

Moving Privacy from *In Place* to *Enhanced*

By Hugh Kominars, CISA, CISM, QSA, ControlCase, and Brian Tretick, CIPP/IT, Athena

Use of governance, risk management and compliance (GRC) tools is necessary for evolution.

An increasingly difficult challenge to manage

Privacy is driven by an increasingly complex and pervasive set of rules and risks, affecting nearly every aspect of the organization. Complexity comes from a vast set of national and local laws and regulations, corporate policies, operational procedures, contractual terms, and service agreements over the use of personal information. Complexity is also derived from the diverse business functions that process personal information, and the information technology used to collect, create, process, store, and transfer the information.

In fact, privacy is an issue in all situations where personal information is handled, from data centers and production systems to third parties and end user devices well outside the control and custody of the organization. This pervasiveness also means that privacy is not the domain of an isolated compliance group, but rather an enterprise-wide concern, spanning research and development, products and services, sales and marketing, information technology operations, human resources, and the third parties with whom the enterprise exchanges personal information. The net result is that privacy has become one of the most demanding business issues faced by organizations today.

With increasing expectations of excellence

It is rare that management would be content with any part of the organization to be run inefficiently or ineffectively. Yet many organizations have yet to evolve Privacy GRC to efficiently and effectively meet the demands of the new decade and the increasing complexity and pervasiveness of privacy. Throughout the financial crisis, organizations focused not only on cutting costs across the enterprise, but also on improving performance of business operations. To be able to address privacy's complexity and pervasiveness, organizations must also improve the performance of their Privacy GRC functions: privacy must be run like a business.

This means that Privacy GRC needs to attain the levels of operational effectiveness embodied by the rest of the business. This means among other things that processes should be formalized, repeatable, and monitored. There are very few Privacy GRC functions that are done only once: if they were, then they might not even have been worth doing at all. Therefore, it is imperative to build Privacy GRC functions that are formalized, repeatable, and monitored. These are expectations of management, shareholders, regulators, and even customers. If you are not at least incrementally improving your Privacy GRC processes, you will be unlikely able to keep up with the increasingly complex and pervasive rules and risks that affect your use of personal information across the extended enterprise.

That drive the need to evolve from *In Place* to *Enhanced*

Most organizations who have addressed privacy to date have at least put Privacy GRC *In Place*; that is, most have done *something* to manage privacy. Investment in Privacy GRC, therefore, should be focused on evolving from *In Place* to *Enhanced*. This is even more critical for organizations with multiple business units, in multiple countries or jurisdictions, or with multiple regulators. *Enhanced* Privacy GRC means that the processes in response to risk and compliance obligations are done well and operate with efficiency. To do this, organizations should:

- ❑ **Formalize Privacy GRC functions.** The Sarbanes-Oxley era ushered in the saying, “If it isn’t documented, it isn’t done.” The saying implied that there was a lack of assurance that something was being done if there was no record of it, and if it was actually done there was little evidence that it was done well and could be done again with a similar outcome. Business functions worth doing are worth documenting. This goes for Privacy GRC functions as well. Therefore, the first objective in moving from *In Place* to *Enhanced* is refining and documenting the supporting processes.
- ❑ **Monitor Privacy GRC functions.** There are several truths relevant to monitoring. The first is, “Anything that can be done can be measured.” In fact, the biggest challenge is taking measurements that matter. That saying is further supported with the following, “That which gets measured gets done.” If you do something but do not measure it, you cannot demonstrate that your Privacy GRC initiatives are in place, complete, compliant or effective. The next objective, therefore, is adding monitoring to Privacy GRC functions, not just at a central point but also throughout the organization where the functions are performed. This monitoring could be performed through administrative procedures, but as we will see with the next objective technology-enablement is fundamental.
- ❑ **Automate Privacy GRC functions.** Dozens of national laws and hundreds of implementing regulations and good practice guidelines affect multinational companies. If you add to that burden the US states, Canadian provinces, industry standards, corporate policies, and contractual requirements, you get more than will fit neatly in a chart or spreadsheet. The key to technology enablement is to automate an effective process. It has been said of automation is that, “Automation applied to an efficient operation will magnify the efficiency, whereas automation applied to an inefficient operation will magnify the inefficiency.” Automation is needed for policy management, risk management, compliance management, incident management, monitoring, and internal control itself, if nothing else but to streamline the non-value added and administratively burdensome activities. The third objective is enabling Privacy GRC functions with technology to support their effective performance and monitoring.

These objectives form a triumvirate for *Enhanced* Privacy GRC. Organizations with a mandate for effective and efficient business processes need to formalize, monitor, and automate the functions in privacy programs and those that operationalize Privacy GRC within the business units themselves.

Requiring a structured view of Privacy GRC

With those objectives in mind, a structured and complete view of Privacy GRC is required. The Athena Privacy Framework offers a method to organize Privacy GRC. It is briefly illustrated below.

Governance Level					
Governance		Risk Management		Compliance	

Control Level					
Policy	Internal Control	Technology Management	Third Party Management	Incident Management	Training and Awareness

Information Level		
Process	Entities	Technology

Starting at the **Information Level** as a foundation, the organization must understand and account for the processes that handle personal information, the entities that perform those processes (i.e., the first, second, third and even fourth parties), and the technology and media used to collect, create, use, store, and transfer the personal information. Without such an understanding, the organization cannot effectively apply controls or govern the use and protection of the personal information.

At the **Control Level**, the organization establishes business rules (e.g., through policies and procedures) over personal information, implements an environment of internal control, manages the technology and other parties involved, manages incidents and other events including those that might be indicative of a breach, and undertakes the training and education of users of personal information.

At the **Governance Level**, the organization establishes the roles and responsibilities throughout the enterprise, identifies and assesses privacy risk, and establishes compliance functions associated with privacy and personal information.

Organizations with Privacy GRC *In Place* will have something in each of the components of the framework. Improvements in Privacy GRC from *In Place* to *Enhanced* will require changes not in what gets done but rather in how it gets done. Formalization, monitoring, and automation are key to evolving to *Enhanced* Privacy GRC.

And requiring the automation of key functions

Using the privacy framework, an organization can develop a comprehensive approach to automating Privacy GRC. With technology enablement in mind, key considerations include the following:

□ Information Level

- **Process.** Cataloging processes that handle personal information.

Many organizations focus on information in databases, servers, and workstations; the purpose for which the personal information is used, however, is key to determining privacy requirements, such as those for notice, choice and consent, subject access, and even process and application controls.

- **Entities.** Cataloging legal entities that handle personal information.
As legal entities are ultimately responsible for complying with privacy laws and regulations, and the nature of the legal entities is a factor in privacy risk. Entities include affiliated (e.g., parent, subsidiary, and peer companies) parties and unaffiliated (e.g., third and even fourth) parties.
- **Technology.** Scanning to discover personal information in networks, databases, servers, workstations, and other user devices.
The presence of personal information can be assessed for its appropriateness, and the protection measures for personal information in the different technologies may be assessed for adequacy.

□ Control Level

- **Policy.** Creating and registering policies, procedures, and guidelines and communicating them throughout the organization.
Policy needs to be in the right hands at the right time. Policy management may automate the communications of policy, acknowledgement and certification to its objectives, and updates and clarifications over time.
- **Internal Control.** Implementing and assessing the effectiveness of process and application controls over personal information.
In fact, without automation of internal control, both implementing it and monitoring it, an organization cannot effectively manage privacy. Many organizations need to move beyond automation of internal control solely for financial process and rather deliberately include the myriad of other business processes that use personal information.
- **Technology Management.** Identifying and managing technology assets and their configurations (e.g., related to vulnerability management).
Many organizations have insight regarding core technology assets but lack coverage of portable devices. As we see personal information being processed more and more in end user devices that are not within the direct control or custody of the organization, technology management becomes an increasingly important element of Privacy GRC.
- **Incident Management.** Managing the lifespan of incidents and other events related to personal information, including discovery, analysis, resolution, communication, root cause analysis, and tracking.
Regulations over incident management and breach notification require effective approaches, which cannot be effective unless enabled with technology for recording facts and decisions, and managing workflow throughout the lifespan of an incident.
- **Third Party Management.** Managing the selection, contracts, engagement, ongoing assurance, and termination of third parties that handle personal information for the organization.
It is difficult enough to manage risk, compliance, and internal control within the organization. Tools, therefore, are critical in managing the processes associated with third parties with which you exchange or who access your personal information.

- **Training and Awareness.** Publishing, communicating, and monitoring privacy-related training programs, including ongoing awareness communications.

Many organizations already deliver some training and awareness through web-based learning tools, email, and intranets. The next step is monitoring progress and measuring the effectiveness of that delivery.

□ **Governance Level**

- **Governance.** Documenting and communicating responsibilities to employees and management, and monitoring performance to those responsibilities as a component of performance management. Reporting on policy and business decisions made related to privacy risk management and compliance.

For many, the first step in improving governance will be formalizing it, especially within business units, and integrating that formalization into role and performance management systems. However, automating governance also involves integrating reviews, decisioning, and authorizations within business processes themselves. Enabling governance with technology, therefore, will involve its integration into other process automation throughout the organization.

- **Risk Management.** Identifying, planning, and assessing privacy risk across the enterprise and in a manner integrated with other enterprise risk management functions.

This aspect of automation often involves applying enterprise risk management and IT risk management tools to specifically address privacy risk. Often the first step is using those tools to discretely address privacy-related risk, whereas more mature organizations will move to integrate privacy-related risk with the management of the other business risks faced by the organization.

- **Compliance.** Managing compliance requirements and correlating them with operational, technical, legal, and administrative controls. Planning and conducting compliance assessments and audits. Implementing technical and process control monitoring, and where feasible continuous controls monitoring.

An initial step to improving the performance of compliance is accounting for the various often-overlapping rules and regulations over personal information. However, real improvement can be seen when those overlapping rules and regulations are correlated so that internal control and monitoring can be rationalized. That rationalization is among the improvements with the highest potential in the effective performance of Privacy GRC.

Addressing these dimensions will help you move to an enhanced posture for managing Privacy GRC across the enterprise.

To achieve *Enhanced Privacy GRC*

Ten years ago, privacy management involved putting key elements of a program in place. Over the past few years, it has been about extending coverage of privacy functions and activities across the enterprise, with better integration with the information technology department and liaisons within various business units. For organizations with

Privacy GRC *In Place* and coverage nearly there, the focus needs to include running the privacy function like you would other parts of the business: effectively and efficiently. A goal for *Enhanced* Privacy GRC in the new decade will require you to begin formalizing, monitoring, and automating privacy now.

About the authors

Hugh Kominars is Vice President of Managed Compliance Services at ControlCase. He may be reached at hkominars@controlcase.com.

Brian Tretick is Managing Director for Athena and a member of the board of directors for the International Association of Privacy Professionals. He may be reached at brian.tretick@athenaprivacy.com.