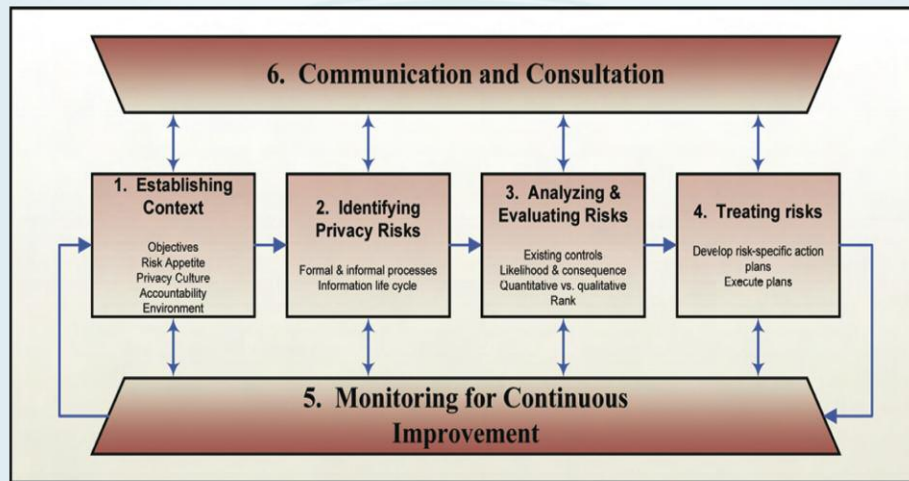
If your organization is ready to implement Privacy Risk Management, then you proceed by integrating the 7 Foundational Principles of *Privacy by Design* principles into your existing risk management framework.

Privacy by Design is compatible with virtually any risk management regime. The figure in this slide shows the framework described in ISO 31000 as an example.

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

Embedding privacy into the design of everything that comes in contact with personal information ensures that privacy becomes an organization's default mode of operation, which is an important principle of *Privacy by Design*.

Working Through the Process



Based on ISO 31000:2009 - Risk Management -- Principles and Guidelines

Slide 15

1. Establishing Context

The management of privacy risk takes place within an organization's broad strategic and general risk management environment. External factors to consider may include the social, legal, technological, and competitive environment, drivers and trends in privacy issues, and perceptions and expectations of external stakeholders regarding privacy.

Internal context includes governance, operational and strategic objectives, roles and accountabilities, policies, information systems and data flows, decision-making processes, relationships with and perceptions of internal stakeholders, and organizational culture.

2. Identifying Privacy Risks

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.

3. Analyzing and Evaluating Risks

The likelihood of a privacy event occurring multiplied by its potential impact is the starting point. Next, each privacy risk must be considered within the context of an organization's existing technological, process and physical controls.

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.

4. Treating Risks

Traditional risk management treatment options 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 measures, to risk transfer by making use of third party remedies, like purchasing internet liability insurance, for example. Importantly, insurance is not available for all types of privacy risks.


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

5. Monitoring for Continuous Improvement

Privacy risks continuously evolve and monitoring will uncover the need to revisit or introduce new strategies to address evolving technology, as well as legal and public expectations.

6. Communication and Consultation

The ISO 31000 Standard defines this step as the "continual and iterative process that an organization conducts to provide, share, or obtain information and to engage in dialogue with stakeholders regarding the management of risk." Among other things, this would include privacy education and ongoing monitoring.



Just as *PbD* can be integrated into Risk Management, it can also be incorporated into other management processes in much the same way.

Slide 16

Just as the principles of *Privacy by Design* can be incorporated into an organization's risk management process, they can also be integrated into other processes, such as product development, IT management, funding approvals, etc.

In a mature organization, therefore, the introduction of *Privacy by Design* may not require the establishment of new process, but rather the modification of existing ones.

Tools

All of these processes may be supported by a range of tools such as:

- Privacy Impact Assessments
- Staff Education
- Certification or privacy seal programs

www.privacybydesign.ca

Slide 17

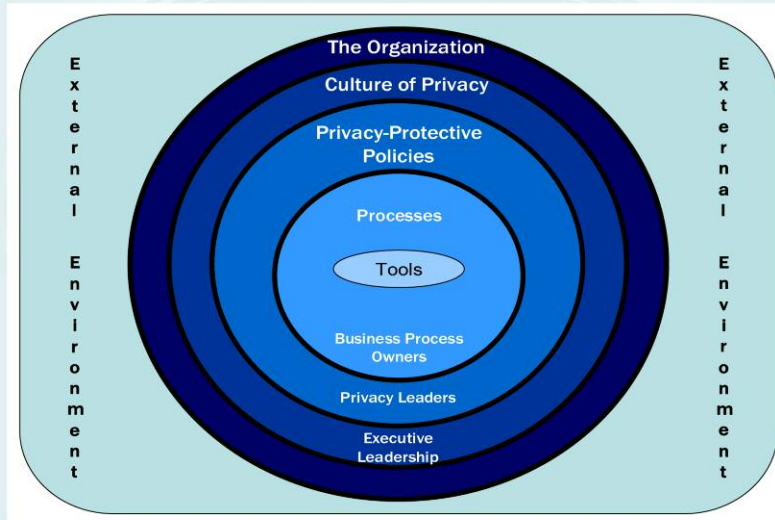
Processes, including Privacy Risk Management, may be supported by tools. Tools include a broad collection of resources which facilitate either or both processes and projects. Many of them may be described as necessary, but not sufficient, to ensure end-to-end privacy protectiveness. They include:

- Privacy Impact Assessments
- Staff education modules;
- Services, such as certification regimes (like the *Europrise* European Privacy Seal and Japan's *PrivacyMark* or Deloitte's "PBD" Assessment Methodology).

PIAs involve developing an information flow map, applying a set of privacy questions to the information flow, identifying risks, and developing an approach to managing these risks. A PIA is generally modular in nature and involves people from throughout an organization, since most policies, governance frameworks and systems are neither the purview nor the expertise of a single person.

The link at the end of this presentation, and the list of Further Readings that are part of the Instructor Resources for this presentation, offer information on different PIA approaches.

The End Result: Privacy Embedded Throughout the Organization!



Slide 18

In summary: when *PbD* is fully implemented, privacy becomes part of the fabric of how an organization thinks and operates, at every level. It touches every aspect of the organization, and makes privacy a core competency.

This enables the organization to reap the rewards of strong privacy practices...

Reaping the Rewards...



www.privacybydesign.co

Slide 19

**More information and a growing
library of resources are available at**

www.privacybydesign.ca

Slide 20