

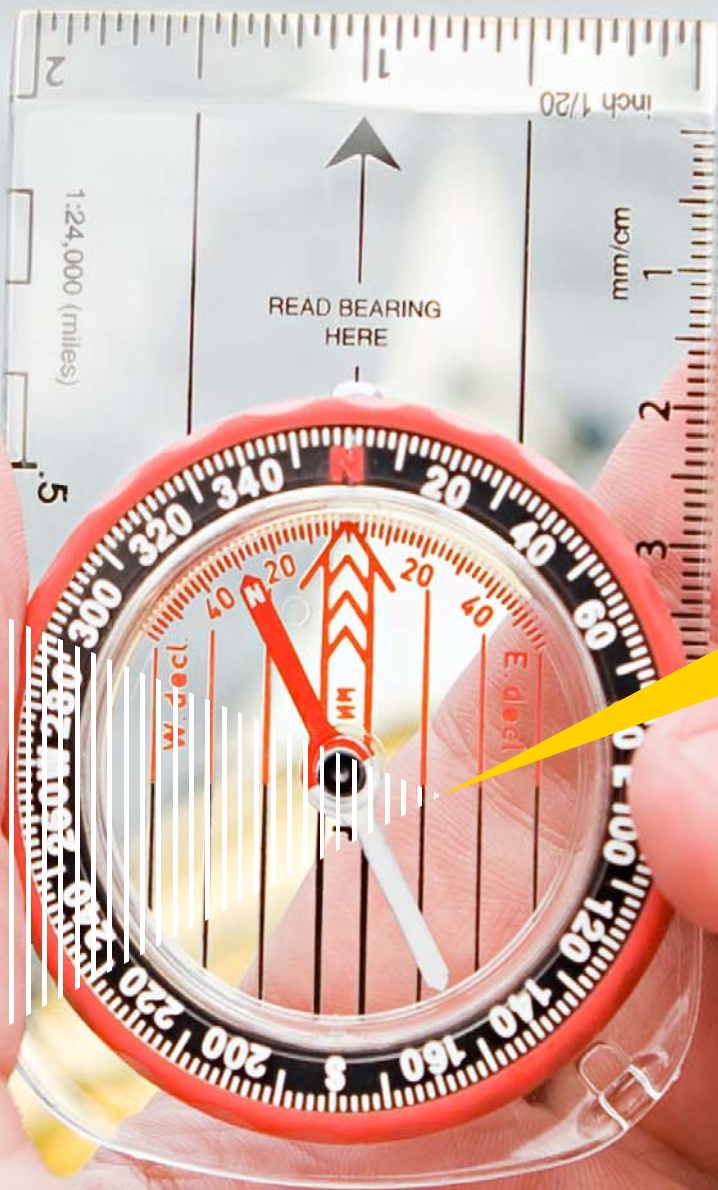
Insights on IT risk

Technical briefing

October 2011

A path to making privacy count

Five steps to integrating privacy protection into IT transformations



The technology revolution has enabled organizations across all sectors to electronically collect and store reams of personal information. But as business demands often outpace integrated IT solutions, managing the security and privacy of that information often occurs over a patchwork of existing and legacy systems.





IT's increasing role in privacy protection

In June 2011, the University of California at Los Angeles (UCLA) Health System agreed to a \$865,500 settlement with the US Department of Health and Human Services (HHS) for violating Health Insurance Portability and Accountability Act (HIPAA) privacy and security rules. UCLA Health System employees were accused of improperly accessing protected health information of high-profile celebrities and other patients. HHS further concluded that UCLA Health System itself had not sanctioned or otherwise taken action against the employees who had committed the privacy violations.¹

The UCLA Health System enforcement was the third major action HHS has taken in 2011, bringing total enforcement fines for the first half of the year to more than \$6 million. Since 2003, HHS and the Office of Civil Rights has investigated and resolved more than 14,105 privacy violations.

The US health system is not alone, however. Last year in the UK, the National Health Service Blood and Transplant (NHSBT), which manages the Organ Donation Registry (ODR), discovered mismatches between the donation preferences indicated on driver's license application forms and the information that was subsequently recorded in the ODR. The more than 400,000 irregularities identified resulted from an ODR software glitch dating back to 1999.² And in Australia, a medical laboratory inadvertently published online personal data and customer invoices of patients who sought medical tests.³

The technology revolution has enabled organizations across all sectors to electronically collect and store reams of personal information. But as business demands often outpace integrated IT solutions, managing the security and privacy of that information often occurs over a patchwork of existing and legacy systems.

Common characteristics of IT environments can include:

- ▶ Regulatory pressures and high-risk operations
- ▶ No single view of user activities
- ▶ Duplication, inefficiency and non-compliance
- ▶ A high cost of controls operating model
- ▶ Limited means to assess and report privacy or security posture
- ▶ Complex compliance requirements
- ▶ Reactive risk mitigation strategy and perpetual remediation

To address these challenges, as well as other increasing demands on enterprise systems, many organizations are undertaking large-scale IT transformations. IT transformation projects often center on information security:

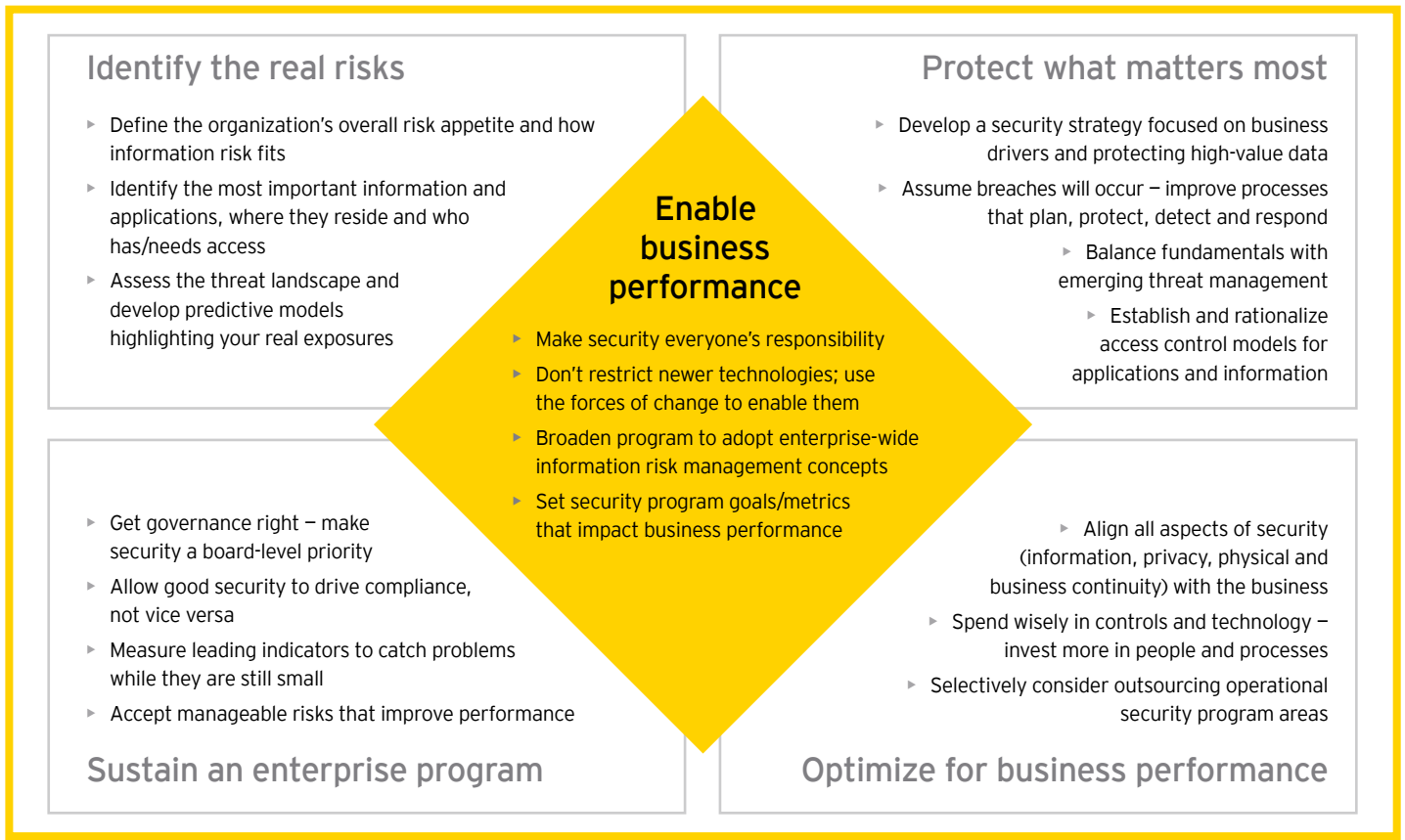
- ▶ Identify the real risks
- ▶ Protect the information that matters most
- ▶ Optimize for business performance
- ▶ Sustain an enterprise program

Privacy cannot be a secondary consideration. It needs to be included as a fundamental part of any IT transformation. By effectively managing the risk that privacy issues can pose, organizations can generate additional value and improve performance by safeguarding their reputations and their brands.

¹ Hunton and Williams LLP, "HHS Announces \$865,500 Settlement with UCLA Health System for HIPAA Violations," *Privacy and Information Security Law Blog*, 8 July 2011, <http://www.huntonprivacyblog.com/2011/07/articles/hipaa-1/hhs-announces-865500-settlement-with-ucla-health-system-for-hipaa-violations>.

² Sade Laja "NHSBT rapped for incorrect data on 444,000 donors," *theguardian.co.uk*, 21 January 2011, © 2011 Guardian News and Media Limited or its affiliated companies. All rights reserved, <http://www.guardian.co.uk/healthcare-network/2011/aug/30/organ-donor-register-nhsbt-dvla-errors>.

³ Sara Martin, "Investigation into South Australia's Medvet lab after serious privacy breach," *News.com.au*, 18 July 2011, <http://www.news.com.au/national/south-australias-medvet-blood-lab-publishes-details-of-paternity-and-drug-test-applicants/story-e6frfkx9-1226096476780>.



A privacy model designed for IT transformations

In 2009, Ann Cavoukian, the Information and Privacy Commissioner of Ontario in Canada, introduced *Privacy by Design (PbD)*, a model to embed privacy into new system implementations.

PbD is based upon **seven foundational principles** for protecting personal information:

1. Being proactive and preventative
2. Making privacy the default setting in IT systems
3. Embedding privacy into IT system design and architecture
4. Taking a positive-sum rather than a zero-sum approach
5. Embedding privacy from end to end within an IT security system
6. Providing visibility and transparency
7. Respecting user privacy⁴

Since its introduction, several organizations, including the U.S. Federal Trade Commission and the European Commission, have endorsed the *Privacy by Design* principles. And in 2010, at a meeting of Data Protection and Privacy Commissioners in Jerusalem, participants unanimously adopted the *PbD Resolution*, which pushes regulators globally to adopt *PbD* principles.

However, *PbD*'s focus is on embedding privacy protection from the beginning. For large organizations with existing and legacy systems that are already operational and pervasive throughout the enterprise, embedding privacy from the beginning is not feasible. As a result, in May 2011, Ms. Cavoukian and Marilyn Prosch, an Associate Professor with the W.P. Carey School of Business, introduced *Privacy by Redesign (PbRD)*.

In *PbRD*, Ms. Cavoukian and Ms. Prosch extend the original *PbD* principles to include existing and legacy systems, challenging organizations to:

- ▶ **Rethink** existing mitigation strategies, systems and processes with a view to finding new privacy-focused approaches.
- ▶ **Redesign** system functionality to achieve better standards of privacy protection, without losing sight of business objectives.
- ▶ **Revive** systems through an IT transformation that incorporates privacy protection as a fundamental tenet.⁵

Rethinking, redesigning and reviving legacy systems to improve privacy protection will help organizations not only meet compliance objectives, but also achieve cost savings and improve business performance.

⁴ Ann Cavoukian, Ph.D., *Privacy by Design*, August 2009/January 2011, <http://www.ipc.on.ca/images/Resources/7foundationalprinciples.pdf>.

⁵ Ann Cavoukian, Ph.D., *Privacy by ReDesign: Building a Better Legacy*, May 2011.

Measuring your IT function's privacy protection maturity

As technology matures and evolves, expectations from the business are growing. Organizations expect IT environments to do more than merely support business operations; they expect them to provide end-to-end support for the automated enforcement of privacy controls.

IT functions face a number of challenges that impact an organization's ability to comply with its privacy obligations and to protect personal information. The following maturity model can help your organization determine the current state of your IT environment on a scale from "ad hoc" to "optimized."

Privacy maturity model

Common challenges	Maturity/stages of improvement				
	Ad hoc	Repeatable	Defined	Managed	Optimized
Network layer					
Legacy data interfaces create traffic containing unnecessary personal information.	Existing interfaces are undocumented and uncontrolled.	Policies and procedures exist for data transport but do not apply controls based on data sensitivity or classification.	Policies and procedures exist to identify and document the transport of personal information and are followed.	Formalized procedures exist to support authorization, use, transport, monitoring and control of personal information.	Management reviews compliance requirements and updates policies and procedures for the authorization, use, transport and control of personal information.
There is unrestricted access to network folders and shared drives containing personal information.	Network shares are not managed and do not have technical controls to restrict access to personal information.	Departmental share drive access controls are in place; however, data storage is not actively monitored for content or compliance.	Documented procedures define network data storage controls but are commonly ineffective or not properly enforced to provide the designed protection.	Documented procedures define data storage controls. File shares containing personal information are inventoried and monitored for content and user access.	Understanding of personal information and how it is mapped to its owners, business drivers, data storage locations, and access roles is centrally managed and validated through testing.

Maturity/stages of improvement

Common challenges	Ad hoc	Repeatable	Defined	Managed	Optimized
Application layer					
<p>User access is provisioned without consideration for data protection, information sensitivity, classifications, or access roles.</p>	<p>Access is assigned at the network, active directory, or system level without granular control over specific screens, reports, or network shares containing personal information.</p>	<p>User access to personal information is granted by copying the access rights of existing user accounts. User-based assignments are not role-based, and may result in inappropriate assignment of access.</p>	<p>Defined access roles exist and are assigned by departmental functions. Review of access roles exists but is not managed through a defined process and does not account for data protection risks.</p>	<p>Role-based access assignments for personal information provide the minimum necessary access needed to perform job functions. There is effective authorization, control, and tracking over personal information.</p>	<p>Access is assigned based on authorized roles and provisioned via a combination of manual and automated workflow tools. Access is assigned through single sign-on processes, and access to personal information is managed across the enterprise.</p>
<p>Legacy systems contain unnecessary personal information.</p>	<p>Personal information is contained in most legacy systems for identification purposes. There is no inventory of systems containing personal information.</p>	<p>There is an inventory of systems; however, it does not identify data categories and sensitivity. Copies of personal information exist across many systems, resulting in data quality issues.</p>	<p>Policies require business areas to identify instances where systems contain unnecessary personal information. Risk mitigation activities are not taken in light of technical limitations in legacy systems.</p>	<p>Privacy and security risks related to legacy systems containing personal information are mitigated through technical and administrative controls.</p>	<p>Personal information stored and processed in legacy systems is controlled through prevent and detect controls. Regular security reviews are performed across systems containing personal information to identify threats and vulnerabilities.</p>
Infrastructure layer (e.g., operating systems, databases)					
<p>There is a lack of data ownership.</p>	<p>Limited understanding of personal data types and ownership, and limited functionality and resources to support monitoring activities.</p>	<p>Limited tracking of data ownership. Databases containing personal information are generally known but not documented. Orphaned data has not been addressed.</p>	<p>Policies require the designation of information owners and responsibilities to determine the appropriate collection, use, storage, and disclosure of personal information. Owners are assigned and tracked.</p>	<p>Application development lifecycle processes and tollgates document the use and owners' authorization of personal information in new databases.</p>	<p>Databases containing personal information are monitored for proper use, access, and controls (e.g., data quality, retention, integrity).</p>
<p>Increased threats expose database vulnerabilities or other security weaknesses.</p>	<p>Rogue databases, spreadsheets, and documents (i.e., not monitored by IT) are used to store personal information. Furthermore, there is limited deployment of data loss prevention (DLP) technologies and vulnerability management tools.</p>	<p>Some vulnerability tests and DLP scanning are conducted. Use of these tools is for initial inventory and cataloging of risks to personal information. However, results are not tracked through remediation.</p>	<p>DLP, vulnerability scanning and some penetration tests at the application level are completed on an ad hoc basis.</p>	<p>DLP and vulnerability scanning completed regularly, with follow-up of critical issues found. Penetration tests of applications completed on new systems and systems with external interface (e.g., web-based applications).</p>	<p>DLP implemented for data in motion and data at rest. Vulnerability scanning against perimeter regularly, with critical vulnerabilities cleared within agreed-upon criteria. Independent assessors periodically check the approach taken.</p>

Five steps to integrating privacy into IT transformations

There are five key steps IT can take to embed privacy protection into its IT transformation.



1. Create a system inventory

Before a case can be made for embedding privacy protection into an IT transformation initiative, IT needs to first catalog the organization's systems and databases. The inventory needs to identify the most important information and applications, where they reside and who has or needs access to it. The systems may number in the hundreds or thousands. For some organizations, knowing what systems exist in its IT environment may pose the first challenge.

Once IT completes its inventory of systems, it can begin to identify system names, owners and users. IT can then analyze meaningful data points to characterize the system population across regions, business functions and users.

A system inventory should answer some fundamental questions:

- ▶ What is the population of relevant systems in operation?
- ▶ Of the population, what percentage of those systems is directly impacted by privacy regulations?
- ▶ Who within the organization owns those systems?
- ▶ Is it clear what systems the organization as a whole depends on most?
- ▶ How many people use those systems?

Key insights will begin to emerge that could impact the organization of the project.

2. Develop a business case

Ideally, to make the case for embedding privacy into IT transformation, future savings will want to amount to more than current spend. Current-state spend should consider both operational and compliance costs. IT may also want to consider benchmarking against peers, as well as the use of case studies to demonstrate what is working well, from a privacy perspective, within the organization.

Identify operational costs

Operational costs are the costs related to performing privacy related activities and protecting personal information. Current-state operational costs should consider costs throughout the lifecycle of a particular business process. The cost calculation should factor in time and cost of resource related to a particular activity, incurred not only by the doer but also the reviewer or approver, if applicable.

Operational cost drivers include:

- ▶ The number of tasks that need to be performed
- ▶ How long the tasks take to perform
- ▶ The complexity of the tasks (e.g., need for junior-level versus senior people)

Once there is an estimate for a per-activity effort, it may need to be multiplied by the number of instances the activity occurs per week, per month or annually. These data points can be collected through various means, e.g., sample of interviews, surveys and existing statistics, such as help desk key performance indicators (KPIs). The numbers are then multiplied based on the inventory of in-scope applications.

Identify compliance costs

Compliance costs include costs associated with fulfilling policy, contractual, and regulatory privacy obligations. Calculating the current-state cost of compliance should include:

- ▶ The frequency of compliance activities
- ▶ Fines and penalties associated with relevant regulations and agreements
- ▶ The complexity of issues arising from compliance activities

Compliance costs can include fees for resources related to:

- ▶ External audit, internal audit (e.g., management testing), HIPAA, the Sarbanes-Oxley Act (SOX) or other regulatory-related testing
- ▶ Self-testing (e.g., business unit testing)
- ▶ Other compliance monitoring activities

Costs incurred should be estimated for external resources, internal compliance resources, and audit support (e.g., internal business time required to supply audit evidence).

Calculations of the time and effort required to perform a business process should factor in the relevant level of complexity. Once data points are collected, meaningful information again will emerge to strengthen the business case. An organization may find that:

- ▶ A majority of applications use manual versus automated processes
- ▶ Multiple independent functions, systems or processes exist to do the same thing
- ▶ A majority of applications with the highest impact or volume of activity use manual processes

Leverage benchmarking and case studies

In addition to a cost analysis, there may be opportunities to leverage industry benchmarking across similar or peer organizations. For example, benchmarks could enable IT to compare the head count or resources of a particular privacy management function, showing that the current-state organization is more dispersed and more inefficient than its peers.

Using case studies to demonstrate automated systems or processes within the organization that already support good privacy practices while reducing operational and compliance costs may also help to make the business case for privacy.

Project future-state costs

Future-state costs are a bit softer. Data points for future-state costs can typically come from industry benchmarks (e.g., Gartner), vendors (e.g., product price lists), or peers that have implemented similar solutions. It is important to realize that future-state costs will vary from year to year and should be projected across multiple years.

For example, capital expenditures may start off high in the first few years and then fade in later years. Conversely, operating expenditures may be low in the first few years, peak midway through the project as the project costs reach a break-even point and then level off again at a lower level.

Future-state costs should also include quantitative benefits such as mitigating potential privacy breaches that result in:

- ▶ Identity theft
- ▶ Litigation or regulatory action
- ▶ Direct financial loss or loss of market value
- ▶ Loss of consumer and business partner confidence
- ▶ Damage to the brand
- ▶ Becoming the example of what could go wrong

A successful business case for privacy should demonstrate the opportunity for a positive return on investment and increased cash flow, as well as improved business performance.

Components of cost

People

- ▶ Internal costs for employees needed to perform tasks
- ▶ External rate per hour for contingent workers needed to augment team
- ▶ Guidance on strategy and approach (e.g., attorneys, accountants, other professionals)

Processes

- ▶ Time to prepare for tasks
- ▶ Time to execute tasks
- ▶ Process management costs

Technology

- ▶ Costs for hardware and software
- ▶ Procurement
- ▶ Maintenance

Five steps to integrating privacy into IT transformations

3. Conduct an in-depth assessment

Once an organization has approved IT's business case, it's time to develop a detailed roadmap for implementation, which should include determining the scope of the project and conducting an in-depth assessment.

An assessment will typically involve three components:

- ▶ Gaining an understanding of the system and supporting processes (e.g., data/process mapping identifying inputs, process, outputs, users)
- ▶ Identifying weaknesses and how those weaknesses might impact other systems and processes
- ▶ Identifying duplication and process inefficiencies

IT functions may want to consider using a privacy impact assessment, which has become commonplace, to help perform consistent and structured evaluations of risk. The privacy impact assessment can also be critical in prioritizing implementation efforts and if budget constraints exist.

4. Consolidate systems

In many IT environments, systems and processes have often been developed to meet specific business needs, without determining whether similar solutions already exist or evaluating the impact on downstream processes. The result in most cases is duplication and inefficiencies.

Where duplication of systems and supporting processes exists, organizations should consider plans to sunset systems that are no longer needed and consolidate like functions where possible. There may be some considerations where this may not be possible. A health care organization, for example, may have intentionally created separate processes to separate HIPAA and non-HIPAA functions.

By consolidating processes and systems, organizations may find that they have not only achieved cost savings and improved efficiencies, but also freed up much-needed resources for other high-priority projects.

5. Standardize and automate

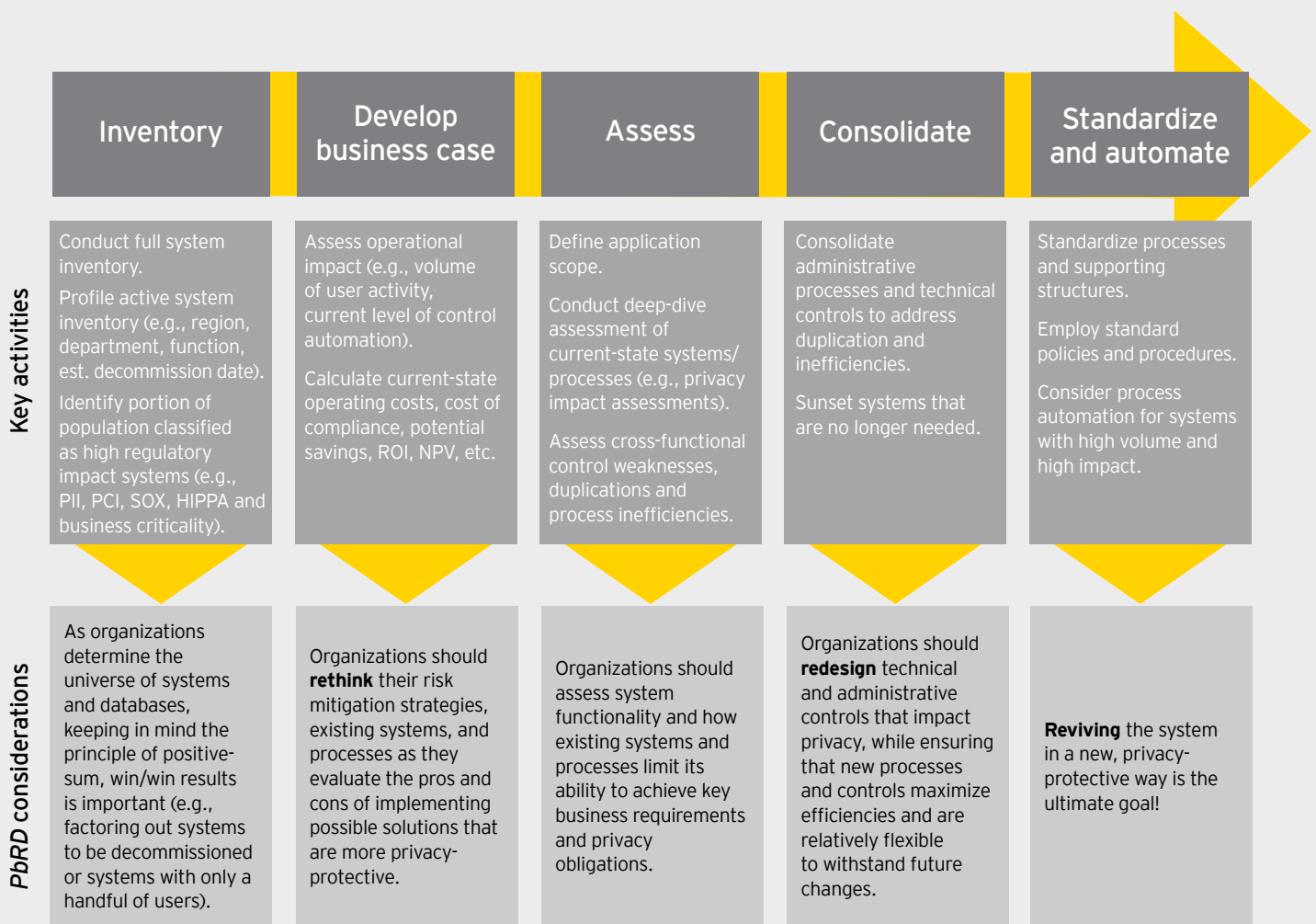
Following consolidation, IT functions will need to set privacy or security policies, standardize processes and ensure that supporting infrastructures are in place. IT will also have to decide whether process automation is practical to "achieve key business requirements in a doubly-enabling positive-sum, win/win relationship" that Ann Cavoukian outlines in *PbRD*.

Using the assessment, an organization can elect to:

- ▶ Standardize consolidated processes without automating
- ▶ Implement a fully automated solution
- ▶ Develop a hybrid solution that automates high-volume and high-impact systems and processes, while implementing manual consolidated processes for lower-impact systems and processes

Finding alignment between the five-step framework and *PbRD*

Our five-step model for embedding privacy protection into an IT transformation considers the fundamental three “Rs” of *PbRD* – rethink, redesign, revive.



case study

Too much information

A health care provider struggles to limit access to personal information across enterprise systems

The challenge

A large health care provider comprising a network of hospitals, medical groups, and health insurance plans faced ongoing compliance challenges. The provider was struggling to balance requirements for SOX, HIPAA, PCI, and various other state- and industry-specific regulations and standards. Management became frustrated with persistent audit failures and regulatory scrutiny. As a result, in conjunction with a number of other privacy and security projects, the organization decided to limit the use of and access to personal information across business functions and enterprise systems, which numbered in the hundreds.

The health care provider was aware that there were prevalent issues across systems and that some of the information viewable by users was critical to the execution of business operations. However, there were various instances where users had access to more personal information than they needed to perform their job functions.

The solution

The provider hoped to mitigate the privacy risk to the organization by using only the information that was absolutely necessary. This included truncating, obfuscating, or eliminating certain personally identifiable information data elements. To achieve that objective, it embarked on implementing the following remediation solutions:

- 1. Limiting the storage and processing of personal information to a few key systems and databases.** By doing this, the company sought to eliminate situations where systems and databases were used to store and process personal information when it was not needed.
- 2. Redesigning access provisioning so that access rights that allowed users to view personal information were tied to a centralized access management solution.** In this scenario, the privilege to view different sensitivities of personal information would be tied to a user's Active Directory account, restricting access to systems containing personal information based on his or her profile.
- 3. Developing bolt-on solutions for each database to further control views of personally identifiable information data elements.** This would limit personal information viewable on screens to the minimum necessary, while keeping more open views reserved to a few authorized functions.



The benefit

By implementing these three solutions and integrating *PbRD* into its IT transformation, the health care provider was able to achieve the following benefits:

- ▶ **Identification of 500 systems, 250 of which were relevant to the project objectives.** The 500 systems represented the systems used to store or process personal information, had regulatory requirements tied to the systems, had a user base greater than 50 users, were not set to be decommissioned in the near term, and were not subsystems that receive data from source systems further upstream in the process.
- ▶ **Development of a transformation project for centralized authentication and database controls.** The provider developed a survey to determine the tasks and level of effort associated with providing access to systems. The organization determined that on average in its current state, it spent \$2 million on access management annually across 250 systems, and an additional \$200,000 on compliance activities, totaling \$2.2 million.
- ▶ **Completion of a financial analysis.** The analysis demonstrated a potential overall cost savings of 25% after five years, and the company chose to go forward with the investment.
- ▶ **Systems assessment that included a privacy impact assessment and high-level process and data mapping.** The provider piloted 50 applications and conducted the remaining assessments over the next 18 months. The organization aggregated its findings and remediation plans to develop solutions with a view across all the systems in scope. The organization found both process and function duplications, and decided that it could sunset a third of the systems and consolidate related processes.
- ▶ **Implementation of central authentication.** The provider determined that only 100 of the 250 systems required the use of personal information, and that the remaining systems could use non-personal information. In addition to central authentication, the provider also considered the impact of access roles and the ability to view personal information.
- ▶ **Development of an automated solution for databases.** This enabled the organization to address excessive access to personal information at the database level rather than at the application level.

Privacy protection in action: tips for success

Privacy alone is rarely a pivotal motivator of IT transformations. However, when an organization decides to undertake an IT transformation, integrating privacy objectives is critical. To make sure this happens, organizations may wish to consider the following tips for success:

- 1. Assign a privacy champion.** Assign a champion to own the project with the authority to: influence key stakeholders; bring together the right resources; and gain buy-in from constituents who will be impacted by the change. The privacy champion will need to have a seat at the table from the outset to help identify privacy and personal data protection risks and to ensure that privacy becomes a primary driver rather than an afterthought.
- 2. Bridge the gaps between CSO and CPO objectives.** Transformation initiatives lead by the CSO can unearth significant opportunities for integrating privacy and data protection and following the principles of *PbRD*.
- 3. Understand the key buyers, influencers and drivers.** Transformation projects often require horizontal and vertical buy-in. The ability to demonstrate cross-functional cost savings can be a motivator for support.

- 4. Broaden your view.** Expand your perspective beyond individual issues and silos. It will be easier in the long run if you build solutions with the overall IT enterprise in mind.
- 5. Involve external expertise to provide fresh insights.** Security management functions often do not have the privacy knowledge, and privacy management functions do not have security expertise. Consultants and subject matter experts can offer invaluable insights into lessons learned and experiences in integrating *PbRD* in transformation projects, helping to mitigate the risk of common pitfalls.

Technology continues to advance at an unprecedented pace. As IT departments everywhere grapple with this evolution and how it impacts legacy systems and new integrations alike, privacy needs to be a vital consideration.

Organizations will find that effectively managing privacy-related risks can safeguard against costly breaches that can harm their reputation and shareholder value. It can also provide opportunities to improve business performance and achieve competitive advantage.



About Ernst & Young

At Ernst & Young, our services focus on our individual clients' specific business needs and issues because we recognize that each is unique to that business.

IT is a key to allowing modern organizations to compete. It offers the opportunity to become closer to customers and more focused and faster in responses, and can redefine both the effectiveness and efficiency of operations. But as opportunity grows, so does risk. Effective ITRM helps you to improve the competitive advantage of your IT operations by making these operations more cost efficient and managing down the risks related to running your systems. Our 6,000 IT risk professionals draw on extensive personal experience to give you fresh perspectives and open, objective advice – wherever you are in the world. We work with you to develop an integrated, holistic approach to your IT risk or to deal with a specific risk and information security issue. We understand that to achieve your potential you need tailored services as much as consistent methodologies. We work to give you the benefit of our broad sector experience, our deep subject-matter knowledge and the latest insights from our work worldwide. It's how Ernst & Young makes a difference.

For more information on how we can make a difference in your organization, contact your local Ernst & Young professional or a member of our team listed below.

Contacts

Global

Norman Lonergan (Advisory Services Leader, London)	+44 20 7980 0596	norman.lonergan@uk.ey.com
Paul van Kessel (IT Risk and Assurance Services Leader, Amsterdam)	+31 88 40 71271	paul.van.kessel@nl.ey.com

Advisory Services

Robert Patton (Americas Leader, Atlanta)	+1 404 817 5579	robert.patton@ey.com
Andrew Embury (Europe, Middle East, India and Africa Leader, London)	+44 20 7951 1802	aembury@uk.ey.com
Doug Simpson (Asia-Pacific Leader, Sydney)	+61 2 9248 4923	doug.simpson@au.ey.com
Naoki Matsumura (Japan Leader, Tokyo)	+81 3 3503 1100	matsumura-nk@shinnihon.or.jp

IT Risk and Assurance Services

Bernie Wedge (Americas Leader, Atlanta)	+1 404 817 5120	bernard.wedge@ey.com
Manuel Giralte Herrero (Europe, Middle East, India and Africa Leader, Madrid)	+34 91 572 7479	manuel.giraltherrero@es.ey.com
Troy Kelly (Asia-Pacific Leader, Hong Kong)	+852 2629 3238	troy.kelly@hk.ey.com
Giovanni Stagno (Japan Leader, Chiyoda-ku)	+81 3 3503 1159	stagno-gvnn@shinnihon.or.jp

About Ernst & Young

Ernst & Young is a global leader in assurance, tax, transaction and advisory services.

Worldwide, our 152,000 people are united by our shared values and an unwavering commitment to quality. We make a difference by helping our people, our clients and our wider communities achieve their potential.

Ernst & Young refers to the global organization of member firms of Ernst & Young Global Limited, each of which is a separate legal entity.

Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit www.ey.com.

About Ernst & Young's Advisory Services

The relationship between risk and performance improvement is an increasingly complex and central business challenge, with business performance directly connected to the recognition and effective management of risk.

Whether your focus is on business transformation or sustaining achievement, having the right advisors on your side can make all the difference.

Our 20,000 advisory professionals form one of the broadest global advisory networks of any professional organization, delivering seasoned multidisciplinary teams that work with our clients to deliver a powerful and superior client experience. We use proven, integrated methodologies to help you achieve your strategic priorities and make improvements that are sustainable for the longer term. We understand that to achieve your potential as an organization you require services that respond to your specific issues, so we bring our broad sector experience and deep subject matter knowledge to bear in a proactive and objective way. Above all, we are committed to measuring the gains and identifying where the strategy is delivering the value your business needs. It's how Ernst & Young makes a difference.

© 2011 EYGM Limited.

All Rights Reserved.

EYG no. AU0990



In line with Ernst & Young's commitment to minimize its impact on the environment, this document has been printed on paper with a high recycled content.

This publication contains information in summary form and is therefore intended for general guidance only. It is not intended to be a substitute for detailed research or the exercise of professional judgment. Neither EYGM Limited nor any other member of the global Ernst & Young organization can accept any responsibility for loss occasioned to any person acting or refraining from action as a result of any material in this publication. On any specific matter, reference should be made to the appropriate advisor.