Privacy Meets Risk Management

Ken Anderson

Assistant Commissioner (Privacy)

Ontario

Risk Insurance Management Society
Annual Conference
April 28, 2010

THINK FORWARD THINK RISK

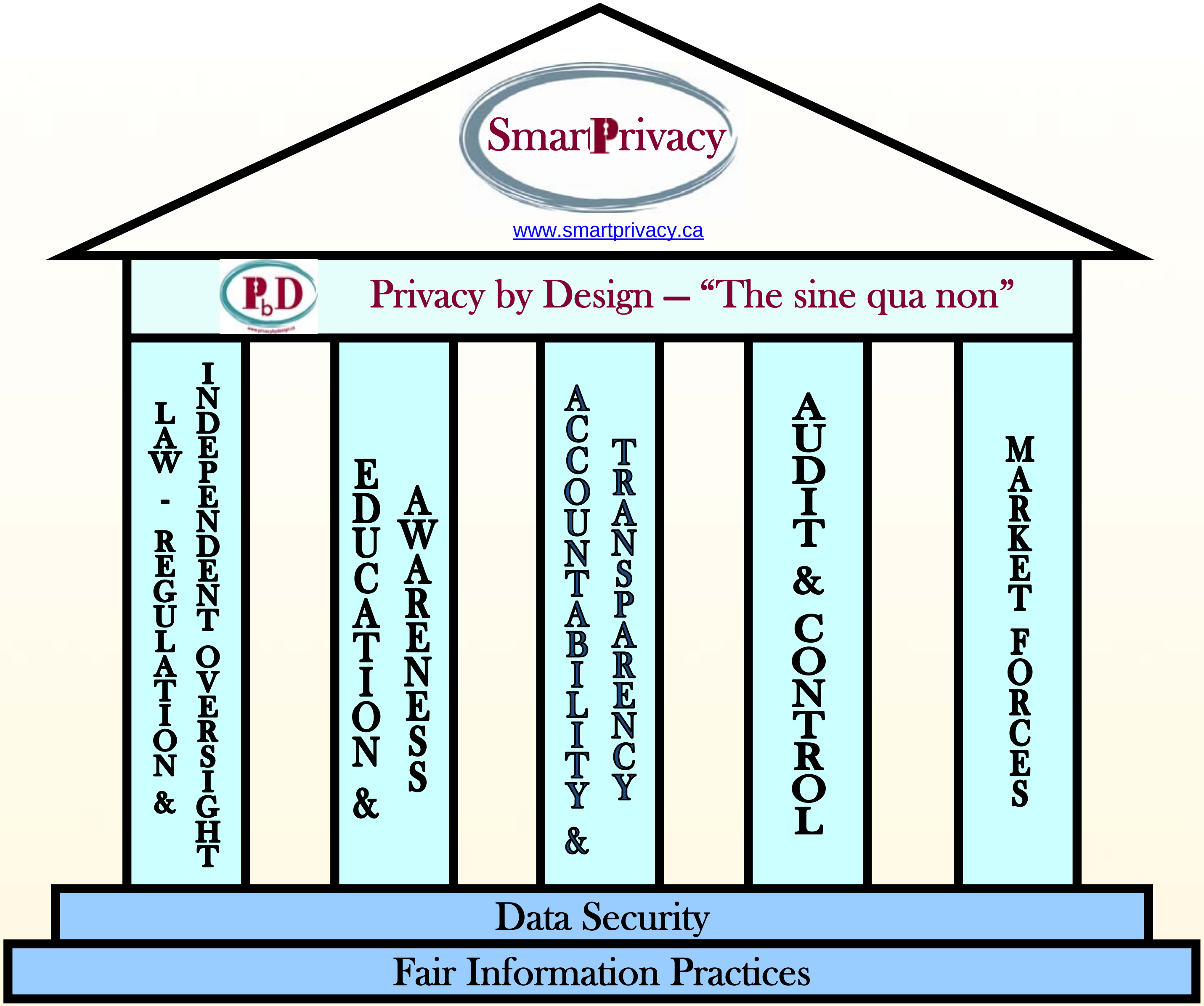
RIMS 2010.

Presentation Outline

1. *SmartPrivacy*
2. *Privacy by Design*
3. *Privacy Risk Management (PRM)*
4. *When is an organization ready to implement PRM*
5. *What is the role of the PRM Practitioner?*
6. *What is the PRM Model?*
7. *Conclusions*

SmartPrivacy

www.smartprivacy.ca



SmartPrivacy

www.smartprivacy.ca

Privacy by Design – “The sine qua non”

LAW - REGULATION & INDEPENDENT OVERSIGHT

EDUCATION & AWARENESS

ACCOUNTABILITY & TRANSPARENCY

AUDIT & CONTROL

MARKET FORCES

Data Security

Fair Information Practices

SmartPrivacy:
A Model of Effective Privacy Protection

- **Fair Information Practices**: Describing the manner in which organizations collect and use personal information as well as the safeguards employed to protect it;
- **Law, Regulation and Independent Oversight**: Typically reactive and remedial, they are important, nonetheless, because they describe the consequences of a failure to protect personal information. I would argue that user privacy is more strongly protected through the use of Privacy-Enhancing Technologies embedded into the design of systems;
- **Education and Awareness**: It is vitally important that the public is well-educated regarding the privacy implications posed by the technology or environments with which they interact – doubly so when it comes to the youngest members of our society, our children;

SmartPrivacy:
A Model of Effective Privacy Protection

- **Accountability and Transparency**: Individual accountability for information management decisions and assured operational transparency, once regarded as best practices, will quickly come to be thought of as elements of hygiene. Organizations will come to practice both naturally;

- **Audit and Control**: Audits should be viewed as thorough examinations of an institution’s policies, practices and procedures, as well as a test of internal compliance with legal and other obligations. Regular audits will lower the risk of security breaches;

- **Market Forces**: Whether there is a breach or not, organizations who fail to treat the privacy of their personal information as a core business requirement will likely see the equity of their brand diminish, finding themselves at a competitive disadvantage. I believe that users will increasingly seek organizations who offer them control over their personal information.

Privacy by Design

www.privacybydesign.ca

Why We Need *Privacy by Design*

- Most privacy breaches remain undetected
  – as regulators, we only see the tip of the iceberg;
- The majority of privacy breaches remain unchallenged, unregulated ... unknown;
- Compliance alone, is unsustainable as the sole model for ensuring the future of privacy; for that, we must turn to proactive measures such as ***Privacy by Design:*** embedding privacy proactively into the core of all that we do.

***Privacy by Design*: “Build It In”**

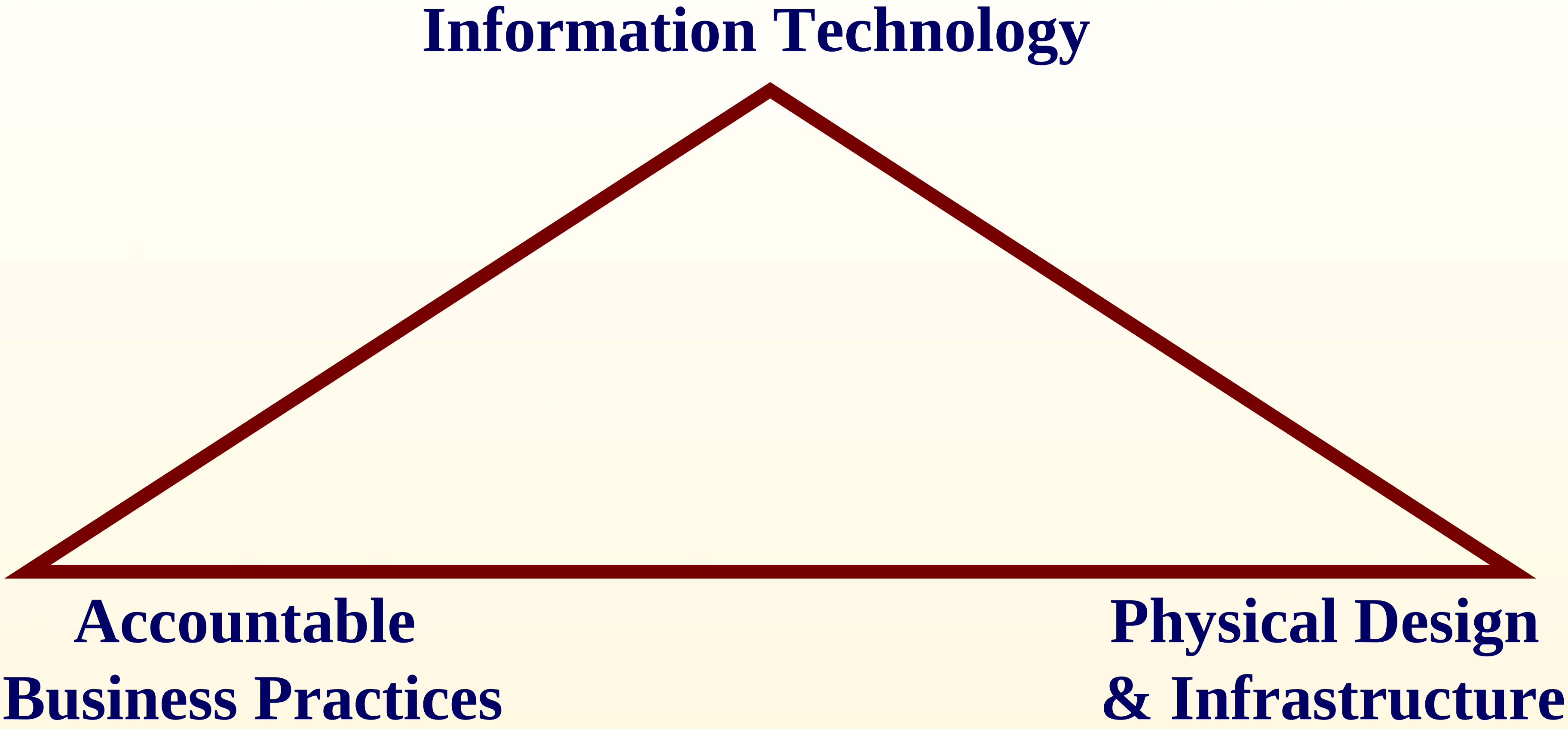
- I first developed the concept of ***Privacy by Design*** in the ‘90s, as a response to the growing threats to online privacy that were beginning to emerge;

- ***Privacy by Design*** **seeks to build in privacy –** up front, right into the design specifications; into the architecture; embedding privacy into the very technology used **–** ***bake it in***;

- **Data minimization is key**: minimize the routine collection and use of personally identifiable information **–** use encrypted or coded information, whenever possible;

- **Use privacy-enhancing technologies** (PETs) where possible, but make it PETs *Plus*, invoking a positive-sum paradigm, and giving people maximum control over their own data.

Privacy by Design:
The Trilogy of Applications



Information Technology

Accountable
Business Practices

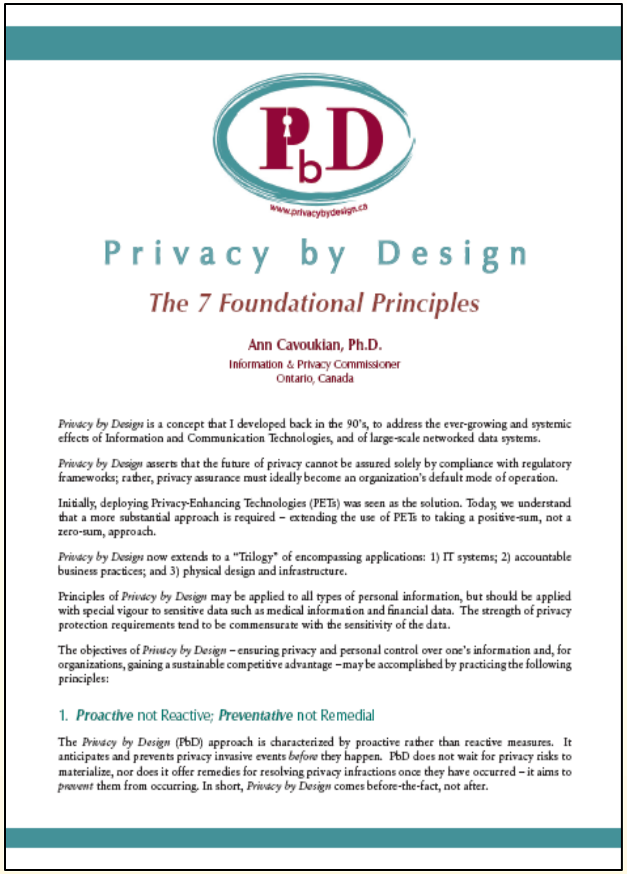
Physical Design
& Infrastructure

Privacy by Design:
Focus for 2010

- **Technology –**
  Building privacy directly into technology, at the earliest developmental stage;
- **Accountable Business Practices –**
  Incorporating privacy into competitive business strategies and operations;
- **Physical Design and Infrastructure –**
  Ensuring privacy in health care settings and networked infrastructure.

Privacy by Design:
The 7 Foundational Principles

1. *Proactive* not Reactive;
   Preventative not Remedial
2. Privacy as the *Default*
3. Privacy E*mbedded* into Design
4. Full Functionality:
   Positive-Sum, not Zero-Sum
5. End-to-End Lifecycle Protection
6. Visibility and Transparency
7. Respect for User Privacy



Privacy by Design

The 7 Foundational Principles

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

Privacy by Design is a concept that I developed back in the 90's, to address the ever-growing and systemic effects of Information and Communication Technologies, and of large-scale networked data systems.

Privacy by Design asserts that the future of privacy cannot be assured solely by compliance with regulatory frameworks; rather, privacy assurance must ideally become an organization's default mode of operation.

Initially, deploying Privacy-Enhancing Technologies (PETs) was seen as the solution. Today, we understand that a more substantial approach is required – extending the use of PETs to taking a positive-sum, not a zero-sum, approach.

Privacy by Design now extends to a "Trilogy" of encompassing applications: 1) IT systems; 2) accountable business practices; and 3) physical design and infrastructure.

Principles of *Privacy by Design* may be applied to all types of personal information, but should be applied with special vigour to sensitive data such as medical information and financial data. The strength of privacy protection requirements tend to be commensurate with the sensitivity of the data.

The objectives of *Privacy by Design* – ensuring privacy and personal control over one's information and, for organizations, gaining a sustainable competitive advantage – may be accomplished by practicing the following principles:

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.

www.ipc.on.ca/images/Resources/7foundationalprinciples.pdf

Privacy by Design: The 7 Foundational Principles

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;

Privacy by Design: *The 7 Foundational Principles* (Cont’d)

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;

Privacy by Design:
The 7 Foundational Principles (Cont'd)

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.

Privacy Risk Management

IPC Publication:
Privacy Meets Risk Management

- When is an organization ready to implement Privacy Risk Management?

- What is the role of the Privacy Risk Management Practitioner?

- What is the Privacy Risk Management Model?

[Cover of Publication here]

Publication URL here]

When is an organization ready to implement Privacy Risk Management?

When is an organization ready to implement Privacy Risk Management?

- Successful PRM depends upon an organization’s approach to both the privacy and risk management disciplines;

- 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.

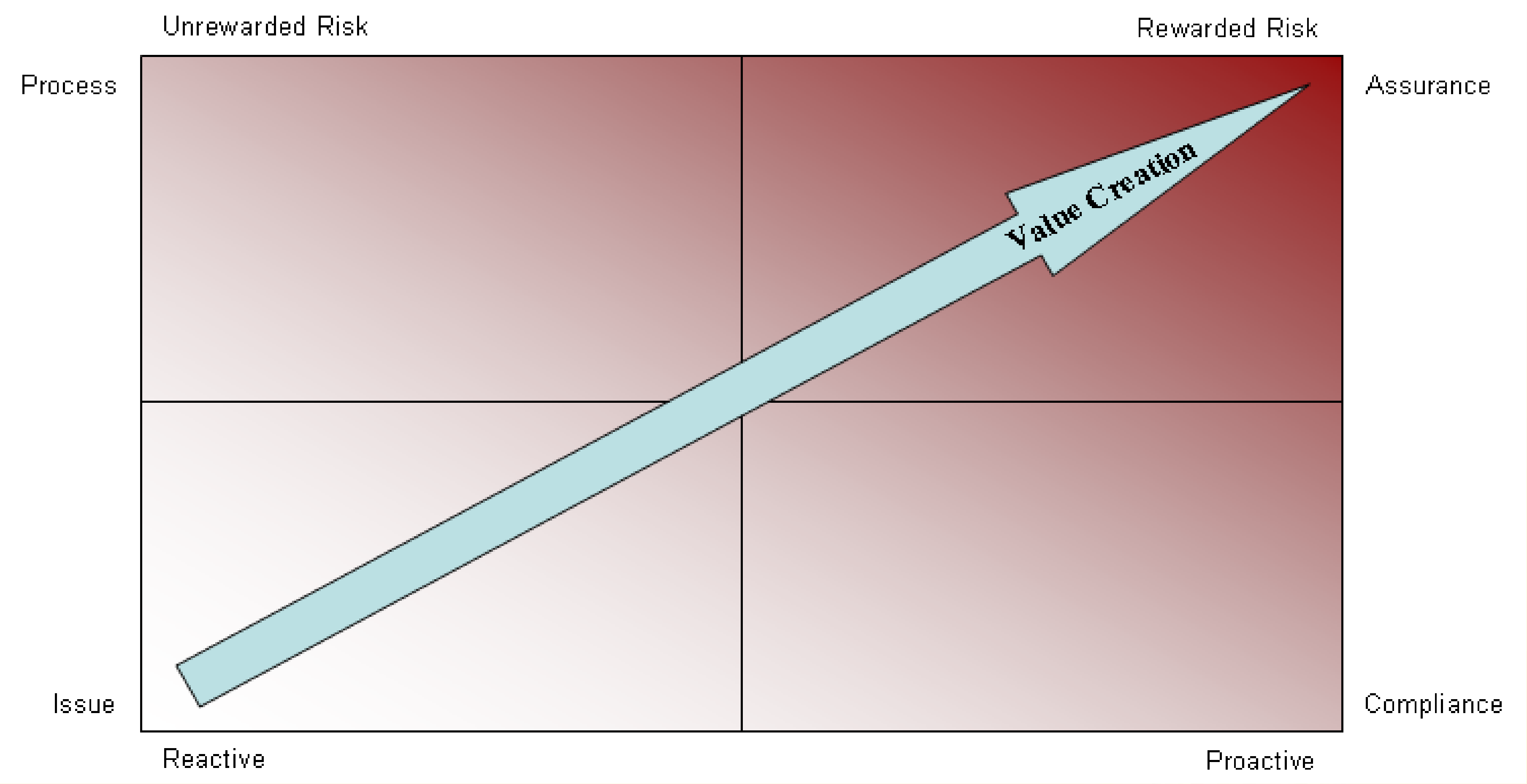
Rewarded Risk

- **As with traditional risk management, organizations which successfully launch a PRM discipline discover that it creates value through attention to “rewarded risk;”**

  “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.”

Pertinent Dimensions of Privacy and Risk Management Task Maturity



What is the role of the Privacy Risk Management Practitioner?

What is the role of the Privacy Risk Management Practitioner?

Effective Privacy Risk Management Practitioners, fulfill two fundamental roles:

1. **Change Agent –** The risk manager embarks on a strategic journey by taking the first steps in embedding privacy within the risk management process;
2. **Process Custodian –** The risk manager is ideally-positioned to work alongside others involved in managing privacy risk including an organization’s executive, business unit managers and support functions.

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 privacy assessment and treatment processes are effective.

Roles and contributions associated with the PRM process

Successful PRM Practitioners will generally demonstrate the following characteristics:

- **Process-Oriented –** Methodical and possessing a clear, end-to-end vision of business operations, will assist in the development of privacy protective processes throughout the organization;
- **Organizationally Astute –** As some tension between functional areas may arise while engaging in cross-functional activity, the PRM practitioner should focus on how they can complement what others are already doing;
- **Effective Communicator –** The PRM Practitioner manages through a blend of technical expertise and, more importantly, moral suasion.

YMCA: Privacy as Catalyst for Broadening a 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;

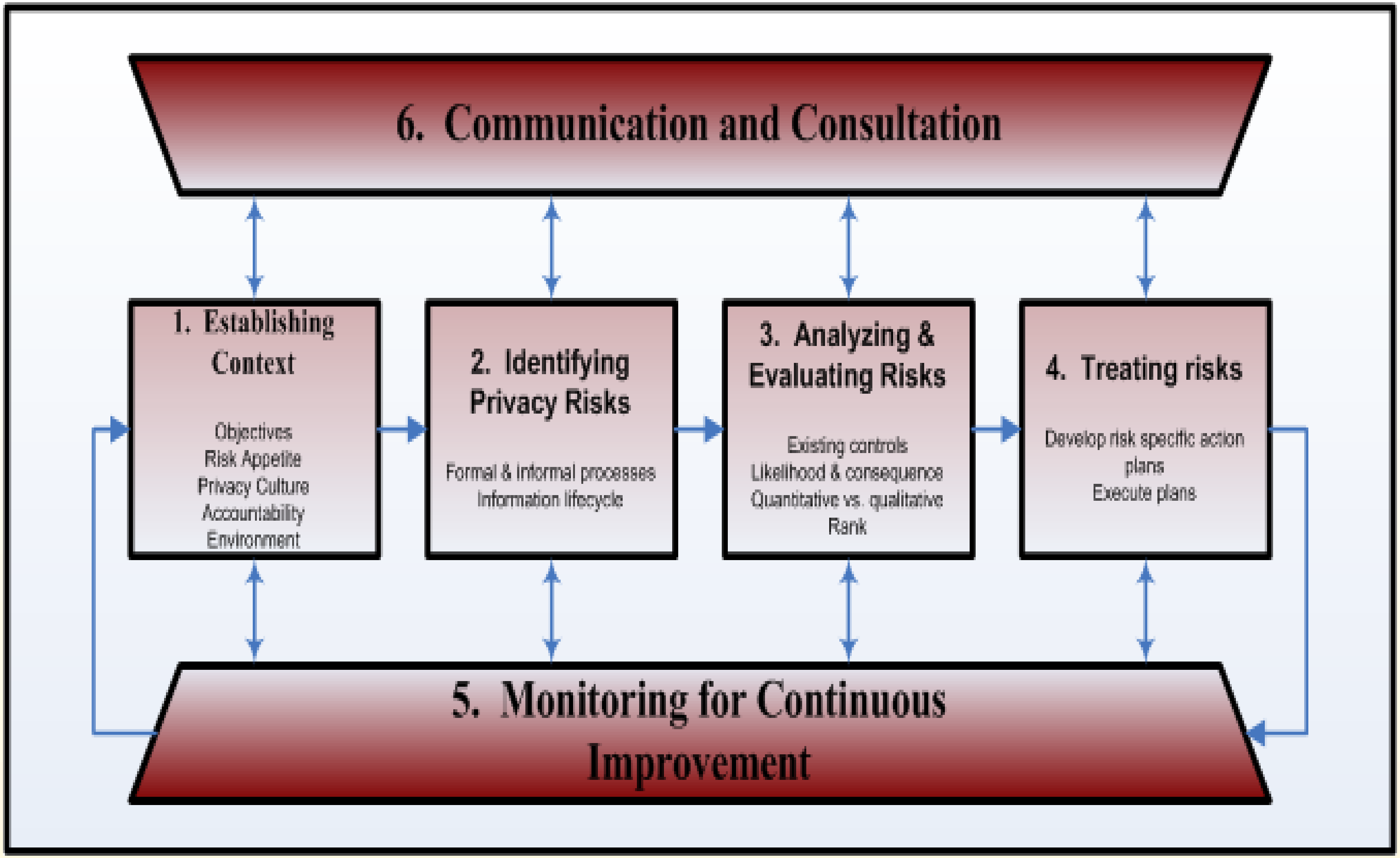
- Approaching ‘privacy’ as both an operational and strategic risk flowing through the entire organization, the Risk Manager began cross-functional activity working alongside program and process owners, to ensure readiness for changes in privacy law and to enhance the YMCA’s commitment to privacy;

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

What is the Privacy Risk Management Model?

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;
- 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.



6. Communication and Consultation

1. Establishing Context

Objectives
Risk Appetite
Privacy Culture
Accountability
Environment

2. Identifying Privacy Risks

Formal & informal processes
Information lifecycle

3. Analyzing & Evaluating Risks

Existing controls
Likelihood & consequence
Quantitative vs. qualitative
Rank

4. Treating risks

Develop risk specific action plans
Execute plans

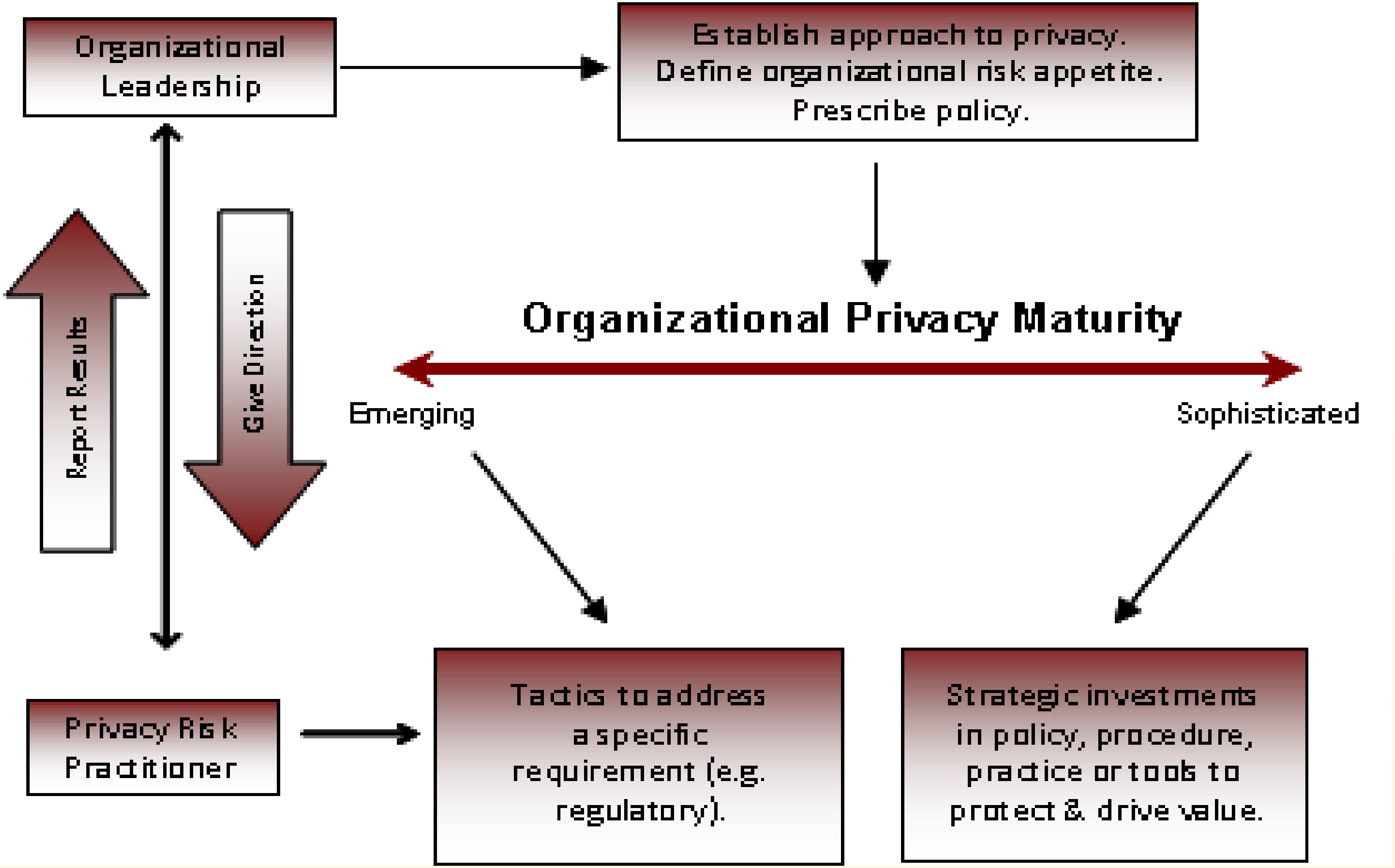
5. Monitoring for Continuous Improvement

Establishing Context

- It is critical to fully appreciate the external and internal context that affects privacy and how privacy risks are managed;
- Establishing context is a prerequisite in undertaking a strategic approach to, and setting the scope for, PRM;
- 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.

Establishing Context (Cont'd)

- When evaluating the internal context, elements to be considered are an organization's governance structure, operational and strategic objectives, roles and accountabilities, its policies, information systems and flows, decision-making processes, relationships with and perceptions of internal stakeholders, the organization's culture;
- Once the context is established, design and implementation of a framework for managing risks may follow;
- Senior leadership is critical in nurturing the integration of privacy, *PbD* and risk management.



Organizational Leadership

Establish approach to privacy. Define organizational risk appetite. Prescribe policy.

Report Results

Give Direction

Organizational Privacy Maturity

Emerging

Sophisticated

Privacy Risk Practitioner

Tactics to address a specific requirement (e.g. regulatory).

Strategic investments in policy, procedure, practice or tools to protect & drive value.

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;

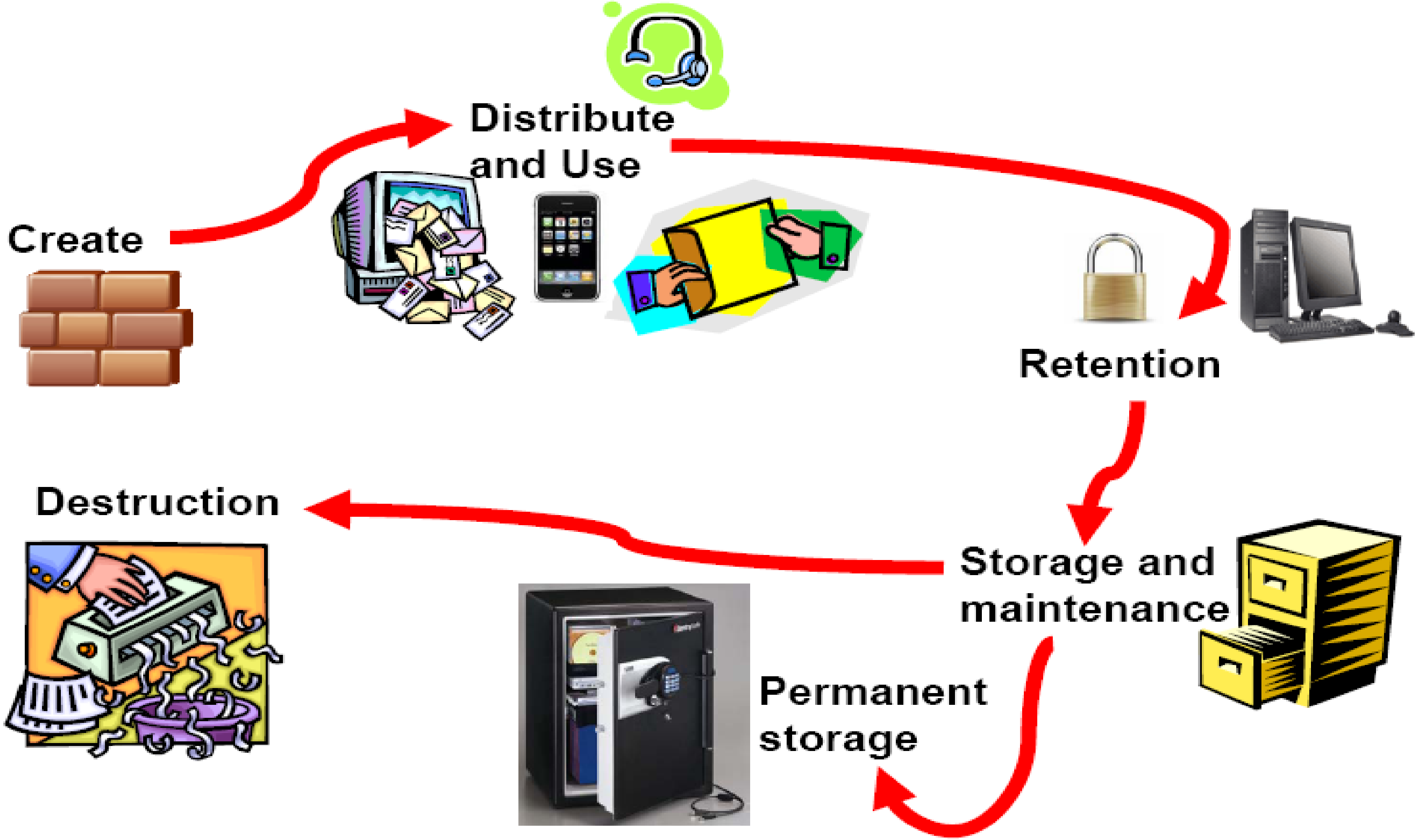
- They also include risks related to a company's outsourced service providers, ***an area that is often overlooked until it is too late.***

Identifying Privacy Risks (Cont'd)

In addition to traditional risk identification processes, such as Privacy Impact Assessments (PIAs) and privacy audits, there other techniques that can be leveraged to identify privacy risks:

1. Developing a Culture of Privacy Protection;
2. Listening to Employee and Business Partner Feedback;
3. Enhancing Security Measures;
4. Following the Flow of Your Organization's Information;
5. Examining the Key Business Processes;
6. Embedding a Formal Change Management Program;
7. Reviewing Third Party Processes;
8. Performing Self-Assessments;
9. Establishing Privacy Committees;
10. Engaging Internal Audit.

Managing the Lifecycle of Information



Create

Distribute and Use

Retention

Storage and maintenance

Permanent storage

Destruction

Analyzing and Evaluating Risks

- As with traditional risk assessment, determining the inherent risk of a privacy event is the starting point and 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 Practitioner –*** those with the greatest residual risk are the highest priority;
- 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 may only warrant monitoring;
- In addition, PRM Practitioners should also avail themselves of relevant case judgements, interpretations and guidance published by privacy authorities.

Identified Risks

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

- **Qualitative Analysis –** using words and descriptive scales to quickly assess the relative magnitude of identified risks;
- **Semi-Quantitative Analysis –** associates a numeric score with points on an otherwise descriptive scale;
- **Quantitative Analysis –** relies upon actual numeric values to communicate specific consequences (expressed in monetary, technical or human terms) and probabilities of outcomes.

Treating Risks

- 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.

Treatment Strategies

- Ensuring compliance with privacy laws, industry best practices, and following Fair Information Practices 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;

Treatment Strategies (Cont'd)

- Developing response protocols to ensure appropriate escalation and management in case of a major privacy incident or breach;
- Performing Privacy Impact Assessments and Information Lifecycle 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;
- Providing ongoing awareness through training, regular employee communications and de-brief 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.

Practical Strategies in Mitigating Privacy Risk and Creating Value

1. Ensuring Compliance;
2. Responding to Privacy Incidents or Breaches;
   - Containment;
   - Notification;
3. Re-engineering;
4. Risk Transfer.

Monitoring for Continuous Improvement

- Monitoring is an essential step in the PRM process as it helps organizations determine whether chosen strategies have achieved desired outcomes;
- Privacy risks continuously evolve and monitoring will uncover the need to re-visit or introduce new strategies;
- Monitoring trends in privacy incidents and complaints, and taking the time to review lessons learned, also enhances an organization’s privacy protection efforts;
- Early warning and other forms of monitoring are not only good governance, they are assurance activities which create value for the organization.

OLG: Case Study

- OLG’s (Ontario Lottery and Gaming Corporation) program of ***Voluntary Self-Exclusion* –** participants, if discovered at an OLG site, are escorted from the premises by security staff;
- To facilitate identification, they provide their picture as well as a collection of personal information;
- As the number of subscribed patrons began to grow over time, OLG, through a process of continuous monitoring discerned that their practice was growing less secure and increasingly challenging;
- Following the principles of ***PbD*,** they developed a sophisticated, on-line, facial recognition system;
- Protecting PI with a leading edge biometric encryption solution has improved patron protection and safely eliminated the need to keep hardcopy personal information.

Communication and Consultation

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

Conclusions

- Privacy risks can be further mitigated by employing the principles of ***Privacy by Design***;
- By embedding privacy in all personal information-related processes and practices, organizations can help to ensure that privacy risks will be managed by default;
- By also embedding privacy into their existing risk management framework, they can manage risks associated with the protection of personal information;
- Privacy Risk Management Practitioners are more than simply "Process Custodians". They are also "Agents of Change" which require executive support;
- 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.

How to Contact Us

Ken Anderson – Assistant Commissioner (Privacy)

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

Phone:	(416) 326-3333 / 1-800-387-0073
Web:	www.ipc.on.ca
E-mail:	info@ipc.on.ca