



THE CIO AND THE CPO — A VISION FOR TEAMWORK AND SUCCESS

A Best Practices White Paper
December 2006

Abstract

Many organizations understand the value of protecting personally identifiable information (PII) in today's business environment and yet their privacy programs are often not well integrated with their IT organization which has the responsibility for the IT systems that must protect this data. In some cases the connection between the Chief Information Officer (CIO) and the Chief Privacy Officer (CPO) is so limited that the CIO doesn't really understand the difference between security and privacy. Similarly, the CPO may not have much knowledge about IT systems and IT processes. This paper provides background on the different perspectives of the IT organization and the privacy office and it offers practical tips for how these two organizations can work together to effectively guard against security and privacy risks. The best practices outlined in this paper are based on Sun's experience within its own organization as well as input that was gathered from other experts in the industry.

"I believe that this paper makes a significant contribution in helping to bridge a gap in understanding and awareness that often exists between CPOs and CIOs. It explains the roles and functions of the CPO and CIO quite clearly and demonstrates why these roles must be aligned in order to achieve responsible information management practices in a complex organization."

Larry Ponemon
Founder and Chairman
Ponemon Institute, LLC

Acknowledgements

Sun is grateful to the many customers and partners who have provided their input to shape the content of this document.

Table of Contents

Introduction	1
The Need for Aligning Privacy with Security and IT Functions	1
Business Benefits of Greater Alignment	2
Recognizing Common Mistakes	3
Differing Perspectives.	5
Best Practices for Aligning CIO's, CPO's, and the Work of Their Organizations	6
Define Roles and Responsibilities and Develop Cross-functional Understanding	8
Define and Document Policies, Processes, and Standards	10
Base IT and Privacy Decisions on a Sound Understanding of Business Risk and Requirements.	12
Implement Privacy Requirements by Integrating Them with Existing IT Disciplines, Methodologies, and Processes	14
Define Global Policies That Work Across All Geographies	16
Implement an Organizational Structure That Supports Cross-Functional Influence and a Business Perspective of Risk Management	18
Strike a Balance between Reactive and Proactive Measures	20
Integrate Privacy into Existing IT Disciplines for Incident Management and Change Management	20
Set Aside Time for Proactive Measures	21
Measure Progress and Assure Compliance with Policies	22
Compliance Assurance	23
Begin Right Away and Start with an Achievable Project.	24
Promote a Culture of Data Governance and Data Stewardship Throughout the Organization	25
Empowering the Community to Help.	25
Benefits of Delegating Data Governance	26
Conclusion	28
For More Information.	28

Chapter 1

Introduction

Today's business environment relies predominantly on electronic means for collecting and managing all kinds of data that is used to run the organization and enable fast-paced innovation. Increasingly, this means that many forms of personally identifiable information (PII) — information such as a phone number or frequent flyer number that can be linked to a unique person — are being captured and used within IT systems. Forward-thinking executives understand the importance of closely protecting this personal data as it flows through business systems where it can be subject to unauthorized access and misuse or negligence, and can result in non-compliance with laws and regulations. The potential risks to the organization can include not only the financial risk from lost business, recovery costs, or regulatory fines, but also the potential damage to the organization's reputation in the marketplace and the confidence of its stakeholders. In addition to posing risks if not properly protected, PII is also becoming recognized as an important business asset that can create value when it is used properly by people, processes, and business systems throughout the organization.

In response to the value of PII and the seriousness of the risks associated with not properly protecting it, many organizations have created a position for a Chief Privacy Officer (CPO) that carries the responsibility for protecting business and personal interests from a privacy perspective. The CPO role brings new clout to privacy issues, enabling a peer relationship with the Chief Information Officer (CIO) and the Chief Information Security Officer (CISO), a relatively new role that usually sits within IT. While some smaller companies may not have an executive level CIO, CISO or CPO position, they will most likely have identified a person who is in charge of these functions. There will be someone in charge of IT (CIO), someone who is in charge of protecting against security risks related to IT (CISO), and someone in charge of protecting personal information (CPO). In any case, it is important for these roles to work together so that privacy policies and related requirements for IT systems can be communicated. The working relationship between the roles of the CPO and the corresponding roles for CIO and CISO¹ is critically important. It sets the tone for how efficiently and effectively the different departments can work together to support business processes while reducing risk.

The Need for Aligning Privacy with Security and IT Functions

Protecting personal data within business processes and associated systems requires strict control over its access, distribution, and destruction as well as internal policies that govern the use of the data throughout its life cycle. However, one cannot control access to the data if the IT systems or the physical landscape in which the data resides are not secure. Thus privacy is intimately connected with security policies and procedures and with IT systems. Yet privacy policies and procedures are often not effectively integrated with security nor within the IT organization as a whole. Indeed, it is not uncommon for a disparity to exist between what privacy requires and what is actually implemented in IT systems. The difference can be enough to inadvertently result in privacy vulnerabilities or privacy violations in spite of the best intentions.

By working together, the CPO and the CIO can build greater alignment between their organizations so that they can leverage each other's expertise and knowledge, can establish efficient business processes, and do a better job

1. For the sake of simplicity in this paper, the CIO and CISO organizations shall be referred to collectively as "CIO".

of protecting the organization's interests. However, the relationship and teaming between the CPO and CIO is still quite new in most organizations. While the CIO and CPO may be attempting to cooperate, they often fail to take full advantage of their ability to leverage information and to jointly define IT requirements related to privacy. They may not dedicate sufficient attention or resources to cooperating or actively sharing information and may not implement capabilities that could help achieve mutually desirable objectives. The benefits of working together will not be fully exploited until there is significant alignment between the CIO and the CPO and their respective staffs.

Business Benefits of Greater Alignment

The major business benefits that can be achieved through greater alignment between the CPO and the CIO include:

- *Increased control over access to data and more efficient usage* — Privacy policies can support the need for more structure and oversight of data collection and data management, resulting in greater control over data access, increased value from appropriate use of data, and greater efficiency throughout the data life cycle.
- *Less duplication of effort* — Overlapping responsibilities in areas such as requirements definition, regulatory compliance, protection of intellectual property (IP), and generating awareness throughout the organization can be streamlined, allowing both the CIO and CPO offices to get the most from their limited resources and reduce operating costs.
- *Lower cost of developing and deploying IT systems* — When all IT system requirements including security and privacy requirements are identified up-front, the time and money to address these requirements can be reduced. Identifying these requirements early helps to avoid last minute changes or the need to retrofit a system after it is in production.
- *Reduced risk of schedule impact on IT solution delivery* — When privacy and security requirements are built into the solution from the design stage, the risk of last minute delays related to data protection are minimized, helping to keep IT system deliveries on schedule.
- *More efficient processes* — Greater sharing of information and processes combined with a mutual understanding of business requirements enables both parties to better help each other and results in a more efficient working relationship. For example, the mapping of data that is required for tracking and protecting personal information can also be used by other IT processes such as change control and problem resolution.
- *Better and more comprehensive decision-making about implementation* — Trade-offs between cost and methods of achieving the desired security and privacy results can be more fully explored and balanced when both parties are engaged in a cooperative process that captures multiple perspectives.
- *Greater support to achieve objectives* — By teaming together and presenting a unified front to business process owners regarding security and privacy risks, there is a greater possibility for business decisions to be based on a sound understanding of costs, risks and opportunities.
- *Reduced risk of privacy or security breaches* — By joining forces to promote awareness of security and privacy policies, there is a greater degree of understanding throughout the organization, thus reducing the risk of a breach and enabling a and more efficient recovery if a breach does occur.
- *Improved brand image and better marketing data* — When users trust an organization's privacy practices, it helps build a strong brand image and can also result in a better and more accurate marketing database because users are more willing to share truthful personal information.

Recognizing Common Mistakes

The media is filled with examples of privacy breaches that make front page news. While these highly publicized mistakes are often quite costly, they are far from the only type of problems that can result from poor data governance or privacy practices. A common mistake that can be quite costly, is a failure to recognize potential privacy violations in the early stages of the development lifecycle. IT systems under development or new solutions that involve vendor managed data processing systems may not get a full compliance review, or the compliance review may not happen until a stage where it is costly and time consuming to remediate the problem. This is an example of a process breakdown in the organization. Mistakes can also happen from poor training or lack of institutional awareness even when effective processes are in place.

Table 1-1. Examples of common mistakes in privacy programs

Example	Business Impact	Source of Problem
<p>A global Customer Relationship Management (CRM) system may be ready to go into production when someone discovers that the legal mechanism for addressing the cross-border flow of PII has not been put into place.</p>	<ul style="list-style-type: none"> • Delayed system delivery that postpones system benefits • Increased costs to retrofit privacy requirements into system • Negative impact on organizational productivity • Potential for an organizational political storm with lasting side effects that can make future projects less efficient and more costly 	<ul style="list-style-type: none"> • Process problem — Late participation by privacy experts (failure to adequately scope and remediate international requirements)
<p>A vendor selection committee for an outsourcing business partner fails to include security and privacy requirements as part of the selection criteria. A partner is chosen based solely on cost reduction and service availability objectives and security and privacy requirements are left to be dealt with after the deal is signed.</p>	<ul style="list-style-type: none"> • Unanticipated costs to retrofit vendor's IT systems or processes in order to address security and privacy requirements • Potential for lasting security and privacy vulnerabilities • Delayed delivery of outsourced services, thus delaying benefits • Inability to manage data assets entrusted to vendors 	<ul style="list-style-type: none"> • Process problem — Late participation by privacy experts (failure to define transferred custody of data assets issues)
<p>An employee loses a laptop after having downloaded a spreadsheet containing PII and then working on it remotely. The data was not encrypted and there is no password protecting access to the computer.</p>	<ul style="list-style-type: none"> • Recovery costs that include time spent identifying the contents of lost data and its impact, notifying customers, and managing damage to the company image • Potential fines and/or sanctions for regulatory violations • Increased legal expenditures • Potential lost revenue from upset customers • Damage to brand 	<ul style="list-style-type: none"> • Institutional awareness problem — Not following guidelines for laptop security (failure to prevent data loss) • Process problem — Inadequate solution for remote access to sensitive data (failure to allow systems for efficient work flows)

Example	Business Impact	Source of Problem
<p>A medical provider inadvertently includes customer names and email addresses in the “To:” line of a mass email that was intended to be sent to an anonymous alias. The email contains content that would identify its recipients with a particular type of health problem.</p>	<ul style="list-style-type: none"> • Recovery costs that include time spent identifying the contents of lost data and its impact, notifying customers, and managing damage to the company image • Potential fines and/or sanctions for regulatory violations • Potential lost revenue from upset customers • Increased legal expenditures • Damage to brand 	<ul style="list-style-type: none"> • Process problem — Inadequate controls for electronic distribution (failure to maintain PII control and customer satisfaction) • Institutional awareness problem — Not following e-communications protocols (failure to provide secure communication protocols)

Some other commonly observed scenarios in organizations with less than mature privacy programs include:

- The overlap and integration of the charters, missions and goals of the CPO and CIO are not sufficiently refined, are inconsistent, or may not even exist. This results in confusion between departments and either redundant or incomplete efforts.
- Policies are unclear or conflicting, making them difficult to implement and resulting in failed or incomplete controls.
- Poor enforcement of policies and lack of accountability enables slack performance resulting in vulnerabilities.
- Lack of alignment between privacy and security regarding internal audits, investigations, and other compliance functions requires redundant spending to complete the tasks and results in multiple separate reports instead of a unified report that provides all of the information required for executive decision making.
- Insufficient resources or emphasis are placed on process management, data stewardship, and governance, resulting in inconsistent or incomplete controls for PII and lack of adherence to policies.
- There is not enough communication and coordination between the CIO and CPO organizations to enable collaborative problem solving, resulting in increased risk of privacy and security vulnerabilities and missed opportunities for optimizing business processes.
- False assumptions get in the way of effective alignment. For example, a developer may think he or she already understands the privacy policy and how it applies to data involved in a business process. Thus he or she may not ask for help from the privacy office in assessing the potential risks. This can result in a system design with potential privacy risks — risks that may well have been anticipated by a privacy expert. Similarly, a privacy staff member may incorrectly assume that security capabilities are adequate where those risks would be better addressed by a security expert.

Ultimately, a lack of alignment and communication between the CPO and CIO can translate to increased risk for the organization, reduced control over data, missed opportunities for creating business value, and limited process efficiency with a resulting increase in cost. To help understand why close alignment has seemed challenging, it is helpful to consider the differing perspectives of the CPO and CIO.

Differing Perspectives

One explanation for the potential for miscommunication between the CPO and CIO offices is that they come from different perspectives and have different focuses or interests. They also tend to have similar but not identical vocabularies, which can afford greater opportunity for miscommunication. The same word may not mean the same thing or imply the same level of priority to both sides. Until both parties are able to understand each other and arrive at a common definition of terms, communication will likely remain a challenge.

Table 1-2. Differing perspectives between internal work groups

	Perspective of CPO	Perspective of CIO ^a	Overall Business Perspective
Focal point for risk management	<ul style="list-style-type: none"> • Risk is associated with the use, access and transfer of personally identifiable information (PII) • Process owners must be responsible for understanding risks associated with their data and taking steps to protect it 	<ul style="list-style-type: none"> • Risk is associated with the availability and security of the IT infrastructure so that information is protected and is usable 	<ul style="list-style-type: none"> • Executives must have access to data to execute business objectives and must be informed about potential business risks in order to make good business decisions
Compliance	<ul style="list-style-type: none"> • We are in compliance when we are doing exactly what we told users we would do with their PII and we are abiding by global regulations and industry standards • Compliance requires that PII is secure and protected from unauthorized use and access 	<ul style="list-style-type: none"> • We are in compliance when our IT systems are performing according to internal security policies, standards, and guidelines and meet specific regulatory compliance requirements as identified by business owners (e.g. export compliance) 	<ul style="list-style-type: none"> • We are in compliance when we are not in violation of the law in any country in which we operate
Data Governance	<ul style="list-style-type: none"> • Strict control over personally identifiable information to limit regulatory risk and protect privacy • Recognition of PII as valuable corporate asset 	<ul style="list-style-type: none"> • Intellectual property must be protected and confidentiality must be respected 	<ul style="list-style-type: none"> • Maximize relationships with customers and partners, economically manage employees, minimize regulatory risks, protect IP, and balance all of this against implementation costs
Systems Lifecycle	<ul style="list-style-type: none"> • Focus is on data • The lifecycle spans from the point at which personal data is collected until it is destroyed 	<ul style="list-style-type: none"> • Focus is on the system • The lifecycle spans from the time we start systems development until the system is pulled out of production 	<ul style="list-style-type: none"> • Business processes are constantly evolving and our IT systems should evolve with the business processes and meet business requirements
Encryption	<ul style="list-style-type: none"> • For situations where access cannot be fully controlled (e.g. laptop usage or data transfers over the Internet), encryption should be used to reduce business risk 	<ul style="list-style-type: none"> • The more data is encrypted, the less risk there is to the business, but enough data must be accessible to effectively administer and police the systems • Encryption can be very difficult to implement and manage on an enterprise wide basis 	<ul style="list-style-type: none"> • Encrypt enough data to limit risk when absolutely necessary, but balance cost versus risk • Provide user friendly systems with ample access to relevant data

	Perspective of CPO	Perspective of CIO ^a	Overall Business Perspective
Identity Management	<ul style="list-style-type: none"> Preventing unauthorized access is a great starting point, but privacy also requires control over how data is distributed and when/how it is destroyed Auditing tools can simplify compliance reporting by providing proof of accountability and data integrity 	<ul style="list-style-type: none"> Identity management is a tool for preventing unauthorized access to data and applications while streamlining business processes Auditing tools can assist in system accountability 	<ul style="list-style-type: none"> Identity management is the most cost-effective way to begin to meet regulatory requirements Auditing tools can reduce the cost of audits and compliance reporting Single sign-on or fewer sign-ons along with password management may reduce administrative costs
New Technologies	<ul style="list-style-type: none"> Advanced technologies can have unintended consequences and risks (when planning and execution are misplaced or absent) 	<ul style="list-style-type: none"> New technologies can offer more efficient processes (when planning is executed well) 	<ul style="list-style-type: none"> New technologies should be employed when they offer significant return on investment (ROI) and reasonable business risk
System Design	<ul style="list-style-type: none"> The system should be designed with a baseline of globally consistent processes, but must also offer flexibility for customization down to the data level so that different geographical areas can manage required local exceptions to the global policy 	<ul style="list-style-type: none"> A single common global architecture and design offers ease of administration and is less vulnerable to security threats 	<ul style="list-style-type: none"> The system design should be cost-effective to build and maintain while providing all of the necessary functionality ("necessary" and "functional" requirements will change over time)

a. In some cases, the CISO perspective may differ from that of the CIO, but they are lumped together here because the viewpoints are often similar.

While their perspectives may differ, the CPO and CIO are both focused on delivering effective business processes and minimizing business risk. It is obvious that business risk will never be completely eliminated, so the goal is to identify the risks and then to work with business process owners to decide upon acceptable levels of business risk while balancing other costs and benefits.

In addition to their business interests being in alignment, the CPO and CIO also share the same IT systems as the means to accomplish their objectives. As a result, there is much to be gained from cooperation and aligning their resources to achieve greater efficiency.

Best Practices for Aligning CIO's, CPO's, and the Work of Their Organizations

Having had the opportunity to learn through internal implementations and to observe the effectiveness of the privacy practices within its client base, Sun Microsystems has identified a set of best practices for improving how the CIO and CPO (and their organizations) can work together.

One of the key themes emphasized by the best practices identified in this paper is that strategic alignment concerns much more than policy. Rather than simply focusing on protecting PII and reducing risk, alignment can include cooperation and collaboration on how to best utilize PII as a key asset of the organization and how to efficiently and effectively accomplish shared objectives.

The end result of strategic alignment will be to reduce business risk, build greater value for stakeholders, and to improve operational efficiency throughout the organization. The following best practices can help drive this kind of strategic alignment.

- Define roles and responsibilities and develop cross-functional understanding
- Define and document policies, processes, and standards
- Base IT and privacy decisions on a sound understanding of business risk and requirements
- Implement privacy requirements by integrating them with existing IT disciplines, methodologies, and processes
- Define global policies that work across all geographies
- Implement an organizational structure that supports cross-functional influence and a business perspective of risk management
- Strike a balance between reactive and proactive measures
- Measure the progress and assure compliance with policies
- Begin right away and start with an achievable project
- Promote a culture of data governance and data stewardship throughout the organization

The subsequent chapters of this paper provide a description of each of these best practices and the potential benefits that they can help organizations to achieve.

Chapter 2

Define Roles and Responsibilities and Develop Cross-functional Understanding

To effectively cooperate, the IT organization and the privacy office must have a good understanding of each other's roles and functions and must develop confidence in how the other can help their cause. The first step in this process is basic education. This could start with simply meeting to discuss each other's mission and charter and to share information about the roles and responsibilities of the people within each department.

There is no need to become expert in what the other does, but IT staff must learn enough about privacy policies and goals to be able to know when there is a potential privacy issue and must know who to call to check it out. Similarly, the privacy office must build their knowledge about the IT infrastructure and processes. They should have a basic understanding of the primary business systems and how they utilize data as well as a working knowledge of the IT processes. Unfamiliar jargon and areas of expertise should never be allowed to impede progress.

After engaging in a few initial meetings and sharing some documentation, the roles and responsibilities as well as the goals for both sides should become reasonably clear. This will create a solid foundation for continued growth and understanding in the relationship. Once the roles and charter are well defined, each party can focus on their own charter and successfully navigate the areas where there is a mutual dependency and a need to engage the other party. As new employees come on board, it may also be helpful to provide formal training that helps them understand how to work with their counterparts in the privacy office (for IT staff) or the IT organization (for privacy staff).

The following steps may be helpful to deepen the relationship and to maintain alignment after an initial foundation has been built:

- Hold regularly scheduled meetings to address communication issues and ask questions whenever things are not clear
- Define terms in a common vocabulary so that everybody speaks the same language
- Clearly delineate roles and charters between and within the teams to create clarity, minimize wasted efforts and prevent frustration
- Engage each other early and often in the IT project lifecycle and make sure that there is at least one check point in the IT process where privacy and security requirements are reviewed and potential privacy issues vetted with the privacy office
- Develop training materials for new employees that incorporate cross-functional topics including roles and responsibilities
- Include cross-functional representation on councils or steering committees (e.g. a single enterprise data protection council/steering committee could incorporate both security and privacy security concerns — or if separate councils are necessary, then the security council should have representation from the privacy office and the privacy council should have representation from the CIO organization)

- Include representation from the privacy office in IT response teams that are responsible for reactive processes such as incident response, investigations and business continuity planning so that privacy issues that arise in emergency situations can be managed quickly and investigations can properly address PII control
- Encourage staff transfers from CIO office to CPO office or vice versa to build cross-functional knowledge within each team

Table 2-1. Benefits of improved cross-functional understanding

Benefits to Team Members	Benefits to the Organization
<ul style="list-style-type: none"> • Be a better consumer of the other's services • Know who to call for help and when to call them • Be able to ask good questions and anticipate potential pitfalls • Be positioned to help promote the other's policies • Organizational clarity leaves room for individual excellence 	<ul style="list-style-type: none"> • Reduced risk of disconnect between policy and the actual implementation • Reduction in security and privacy vulnerabilities and incidents • Greater awareness of security and privacy throughout the organization because both parties help promote each other

Chapter 3

Define and Document Policies, Processes, and Standards

The term privacy program is used in this document to denote the entire course of action of the privacy office. It includes both the program objectives and the means of implementing these objectives such as the business processes and standards that define the policy. Processes are the actual business workflows that are used to implement the privacy policy. Standards are defined as the objective benchmarks or guidelines which must be upheld to be compliant with the policy.

Defining and documenting policies, processes, and standards are an efficient means to communicate priorities and requirements and can also help create a common understanding throughout the organization. Despite the obvious value of such documentation, organizations often do not give this activity enough priority due to scarce resources and conflicting priorities. The creation of this documentation is sometimes postponed or ignored. If a baseline set of policies, standards, and procedures for IT projects is not already available, these documents must be created.

Formal policies and guidelines that document the institution's privacy requirements for system development are also important because they offer an efficient and consistent method to publicize privacy requirements to IT project teams. Where possible, the documentation should identify specific IT systems, processes and tools that will play a role in implementing privacy policies. Requirements for mobile data stored on laptops, USB drives, and other removable media should also be carefully documented since there are increased privacy risks with mobile data. Mobile data sources are often forgotten because they are outside of the typical "systems" focus.

It can also be helpful to define policies, processes, and standards for monitoring risk and assessing compliance within IT projects throughout their lifecycle. For example, it may be appropriate to require a privacy impact assessment and/or a security risk assessment starting at the design stage of every new IT system and then again at key junctures of development and upgrades until the system is retired. Similarly, legacy systems and third-party outsourced systems that house PII, or interface with internal IT systems must also be scrutinized at predetermined intervals to help ensure adherence to a company's privacy protection and security policies.

Just because a system has been reviewed during the design phase, does not ensure that changes throughout the system lifecycle will keep the system safe from security or privacy vulnerabilities. Because systems change over time in response to ever changing business requirements, periodic reviews are an important safeguard. The concept of integrating privacy concerns with existing IT change management disciplines is further explored in Chapter 8 titled, "Strike a Balance between Reactive and Proactive Measures."

Documenting the policies, processes, and standards, and making them available on internal Web sites allows the entire organization to have easy access to the information. It can also enable the staff of security and privacy experts to focus less on the administrative tasks of disseminating privacy information and more on responding to questions and assisting in the interpretation and application of the policies, processes, and standards.

Table 3-1. Benefits of documentation

Benefits to Team Members	Benefits to the Organization
<ul style="list-style-type: none"> • IT project teams can have a base from which to start and can have a better chance to correctly incorporate privacy goals in their designs • Privacy office personnel can learn about existing IT processes by reading the documented policies, processes, and standards, allowing them to understand more about how privacy can be integrated into systems • Skill sets of security and privacy experts can be strengthened and leveraged through available documentation 	<ul style="list-style-type: none"> • Documentation can act as a training vehicle to promote greater awareness of security and privacy throughout the organization • Documenting the policies, processes, and standards forces a degree of rigor that can help clarify the requirements and bring out greater efficiency in business processes • Working together on documentation can improve cooperation between privacy and IT and enable creative solutions to business problems • Reduced likelihood of security or privacy breaches due to improved controls for monitoring compliance to policies • Compliance audits and assessment activities, both external and internal, can be simplified when there is documentation to use as the baseline for the control activities

Chapter 4

Base IT and Privacy Decisions on a Sound Understanding of Business Risk and Requirements

Managing business risk is an important and common goal of the CPO and CIO organizations. It includes balancing business priorities, information needs, and operational efficiencies against known and potential security and privacy vulnerabilities. For example, operational efficiency requires easy and timely access to information throughout the organization. However, access to this information must be controlled in ways that protect the security and confidentiality of IP, and the security and privacy of PII.

The CPO and CIO teams are not always in the best position to decide what risk the business is willing to take where there are no specific regulatory boundaries. The facts needed to make a balanced analysis and the ownership of the decision often belong with the business data owners. The role of privacy and IT experts should be to act as advisors to the business decision makers. They must be able to gather and accurately portray the facts and assess the risks so that good business decisions can be made. They must also balance business unit or specialty needs with the interest of the organization as a whole. At times, the business stakeholders may have to adjust their expectations and data requirements.

Business needs and business risks may also be seen differently by IT and privacy experts and by the business data owners. For example, a global organization may want to monitor certain activities of its worldwide employees. The human resources organization, acting as the business data owner, may be primarily concerned with obtaining summary reports that can help identify worldwide trends about how employees use their benefits. The IT organization may decide that it is most efficient to monitor employee usage of benefits from a centralized location in the United States and to store the resulting data in a single data repository that can be easily managed. The privacy office, on the other hand, may find the centralized approach problematic, and must highlight the business risk of moving PII across international borders without adequate protections and must plan accordingly.

One solution in this example might involve blinding the data (removing personal content) when collecting it or before centralizing it for analysis and reporting. This example shows that it is important that both IT and privacy perspectives be considered within the context of the business situation and that business decisions be based on well informed counsel. By working collaboratively with business decision makers, IT and privacy experts can help define solutions that provide maximum business benefit while helping to minimize the risk of security and privacy vulnerabilities.

In their roles as advisors and business advocates, the CPO and CIO must be ready to execute on the following duties:

- *Gather the facts* — IT and privacy experts team together to collect the appropriate details about a given situation in preparation for assessing the potential risk to the organization. Input should be as quantitative as possible, without introducing significant additional work to produce the information. The CIO office can share its experience of working with metrics and probabilities to help the privacy office analyze legal risks that are often difficult to quantify.

- *Assess the business risk and business value* — Based on the input from business data owners as well as from IT and privacy experts, a collaborative process should be used to develop a firm understanding of business risks and identify possible means for achieving objectives and creating business value. The understanding of business risk should also be informed by ongoing monitoring activities that rigorously monitor the effectiveness of IT security and privacy policies as they are currently implemented.
- *Present the facts and risks* — Business decision makers should be presented with the appropriate facts along with the risk assessment and should be given the opportunity to probe for more details as needed to make a sound business decision. A good business decision can begin with the perennial question, “Who goes to jail if we do or don't do this?” It should conclude with questions such as, “Will this solution maximize value, minimize risk, and can we sustain this solution?”
- *Prohibit high-risk decisions* — A business decision should not be final until there is agreement among the business decision makers and the CPO and CIO teams. If a proposed course of action threatens to put the organization in a position of high-risk, the CPO or CIO should be empowered to block that course of action. When this happens, they must also have a close enough alliance with the business to be able to suggest proactive solutions to meet the business challenge. This can move the discussion from a “no” from a compliance or risk perspective, to a discussion of “how” to achieve information governance. Finally, organizations must ensure that there is always a designated business owner who will understand and remain accountable for the data.

The CPO and CIO can and should partner when assessing risk or presenting information to business decision makers. It is similarly helpful to join together to present one cohesive and actionable case to business decision makers. If the CPO and CIO are presenting an argument for or against a specific business decision, there will be a stronger case if it is presented from both the IT and privacy perspective and there is agreement about the risk assessment. By cooperating on the risk assessment process, they can join their respective IT and privacy perspectives and can propose or design new approaches to minimize business risk and manage value.

Table 4-1. Benefits of focusing on business risk

Benefits to Team Members	Benefits to the Organization
<ul style="list-style-type: none"> • Remain focused on highlighting business risks and monitoring policy implementation with ownership and input from business data owners • Obtain greater support for ideas by getting backing from other departments across the organization — CIO and CPO teams unify for common goals • Ideas are more persuasive to stakeholders when they are presented from multiple points of view and there is consensus from multiple departments on the best course of action 	<ul style="list-style-type: none"> • Business decisions can be based on more complete understanding of the balance between benefits and risks • Risk analysis becomes a process that is grounded in organization and customer centric goals and IT remains aligned with the organization's goals • Data utilization is maximized and becomes a strategic asset for the organization

Chapter 5

Implement Privacy Requirements by Integrating Them with Existing IT Disciplines, Methodologies, and Processes

It is important that privacy policies, processes, and standards take into consideration what is possible from an IT perspective. They must not be seen as red tape that creates an impediment to the delivery of IT systems. Project teams may already feel burdened by existing security and architecture reviews. Therefore, adding yet another review process to address privacy requirements may create a backlash from IT staff if that review is poorly integrated into similar processes.

Integrating privacy requirements into existing IT security or architecture review process can be a more desirable approach than creating separate review tracks. A privacy impact assessment fits well with a security review, so if there is an existing security review process, a privacy assessment can usually be incorporated into that process without much difficulty. IT project teams will likely view this addition as a minor enhancement to an existing process as opposed to an extra hurdle in the development cycle. In addition, the fact that privacy requirements force scrutiny over the data that is maintained in an IT system can serve to enhance IT project disciplines. This can help improve overall quality and reduce the incidence of costly late-stage changes.

Other areas where it makes sense to integrate privacy functions with IT functions include interfacing with the business/user community, providing training, and building organizational awareness. IT organizations typically have existing processes and dedicated staff for working with business owners and users to make sure that IT systems meet their needs. If the privacy office is involved in these processes, they can work with IT staff so that privacy requirements can be gathered within these existing processes.

Training and awareness generation can also be done more efficiently with an integrated approach. Users can be trained on security and privacy policies in a single integrated offering rather than through separate training programs. This not only saves times for users, but can also help reduce the cost of developing the training since costs would be shared between the IT organization and the privacy office. Likewise, an awareness campaign that combines security and privacy objectives can be more cost-effective and may have more impact than overlapping but independent efforts sponsored by the privacy office and by the CIO.

Finally, sharing processes for development, review and awareness can help educate stakeholders regarding the synergies and sometimes subtle differences between privacy and security practices and priorities.

Table 5-1. Benefits of utilizing existing disciplines and processes

Benefits to Team Members	Benefits to the Organization
<ul style="list-style-type: none">• Project managers will not see privacy policy as just another roadblock and thus will be more likely to integrate privacy requirements into the development process• It is less work to add to an existing process than to create a new process• Procedures for enforcing project reviews are already in place, so there is minimal additional effort required to enforce compliance for privacy requirements	<ul style="list-style-type: none">• Smooth implementation of privacy policies with minimal resistance from IT project teams• Integration of privacy with other IT policies provides opportunity for privacy policies to become more ingrained in the corporate culture• Improved efficiency for IT development

Chapter 6

Define Global Policies That Work Across All Geographies

One of the greatest challenges in adopting and implementing a privacy program is that laws and regulations vary from country to country. And yet it can be difficult or nearly impossible to implement different policies across different geographies, especially if the necessary flexibility has not been designed into the IT systems. Therefore, a global policy should be defined that can be consistently implemented across all countries in which the organization operates, and which meets or exceeds most local regulations in those countries.

Because it is not realistic for the global policy to encompass all local regulations from all countries of operation, a balance must be struck wherein most local laws and regulations are included in the global policy and the more uncommon local regulations are handled as exceptions. In cases where local rules require a variance from the global policy, operations in that country must go beyond the reaches of the global policy to implement processes and standards that maintain compliance with local laws or regulations while remaining consistent with the overall risk-based architecture of the global system. IT systems must have enough flexibility to accommodate these local variances in privacy regulations without requiring extensive effort to implement the exceptions.

The global policy must also be aligned with the organization's security policies and must take into consideration the capabilities of its IT infrastructure as well as the limited resources that the organization can allocate to its implementation. In other words the privacy team cannot create a standard which is infeasible or impossible to adhere, enforce and monitor. Impractical rules create the potential for international problems.

The CPO will have to rely on the CIO to help define a global privacy policy that is realistic to implement while still meeting most regulations in countries of operation. The global privacy is therefore best defined through a collaborative process that strives to optimize the requirements of three parties: the CPO, the CIO, and the business owner/users. This process should result in a single global policy for privacy and security that can be implemented across the existing IT infrastructure.

The decision about what to incorporate in a global policy and its corresponding global processes and standards must also be informed by international directives and regulations that define privacy requirements for data that crosses international borders. For example, the European Commission's Directive on Data Protection (http://ec.europa.eu/justice_home/fsj/privacy/index_en.htm) prohibits the transfer of personal data to non-European Union nations that do not meet the European "adequacy" standard for privacy protection. Multinational corporations that do business in the European Union (EU) can utilize any of the following initiatives as a means to demonstrate adequacy of their privacy policies in supporting the European Commission's Directive:

- The U.S. Safe Harbor framework which provides a streamlined means for U.S. organizations to self-certify that their organization provides adequate privacy protection as defined by the Directive
- International Data Transfer Agreements
- The European Union's Binding Corporate Rules (BCR) directive which was developed to guide multinational organizations in creating an internal code of conduct for transfers of PII to third countries
- Data subject consent²

Other jurisdictions such as Argentina, Australia, Canada, Hong Kong or Japan may also impose data regulation requirements that should be included in a multinational framework for use and protection. Much like an architectural plan that governs physical machines and code, policy can and should be converted into a workable blueprint that builds a global framework with the necessary flexibility. This framework should be designed to meet the geographic and business operating challenges.

Table 6-1. Benefits of a joint effort to define a single global policy

Benefits to Team Members	Benefits to the Organization
<ul style="list-style-type: none"> • The task of the privacy office can be streamlined by reducing the complexity of many local regulations to a single global policy that will be implemented • Collaborative process can result in new and better ideas for implementation • Easier implementation due to input and agreement from all three parties 	<ul style="list-style-type: none"> • Lower cost global implementation • Reduced risk of non-compliance to regulations by having a single policy framework that is easier to enforce • Greater efficiency due to process optimization • Reduced number of policies are easier to communicate and monitor

2. Data subject consent is relevant where workers data is being transferred outside of the EU. Special caution should be noted before an organization chooses to use consent as its means to export data. (See www.dataprotection.ie/docs/Article_29_Working_Party/181.htm.)

Chapter 7

Implement an Organizational Structure That Supports Cross-Functional Influence and a Business Perspective of Risk Management

The security, privacy and IT functions within an organization must provide ample opportunity for cooperation and for cross-functional flow of information. Organizational silos that isolate privacy or security functions from one another or from other groups within the organization can limit cooperation between the groups and can reduce the ability to influence other parts of the organization effectively. Similarly, a well designed organizational structure can lead to increased communication which supports improved practices and policies in addition to well defined requirements.

Traditionally the CISO has reported into the IT organization where he or she can have direct authority over IT systems to implement and address information security. Even where the CISO does not work within the IT organization, it is important for the CISO organization to maintain appropriate linkage to the IT organization so as not to jeopardize the CISO's authority over security implementations in IT systems. If the CISO remains in the IT organization, it is equally important that the CISO establish relationships with various business unit leaders to effectively manage security risks.

The role of the CPO and the privacy office has only been spelled out as a discrete business function within the last decade. Consequently, there is no traditional path or reporting structure for the CPO in the majority of organizations. Chief privacy officers and their teams have come from the legal, public policy, HR, marketing, audit and IT functions.

The reporting structure for the privacy function can take different forms depending on the business environment. For instance, in a consumer products company, it may make sense for the privacy office to reside in the marketing organization with a primary focus on managing consumer preferences. Conversely, in a highly regulated business, the CPO may spend more time dealing with regulators, making it more compelling for the privacy office to reside within the legal organization.

One key factor in deciding where to locate the privacy office is that its parent organization will likely impact the initial priorities of the CPO and the privacy team. The CPO's priorities will tend to be aligned with those of their parent organization. A second factor to consider is that placement of the CPO role in certain business units may make it more or less difficult to cooperate with other parts of the organization, including the CIO's teams. Wherever the privacy office resides, it must have some degree of parity with the CIO and must leverage other disciplines and cooperate with the CIO's teams to ensure a balanced approach to business risk management.

The combined organizational structure should be horizontal in nature so that security and privacy teams can work closely with each other and with business stakeholders throughout the organization. To function effectively, horizontal organizations require the use of shared goals that span multiple departments. These shared goals do not equate to redundant tasks by separate teams. Rather they foster cooperation between the members of a cross-functional team because everyone benefits from achieving the same outcomes even though their traditional or formal reporting structures will inevitably have overlapping or conflicting interests. For example, a system review should include both a privacy impact assessment and a security review. Although each review may be performed by

a CIO or CPO staff person, the resulting assessment should be one cohesive assessment with a single plan of action that is jointly delivered to the business unit that is the data steward.

The shared goals should provide incentives that encourage these teams to work together in assessing business risk, presenting these risks to business owners, and making business decisions that help business data owners accomplish their objectives.

If the organization is set up to support both cross-functional cooperation and a business perspective of risk management, it will go a long way toward aligning the functions of the CIO and CPO and to further enhance overall effectiveness. In any case, appropriate alignment is essential and will greatly impact the level of success achieved.

Table 7-1. Benefits of aligning the organization

Benefits to Team Members	Benefits to the Organization
<ul style="list-style-type: none"> • Greater freedom to direct activities toward successful policy implementation • Increased cooperation • Compatible sets of goals across the organization allow experts to perform task that they do best and not what other groups can do better 	<ul style="list-style-type: none"> • Better alignment of the organization toward business risk and requirements • Better decision making through cooperation across the organization • Reduced spending on audits and measurement of policy effectiveness due to elimination of redundant efforts • Increased coverage and resources available across the organization • Reduce costs of effective programs

Chapter 8

Strike a Balance between Reactive and Proactive Measures

In the beginning stages of a privacy program, it may be necessary to spend more time on reactive measures such as responding to privacy incidents and redressing privacy and security violations. It can also be important in the early stages to demonstrate effectiveness through audit reports or scorecards. As the privacy program begins to mature, less time will be required for reactive incident management because more IT systems, applications, and processes will have already been retrofitted.

Many existing IT systems were designed before privacy policies were even conceived or adopted. Incidents involving these legacy systems may be brought to light through daily operations. Nonetheless, a well designed plan for action between the privacy and technology specialists should include a proactive plan for assessing and remedying these privacy risks. Given that some number of security and privacy incidents are unavoidable, it is best to have a structured approach for dealing with incident management. The unexpected breach becomes an element of planned action and procedure much like any sound business continuity or disaster recovery plan.

Integrate Privacy into Existing IT Disciplines for Incident Management and Change Management

Fortunately, incident management and change management are relatively mature disciplines in most IT organizations. It is recommended that the existing IT processes for incident management and change management be leveraged to incorporate the relatively newer practice of managing security and privacy incidents. This will immediately provide an escalation process for security and privacy incidents, enabling them to be tracked and managed in the same way that IT incidents have historically been tracked and managed.

Unlike IT incidents which have traditionally been handled from a forensic perspective of finding the root cause and then fixing it, privacy incidents also require some proactive steps that go beyond the typical IT problem resolution workflow. Most IT change management and incident management workflows should be flexible enough to accommodate this. For example, if there is a privacy breach wherein PII has been exposed to an outside party, there may be a need to take proactive measures to communicate the breach to affected persons and perhaps to develop a plan to compensate people if damage has been incurred. The workflow for privacy incidents may therefore need to include an approval from a senior manager in the privacy office that confirms the existence of a communication plan if necessary.

Because many different IT systems and processes are intricately interconnected, IT change control procedures typically include a change impact analysis to identify whether a proposed change will affect other systems, applications, or processes. To help simplify this change impact analysis, many IT organizations maintain a comprehensive map of the dependencies between their IT systems, applications and processes. This makes it easier to trace which applications make use of specific system components and so on. To truly integrate privacy into the change impact analysis, may require a similar dependency map that identifies all of the business processes and associated systems that collect, process, transmit, or store PII. This will help reviewers to analyze proposed changes for their impact on privacy as well as their impact on IT solutions.

Following the established IT processes for incident management and change management can provide structure for gathering the facts and making an accurate assessment of business risk when privacy incidents occur. Furthermore, where incidents reveal a need to modify an existing IT system or organizational processes, those changes can be made by utilizing the review and approval processes within IT change management processes. Some of these workflows will need to be revised to include the privacy office in the review process. By following a structured process for change management, changes can be made in an orderly fashion that is designed to prevent disruption yet support proper control of PII.

Set Aside Time for Proactive Measures

Even when a privacy program is new and much time is spent to responding to incidents or remediating privacy risks, it is crucial to allocate some resources to proactive activities such as defining policies, processes and standards. Proactive measures must also be balanced against the overall cost of implementing privacy policies. Taking on too much too fast could be prohibitively expensive, but taking no proactive measures could be an even more expensive approach because this would deter progress on reducing business risk.

Proactive policies can forge the way for reducing future incidents, thus helping to reduce business risk and also providing more time for proactive solutions. Proactive measures not only accelerate the process of building awareness in the organization, but they can also provide a baseline for new IT projects to succeed in meeting privacy objectives. New IT projects should be subject to a review process that addresses privacy at an early stage in the development cycle.

When the number of privacy incidents begins to decline, this can be an indicator that the privacy program is maturing and that the proactive measures are working.

Table 8-1. Benefits of these recommended approaches for reactive and proactive measures

Benefits to Team Members	Benefits to the Organization
<ul style="list-style-type: none"> • Balancing emphasis between proactive and reactive measures can help reduce chaos, motivate key players, and relieve job stress • Using incident management and change management processes for privacy and security incidents improves the likelihood that processes will be followed because employees are already familiar with the processes • Winning short term successes can accumulate momentum and add to long term accomplishments for team members 	<ul style="list-style-type: none"> • Leveraging mature IT processes provides better control over incident management and the business risk associated with security and privacy incidents • Process improvements continue (proactive measures) while daily operations are being managed • Short term successes begin to accumulate momentum within the organization

Chapter 9

Measure Progress and Assure Compliance with Policies

As with any organizational initiative, it is important to have some objective metrics to measure the progress of the privacy and security programs and IT effectiveness in supporting these programs. The level and quality of communication between those in the CPO office and their counterparts in the IT organization is a good indicator of success. Goals that identify desired types of communication and how and when they will occur should be shared goals that provide incentives for all parties to meet their performance plans. For example, joint meetings or extended staff appointments should be set up with an explicit instruction to share information in a timely manner across the team. Personnel should be leveraged easily to perform investigations, deal proactively with organizational change management, and to pull in expertise where necessary.

Objective metrics that identify how well security and privacy policies are being implemented and whether they are being executed as they were intended can and should be created by the CPO and CIO teams. For example, tracking the number of security and privacy incidents that occur on a monthly basis is one good overall measure of the progress of the program. Training campaigns should include a record for numbers and job type of attendees to objectively show the level of outbound communication. Follow-up requests for additional training and increases in requests for assistance from outside of these organizational specialties should also be tracked as a means to monitor communication and organizational awareness. It may also be helpful to do periodic surveys of the user community to determine the effectiveness of an awareness campaign or training program.

The metrics that are best for one organization won't necessarily work for another. The important thing is to decide what measurements should be taken and how the results of those measurements will be used. The following basic recommendations for measuring progress should apply to most organizations:

- Establish metrics/goals at the beginning of each project and include an overlap of privacy, security and IT systems.
- Choose metrics that are specific to the goals and strategy of the organization.
- Assess how the metric can help predict future success or past learning points.
- Determine how frequently measurements must be taken in order to maximize value and minimize the cost to the organization for obtaining the measurement.
- Create shared goals for privacy and IT teams so that everyone is bought into the intended outcomes. Shared goals should include some stipulations for knowledge transfer between departments.
- Promote periodic reviews of systems and to measure against identified metrics for security, privacy and IT policies.
- Report observed results back to the business in a meaningful way. This will likely require translation of the observed results into business terms. Reports should offer an interpretation of any risks associated with the process or IT system to the business as well as its requirements.
- Define how compliance with policies will be monitored and what actions are to be taken to remedy non-compliance.

Compliance Assurance

Assuring compliance with policies is an important component of reducing business risk. Measuring organizational progress and monitoring systems and data must be accompanied by some kind of formal assessment against the objectives set forth in policies. If non-compliant conditions are discovered, some action is required to find the root cause of the problem and to make the changes that will remedy the situation.

IT organizations typically have existing disciplines and systems in place for 24 x 7 monitoring of security and the overall health of IT systems. The privacy office may be able to leverage the expertise and processes within the IT organization to establish effective solutions for monitoring privacy risks. In some cases, it may be helpful to create a compliance assurance program that monitors data governance with stated policy guidelines that are shared across the organization. For example, a data protection manager within the privacy office might manage privacy impact assessments even if the reviews are self-imposed by the IT project teams. Similarly, a security or IT manager might audit the systems of another organization using a privacy module of questions where PII is part of systems, processes or procedures.

Table 9-1. Benefits of measuring progress

Benefits to Team Members	Benefits to the Organization
<ul style="list-style-type: none"> • Creating metrics forces dialog and consensus about what is important to the office of the CPO and CIO (and the auditors) • Successful execution of a privacy/security program will likely be recognized and rewarded • Clarity between and among the various functions makes work more productive and lessens frustration 	<ul style="list-style-type: none"> • Proof of success and identification of vulnerabilities is easily visible to business decision makers and can help demonstrate the effectiveness of the program • Prioritization of risk initiatives becomes easier with shared objectives • Gained knowledge of what techniques are effective across the organization leads to better overall data governance • Greater degree of focus toward desired outcomes • Monitoring can help identify issues with processes in order to improve them

Chapter 10

Begin Right Away and Start with an Achievable Project

It may be readily apparent that it is important to get started right away in building a partnership between the CPO and CIO. However, there are many tasks competing for the attention of the CPO and the CIO, making it easy to put off pursuing this important goal. It is recommended to begin the partnering process immediately by agreeing on a project that should receive attention from the CIO and the CPO, and senior management. An active project brings conceptual ideas into focus, making it easy to recognize both common interests and the challenges of working together. Once recognized, the challenges can more easily be addressed.

It is best to start with something that is very achievable such as augmenting security policies with privacy requirements or defining standards for new IT systems. Whatever project is chosen, it is prudent to make the project narrow in scope and the time frame required to complete the project short. This will help get the relationship off to a good start by achieving initial success and can also be a good way for the CPO and the CIO to begin learning how to work well together.

Table 10-1. Benefits of beginning right away with an achievable project

Benefits to Team Members	Benefits to the Organization
<ul style="list-style-type: none"> • The relationship will develop more quickly when actively working on an achievable project (rather than just having meetings, going to lunch, etc.) • Get started on the right foot by achieving success 	<ul style="list-style-type: none"> • Privacy will be integrated into IT systems more quickly

Chapter 11

Promote a Culture of Data Governance and Data Stewardship Throughout the Organization

Data governance can be thought of as good housekeeping rules for managing data throughout its lifecycle from collection or creation to access control and dissemination, and finally, destruction. Data stewardship, on the other hand, represents the actual caring for the data, including ensuring that access controls are well maintained, backups are properly performed, and that data is safeguarded against security threats.

The overlap of the charters of the CPO and CIO regarding data governance, creates natural partnering opportunities between these two parties. The CIO is responsible for data governance in general and the CPO is responsible for the governance of PII. Because data governance is a mature discipline within many IT organizations, the CPO should work within the larger framework that the CIO already has for governance of data. The CPO can then provide input on how to apply this framework to the governance of PII. Partnering in this fashion allows the CPO to focus on unique priorities without being forced to reinvent the basics.

Empowering the Community to Help

A key to implementing a successful privacy program is empowering employees and stakeholders of the organization to assist the company in preventing privacy problems. The entire organization can be turned into privacy stewards and allies by educating and training all people in the organization to understand the fundamentals of privacy. More advanced instruction can be provided to key people within the organization whose duties involve more exposure to systems or processes that implicate PII. To accomplish this, employees must recognize the importance and value of privacy to the business and must have enough understanding about privacy requirements to be able to identify business risks and vulnerabilities. Armed with this knowledge, the entire organization will be a watchdog for privacy compliance and can alert the right people in the privacy office if they identify something as a potential risk.

Along this same line of thinking, one can promote a culture of data governance and data stewardship by helping business users and business process owners to understand that they are the ultimate owners of their data and are thus responsible for its proper governance. The focus of the CPO and CIO should be on empowering these process owners to become good stewards of their own data.

The CPO and CIO should look at data governance from a broad perspective across the organization and are in a position to provide direction that can help others be better stewards of their own data. Some examples of ways the CPO and CIO can help include:

- *Promote standardization of data representation*

A common problem in data governance is that different systems have different ways of representing the same data. This makes it more difficult to maintain consistent and accurate information across the organization. For example, customer address may be maintained as a single string of characters separated by commas in one system, whereas another system might have separate fields for each item including a nine digit zip code. The process of managing and sharing data is greatly simplified if the organization agrees upon a standard

representation of commonly repeated data structures such as customer name. If possible, the decisions about standardized data fields should be made by the primary owners of the data with input from their users and from the CPO and CIO.

- *Provide oversight for access control policies*

The CPO and CIO often support responsibility in the user community by giving process owners the ability to define or approve user access privileges for their data based on business requirements. While it is important for these users to be empowered, it is still the responsibility of the CPO and CIO to ensure that access controls are implemented in a manner that is consistent with overall organizational policies. In many organizations, access control policies are enforced by giving the IT organization the sole right to modify access rights for users, but giving process owners the power to decide which users may be granted access. In other cases, process owners may maintain their own access controls and may be subject to a periodic audit to help ensure compliance. In any case, these process owners should be trained in privacy and security guidelines to help reduce the risk of a privacy breach.

- *Resolve conflicts*

Occasional conflicts between different groups of users may arise when it comes to claiming ownership of data or defining standard data structures. The CPO and CIO may need to get involved to recommend solutions to the conflicts. In such cases, the CPO and CIO should take the perspective of the entire organization into account when offering a solution. Where possible, potential conflicts should be anticipated and addressed before the need becomes urgent.

- *Make ease-of-use a priority*

Data governance solutions can be much more effective if they are easy to implement. Therefore ease-of-use should be given high priority when data governance options are being considered. By aligning privacy and data governance requirements with the goals of the CIO's and by simplifying data governance for business users, the likelihood of success can be improved.

Benefits of Delegating Data Governance

Not only would it be prohibitively expensive to have a security and/or privacy staff that is big enough to adequately enforce high standards for data governance in every business unit, this approach would also be highly inefficient. The business process owners have the best understanding of how to protect their data and know which users should be granted access. They also have a strong incentive to protect the data that directly relates to their business objectives or employee base. When they understand the organization's approach to privacy and can work collaboratively with the CIO and the CPO, business process owners can accomplish their business objectives without compromising the company's commitment to policy.

Table 11-1. Benefits of focusing on data governance and data stewardship

Benefits to Team Members	Benefits to the Organization
<ul style="list-style-type: none">• Reduced confusion over who's responsible for data stewardship• Greater efficiency by leveraging each other's expertise• Reduced workload as users become more informed and become better stewards of their own data	<ul style="list-style-type: none">• Improved efficiency• Better control of data• More accountability across the organization

Chapter 12

Conclusion

Alignment between the CPO and the CIO can have a direct effect on reducing business risk and enabling more efficient operations. By cooperating to implement privacy requirements in ways that take into consideration the needs of both parties and the greater business objectives, the best interests of the organization as a whole are served. The CIO and the CPO must educate each other and cross-train their respective staffs in order to achieve true cooperation and work effectively to reduce business risk.

The best practices outlined in this paper are intended to offer a good starting point for effective cooperation. They should be seen as guidelines only, and should be implemented within the context of existing organizational policies and strategies, allowing for customizing to match organizational needs.

For More Information

For additional information on how Sun can help improve the design and execution of security and privacy policies, visit the Web sites below or contact a local Sun representative.

Table 12-1. Web Links for Additional Information

Web Site URL	Description
sun.com/	Sun Microsystems home page
sun.com/privacy/	Sun online privacy policy
sun.com/security/	Sun security solutions
sun.com/identity/	Sun identity management solutions

Copyright © 2006 Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, California 95054, U.S.A.

All rights reserved.

This product or document is protected by copyright and distributed under licenses restricting its use, copying, distribution, and decompilation. No part of this product or document may be reproduced in any form by any means without prior written authorization of Sun and its licensors, if any. Third-party software, including font technology, is copyrighted and licensed from Sun suppliers.

Sun, Sun Microsystems and the Sun logo are trademarks or registered trademarks of Sun Microsystems, Inc. in the U.S. and other countries.

All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. in the U.S. and other countries. Products bearing SPARC trademarks are based upon architecture developed by Sun Microsystems, Inc.

RESTRICTED RIGHTS: Use, duplication, or disclosure by the U.S. Government is subject to restrictions of FAR 52.227-14(g)(2)(6/87) and FAR 52.227-19(6/87), or DFAR 252.227-7015(b)(6/95) and DFAR 227.7202-3(a). DOCUMENTATION IS PROVIDED AS IS AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS HELD TO BE LEGALLY INVALID.