CHAPTER 12

Organizational Design and Alignment

> *My model for business is the Beatles. They were four guys who kept each other's kind of negative tendencies in check. They balanced each other, and the total was greater than the sum of the parts. That's how I see business: Great things in business are never done by one person. They're done by a team of people.*
>
> —Steve Jobs, interview on *60 Minutes*, 2003

This chapter discusses options for the organizational placement and structure of the privacy team in an organization that has embraced privacy engineering. It describes the new and evolving roles necessary to support a successful effort and suggests best practices for aligning key organizational functions with your privacy program and privacy engineering goals. Finally, this chapter explores the key organizational challenges for privacy programs.

Just as privacy engineering requires rethinking responsibilities across the organization, so too it may require redesigning the privacy team and the organization's information governance function. Traditional organizational structures may not be sufficient to support the cross-functional demands of privacy or privacy engineering, especially because these structures have not historically emphasized roles that contain deep privacy expertise.

Organizational Placement and Structure

The organizational placement and structure of the privacy team can be critical to the success of a privacy engineering program and therefore deserves careful consideration. The optimal location and team structure may vary, depending on factors such as the organization's goals, requirements, and culture.

First, let's look at leveling of the CPO (chief privacy officer—or whomever leads the privacy function); where in the organizational hierarchy should the CPO sit? Titles aside, the CPO should have equal footing with the head of IT and the head of product engineering. This is to facilitate alignment as well as governance (i.e., checks and balances). Also, it is equally important that unless the CPO is also the head of the

privacy engineering program, the CPO should be at a higher or equal management level than that of the lead for privacy engineering. This helps avoid competing empires and lessens hindrances to alignment. Ideally, the privacy function would report directly to executive management.

The truth is, however, that many organizations have taken an organic approach and have located privacy groups within the organization that initially recognized the need (e.g., human resources, legal, marketing) and were willing to staff and fund such initiatives. If this is the case in your organization, it's important to reconsider the location of the privacy office: it is more than likely to tilt its charter, its focus, and its goals (official and unofficial). Where in your organization the privacy team is located will also affect how the privacy function is viewed and its reach across programs and divisions of the enterprise.

Any location, even one that is legitimately enterprise wide, will involve tradeoffs. For example, it may often make sense to place the privacy office within product engineering, to make it easier to engineer privacy into products and services. However, in this case, a CPO who resides within the product engineering group may have to work harder to exert influence within business groups that have a very different culture and focus, such as marketing or IT. The converse is true as well: An enterprise-wide privacy function, hosted in human resources will have trouble getting attention from engineering. The fact is that in most organizational cultures, there is no absolutely perfect location. Even if the privacy group is positioned as a legitimate enterprise-wide function reporting to the CEO, it runs the risk as being perceived as "corporate" or outside the business. Thus, the goal should be to position the privacy group where it has the greatest reach and opportunity to be effective across the organization. Fortunately (or perhaps unfortunately), there is no wholly right or wrong answer to this question—just a best one for the given circumstances.

Note that the challenges that come with organizational placement are not impossible to overcome. They just require acknowledgment and factoring into the overall change management plan.

Horizontal Privacy Team: Pros

Because the implementation of privacy engineering requires a substantial privacy focus within other functional groups, many privacy professionals find that a horizontal or virtual privacy team structure is more effective than a traditional vertically integrated group. A horizontal structure spans traditional organizational boundaries by building a team of people from different functional groups. Horizontal teams typically use a matrix management reporting structure in which team members report directly to their business groups and also to the CPO (Figure 12-1).

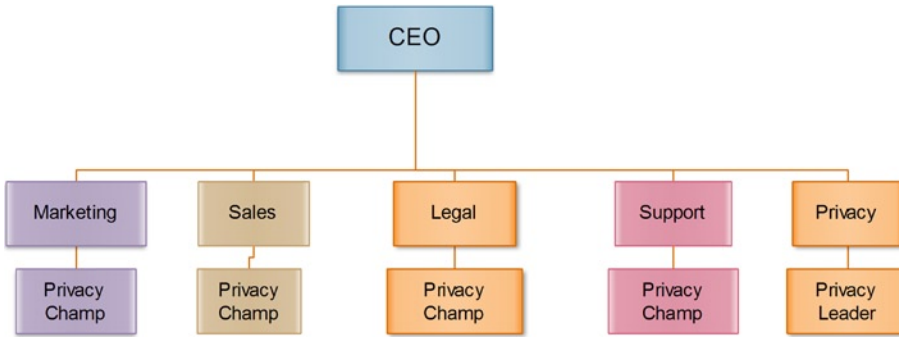

Figure 12-1. *An example of an horizontal organization chart*

A horizontal structure or matrix management reporting structure offers several important advantages. Because team members reside within business groups, they may already have existing personal alliances within the business group, and they may have accumulated valuable domain knowledge. Not only can they leverage these relationships and their knowledge for the good of the overall program, but they can also use it to help the CPO build strong alliances with those groups. In addition, they are ideally positioned to develop a deep understanding of the business group's privacy program needs and to accelerate the group's adoption of a privacy program, ensuring that the program and its goals are aligned. In short, horizontal teams can help ensure that different groups work toward the same privacy goals to the benefit of the organization overall. For example, a horizontal privacy team with members in both marketing and engineering can help ensure both functional groups' leverage and apply the same policies and, where it makes sense, the same tools for handling PI.

One caveat is that horizontal organizations can require more effort from the CPO to manage, coordinate, and guide. It may be harder to make progress on privacy initiatives when team members need to deal with other urgent issues that affect their functional groups. The CPO may need to expend more effort to maintain communication among team members, ensure the team shares information, and gain agreement about how to handle problems. The CPO and the privacy team will also have to learn how to speak to each domain in terms it understands.

Additionally, in this scenario the structure must provide incentives for the people performing the roles to collaborate with other people involved in privacy-related tasks. Sometimes these incentives are provided by a matrix management structure in which individuals report both to a manager in their host organization and to a manager in a centralized privacy office. In other cases, collaboration may be incentivized through goals and objectives within the host organizations.

Horizontal Privacy Teams: Cons

There are some situations in which a horizontal organization may not be adequate. Typically, these are where the risks of a privacy breach are so high that extremely close collaboration among privacy team members is vital to the organization's success. These situations may require a vertically structured privacy team rather than a horizontally

structured team. At a company in a regulated industry, such as banking or health care, a breach involving customer or patient data might jeopardize the future of the entire organization. A colocated privacy team, with all members reporting directly to the CPO, may find it easier to continuously share information in ways that help the team identify additional privacy vulnerabilities or new opportunities (Figure 12-2).

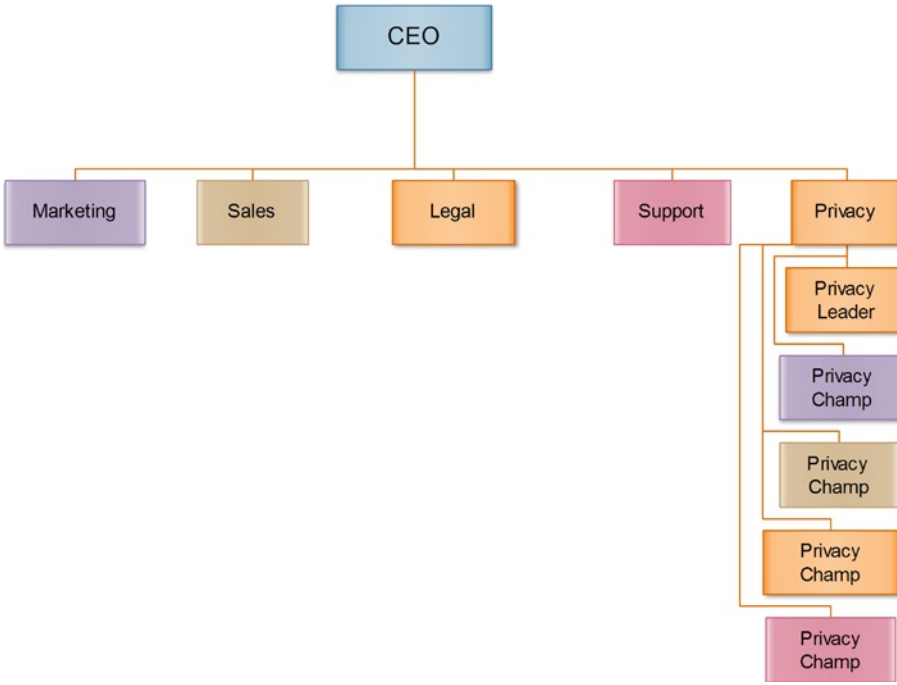

Figure 12-2. *An example of a vertical organization chart*

Common Privacy Engineering Roles

Regardless of the organizational structure, there is a set of privacy roles that typically need to exist in an organization that has embraced privacy and privacy engineering. The following are important roles[1] to consider when defining a privacy organization:

- *Chief privacy officer (CPO):* The CPO carries the responsibility for building a privacy program designed to protect business and personal interests, as well as working with business users and IT teams to identify ways to create value from data.

[1]These are *roles*, not necessarily *job titles*.

- *Privacy architect:* The privacy architect is responsible for designing and implementing process, product, system, and service architectures designed to protect personal information.
- *Privacy engineer:* The privacy engineer uses engineering principles and processes to build controls and measures into processes, systems, components, and products that enable the authorized processing of personal information.
- *Privacy analyst:* The privacy analyst assesses whether processes, products, services, and systems (including third-party vendors and service providers) that process personal information meet privacy policy, standards, and guidelines to ensure that personal information is being processed in a fair and legitimate way.
- *Privacy attorney:* The privacy attorney provides legal analysis of laws and regulations and makes recommendations regarding their application. The privacy attorney also performs the same functions for internal policies, guidelines, and standards.
- *Chief information security officer (CISO):* The CISO is in charge of protecting against security risks related to an organization's information assets, systems, and processes.

In large organizations, each role may be performed by a single dedicated individual. In smaller organizations, an individual may perform multiple roles.

Challenges of Bringing Privacy Engineering to the Forefront

Organizations tend to resist change. Because of this, implementing privacy programs or privacy engineering can be challenging, especially in large organizations. Functional groups across the entire organization, at all levels, must become attuned to privacy requirements and apply consistent principles and policies to its use. Also, they must pay heed and respond to governance models that may not be hierarchal. The following sections outline some of the typical challenges that such privacy initiatives must overcome.

Expanding Executive Management Support

To be effective, any organization-wide privacy program requires support from senior management. Privacy engineering may require an even higher level of executive engagement and sponsorship because it involves designing privacy into the organization's products, processes, and infrastructure. If you don't already have this level of commitment, you will need to push toward this goal. Strong executive support helps ensure funding and provides the privacy team with the authority to implement privacy engineering across the organization. Executive-level commitment also means you'll have more places to turn for help when the inevitable problems arise.

Spreading Awareness and Gaining Cultural Acceptance

Privacy engineering programs often initially face the challenge that many people across the organization have little awareness or understanding of the program's purpose and value. There may be confusion about why privacy engineering is necessary, how it differs from existing efforts to keep information secure and confidential, and whether projects need to involve the privacy team or require its approval. The success of a privacy engineering effort will rely on its ability to work within the existing culture, add value to other groups and functions, and ultimately create understanding and recognition of the responsibility for privacy throughout the organization. These changes may take time and require considerable patience.

Extending Your Reach with Limited Resources

Even with executive sponsorship, privacy programs often operate with limited resources. Privacy engineering places even greater demands on resources because its scope is both broad and deep, spanning multiple functional groups and people at different organizational levels. To maximize its reach and effectiveness, the privacy engineering team may need to creatively evolve new roles within different groups across the organization, as we'll discuss later in this chapter. For the CPO, this creates the challenge of managing a large team of people who are distributed across multiple groups the organization. Keys to success include effective communication, training, and leveraging processes and resources across the extended privacy team.

Creating Alliances

Due to the need to influence the way personal information is handled across the entire organization, any privacy program is likely to require partnerships with key business groups, especially those that use PI intensively. Privacy engineering makes it even more important to identify important partners and build strategic alliances with them, because it will require the involvement of a broader range of people within each group, including product developers, quality assurance specialists, IT professionals, data stewards, and program managers.

Expanding the Scope of Data Governance

Implementing privacy engineering requires that business groups actively participate in the protection of personal information. Some organizations may already have existing data governance programs, as discussed in Chapter 3 and in parts of Chapter 6, including data stewards responsible for maintaining data quality, accessibility, and availability. However, these existing data governance programs often do not consider privacy requirements. The challenge for the CPO is therefore to expand the scope of data governance to include privacy. Data stewards should be a crucial part of the privacy engineering team, ensuring that privacy rules are followed throughout the development process in requirements, specifications, use cases, and metadata.

Remaining Productive Amid Competing Priorities and Demands

The ultimate success of the privacy engineering program depends on continuing to make progress on foundational tasks such as forging alliances, creating program structure, and developing policies. But the privacy team also has to react to day-to-day operational emergencies such as the discovery of new vulnerabilities. With limited resources, it can be challenging to make progress toward long-term goals amid competing demands and priorities. This is particularly the case because privacy roles may be embedded in other groups that have their own pressing business needs.

The use of a privacy component, as defined in Part 2 of this book, can help the privacy engineering team remain productive by reducing the effort required to change privacy rules throughout the enterprise. This will require the privacy team to work with data stewards and data administrators to amend privacy indicators and metadata with the new or changed rules.

NAVIGATING PRIVACY AND GOVERNANCE IN THE HIGHLY REGULATED FINANCIAL SERVICES INDUSTRY

By Janet F. Chapman, Senior Vice Vice President, Chief Privacy Officer and Manager, Compliance Group, at Union Bank

To many, it seems that there are many "cooks in the kitchen" when it comes to privacy. In the financial services sector, this analogy is not far off the mark. Financial institutions frequently have an alphabet soup of federal and state regulators depending on the size of the institution, the actual component (organizational) parts, and the jurisdiction of the federal regulatory agencies. Depending on the charter, the services, and the customer base, a bank may deal with, among others, the Office of the Comptroller of the Currency (OCC), the Federal Reserve Board (FRB), the Securities and Exchange Commission (SEC), the Federal Deposit Insurance Corporation (FDIC), the Federal Trade Commission (FTC), the Federal Commerce Commission (FCC), and the newest, the Consumer Financial Protection Bureau (CFPB). Don't forget to add a dash of jurisdiction under the Health and Human Services (HHS) and its enforcement agency, the Office of Civil Rights (OCR) if the financial institution handles protected health information (PHI) via operations such as lockbox processing. Mix well with the additional global privacy and data security laws and regulations, and we have ourselves a hearty soup.

At the state level, there are also many laws, banking regulators, attorneys general, and departments of consumer protection. For example, in 2013, at the time of writing, there were over 25 state privacy-related laws—in such areas as social media, identity theft and fraud prevention, credit freeze rights, and data breach amendments.

All these laws and regulatory bodies are focused on the protection and proper handling of consumer personally identifiable information, or the industry term "consumer nonpublic personal information" (NPI).

With all this regulatory jurisdiction and oversight, financial institutions have a regulatory governance model in addition to whatever internal governance framework exists within the institution.

Financial Regulatory Focus on Governance

The regulatory examiners are increasingly focused on an institution's internal governance processes in the course of their supervisory activities. Among the components they look for are board and senior management oversight; formal meetings with minutes; evidence of a decision-making chain of command; and review of emerging threats, key issues, and relevant risk factors in the organization.

In relation to privacy and data protection, the financial services industry was first called upon to demonstrate a formal governance process with the enactment of the Gramm-Leach-Bliley Act in 1999 and the subsequent publication of Regulations P (for banks) and SP (for brokerage firms) that included governance requirements for the protection of consumer customer data. Because the law covered the entire financial services industry, all the financial services regulators cooperated to develop consistent guidance via the Federal Financial Institutions' Examination Council (FFIEC).

The FFIEC is a formal council of federal agencies that collaborates to develop regulatory guidance and uniform principles, standards, and reporting forms for the federal examination of financial institutions that is consistent across the various financial services jurisdictions. The FFIEC consists of the FRB, the FDIC, the OCC, the CFPB, the SEC, and the National Credit Union Administration (NCUA).

The FFIEC routinely publishes regulatory guidance on various issues and requirements involving governance. The current version of the FFIEC Guidance on Information Security (*IT Examinations Handbook*) has a chapter devoted to governance.

Governance

"Governance is achieved through the management structure, assignment of responsibilities and authority, establishment of policies, standards and procedures, allocation of resources, monitoring, and accountability. Governance is required to ensure that tasks are completed appropriately, that accountability is maintained, and that risk is managed for the entire enterprise."[2]

The section goes on to address the elements of management structure, responsibilities, and accountability.

[2]FFIEC Information Security IT Examination Standards; July, 2006; page 4

- *Management structure:* This regulation requires the active engagement of the Board of Directors and senior business management. Financial services examiners look for demonstrated discussions by board-level risk committees along with annual approval of an annual report on a financial institution's information security program.
- *Responsibility and accountability:* As stated above, the Board of Directors, or an appropriate committee of the board, is responsible for overseeing an institution's information security program and providing formal approval of the annual program. Examiners are looking to executive management to be aware of the components of the program, be advised of emerging threats and risks, and have an understanding of the action plans designed to address identified issues. Executive engagement and support are crucial, and failure at that level could undermine the entire organization's commitment to security.

More recently, in early 2013, the FFIEC published proposed its "Social Media Guidance," with the final version published in December 2013, which requires each financial institution that engages in social media activities to implement a formal risk management program to provide oversight of all associated activities. As noted in the Federal Register, the Guidance states:

"Components of a risk management program should include the following:

- A governance structure with clear roles and responsibilities whereby the board of directors or senior management direct how using social media contributes to the strategic goals of the institution (for example, through increasing brand awareness, product advertising, or researching new customer bases) and establishes controls and ongoing assessment of risk in social media activities."[3]

Essentially, each bank that uses social media as a channel for communicating with customers and the community must now establish an oversight committee of senior management that reviews the bank's social media program in light of overall strategy and how the program complies with all the requirements of the risk management program. The Guidance expects that banks should address an array of risks, including compliance and legal considerations, payments, consumer privacy,

[3]www.fdic.gov/news/news/financial/2013/fil13056.html?source=govdelivery&utm_medium=email&utm_source=govdelivery

and reputational and operational concerns. The Guidance also requires the ongoing risk management program to identify, measure, monitor, and control the risks related to social media, including:

- Governance structure
- Policies and procedures for employees
- Due diligence process for third-party service providers
- Employee training
- Monitoring and oversight for all postings to proprietary social media sites
- Audit and compliance reviews
- Periodic reporting to the financial institution's Board of Directors or senior management for purposes of gauging program effectiveness.
- Complaint management
- Incident response

The underlying theme in the Guidance is governance, integration with key risk management controls, and senior management awareness and accountability.

Governance Applied to Privacy Programs

Recognizing that, in a regulated environment, the focus on governance is here to stay for the foreseeable future, the next concern is applying it to an individual privacy program inside a financial institution.

Financial institutions frequently place privacy functions within legal or compliance departments, appropriate organizations, given the typical privacy office charter, which provides enterprise-wide direction and support on all matters associated with consumer privacy rules and regulations, as well as risk management. Some privacy functions also have responsibility for overseeing compliance with information security laws and regulations and data breach or incident response programs.

The privacy office is typically responsible for guiding a financial institution in the establishment and implementation of controls to manage privacy risk. The privacy office also serves as the clearinghouse for any privacy-related customer concerns or complaints, policy questions, and implementation of new regulations and engages the appropriate parties within the financial institution to participate and support implementation of relevant initiatives and ongoing programs. Because privacy requirements impact every area within the organization that collects, accesses, or uses consumer data, a broad-based governance model is key to increased awareness and acceptance, as well as successful risk management.

An effective method to accomplish this is the creation of an enterprise-wide privacy governing committee or council. Depending on the scope of the privacy program, the CPO should consider including representatives from all affected lines of business: compliance, marketing, legal, information security, operations, fraud, physical security, the online channel, customer service, corporate communications or public relations, records management, human resources, vendor management, and internal audit. A council composed of a variety of business and risk personnel can effectively bring multiple points of view to assessments of privacy requirements, helping all to understand the core purpose behind a requirement and thereby reducing the risk of "unintended consequences." Unintended consequences can be the result of short-term (quick and dirty), overly onerous, or inconsistent implementations of solutions to privacy requirements. An example of this would be adding all "unsubscribe" requests to a "do not e-mail list" and not simply unsubscribing the person. Although the solution may adequately meet one team's goals, it unnecessarily undermines or jeopardizes the goals or longer-term strategy of another.

A governance committee so designed can provide a forum for communication, help build awareness of data privacy practices and policies, and help integrate proper handling, protection, and use and sharing of consumer data into the everyday business activities of the financial institution. In short, the committee can serve as privacy evangelists as well as help the privacy office to leverage its typically small resources.

In addition to the privacy governing committee, integration with the overall risk management committee structure is important to ensure that a formal escalation route up to the Board of Directors can be demonstrated. Typically, financial institutions' governance models are designed to provide executive management and the board with comprehensive reporting of a full array of risks including compliance and operational risks to ensure awareness of material issues and action plans, regulatory developments, and emerging risks or trends. In addition, executive management and the board must be apprised of regulatory examinations, as well as any findings or regulatory concerns.

As privacy professionals, we have a lot of complexity to manage, and this will likely increase. How we coordinate our internal processes and stay abreast of regulatory and industry changes will make all the difference for us and our organizations.

Best Practices for Organizational Alignment

Some organizational functions are critical to the success of a privacy engineering program, and the CPO and privacy team should therefore invest in building strategic alliances with these functions. The CPO should first seek out those alliances that have the greatest potential, both in terms of meeting the organization's needs and the strength of preexisting personal or business relationships. Alliances should then be prioritized

based on their ability to help the CPO achieve his or her business goals. Often, a few key relationships with other information-intensive groups, such as IT, human resources, and sales, can produce the biggest impact. The privacy team should first invest time in these relationships; other, less-critical relationships can be addressed later.

Aligning with Information Technology and Information Security

Privacy engineering is dependent on IT both for implementing privacy policies (by means of privacy rules, as discussed in Part 2) and for securing data. It is impossible to control access to data stored in IT systems if those systems and their physical environment are not adequately secured. Therefore, it is particularly important that the privacy function is closely aligned with IT and information security. Yet, traditionally, there have often been inconsistencies between privacy policies and the protection provided by IT systems.

Using privacy engineering, privacy and IT teams can work together more closely to reduce the likelihood of such disparities. The CPO and the chief information officer can better align their teams, take advantage of each other's expertise, jointly establish efficient processes, and define IT requirements related to privacy. The result of this cooperation is better protection for the organization as a whole.

Aligning with Data Governance Functions

Ultimately, an organization's privacy strategy is about data governance—how information is managed and used. Therefore, alignment between the privacy and data governance functions is critical to the success of a privacy engineering effort. Engineers, data analysts, business analysts, and system designers should all work with the CPO and privacy team, following the privacy engineering methodology.

An example of data governance structure, based on a structure that we helped a few of our clients establish, is shown in Figure 12-3. The structure is headed by a steering committee, comprised of senior managers from key domains across the organization, which sets data governance direction and strategy. The CPO should be a member of this committee. The steering committee resolves major issues and authorizes solutions—even if those decisions impact organizational structure or project costs and timelines.

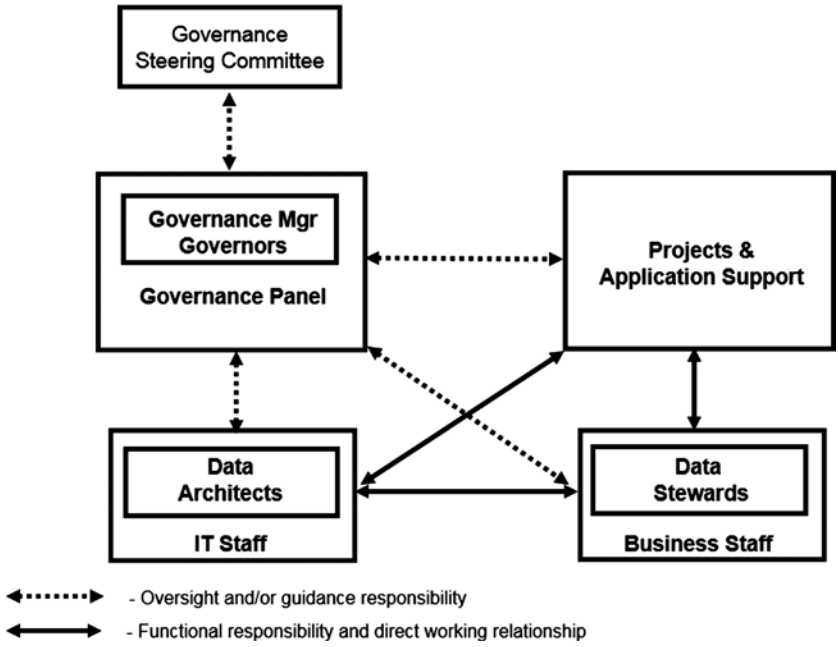

Figure 12-3. *Data governance organization*

The next level of the data governance structure consists of data governors and governance managers, who define overarching data governance requirements based on the strategy set by the steering committee. Below this level are the data stewards and data architects responsible for the day-to-day operational data governance activities required for specific projects. They ensure that the way information is used in these projects is aligned with the overall strategy set by the steering committee. The privacy function is represented at each level of this structure, either directly by one of the CPO's delegates or by ensuring that the person performing each role has adequate knowledge of privacy strategy and principles.

The phases required to create this governance structure include:

- *Gain executive sponsorship*: The CPO works with other stakeholders to build understanding among senior executives of the data governance concept and its value. This helps ensure that executives will agree to be part of the data governance steering committee. Executive backing also is helpful when recruiting people at other levels of the governance structure.
- *Define policies*: As the data governance structure is being established, data governance policies are proposed. These policies define governance rules that are used to create standards and guidelines covering areas such as data management and administration, security, emergency fix procedures, privacy issues, common business definitions, and allowable data values and ranges.

- *Select data governors*: Data governors and governance managers are selected or recruited for each major subject area, such as customer, product, employee, vendor, finance, and human resources. The data governors, who include members of the privacy team, are responsible for the development and implementation of the policies, guidelines, and standards for managing the corporation's data assets.
- *Identify data stewards*: Data stewards, together with content managers, represent the business community. They work with dedicated governance managers to administer data based on business rules. Together with the privacy team, data architects, and data analysts, they manage the data entities and attributes that are used in each project. Data stewards and data analysts share project decisions and concerns at regular data stewardship meetings, which are often held in an agile scrum format. The key data management tasks performed by data stewards include:
    - Creating standard definitions for data
    - Establishing the authority to create, read, update, and delete data
    - Ensuring consistent and appropriate usage of data, including privacy rules
    - Providing subject matter expertise to help resolve data issues

Benefits of Data Governance

Establishing strong data governance delivers a range of benefits to the organization, including:

- Ensuring the effective introduction, implementation, and evolution of architectures within the organization, to guarantee high-quality systems and information that enhance data and privacy protection
- Encouraging reuse of designs, models, information, services, and technology to increase productivity and agility
- Ensuring consistent outcomes and products
- Ensuring that technology investments and capabilities align with business strategy and objectives
- Supporting privacy engineers and data stewards who ensure the quality of information throughout its lifecycle.

ACT TO CREATE ALIGNMENT AND GOVERNANCE

By Richard Purcell, CEO, Corporate Privacy Group

In *Out of the Crisis*, W. Edwards Deming promoted 14 key principles for transforming businesses into effective and efficient engines of success. His principles have been widely adopted by enterprises intent on building reliable and sustainable processes. Principle 13 encouraged businesses to "institute a vigorous program of education and self-improvement." Principle 14 stated "put everybody in the company to work to accomplish the transformation. Every activity and every job is a part of the process."[4]

Deming was focused on optimizing repetitive processes with an engaged workforce to improve efficiency and quality in manufacturing. Putting those principles into action at companies heavily invested in information management requires new approaches. As businesses focused on their digital futures, we developed an education model that adheres to Deming's principles. We call it ACT: Awareness, Communications, and Training. This approach drives understanding of the context, teaches applied skills, and supports empowered employees.

The ACT education strategy is based on learning theories about how information is absorbed, processed, and retained. It starts with building *awareness*, encouraging individuals to recognize beliefs they value and reflect on how their actions support those values.

This is followed by *communications* that stimulate understanding of how individual actions can accomplish specific goals and objectives. Individuals evaluate how their routine activities contribute to the desired transformation of the company, becoming more engaged and involved in the process of self-improvement.

It is critical to then *train* individuals to apply specific skills to their work product, encouraging them to create novel approaches and innovative solutions to challenges. People then learn how to perform a function reliably to achieve the same outcome consistently, greatly increasing effectiveness and efficiency.

For privacy and security, the ACT model creates a foundation of awareness, or context, about how business success and customer trust rely on proper handling of personal information. Detailed information that is realistic and practical leads to a reduction in adverse outcomes, like data breaches. And training individuals to become proficient at specific procedures increases their efficiency and effectiveness in driving business objectives.

[4]W. Edward Deming, *Out of the Crisis*. Cambridge: MIT Press, 2000, p. 24.

The ACT model serves many goals, including regulatory compliance, employee empowerment, process efficiency, and product quality. After more than a decade of employing the ACT model at small and large companies operating locally and globally, each deployment has its own set of stories; here are a few.

Awareness in Action

In the late 1990s, the employees at a large technology company were deeply occupied in developing Internet-enabled products and services. They built web pages, configured web servers, developed backend databases, and generally rushed to utilize this direct communication channel. About that time, the privacy leader developed and released an online privacy awareness course that highlighted principles for collecting, using, and sharing personal information throughout the company. These principles called for transparency through "Notices," individual respect through "Choices," and information protection through "Safeguards" while transferring and sharing personal information. Within 3 months, over 6,000 people had taken the course, connecting their beliefs about fairness, respect, and dignity with the principles in the course. As a result, the privacy office received hundreds of inquiries for more information and guidance. People got it, and they wanted to do something about it. One program manager called the privacy leader to say how much she had learned from the course and how effectively it had created awareness of the issues involved in information privacy. "The only problem," she said, "is that our developer network program, with 27,000 members, doesn't do any of this stuff."

After a long discussion, they decided the program should go dark while they worked on the solution. Over the next 3 weeks, they worked together to develop appropriate notices to the members and choices allowing members to select whether they wanted their information shared with third parties. They developed appropriate policies and protections to maintain control over the information and protect it from unauthorized disclosure and loss. After testing the revisions, the program manager brought the server back online. Immediately, member feedback demonstrated that, although they didn't like being offline for 3 weeks, they appreciated the fact that their personal information was being treated in a trusted way.

Communication in Action

A multinational company had great success in building and distributing personal technology products. Customers registered their purchases, downloaded software updates, bought product accessories, and sought support through the company's web site. Staff in marketing, sales, support, information technology, and other areas all directly collected, used, or managed customer information.

As in many companies, each department was managed with relative independence from the others. The privacy office had been working with each department with what could charitably be called limited success. They struggled with the independent and siloed nature of each.

What they needed was a way to inform each group within the context of each group's language, function, and culture while maintaining a centrally consistent vocabulary and policy framework. Using a communications approach, they developed a single online personal information management course for all the groups.

The privacy office led the development of short online courses for each department with a common introduction. Each module addressed issues specific to the subject department using real-world scenarios. The shared introduction focused on common vocabulary and principles underlying each course's lesson. For instance, the sales group's messaging was about providing notice, the marketing group's was about checking choices, and the database management group's was about running suppression lists. Each was appropriate to its audience, and all audiences got consistent messages.

At the end of 3 months, the privacy office noticed a distinct easing in the way different departments worked together on managing privacy issues. They were sharing a common vocabulary, knew their own jobs within their functions, and recognized the skills that others contributed to achieve the program's objectives.

Short, targeted, and consistent messaging began to link the silos together, and employees were able to apply their efforts to solutions rather than problems.

Training in Action

Don't you just hate it when you have an assignment and no one has told you how to do it? Of course, you try your best to do the task and it might work out. Then again, it might not. All of the awareness and skill development in the world is not going to help when you are given a new task with little or no instruction. It's even worse when several people are all trying in their own way to complete a task and everyone does it differently. The chances that something is going to go horribly wrong for someone are very high.

One multinational consumer goods company discovered how painful this is when the Children's Online Privacy Protection Act (COPPA) was passed in the late 1990s. The act requires that all US-based web sites directed toward children or that know the actual age of children using their sites gain verifiable parental consent before collecting personal information from anyone under 13 years old.

At this company, each product group was responsible for its own web site construction and maintenance. Several marketed children's products like toothpaste, soap, and shampoo, while others marketed products that are not age targeted. Some of the web sites for children's products complied with COPPA, others did not. Although the other product web sites didn't target kids, many of them did collect their users' ages. It was apparent that the COPPA requirements were not part of the web site specifications.

In the end, the company suffered severe reputational damage when the FTC examined all of their web sites and determined that many were out of compliance with COPPA. Following the investigations, negotiations, and fines, the company decided it would be a good idea to train all its webmasters in compliance mechanisms for COPPA and other regulatory requirements.

The privacy office led an effort to develop a single online course that provided detailed instructions about COPPA's requirements and accepted methods of complying. These included age-gating mechanisms, various methods of collecting parental consent, alternatives when consent wasn't available, and even a process to stop collecting age or delete records for those under 13.

In the end, the company was not only able to deploy compliant web sites, but it also provided the compliance training to all its global web operations as a corporate commitment to a single standard for protecting children online.

Business Benefits of Alignment

Greater alignment with key partners can deliver major benefits to the entire organization. Key benefits include:

- *Greater business value from data, with less risk of misuse*: By improving structure and oversight of data collection and management, alignment between the privacy team and other groups helps the organization acquire greater understanding and control over data. The better your understanding of the data, the more value you can derive from its use. Greater control over data use also means there's less likelihood of data misuse or data fatigue.
- *Increased operational efficiency*: Alignment with other groups can eliminate duplication of effort. Without alignment, privacy and information security teams may ask each business group many of the same questions as they seek to understand how the group plans to use personal information. Alignment between privacy and information security means they can create a single set of questions and share the answers. This reduces the effort for each team. It also means less work for business groups, which now need to explain their requirements only once instead of multiple times.
- *Better business decisions*: Cooperation between privacy and other groups enables a broader view of the multiple perspectives and factors that should be considered in business decisions. For example, decision makers can gain a better understanding of the costs, risks, opportunities, and tradeoffs of different approaches for achieving privacy and security goals.

- *Lower cost of developing and deploying products, processes, systems, and applications*: Greater alignment helps identify all privacy, security, and business requirements early in the development cycle. This reduces overall development and deployment costs, reducing the need for costly changes or retrofits. An associated benefit is the reduced risk of impact to development or deployment schedules due to last-minute discovery of unforeseen privacy concerns. The privacy component can lower the cost of privacy rules change management.
- *Reduced risk of privacy or security breaches*: Alignment between privacy, security, data governance, and other functions drives greater awareness of privacy throughout the organization, with stronger data governance and adherence to privacy policies. A broad understanding of privacy requirements helps ensure, for example, that new internally developed systems and third-party solutions receive timely compliance reviews. The increased privacy awareness makes it easier to identify vulnerabilities, reduce the risk of compromise, and recover more quickly if problems occur.
- *Improved brand image and marketing data*: When an organization demonstrates that it employs consistent and clear privacy practices, its brand image is enhanced and users are more willing to honestly share personal information. This information helps the organization build a more accurate and valuable marketing database.

Other Benefits

Alignment can also deliver benefits that are less tangible but equally valuable, while helping avoid common mistakes that lead to inefficiencies or reputational damage. Some of these benefits include:

- *A clearer picture of the organization*: An organization typically contains many information owners, spread across different functional groups, each with its own charter and goals. By aligning, these information owners obtain a clearer picture of others' roles, helping to avoid redundancy, overlap, or confusion. Alignment also creates communication channels that help different groups collaborate to solve problems and identify new opportunities to optimize business processes.
- *Better-understood policies*: Better communication and broader involvement in privacy means policies are likely to be better understood across the organization. This helps create greater accountability. There is less chance that different departments will create conflicting or confusing policies, which can be difficult to implement and result in failed or incomplete controls.

- *A more comprehensive risk dashboard*: Alignment provides the organization with a better view of all the risks associated with the use of data by different groups. It helps avoid redundant or overlapping risk management and compliance activities such as internal audits and investigations. Executives obtain a single unified view containing all the information required to make decisions, rather than having to sift through multiple reports.
- *Avoiding dangerous false assumptions*: If privacy and other groups are not aligned, application developers may believe they understand privacy requirements when in fact they do not. Because of this assumption, the developers may not ask for the privacy team's help in assessing potential risks. As a result, they may design a system with privacy risks that could have been avoided.

Conclusion

It is important to ensure that privacy leadership is well placed within the enterprise. The privacy team must be given serious executive support, strong people resources, robust support of the privacy-oriented roles, and alignment with information technology and with a strongly supported privacy-aware data governance structure. Strong privacy organization management provides business and technological enterprise benefits. The next chapter will discuss the valuation and metrics of our data assets.