fs viewpoint

www.pwc.com/fsi

Closer to fine: Separating data privacy from information security

pwc

Executive summary

The continuously changing privacy-related regulatory environment has placed additional challenges on the data management infrastructure of financial institutions.

In our view, privacy is a legal and compliance issue, and information security is a technology issue. Each requires a distinct organization with its own leaders and obligations.

Reaching a crossroads.

Today's global marketplace demands that financial institutions collect personally identifiable information (PII) from both customers and employees to conduct business. At the same time, many financial organizations are expanding their international operations and engaging vendors and other third-party service providers beyond the borders of their home country. With a deluge of constantly changing privacy-related requirements, the challenge of protecting the personal information of customers and employees has grown exponentially in recent years. We use the term "privacy-related requirements" to refer to the data privacy and protection laws, rules, and data-breach notification regulations in place throughout the world.

More privacy laws.

Numerous privacy-related requirements have been passed in countries around the world, including those granting privacy as a basic human right and others covering financial privacy, data protection, telemarketing, fax and Internet communications, and security. As financial organizations navigate this global privacy maze, they are compelled to re-examine their privacy frameworks. Keeping track of numerous requirements significantly strains many financial organizations' legal, compliance, and technology resources.

Significant financial consequences.

Nearly every passing day brings fresh reports of corporate data breaches that damage the reputations of the financial institutions involved and threaten them with significant financial consequences. Moreover, financial organizations have started to realize that not all privacy breaches are caused by security breaches. But every breach must still be acted upon with direction from the information security team.

New privacy approach required.

How can financial institutions effectively protect the information entrusted to them by customers and employees? Managing privacy as a group of tactical projects under information security is not only inefficient but also inadequate and outdated. In our view, financial organizations should create a separate information privacy organization led by a chief privacy officer (CPO). This new organization should manage the financial organization's privacy obligations with a program that incorporates governance, privacy processes, and training and awareness. This approach should also be designed to drive linkages with other related areas including information security, vendor management, and incident response.

Point of view

Consumers are reeling from multiple retailer privacy breaches. Every financial institution should be concerned.

Financial institutions are increasingly realizing that a robust privacy program is not optional. The following factors are driving financial institutions to act:

- The costs of compliance failure are escalating. In 2013, the average cost of a data breach in the US, including remediation, fines, and relationship-restoring gestures, was $5.9 million.[1]
- Financial institutions commit to adhering to various regulatory privacy obligations, as well as the contractual obligations they make when customer accounts are opened.
- An adequate level of safeguarding is dictated by the law, not by technology. Regulations keep evolving and vary by jurisdiction.

In our view, privacy is a legal and compliance issue, not a technology issue.

The chief compliance officer (CCO), chief information officer (CIO), and office of the general counsel (OGC) should collaborate to design a privacy program with the following in mind:

- The information security organization, led by a chief information security officer (CISO), should spearhead data protection.
- A separate organization, led by a chief privacy officer (CPO), should manage the financial organization's privacy obligations.
- Because privacy compliance is very complicated, some decisions require specialized privacy knowledge that may be beyond some IT or line-of-business managers. Specialists trained in privacy law should support these decisions to help ensure adherence to privacy-related requirements.
- IT staff should focus on keeping the technology infrastructure safe.

- Fines for a single incident have been as high as $15 million. Court costs, settlements, and other legal bills and consent decrees can reach several times that amount.[2]
- As part of a settlement with the Federal Trade Commission, several companies have signed deals requiring monitoring by an independent privacy auditor for the next 20 years.[3]
- European countries are assessing fines for privacy violations individually. In addition, the European Union (EU) is considering implementing measures that would result in significant fines (up to 2% of global turnover).[4]

1 Ponemon Institute, "2014 Cost of Data Breach Study United States, Sponsored by IBM," May 2014, www.ponemon.org, accessed July 15, 2014.

2 PwC, "Fortifying your defenses: The role of internal audit in assuring data security and privacy," July 2012, www.pwc.com, accessed May 28, 2014.

3 Farhad Manjoo, "Another Tech Company Finds the F.T.C. Looking Over Its Shoulder," New York Times, May 10, 2014, www.factiva.com, accessed June 13, 2014.

4 Francis Robinson, "EU Steps Up Bid To Tighten Its Rules on Data Privacy," Dow Jones Top North American Equities Stories, August 9, 2013, www.factiva.com, accessed June 13, 2014.

Financial institutions today are at greater risk of a privacy breach as technology and operating models evolve. The regulatory environment is also evolving.

Technology changes

- Consumers use mobile technology and social media with increasing frequency, which complicates privacy-protection measures.
- Financial institutions operate through multiple legal entities, each with jurisdiction-specific contractual obligations to customers and clients. Complex structures within the same financial institution demand increased communication and coordination.

New operating models

- Cross-border operations, outsourcing, cloud computing, and organizational structures encompassing multiple legal entities are now common characteristics of financial institution operations. Outsourcing options have expanded significantly in recent years as financial organizations step up their search for locations beyond China and India. Eastern Europe, the former Soviet Union, South America, Central America, Asia, Africa, and the Middle East are just some of the other locales that have become outsourcing destinations.
- Multiple jurisdictions complicate compliance regimes. For example, if a US citizen in the EU conducts transactions and the related PII is stored in Europe, that person may gain additional rights based on the laws of the storage country. As a result, US financial institutions will need to modify their procedures to identify and track situations where these additional rights may apply.

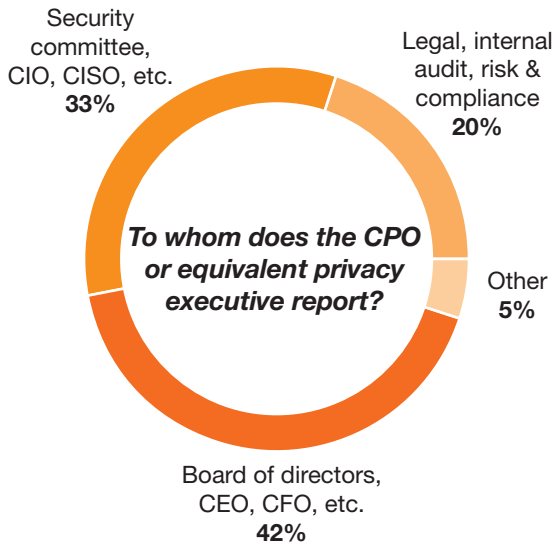
Regulatory changes

- As privacy-related requirements proliferate and change, the challenge of protecting the personally identifiable information (PII) of customers and employees grows exponentially. For example, some US states (Vermont, Massachusetts, and California immediately come to mind, with more sure to follow) are becoming noticeably more active in regard to privacy, as are non-US privacy regulators. As such, financial institutions must comply with a combination of industry/sector, state, and federal privacy laws.
- The ever-changing data privacy regulations in non-US jurisdictions will add further challenges for US financial institutions doing business internationally.
- Regulations are specifically vague and subject to interpretation. These factors significantly complicate privacy-related compliance. Addressing the issue requires a regulatory/legal mindset.

We have observed varying approaches to ownership of privacy within financial institutions.

In the 2014 PwC Global State of Information Security Survey, respondents from financial institutions were asked to whom does the CPO or equivalent privacy executive report?

Figure 1: There is a wide disparity in ownership of privacy across financial institutions.



Source: 2014 PwC Global State of Information Security Survey.

Functional organizations within financial institutions tend to share certain structural features:

- Organizations usually have both a CIO and a CISO.
- Some financial institutions further segregate the information security function and allocate some responsibilities to the chief data officer (CDO).
- Many financial institutions have a cadre of individuals within the technology organization that handle privacy compliance, but have little visibility to other parts of the organization.
- The few financial institutions with an established CPO generally require relatively little formal communication between the CPO and the CISO. For example, there often is no process to dictate a timely discussion between the CISO and CPO when the need arises. In our view, the lack of communication and collaboration on technical actions risks potentially dire consequences.
- Some financial institutions have a CPO who reports directly to the CISO. The CPO relies on external legal counsel for advice. This approach has two potential drawbacks:
  - Without appropriate internal support, the financial institution's leadership may overlook changes in the regulatory environment and/or the operating model.
  - Limited support inside the organization may reduce the CPO's visibility and impact.

We have observed the following job roles associated with privacy.

- CPO: usually from a legal or compliance background; focuses on privacy compliance.
- CIO: usually from a technology background; focuses on keeping systems running.
- CISO: usually from a technology background; focuses on keeping the technology infrastructure safe.
- CDO: usually from an information background; focuses on data governance and classification, and on leveraging data as an asset.
- CRO: usually from a financial background; focuses on business risk.
- The office of the general counsel designates a privacy attorney to oversee the financial organization's compliance with privacy and regulatory requirements.

Leading financial institutions are taking a more strategic view of privacy, while also making operational improvements.

Leading financial institutions are beginning to change their approach to privacy at the strategic, operational, and governance levels as they begin to separate the CISO and CPO functions.

In terms of strategy…

- Leaders are establishing privacy organizations within the institution that span different departments, geographies, and affiliates worldwide and include privacy officers at various levels. This structure encourages a holistic view of privacy, with the clear understanding that privacy-related requirements vary from state to state, jurisdiction to jurisdiction, country to country, and at the supra-national body level, as is the case with the European Economic Area (EEA).
- Leading financial institutions coordinate and collaborate with the applicable stakeholders from security, compliance, and the lines of business to meet legal and regulatory requirements within the key jurisdictions where they handle data. We have also observed some financial institutions engaging in EEA/EU model contracts and binding corporate rules (BCRs) that address the transfer of private information.
- Others have established clear privacy policies and are periodically publishing their privacy notices and statements as regulations require. In addition, marketing teams associated with the lines of business are simplifying customers' opt-in/opt-out choices.

In terms of operational improvements…

- Leaders are proactively defining procedures to track and respond to privacy breaches.
- Leading financial institutions are also increasing their investment in monitoring the privacy of clients' PII as well as regulated financial information by implementing data loss prevention (DLP) tools with a focus on demonstrating greater accountability for protecting sensitive information.
- They are also focusing more on securing their infrastructure through increased investment in cyber security tools and technologies.

In terms of governance…

- Leading financial institutions are linking privacy-related requirements to policies, procedures, and business operations. Routine testing and audits of controls ensure that operational complacency does not set in.

In our view, a successful global privacy strategy builds upon collaboration and communication, but with separate roles and responsibilities that evolve as institutions grow.

Segregate but collaborate.

In our view, financial institutions should separate responsibilities for data-privacy compliance and data protection. At the same time, they should establish mechanisms to help ensure that the functions can collaborate as appropriate. For example, when it comes to privacy-related matters, privacy-trained lawyers and privacy-savvy managers, not IT or lines of business managers, should be the main decision makers. The IT staff should focus instead on planning, building, managing, maintaining, and protecting vital IT assets and technology infrastructure.

Separate but communicate.

The institution should facilitate smooth communication between the CPO and CISO teams, regardless of separation. We recommend using a common integrated platform that enables better communication between the two functions. Privacy handling may be further segregated by geography, regulatory domain, or lines of business. Security may be separated into technical infrastructure security and data security.

As institutions continue to grow, our view is that they should go even further and consider formally separating data and infrastructure security. This division will help ensure that data, especially PII, receives priority attention.

In our view, the following principles should steer the privacy effort:

- *Treat customer privacy as a business imperative.*
- *Design privacy into all business and technology processes.*
- *Respect data-privacy contracts between the customer and the financial institution.*
- *Use IT as a common, integrated communication and sharing platform.*
- *Recognize data-sensitive business operations and applicable processes.*
- *Understand specific mapping of sensitive data to business processes.*
- *Define specific policies for handling sensitive data in various situations.*
- *Document data flows across systems and regions to help ensure compliance.*

In our view, a successful global privacy strategy also takes into account the wide variation in privacy-related requirements worldwide.

A financial institution should have a clear understanding of its key business markets as well as the applicable legal and regulatory requirements within the jurisdictions in which it operates.

Privacy-related requirements vary widely. In response, we recommend that financial institutions do the following:

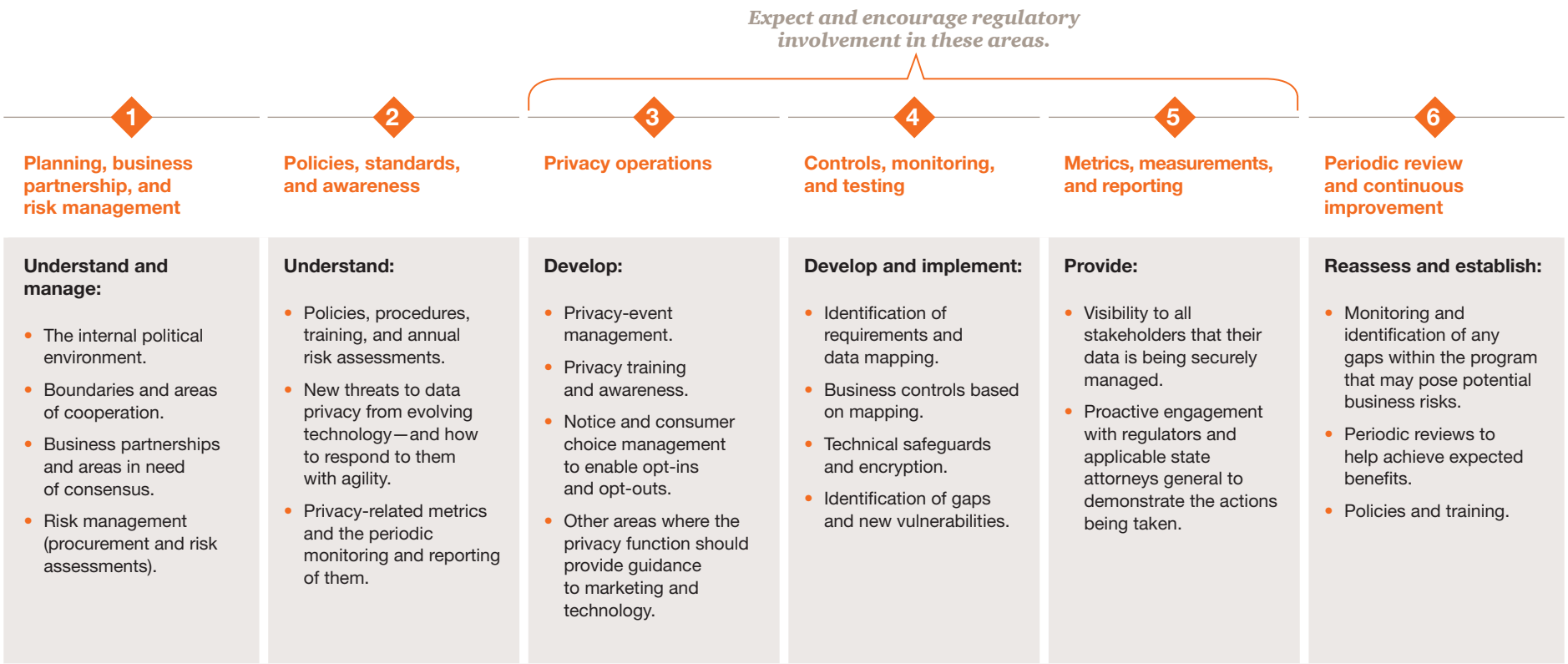
- Define privacy as primarily a legal and compliance regulatory matter.
- Create a privacy office that develops privacy guidelines and interfaces with other stakeholders. If the financial institution does not currently have a separate privacy office, we recommend for the institution to hold an internal "privacy summit" that convenes key stakeholders from the lines of business, technology, compliance, and legal.
- Identify and understand what the data is, where it resides, how it is classified, and how it flows through various systems. For example, financial, medical, and PII are subject to different restrictions in different jurisdictions.
- Develop appropriate global data-transfer agreements for PII and other data that falls under privacy requirements.
- Recognize and adhere to privacy requirements when developing core business processes and cross-border data flows.
- Preserve customer trust as the primary goal.

PwC's integrated privacy and data protection framework includes six key steps.

In a global market notable for its array of ever-increasing privacy-related requirements, a fragmented approach to privacy-related compliance cannot adequately protect financial organizations or their customers.

Financial organizations should develop an integrated privacy and data protection program. PwC has developed the six-step framework described below:

Figure 2: PwC's integrated privacy and data protection framework.

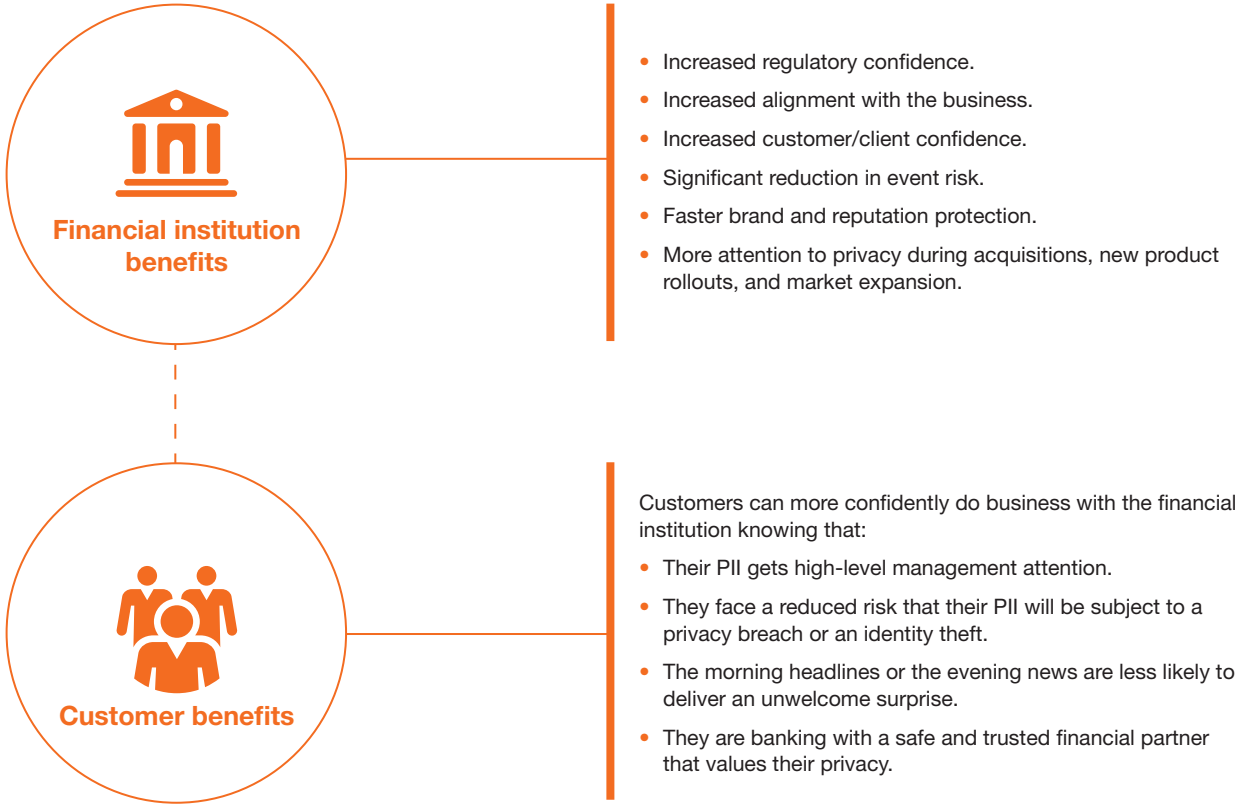


Our approach includes multiple benefits.

The separation of the CPO and CISO functions provides multiple advantages.

Privacy and infrastructure security both get the full attention they demand from appropriately trained people in both the security and the privacy arenas. Each team brings its own perspective, discipline, and skills.

Figure 3: The separation of the CPO and CISO functions provides multiple advantages to both the financial institution and its customers.



The obstacles tend to be organizational/political, financial, and operational. However, with appropriate planning, these obstacles can be overcome.

	Organizational/Political	Financial	Operational
Obstacles	• Corporate culture and politics may become an issue if an established part of the IT organization faces the possibility of reassignment. • Financial institutions may delay steps to improve their privacy posture because of the difficulty of implementing new processes and communication routines. • New processes and routines can complicate relations with existing units and spark turf wars.	• Funding for a new privacy organization may be hard to secure. • Conflicts may arise as budgets are reallocated. • Annual budget costs may become a chronic sore point.	• Overlapping responsibilities across the security and privacy functions may cause operational conflicts and confusion about process ownership.
Solutions	• Actively manage stakeholders and build consensus across the business units that will be impacted. • Enhance communication. • Adjust titles to reflect new duties and status. • Define specific boundaries to avoid contention. • Staff appropriately for the new roles and responsibilities, and present change as a welcome reduction in workload. • Present as “headache relief.”	• Consider leveraging existing personnel instead of hiring additional employees. Limit new costs to hiring personnel with specific skills that do not exist within the current organization. For example, consider hiring a lawyer specializing in privacy if the corporate counsel’s office lacks that resource. • Re-allocate existing budgets rather than try to secure new funding. • Elevate the status and decision rights of the newly defined privacy group to help secure ongoing funding.	• Enhance communication and collaboration among groups. • Clearly define the roles of each organization to prevent potential confusion. • Define specific boundaries in writing. Clarify that privacy professionals address regulatory and legal requirements only; IT addresses everything else, including the operational implementation of privacy policies and procedures.

The consequences associated with inadequate internal controls over privacy and data protection continue to mount.

The cost of inaction includes the following:	
Direct costs	• Cost of hiring forensic experts. • Customer service support costs. • Cost of providing free credit monitoring and discounts or free services to those impacted. • Remediation of impacted technical systems. • Penalties, fines, and other costs from regulators.
Indirect costs	• Customer attrition resulting from lost trust. • Diminished brand value resulting from overall reputational damage and a reduction in customer satisfaction, leading to a loss of share in the marketplace and/or reduction in share value.
Other considerations	• Loss of potential benefits as discussed earlier. • Continued exposure to additional regulatory and compliance scrutiny such as 20-year consent decrees. • Potential increase in business risk because of exposure to privacy concerns.

The bottom line:

Financial institutions that embrace privacy as a separate yet integral component of their risk management structure position themselves strategically to compete for and retain market share.

Competitive intelligence

Our observations of industry practices.

The following table outlines our observations of three financial institutions.

	Financial institution A	Financial institution B	Financial institution C
Planning, business partnership, and risk management	Embedded in compliance, privacy is broadly engaged across the enterprise. Segregated IT security and privacy organizations collaborate for the overall benefit of the financial organization.	Risk and security offices suffer from a lack of business partnership and inadequate coordination. The organization lacks a formal privacy office.	The global financial organization with a segmented privacy focus produces strong local privacy partnerships. But segmentation also results in lack of uniformity across lines of business.
Policies, standards, and awareness	Uniform, global privacy policy includes regional carve-outs or add-ins as required. The financial organization supports awareness activities such as "privacy week." The financial organization engages intensively in annual information privacy summits and the development and delivery of protection training.	The business units have been delegated to develop uniform policies and receive no guidance on implementation. Despite a general awareness of privacy, no leader has operational ownership of the topic. The information security office performs only minimal additional due diligence after privacy incidents.	Despite well-defined global privacy policies, inconsistent training methods result in uneven levels of awareness within the organization. The financial organization is proactively embracing and improving global standards and awareness.
Privacy operations	The organization defines and maintains globalized and localized privacy operations. Specifically designated systems handle privacy event management, choice management, and other privacy-related automation requirements.	Privacy operations across multiple product lines and business units are federated, non-integrated, and decentralized. The organization maintains multiple, disparate systems for handling customer choice management.	The financial organization centrally manages privacy operations from a non-US location. The financial organization is an early adopter of privacy management technologies.

Leading On par Lagging

The following table outlines our observations of three financial institutions.

	Financial institution A	Financial institution B	Financial institution C
Controls, monitoring, and testing	The financial organization periodically stress-tests clearly defined privacy controls and monitors test outcomes closely.	The financial organization does not regularly test or monitor privacy operations.	In the early days of introduction and implementation of a privacy control monitoring framework. It has been developing a consistent set of technology infrastructure, which will be compliant to privacy, banking secrecy, client confidentiality, and outsourcing regulations once put in place.
Metrics, measurements, and reporting	Clearly defined, quarterly reported metrics and measurements include proactive routine reporting to regulators.	No designated individual or group tracks the limited and indirect privacy metrics that exist within the organization. Units do not report privacy metrics to the privacy compliance office.	Privacy risks are well understood across the bank, yet not clearly documented, and compliance is not demonstrated all the time. Work is being carried out to define privacy risk measurement metrics.
Periodic review and continuous improvement	Metrics review identifies needed process improvements and processes that are running outside of control limits. Metrics and limits enable the financial organization to make proactive improvements before it has regulatory or privacy consequences.	Periodic reviews of privacy-related policies are ad hoc, limited, and informal. The organization's mature privacy operations have no defined processes for continuous improvement.	Continuous improvement is planned; however, the challenge for the bank is to implement a consistent technology infrastructure and solution to manage customers' personally identifiable information (PII) and master data with the following: • Clear roles/responsibilities • Privacy access restrictions • Training and awareness

Leading On par Lagging

A framework for response

Our recommended approach to the issue.

Our approach to protecting privacy involves engaging the organization through the following six steps.

Expect and encourage regulatory involvement in these areas.

1 Planning, business partnership, and risk management

Understand and manage:

- The internal political environment.
- Boundaries and areas of cooperation.
- Business partnerships and areas in need of consensus.
- Risk management (procurement and risk assessments).

2 Policies, standards, and awareness

Understand:

- Policies, procedures, training, and annual risk assessments.
- New threats to data privacy from evolving technology—and how to respond to them with agility.
- Privacy-related metrics and the periodic monitoring and reporting of them.

3 Privacy operations

Develop:

- Privacy-event management.
- Privacy training and awareness.
- Notice and consumer choice management to enable opt-ins and opt-outs.
- Other areas where the privacy function should provide guidance to marketing and technology.

4 Controls, monitoring, and testing

Develop and implement:

- Identification of requirements and data mapping.
- Business controls based on mapping.
- Technical safeguards and encryption.
- Identification of gaps and new vulnerabilities.

5 Metrics, measurements, and reporting

Provide:

- Visibility to all stakeholders that their data is being securely managed.
- Proactive engagement with regulators and applicable state attorneys general to demonstrate the actions being taken.

6 Periodic review and continuous improvement

Reassess and establish:

- Monitoring and identification of any gaps within the program that may pose potential business risks.
- Periodic reviews to help achieve expected benefits.
- Policies and training.

Step 1: Planning, business partnership, and risk management.

Separation anxiety is almost inevitable as a financial organization begins to enable an autonomous and self-directed privacy organization outside the technology, security, compliance, and legal functions.

With the right leadership and nurturing, the new program can become self-sustaining and rapidly begin to provide great value and strong contributions to the financial institution.

Navigating the politics of separation can be the journey's greatest hazard. Obstacles should be met head-on and up-front.

If the financial institution is establishing a new privacy organization, we recommend it hold an internal "privacy summit" that convenes key stakeholders from the lines of business, technology, compliance, and legal. At this meeting, key stakeholders convene to do the following:

- Provide a view into the growing importance of privacy as an independent discipline.
- Discuss the organization's current approach to privacy-related matters.
- Openly discuss shortcomings in the financial organization's current approach, from increased costs to non-uniformity to self-identified audit or compliance issues.
- Review the approaches that peer organizations have taken.
- Understand the staffing and costs of a new organization and the "net new" requirements for talent acquisition or other costs.
- Agree on a maturity lifecycle for the new department, identify the stakeholders that will own responsibility, and define the planned internal structure to which privacy ultimately will report.

To help ensure compliance, financial organizations should take the following steps to assess their internal privacy-related compliance program:

- Identify applicable privacy-related requirements in the jurisdictions where the financial organization conducts business, stores or processes data, or collects personally identifiable information (PII).
- Conduct a data-element inventory and develop a data-classification scheme.
- Develop data-flow maps of PII, including data transfers to third-party service providers across country borders.
- Create a mechanism, based on data mapping, to translate overarching privacy-related requirements into business controls.
- Design or integrate with existing regulatory change management process for monitoring changes to applicable privacy-related requirements.
- Create a process for monitoring changes to data flows throughout the financial organization, including data transfers to third-party service providers and changes due to acquisitions and dispositions of businesses.

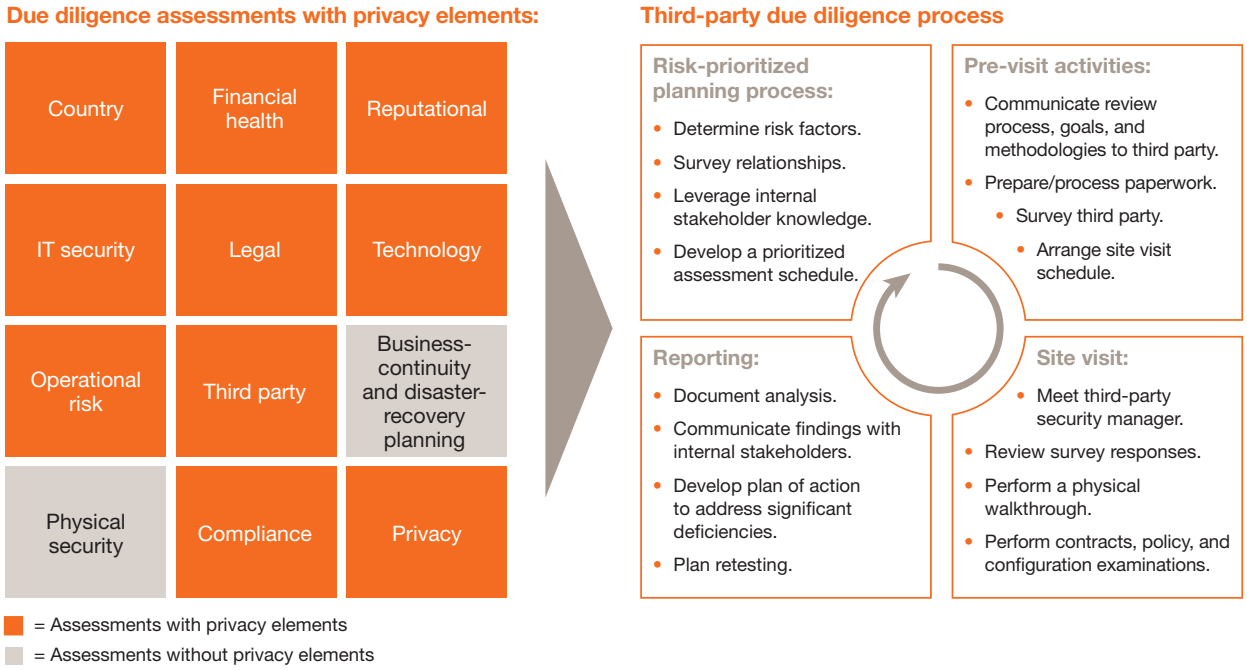
Step 1: Planning, business partnership, and risk management (continued).

Consider the following leading practices when managing third-party service providers that handle customer and employee data:

- During the procurement process, exercise appropriate due diligence by conducting a third-party assessment that examines the ability of the third-party service provider to comply with your financial organization's privacy, information-security, and data-protection policies.
- Provide ongoing role-based privacy compliance training to both employees and third-party service providers.
- Work with legal counsel to include appropriate contract provisions that cover non-disclosure, restrictions on third-party service provider's use of confidential data, financial organization's right to audit, and the third-party service provider's obligation to notify the financial organization of a data-security breach.

As discussed in PwC's "Significant others: How financial institutions can effectively manage the risks of third-party relationships,"[1] select the appropriate third-party assessments based on the type of service being provided, the third-party's inherent risk, and the circumstances of the relationship.

Figure 4: The following due diligence assessments have a privacy element. As part of the third-party due diligence process, we recommend that financial institutions incorporate the following planning in order to address privacy issues.



1 PwC, "Significant others: How financial institutions can effectively manage the risks of third-party relationships," September 2013, www.pwc.com/fsi.

Step 2: Policies, standards, and awareness.

Financial institutions should seek answers to the following questions:

- *Are data-entry points for manual and automated systems securely administered?*
- *Do safeguards such as data encryption and infrastructure security sufficiently enforce written policies?*
- *Are processes and segregation of duties (span of control) in place to reduce threats?*

Financial organizations may want to consider strengthening their privacy governance model to include:

- Formal senior management ownership and sponsorship of privacy, including appointment of a senior executive with responsibility and accountability for privacy. Define the privacy mission statement and strategy.
- Written formal policies and procedures covering customer and employee data, including privacy structure, reporting lines, roles, and responsibilities.
- Inventory of all third parties (including partners, vendors, and third-party service providers) processing data that is subject to privacy-related requirements.
- Cross-functional oversight committee chaired by the CPO that includes key stakeholders from relevant departments such as information technology, information security, human resources, legal, compliance, government affairs, operations, risk, and internal audit.
- Ongoing training and awareness programs for employees and third-party service providers who handle or process data containing information that is subject to privacy-related requirements.
- Annual risk assessments of privacy and data security, as well as ongoing reporting as appropriate to senior management.

The following leading practices should be considered when implementing information security protection as part of a comprehensive privacy program:

- Implement technical, physical, and administrative safeguards to prevent unauthorized access to confidential data (including hard-copy records).
- Encrypt laptops, PCs, and removable media and require the same of third-party service providers with access to sensitive data.
- Secure transmission of confidential data.
- Monitor access privileges and controls.
- Implement data-classification policies.

We recommend that assessments consider the culture of the organization itself:

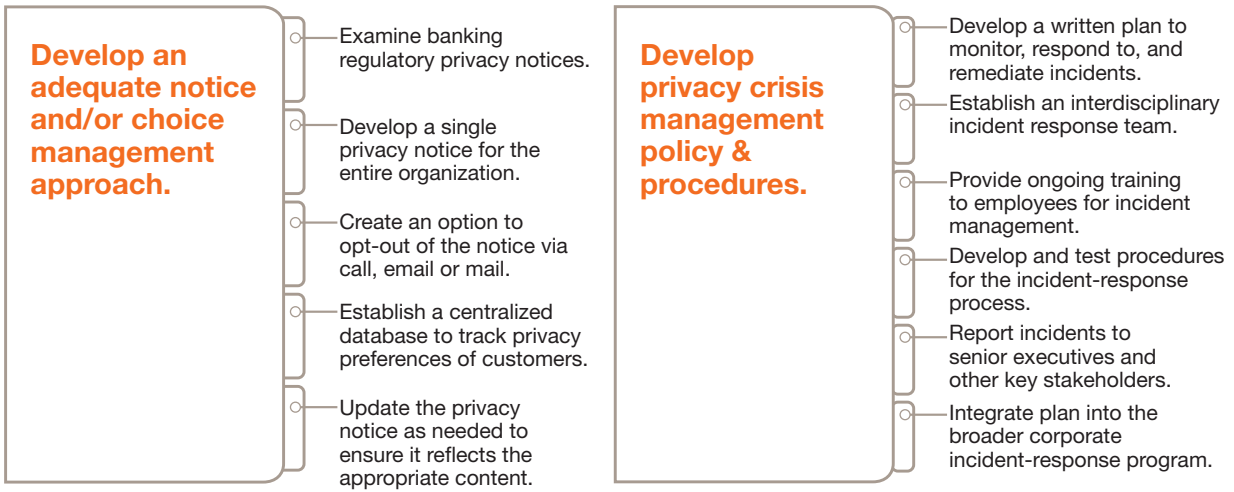
- Assess employee perception, attitude, and behavior toward the protection of personal information.
- Determine the impact and readiness for the privacy program by assessing roadblocks encountered during similar operational changes.
- Define a culture-change plan that consists of communication, behavioral training/development interventions, identification of sponsors, and alignment with HR and performance management policies.
- Assess stakeholder communication and engagement needs to gain stakeholder commitment throughout the change process.

Step 3: Privacy operations.

Develop a privacy notice and a choice management approach that works for the entire financial organization. Develop privacy crisis management policy and procedures.

A privacy statement or notice is a brief document that sets forth the standards in which an organization discloses privacy policies and practices, as well as shares and protects nonpublic personal information pertaining to customers and employees to comply with privacy regulations. These individual, nonpublic data attributes include, but are not limited to, full name, date of birth, social security number, contact information, financial records, and credit information.

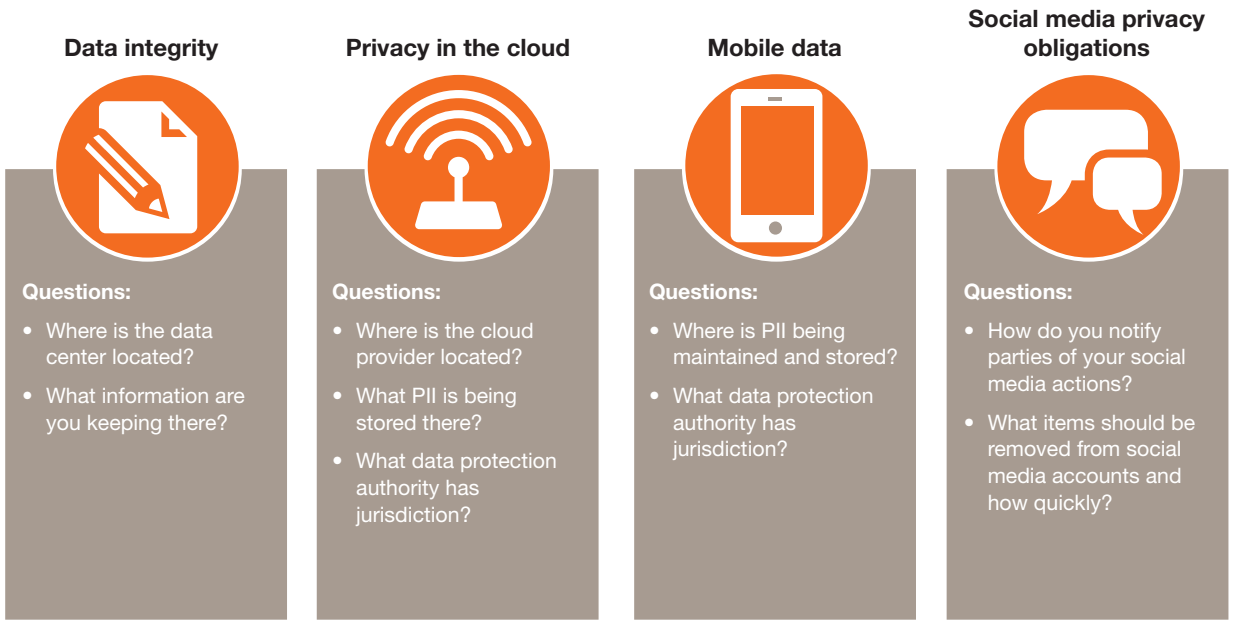
Figure 5: Privacy operations includes the development of both a notice and/or choice management approach as well as a privacy crisis management policy.



Step 4: Controls, monitoring, and testing.

Key steps	Key considerations
Examine current controls in place.	• Design of appropriate controls for each component of the privacy program. • Design of information handling controls for each phase of the information lifecycle for the high-risk business processes. • Design of third-party management and accountability processes, as well as the related controls.
Conduct periodic monitoring and testing of the controls and the overall program.	• Continuously conduct internal and external audits to evaluate the structure and effectiveness of the privacy program, as well as compliance with privacy policies, procedures, and controls across the organization. • Capture metrics and measurements from the audits and reviews.

Figure 6: We recommend that financial institutions consider the following key themes when they conduct controls, monitoring, and testing.



Step 5: Metrics, measurements, and reporting.

A successful privacy program should provide stakeholders visibility into how their privacy concerns are being addressed. Quantifiable metrics may include:

- Number of employees participating in privacy training programs.
- Number of new accounts opened, resulting privacy notices delivered, and consumer choice elections captured.
- Size, scope, and geography of privacy events and quantification of notices resulting from privacy events.

In addition, these metrics can enable a company to proactively engage with regulators, internal auditors, and any other stakeholders to demonstrate the level of concern taken with private data.

In our experience, metrics are one of the most undervalued success factors in improving privacy programs. Privacy requires an integrated set of measures, including metrics for:

Inputs—for example, how many resources are dedicated to privacy? How effective is the privacy program, including training and access to external partners?

Process—what is the quality of our privacy system? How much time is needed before the privacy system is fully in place?

Outputs—have new processes resulted in better privacy detection and fewer events as promised? Has brand image improved?

Value generated—how has profit been impacted?

Like security, the value that privacy brings to an organization may be difficult to quantify, because a good program prevents bad things from happening.

Regardless, the privacy organization may be able to demonstrate the decline in privacy-related events since the implementation of the organization.

A privacy organization can also discuss the causes of typical breaches in the market and demonstrate how the financial organization has successfully mitigated those issues.

Key steps	Key considerations
Identify key metrics	• How many metrics are we monitoring at once? • Are we monitoring the right metrics? Should we review or revise them?
Identify technology platform	• How do we currently monitor privacy events apart from security events? • Do we have the appropriate technology in place to monitor the impact of our privacy programs?
Improve monitoring capabilities	• Are our existing monitoring efforts appropriate? • How do new privacy efforts impact existing efforts that we are monitoring?
Provide regular updates to the business	• Who are the most appropriate stakeholders to review the metrics? Who has the bandwidth and/or interest to review? • When do the business units need to generate their own reporting? When do they need to see results?

Step 6: Periodic review and continuous improvement.

Conduct an independent assurance review to assess the organization's compliance with program requirements.

The review can apply to the whole organization or a specific subsection of the organization. Execute periodic reviews as follows:

Figure 7: A periodic review should include the following seven components.

Key steps	Key considerations
Monitor and track against milestones	• Verify if privacy measures are within prescribed control limits. • Establish implementations dates and improvement activities to be consistently moving the program forward.
Identify risks and changes	• As control and monitoring activities occur, look for trends in the data. • As privacy is a constantly shifting landscape, make certain that regulatory change management is working across all jurisdictions in which you operate.
Monitor quality of deliverables	• Do notices reflect accurate information? • Are applications in design that use PII going through appropriate privacy checkpoints?
Monitor and track benefits	• Individual data points are not as reliable as trends; therefore, monitor the trends. • Establish quarterly reports that clearly illustrate the benefits of the program as well as the opportunities for improvement.
Manage privacy stakeholders	• Have routine meetings with lines-of-business and compliance leadership to discuss results. • Take input as to their concerns about privacy and their forthcoming plans for the business.
Adapt for additional jurisdictions	• Make sure that all of the jurisdictions you are operating in are part of the regulatory change management scope. • Assure that privacy has an active role in planned acquisitions or dispositions with an international flavor to them.
Follow changes in landscape	• As the organization changes, determine whether new privacy requirements will need to be assessed. • Determine whether new lines of business and new methods of interacting with customers (for example. social media) should prompt privacy impact assessments.

Appendix

Select qualifications.

Privacy assessment, recommendations, and target operating model—Global investment bank

Issues

A global investment bank based in the United States wanted to prepare for an upcoming Consumer Finance Protection Bureau (CFPB) examination. The bank lacked a formal privacy program. In addition, it faced the following challenges:

- The bank's management processes for consumer choice, consent, and notification were spread out across multiple lines of business with little coordination among them.
- Despite guidance on financial organization privacy requirements provided by the legal department, the bank did not have any controls in place to verify that the requirements were met.
- In some instances, the job descriptions of entry-level compliance staff or legally accountable staff did not explicitly include privacy-related responsibilities.

The bank engaged us to help them determine potential ways to address these issues.

Approach

PwC worked collaboratively with bank employees across various US entities and lines of business to assist in the following ways:

- Assess the effectiveness of existing consumer choice, consent, and notice management processes.
- Review the incident management processes to help ensure coverage for privacy-related breaches and incidents.
- Assess the bank-wide privacy notices in place and help determine whether they meet the requirements as stated in the model privacy notice.
- Perform a high-level assessment of the privacy practices of several other of the bank's international entities.
- Propose a potential organizational structure for the privacy organization, including a model for interactions with appropriate functions across the bank (such as legal, compliance, and information security).

Benefits

Based on our work, the bank is better able to understand the privacy posture across its various legal entities. This helped the bank make amendments to its privacy practices before the CFPB exam, in addition to standardizing its notices. Our work also laid the foundation for development of an enterprise-wide privacy organization and a governance model.

Implementing global privacy compliance—Major global bank

Issues

A major global bank based in Europe wanted to move client and customer personally identifiable information (PII) between countries. Privacy and bank secrecy laws limit the movement of PII in different countries. The client engaged us to help identify and understand the applicable regulations.

Approach

PwC worked collaboratively with the bank in both Europe and the United States to:

- Draft a risk-based approach to determine what countries to focus on, depending on the types of data and the purpose of the data movements that occur.
- Assess the data ownership lifecycle based on the privacy language agreed upon in each jurisdiction, and discuss possible courses of action (such as sending out notices and signing new agreements).
- Inventory the data moving between jurisdictions.
- Help the domestic compliance team understand the current state of privacy compliance in each applicable country.
- Engage with the technology design teams that were designing the data repositories to understand the planned functions, geography, and current privacy protections of data repository locations.
- Perform country-by-country assessments of the privacy and bank secrecy regulations.
- Work with leadership to coordinate between US and European privacy and technology groups.
- Assist leadership in outlining roles and responsibilities, tools, and techniques, as well as the supporting capabilities required to maintain compliance.

Benefits

Based on our work, the bank was better able to:

- Comply with regulations requiring pre-emptory analysis.
- Maintain ongoing relationships with customers.
- Enable PII to be moved between countries for customer support.
- Improve the customer service experience for corporate treasury and high-wealth clients.

www.pwc.com/fsi

To have a deeper conversation, please contact:

Andrew Toner	andrew.toner@us.pwc.com +1 646 471 8327
Shawn Connors	shawn.joseph.connors@us.pwc.com +1 646 471 7278
Joseph Nocera	joseph.nocera@us.pwc.com +1 312 298 2745
Scott Margolis	scott.margolis@us.pwc.com +1 214 754 5457

Follow us on Twitter @PwC_US_FinSrvcs

We would like to thank Abhishek Bakre for his significant contribution toward this publication.

"Closer to fine: Separating data privacy from information security," PwC FS Viewpoint, August 2014, www.pwc.com/fsi.

LA-14-0228

About our Financial Services practice

PwC serves multinational financial institutions across banking and capital markets, insurance, asset management, hedge funds, private equity, payments, and financial technology. As a result, PwC has the extensive experience needed to advise on the portfolio of business issues that affect the industry, and we apply that knowledge to our clients' individual circumstances. We help address business issues from client impact to product design, and from go-to-market strategy to human capital, across all dimensions of the organization.

About PwC US

PwC US helps organizations and individuals create the value they're looking for. We're a member of the PwC network of firms in 157 countries with more than 184,000 people. We're committed to delivering quality in assurance, tax, and advisory services.

Gain customized access to our insights by downloading our thought leadership app: PwC's 365™ Advancing business thinking every day. Tell us what matters to you and find out more by visiting us at www.pwc.com/us.