Privacy by Design Curriculum 2.0

Instructor Resources

MODULE ONE: THE FUNDAMENTALS

Presentation 2: *Privacy by ReDesign: Building a Better Legacy*

CONTENTS

Overview

Privacy by ReDesign is a new approach to applying the 7 Foundational Principles of *Privacy by Design* to existing systems: information technologies, business practices, physical design, and networked infrastructure.

This sections shows that, since existing systems are already operational and pervasive throughout organizations, the principles of *PbD* cannot be embedded from the outset – these systems are up and running. It suggests instead that the objective must be to approach the end state of *PbD* – the highest standard of privacy protection – by transforming existing systems, seizing opportunities to Rethink, Redesign, and Revive them.

Essential Reading

Ann Cavoukian, Ph.D. and Marilyn Prosch, Ph.D., Privacy by ReDesign: Building a Better Legacy. www.privacybydesign.ca
Ann Cavoukian, Ph.D., Ontario and Claudiu Popa, CIPP, CISA, PMP, CISSP, Privacy by ReDesign: A Practical Framework for Implementation. www.privacybydesign.ca

Learning Objectives

Participants will develop an understanding of how to apply the 7 Foundational Principles of *Privacy by Design* to legacy and existing systems.

Privacy by ReDesign: Building a Better Legacy

Overview of Presentation

Slide	***Title***	***Theme***
2.1	The Ideal	Embedding privacy at the outset
2.2	Reality	Building new systems from the ground up is not always on the agenda
2.3	Is it Too Late?	Do the principles of Privacy by Design have relevance for existing systems?
2.4	No! Of Course Not!	There is still an opportunity to apply the principles of *PbD*
2.5	*Privacy by ReDesign*	Relevance of principles to existing systems
2.6	What is Privacy by ReDesign?	A framework for assessing and addressing gaps proactively and systematically
2.7	Act Now!	*PbD* will apply broadly in the future. Why wait?
2.8	Identifying *PbRD* Projects	Proactive identification through existing management processes
2.9	Prioritizing: Asking the Right Questions	Choosing among possible projects
2.1	Rethink, Redesign, Revive	The 3 R's: the essence of *PbRD*
2.11	Organizing Project Work	Using the 3 R's to organize project work
2.12	Laying the Foundations for Success	Strong leadership, a systematic approach, and consistent follow-through are key
2.13	The Desired End State	Fully implemented, *PbRD* is enterprise-wide in scope

Further Reading

An Ernst & Young paper, under the working title *Making Privacy Count: Five Steps to Integrating Privacy Protection into IT Transformations*, was under development at the time this Curriculum was printed. See www.ey.com.

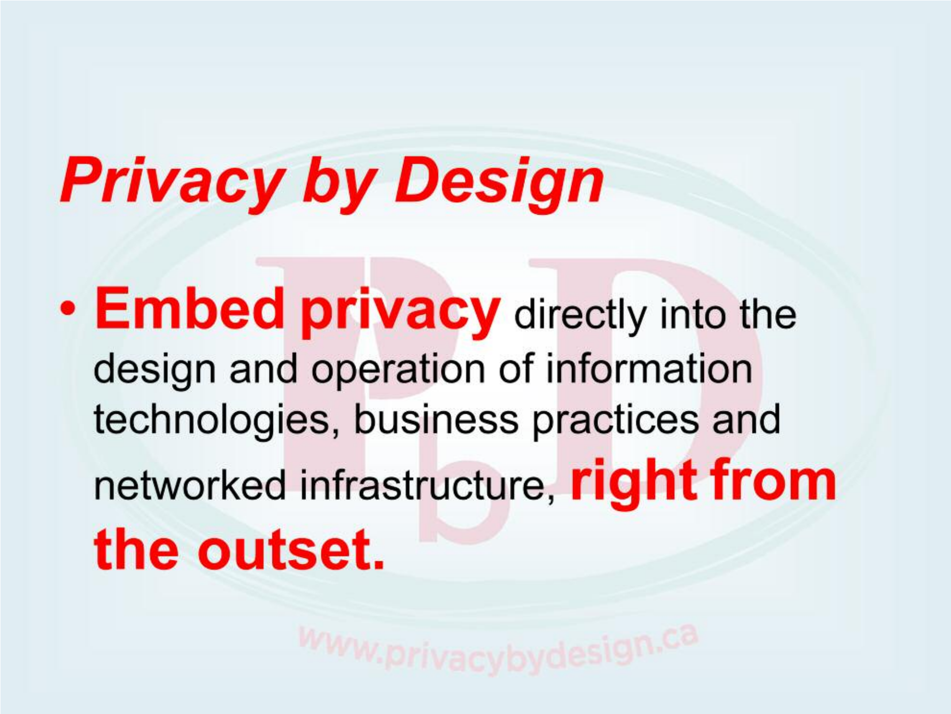
Presentation Materials with Instructor Notes

Privacy by ReDesign

Building a Better Legacy

www.privacybydesign.ca

Slide 1



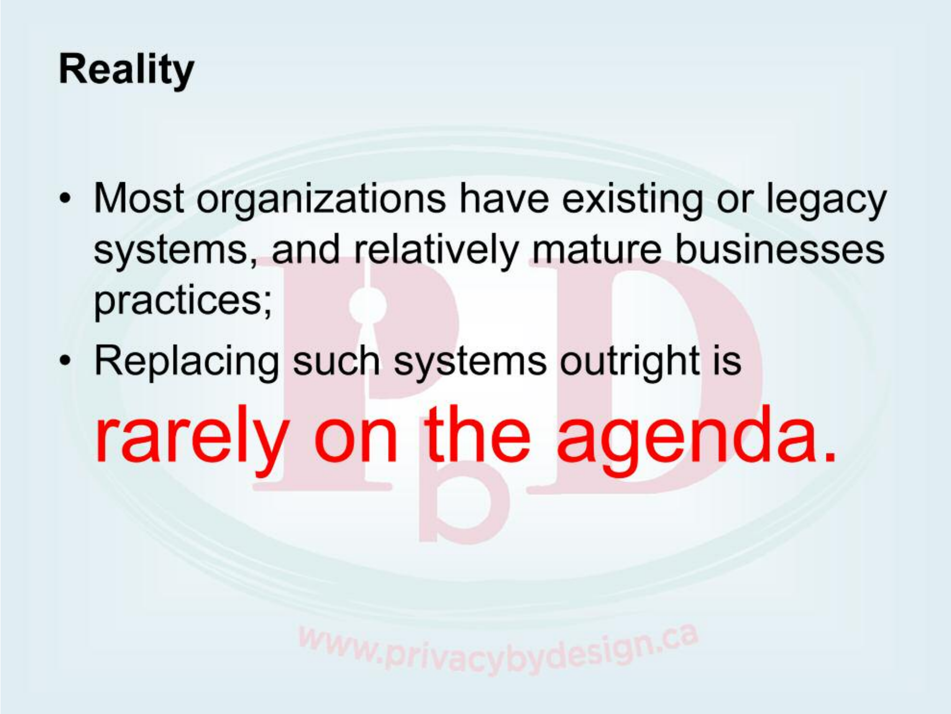
Privacy by Design

- **Embed privacy** directly into the design and operation of information technologies, business practices and networked infrastructure, **right from the outset.**

www.privacybydesign.ca

Slide 2

The ideal….



Reality

- Most organizations have existing or legacy systems, and relatively mature businesses practices;
- Replacing such systems outright is

rarely on the agenda.

Slide 3

Is it….

?

Slide 4

(Of course not!)

Slide 5

Privacy by Design is just as relevant to established systems as it is to nascent ones – enter…

Privacy by ReDesign

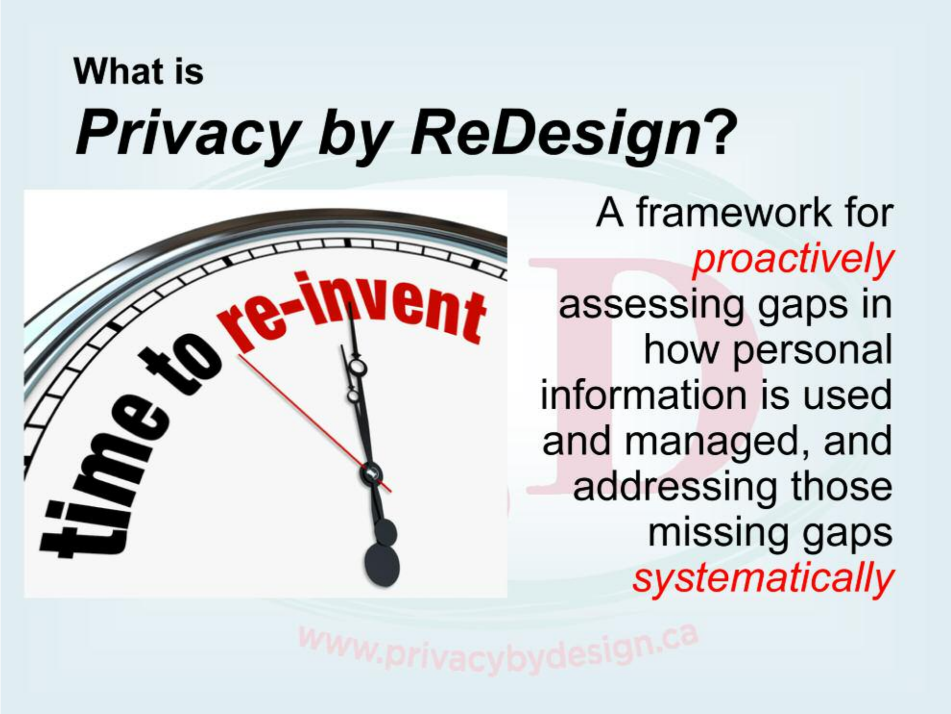
www.privacybydesign.ca

Slide 6

Privacy by Design presents a clear and effective strategy for meeting the objective of attaining the highest degree of privacy protection possible. It benefits individuals, providing them with important assurances about how their personal information is being managed. But it also benefits businesses, which may enjoy sustained competitive advantages from the trust that responsible privacy practices engender with their customers.

PbD is equally relevant to established systems and nascent ones.

Previously developed and implemented systems, however, cannot engage with *Privacy by Design* in the same manner as nascent ones. By definition, privacy cannot be "built in" to these existing systems from the outset. Instead, the task must be approached as one of *Privacy by ReDesign* (*PbRD*) – an extension of *PbD*.



What is

Privacy by ReDesign?

time to re-invent

A framework for *proactively* assessing gaps in how personal information is used and managed, and addressing those missing gaps *systematically*

www.privacybydesign.ca

Slide 7

Privacy by ReDesign is more than a retrofit – which is what often occurs when circumstances force organizations to focus on an immediate issue and quickly apply a band-aid solution.

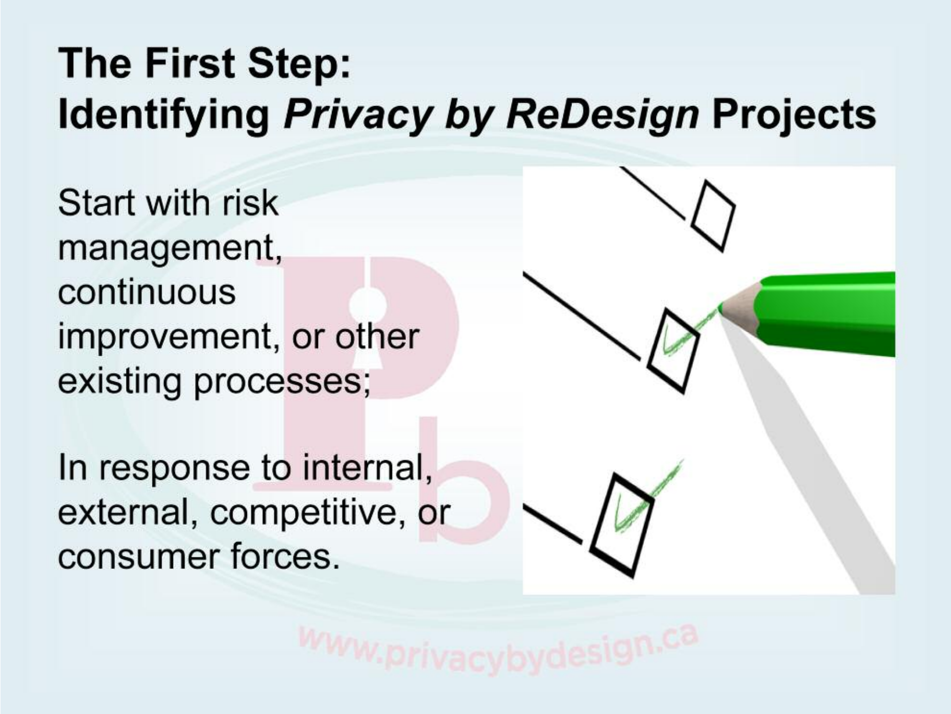
Instead, *PbRD* is a transformative process. It is a framework for undertaking a *proactive* assessment of existing gaps in how personal information is used and managed, and addressing those gaps systematically. In this context, the principles of *PbD* are applied not as goals for a nascent system design, but rather as the end result of a successful *PbRD* initiative.

Why Wait?!

Slide 8

There is so much momentum behind *PbD* – in Canada, the US, Europe, and elsewhere – that there can be little doubt that *Privacy by Design* will apply broadly in the future.

Privacy by ReDesign allows the principles of *PbD* to apply now to existing and legacy systems. Why wait?



The First Step: Identifying *Privacy by ReDesign* Projects

Start with risk management, continuous improvement, or other existing processes;

In response to internal, external, competitive, or consumer forces.

Slide 9

Organizations may be prompted to consider *PbRD* projects for any number of reasons. In some cases, opportunities may arise as a result of a proactive strategy for improving the organization's privacy posture as part of existing management structures that support risk mitigation or brand/market positioning.

Organizations that have mature risk management or continuous improvement frameworks may already include consideration of legacy systems in those processes. Privacy requirements can and should be incorporated into these management frameworks, if they are not already. This can support the identification of possible targets for remediation or transformation.

Opportunities to consider *PbRD* projects may also arise as a result of:

> **External Factors**: such as changes in legal requirements or industry best practices, and new partnerships or outsourcing arrangements (including cloud computing).

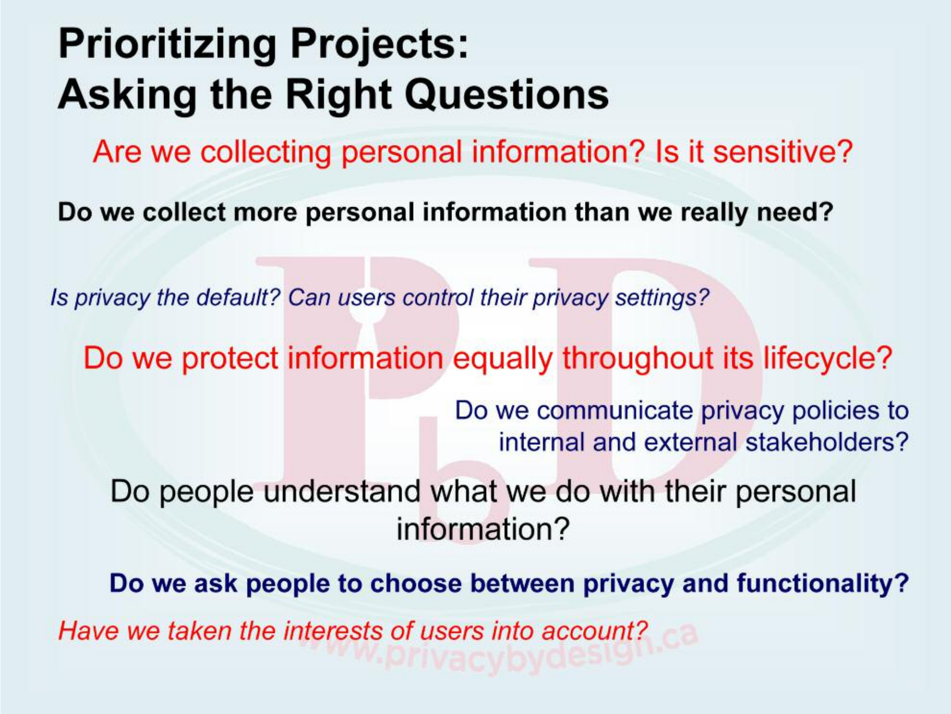
Internal Factors: such as ongoing risk management activities, technology upgrades, software modifications, changes in work processes or workflows, changes in the work force and/or expertise, and changes in accountability and governance.

Competitive Forces: such as the need to build consumer trust and loyalty, the threat of new market entrants, changes in both supply and consumer demand, and opportunities to seize competitive advantages.

Consumer Forces: such as evolving user requirements, changes in customer expectations, and the diversity of customer expectations in various global markets.

Organizational leaders may seize these windows of opportunity to improve privacy protection in existing functionality, or to implement new components to support responsible information management and render privacy the default condition, going forward.

Such opportunities may also arise when a system developed for one purpose evolves to take on another, perhaps unintended use, with unexpected or poorly-understood consequences for privacy.



Prioritizing Projects: Asking the Right Questions

Are we collecting personal information? Is it sensitive?

Do we collect more personal information than we really need?

Is privacy the default? Can users control their privacy settings?

Do we protect information equally throughout its lifecycle?

Do we communicate privacy policies to internal and external stakeholders?

Do people understand what we do with their personal information?

Do we ask people to choose between privacy and functionality?

Have we taken the interests of users into account?

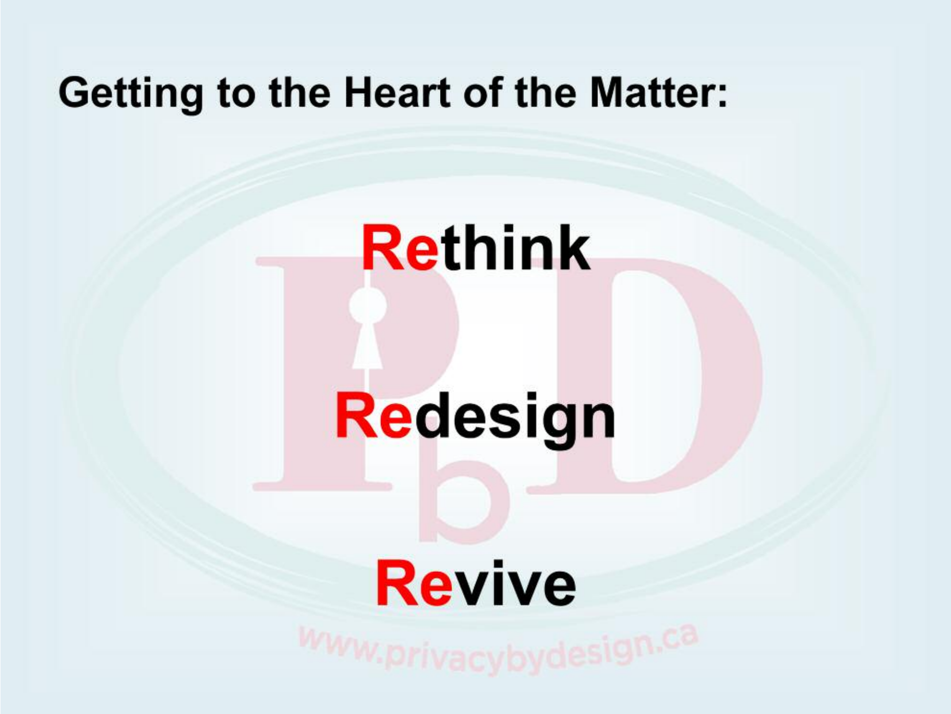
Slide 10

Where several potential targets for remediation have been identified, and resources are finite, it may be necessary to perform an initial, high-level triage in order to prioritize projects. While many techniques can be used, a simple set of focused questions based on The 7 Foundational Principles of *Privacy by Design* may be quite effective. These will vary according to the size of the business or industry sector in which the organization participates.

Sample Questions for Triaging *PbRD* Targets

- Does the target involve the collection, use, or disclosure of personal information? How sensitive is the personal information in question?
- Does the target collect more personal information than is absolutely necessary to fulfill the specified business purposes?
- Are users required to take specific actions to protect their privacy, or is privacy the default setting? Are user privacy preferences configurable?
- Could the introduction of additional privacy features constitute a competitive advantage for the organization?

- Does the target exhibit a potential compromise between functionality and privacy, such as offering conditional access to desirable features only to the detriment of privacy?
- Is personal information consistently protected throughout its entire lifecycle (i.e. collection, use, disclosure, retention, and disposal)?
- Are privacy policies effectively communicated to internal and external stakeholders?
- Is it clear to data subjects when and how personal information about them is being collected, used and/or disclosed?
- Has the target been designed and implemented to embrace the interests of users and data subjects (e.g. through strong privacy defaults, appropriate notice, and user-friendly options)?



Getting to the Heart of the Matter:

Rethink

Redesign

Revive

www.privacybydesign.ca

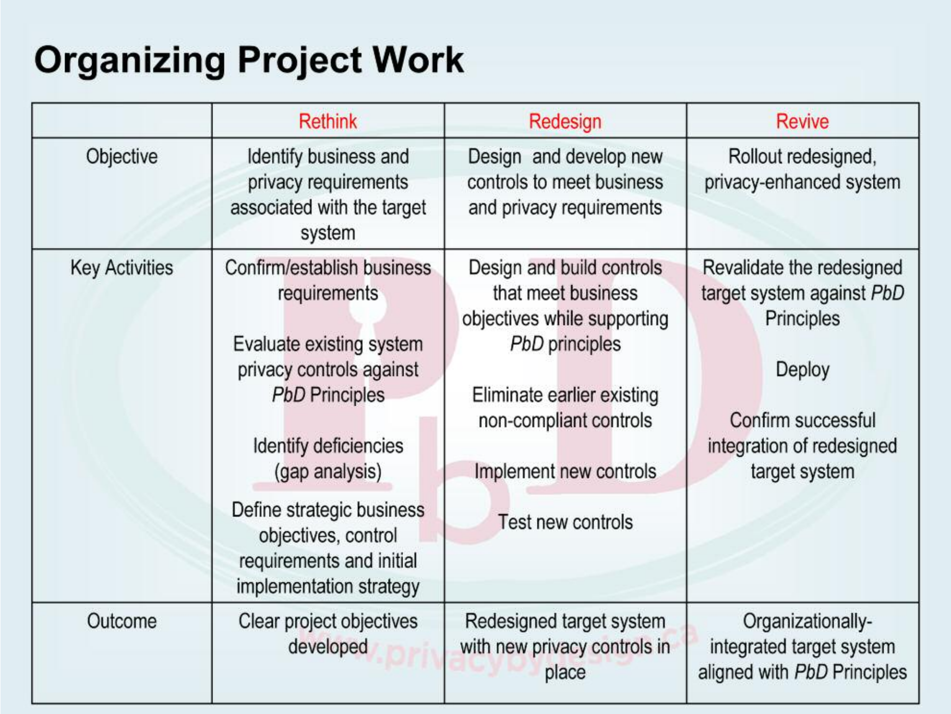
Slide 11

The essence of *Privacy by Redesign* may be summarized by its 3 R's: Rethink, Redesign, and Revive.

Rethinking invites organizations to review their risk mitigation strategies, existing systems, and processes – including information technologies, business practices, physical design, and networked infrastructure – and consider alternative approaches that are more privacy-protective. This may include revisiting assumptions about how much personal information is necessary for the system to operate, and how long it needs to be retained in identifiable form.

Redesigning represents the opportunity to enable or implement improvements in how the system functions from a privacy perspective, while also ensuring that it continues to achieve key business requirements in a doubly-enabling positive-sum, win/win relationship. Redesigning may likely require that less data be collected, and these changes may need to be cascaded back to stored databases where possible, to delete these unnecessary fields of data.

Reviving the system in a new, privacy-protective way is the ultimate goal!



Organizing Project Work

	Rethink	Redesign	Revive
Objective	Identify business and privacy requirements associated with the target system	Design and develop new controls to meet business and privacy requirements	Rollout redesigned, privacy-enhanced system
Key Activities	Confirm/establish business requirements Evaluate existing system privacy controls against *PbD* Principles Identify deficiencies (gap analysis) Define strategic business objectives, control requirements and initial implementation strategy	Design and build controls that meet business objectives while supporting *PbD* principles Eliminate earlier existing non-compliant controls Implement new controls Test new controls	Revalidate the redesigned target system against *PbD* Principles Deploy Confirm successful integration of redesigned target system
Outcome	Clear project objectives developed	Redesigned target system with new privacy controls in place	Organizationally-integrated target system aligned with *PbD* Principles

Slide 12

The 3 R’s can be used to organize project work, as shown here.

Rethink

In the Rethink phase, the core objective is to identify the business and privacy requirements that are associated with the target system. This objective is achieved through a process that begins with establishing or confirming business requirements. A key component of this process is identifying the information requirements that align with the business requirements. Many organizations may find that they are collecting more information than is technically necessary to achieve their goals, thereby increasing their privacy risk.

The system’s existing privacy controls must then be assessed against the requirements of *Privacy by Design*, with deficiencies being identified through a gap analysis. This will enable the strategic business objectives to be defined, and the resulting control requirements and initial implementation strategy to be developed.

By the end of this phase, clear project objectives will have been developed, marking the way forward.

Redesign

In the Redesign phase, the core objective is to design and develop new controls that will align with both the business and privacy requirements identified in the Rethink phase. In some cases, best practices may be available to guide this work. In others, however, innovation and creative thinking will be required to develop positive-sum solutions that achieve full functionality – both privacy and business objectives.

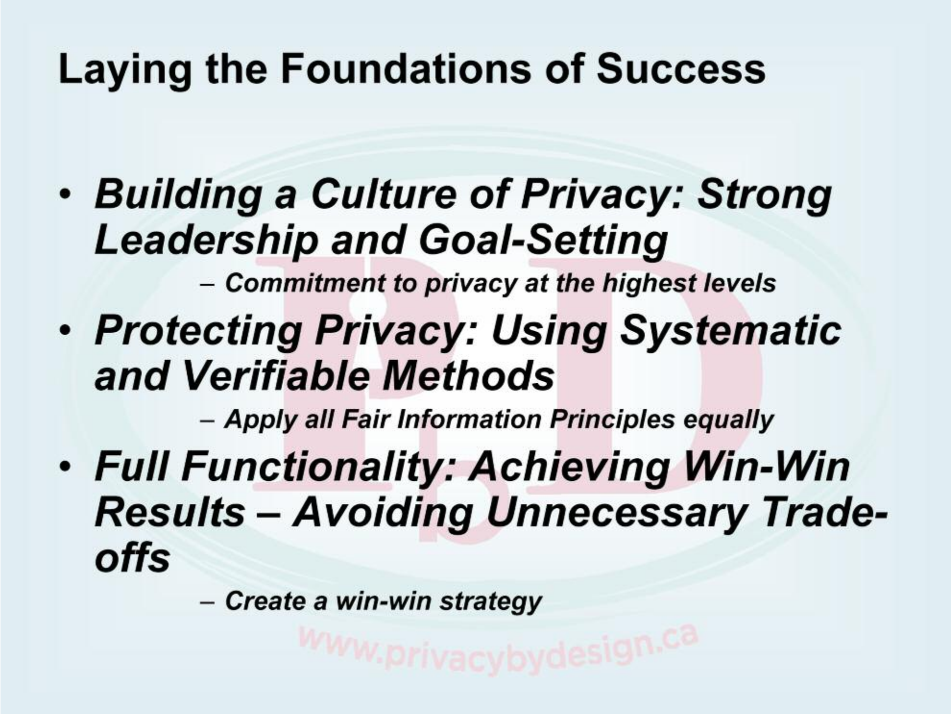
The resulting new or improved controls must then be implemented and tested. The initial non-compliant controls must also be eliminated, once the new controls have been introduced.

By the end of this phase, a redesigned target system, with new privacy controls, will be in place.

Revive

In the Revive phase, the core objective is to integrate the newly redesigned, privacy-enhanced system into the organization. Through this deployment, the real benefits of improved privacy practices will be realized. It is at this time that any issues related to how the improved system interacts with other systems in the organization will also arise and may be addressed.

At the end of the Revive phase, the organization will have achieved a fully-functional, integrated, privacy-enhanced system. Where necessary or appropriate, the process can then be repeated in the context of another target system, until all of the organization's legacy or existing systems have been remediated.



Laying the Foundations of Success

- ***Building a Culture of Privacy: Strong Leadership and Goal-Setting***
  - ***Commitment to privacy at the highest levels***
- ***Protecting Privacy: Using Systematic and Verifiable Methods***
  - ***Apply all Fair Information Principles equally***
- ***Full Functionality: Achieving Win-Win Results – Avoiding Unnecessary Trade-offs***
  - ***Create a win-win strategy***

www.privacybydesign.ca

Slide 13

Experience has shown that the success of *Privacy by Design* projects is dependent, to a large extent, on strong leadership, taking a systematic approach, and consistent follow-through. Similarly, while *Privacy by ReDesign* may be implemented in any of a number of ways, and linked with any of a number of existing processes within the organization, there are some factors that greatly increase the likelihood of success.

Building a Culture of Privacy: Strong Leadership and Goal-Setting

Whether applied to information technologies, organizational practices, or networked information ecosystems, *Privacy by ReDesign* begins with an explicit recognition of the value and benefits of adopting strong privacy practices.

Organizational leaders have a critical role to play in fostering a commitment to privacy at all levels of the organization. They must both foster and support a Culture of Privacy. Such a culture enables sustained collective action by providing people throughout the organization 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.

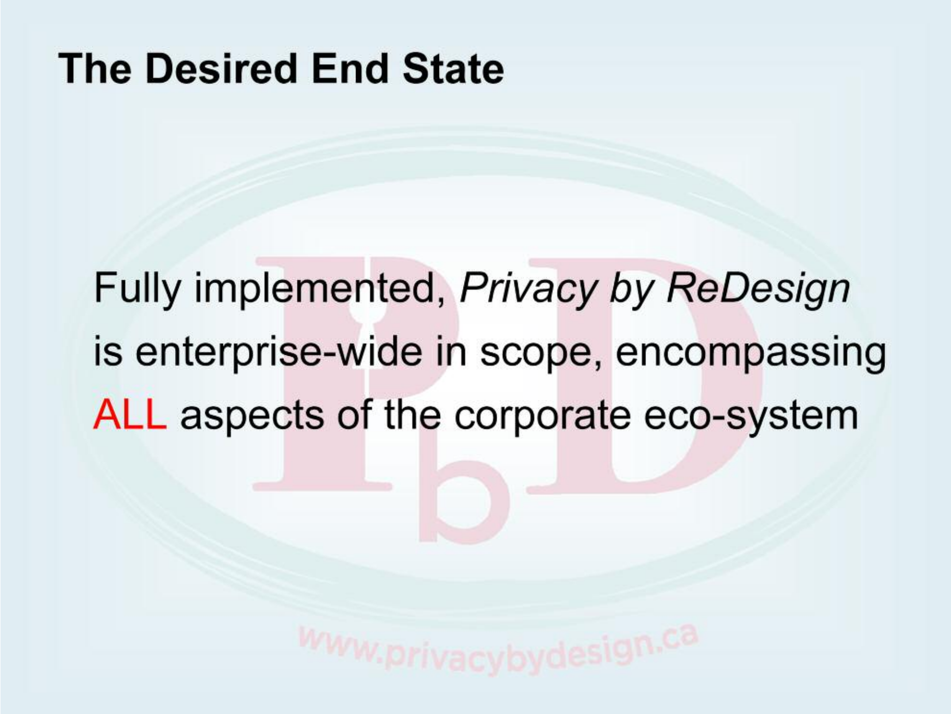
Protecting Privacy: Systematic and Verifiable Methods

A systemic, principled approach to achieving privacy should be adopted – one that relies upon accepted standards and frameworks, which are amenable to external reviews and audits. All fair information practices should be applied with equal rigor, at every step of the exercise.

Full Functionality: Achieving Win-Win Results

The end goal is to achieve real, practical results and beneficial outcomes for multiple interests – a win/win strategy.

In order to achieve such a result, it is essential that all levels of the organization approach privacy with the right mindset. Leaders have a key role in setting the right tone. Privacy must not be positioned as having to "compete" with other legitimate values, design objectives, and technical capabilities, in any given domain. Throughout the remediation or transformation process, full functionality must be supported, and, to the greatest extent possible, all requirements must be optimized in a complementary, not a conflicting, manner.



The Desired End State

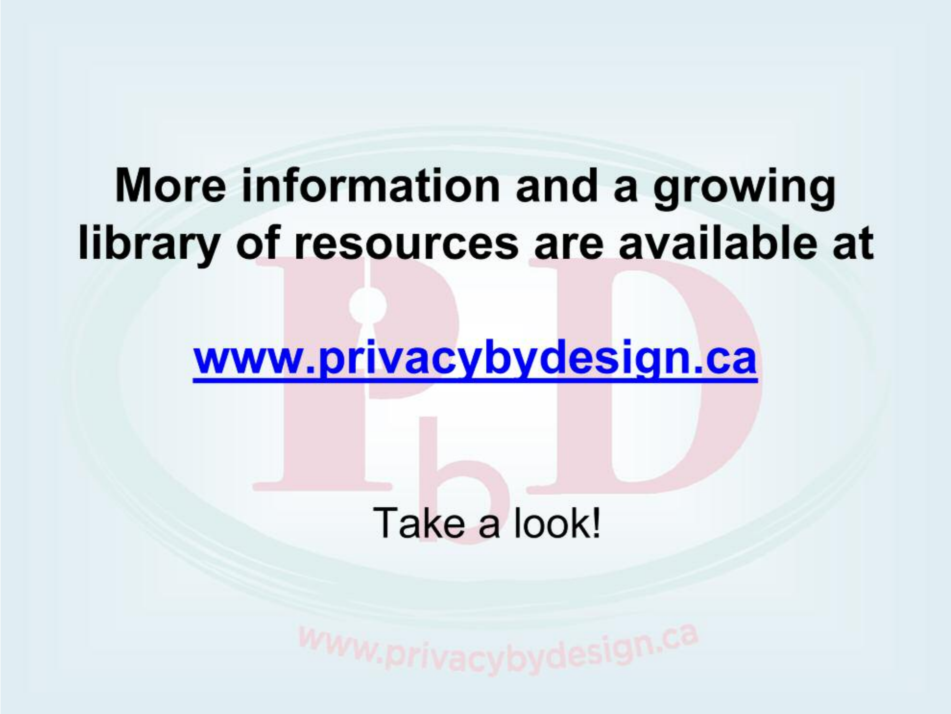
Fully implemented, *Privacy by ReDesign* is enterprise-wide in scope, encompassing ALL aspects of the corporate eco-system

Slide 14

While the full implementation of the principles of *Privacy by Design*, ideally at the outset of a new system, application, or process development, is the end state for which we strive, organizational and economic realities are such that practical, economically-sound approaches to implementing *PbD* in existing systems in the here-and-now are also essential.

Market leaders are increasingly building a body of experience and knowledge about the implementation of *Privacy by Design*. There is a clear need for practical guidance as to how to accomplish its objectives and implement its principles in existing systems.

Fully implemented, *Privacy by ReDesign*, as an extension of *PbD*, is enterprise-wide in scope, encompassing all aspects of the corporate eco-system.



More information and a growing library of resources are available at

www.privacybydesign.ca

Take a look!

Slide 15