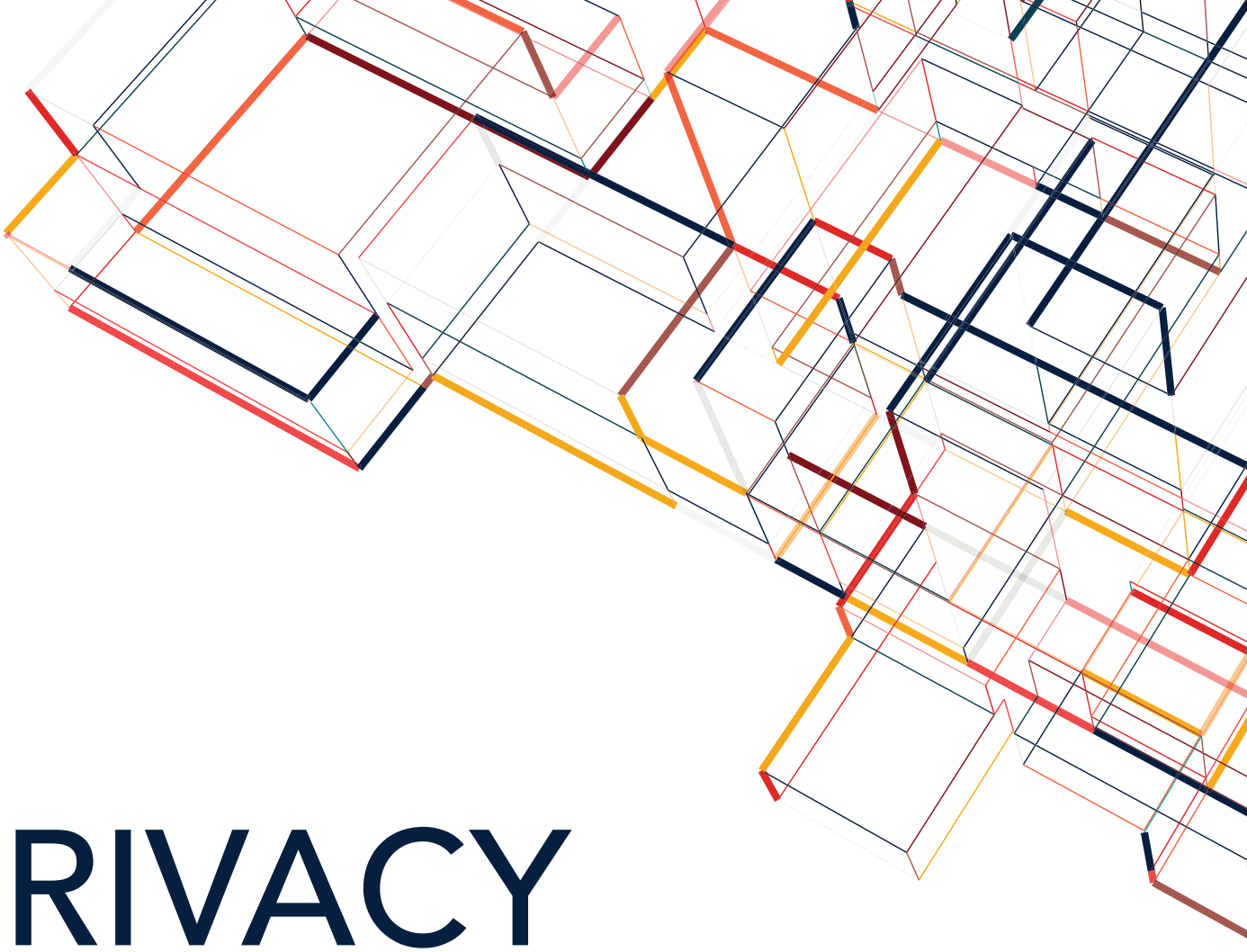


PRIVACY AND DATA PROTECTION

Part 1: Internal Audit's Role in Establishing a Resilient Framework

Pamela S. Hrubey, CCEP, CIPP/US, and R. Michael Varney, CPA, CIA

Crowe

INTERNAL AUDIT FOUNDATION™

Published by the Internal Audit Foundation
1035 Greenwood Blvd., Suite 149
Lake Mary, Florida 32746, USA

The IIA’s International Professional Practices Framework (IPPF) comprises the full range of existing and developing practice guidance for the profession. The IPPF provides guidance to internal auditors globally and paves the way to world-class internal auditing.

The IIA and the Foundation work in partnership with researchers from around the globe who conduct valuable studies on critical issues affecting today’s business world. Much of the content presented in their final reports is a result of Foundation-funded research and prepared as a service to the Foundation and the internal audit profession. Expressed opinions, interpretations, or points of view represent a consensus of the researchers and do not necessarily reflect or represent the official position or policies of The IIA or the Foundation.

ISBN-13: 978-1-63454-075-9
24 23 22 21 20 1 2 3 4 5 6

Table of contents

Introduction and executive summary

Today, virtually every organization with customers, employees, suppliers, or other third-party relationships can find itself subject to a rapidly growing array of specific privacy and data protection requirements. Such regulations can present challenges to organizations in general and pose specific challenges to internal auditors.

These challenges attracted particular attention with the 2018 implementation of the European Union's (EU's) General Data Protection Regulation (GDPR), one of the most prominent recent regulatory actions in this area. In the United States, the Jan. 1, 2020, implementation of the California Consumer Privacy Act of 2018 (CCPA) further complicated the picture. The high-profile GDPR and CCPA are only two of many such regulatory structures that, taken together, create a fast-growing and constantly changing regulatory environment.

Although technological advances are the root cause of many privacy and data protection concerns, it is important to note that these are not exclusively IT issues. Data protection and privacy are cross-functional issues that must be addressed at the enterprise level.

The intent of this report is to assist internal auditors in assessing their current level of preparedness regarding privacy and data protection issues, particularly as their approaches relate to the present state of the profession overall. One component of this self-assessment involves understanding their organizations' current data environments along with potential changes in their approaches to auditing material areas such as third-party relationships and technology.

In addition, the report is intended to help internal auditors understand specific risks and threats and to help them see that relevant controls are developed, implemented, and operated effectively. The framework, audit plan, and implementation discussions in the later sections of this report are designed to provide a foundation on which internal audit departments can build their own structures.

Future steps in this research project, beyond this report, are scheduled to be published over the next 12 to 18 months. These steps will draw on an Internal Audit Foundation member survey and field interviews and examine how internal audit as a profession is responding to data protection and privacy issues. The final phase of the project will examine how privacy officers and other stakeholders view these same issues, with the goal of assessing whether the profession has been successful in meeting the stakeholders' expectations.

1) History and growth of privacy and data protection issues

One of the many consequences of the past few decades' technological revolution has been the emergence of privacy and data protection issues as a critical concern. All types of organizations – public and private, commercial and not-for-profit, local and global – are finding new ways of interacting with customers, suppliers, regulatory agencies, and other stakeholders.

The fuel that drives all these interactions is data. Often, such data is confidential, proprietary, or personal. The need to protect valuable data from theft, loss, or misuse has opened an entirely new area of concern for organizations and an entirely new area of risk for internal auditors to address.

From kilobytes to zettabytes

In many ways, the increased concern over these issues is an inevitable natural consequence of vast market and technological changes over the past 25 years. In 1995, the internet was a 28.8K dial-up modem experience, personal computer desktop mass storage came in 500-megabyte hard drives, cellphones were analog, and people still used pagers. Today, global data storage has reached more than 16 zettabytes (ZB) and is predicted to reach 163 ZB by 2025.[1]

Looking beyond the exponential increase in data volumes, the various ways in which organizations capture and use these increasing amounts of data also have changed dramatically. Questions over who actually owns personal or sensitive data have become more complex as social media and other technology companies face growing scrutiny over how and with whom they choose to share their users' data.

Data ownership questions also are affected by cultural impacts. For example, in very general terms, European cultural outlooks in recent generations have evolved toward the perspective that personal data can be owned only by the individual. This outlook sets up a growing clash between personal rights and perceived organizational ownership of data.

Data-driven new technologies such as the internet of things (IoT) have raised additional new data protection and privacy concerns, as internet-connected security cameras, smart appliances, interactive cable boxes, smartwatches, and other breakthroughs redefine how personal information is used and shared. In 2018, for example, the U.S. military directly encountered some of the unintended consequences of the IoT when analysts discovered that enemies could potentially identify troop locations via GPS-based data from wearable technologies such as fitness trackers worn by military personnel. Consequently, officials were forced to restrict the use of IoT devices by personnel overseas.[2]

The rapidly accelerating deployment of IoT devices adds more urgency to the growing concerns of consumers about the protection and security of their personal data. These consumer concerns, in turn, increase pressure on organizations – and their internal auditors – to address privacy and data protection issues.

In addition to IoT devices, other current technologies are driving even greater concerns about data privacy. Artificial intelligence (AI) and machine learning technologies collect immense amounts of data. By their very nature, they link various disparate data points in ways that offer new insights into individual behaviors and preferences, and they produce information that is inherently personal and private, as one recent online analysis pointed out.[3]

For example, a mobile sales application might use AI technology to track location or internet address data from sales representatives' smartphones and coordinate that information with customers' locations and purchase histories. The patterns revealed by this AI application could help the company and sales reps alike by helping them manage travel, time, and resources more efficiently. But sales reps might be uncomfortable with their employers having visibility into their personal location data, particularly on evenings and weekends.

Complications such as these prompted one analyst, Andras Cser, vice president and principal analyst at Forrester Research, to comment: "AI requires a ton of data, so the privacy implications are bigger. There's potential for a lot more personally identifiable data being collected."[4]

Blockchain, another fast-growing technology, is also highly data-driven, raising its own set of data privacy questions. Blockchain transactions are designed to be immutable and tamper-resistant, since every transaction is visible to all users on the blockchain network throughout all the nodes on the network. Confidential information, even if it is encrypted, could still reveal patterns of transactions that could be used to identify individual users.[5]

Cybercrimes represent another fast-changing aspect of the privacy and data protection landscape. As cybercriminals and their tools became more sophisticated, information technology professionals and organization leaders alike have struggled to stay ahead of the game in protecting information assets, including both proprietary company information and personal data.

Recent high-profile examples illustrate the size and scope of cybercrime-related privacy risks. For example, Facebook has struggled with a series of large-scale data breaches over the past 18 months, including a September 2018 breach that affected 50 million users,[6] an April 2019 breach that publicly exposed 540 million user records,[7] and a December 2019 breach that exposed 267 million accounts.[8]

Facebook is only one prominent example, of course. Banks, healthcare organizations, credit reporting agencies, and retailers of all types and sizes have been attacked in recent years. One research organization, Comparitech, collated 10 years' worth of data breaches across the United States and discovered that, from 2008 through mid-2019, 9,696 separate cybersecurity breaches affected a total of 10.7 billion individual records.[9] Governments and regulators have responded in various ways, some of which are discussed in the next section. In their capacity as the third line of defense, internal auditors have a well-recognized role to play in verifying that their organizations are responding effectively in compliance with legislative and regulatory obligations.

But the risks associated with privacy and data protection extend beyond potential fines and penalties stemming from regulatory noncompliance. Reputational, operational, and business continuity risks also can be affected by the unauthorized use of personal data, data breaches, inadequate notification and consent practices, or other related issues.

As a result, today's internal auditors – and the organizations they serve – must think strategically about privacy and how they maintain and protect sensitive data. For internal auditors specifically, an obvious need exists to verify or provide assurance regarding data protection issues. Yet concurrent with this need is an opportunity for internal auditors to provide additional insights and to lead their organizations toward more proactive approaches to monitoring and addressing these risks.

Defining the issue, defining the terms

Before exploring data protection and privacy issues further, it can be useful to clarify the concept and the terms involved. What exactly is meant by the term "personal data"? Certainly it includes obvious examples such as an individual's name, address, date of birth, and various account numbers. But what about less obvious types of information, such as a computer's IP address or the cookies stored in an individual's web browser?

Europe's GDPR defines personal data as "any information relating to an identified or identifiable natural person ('data subject')"[10] – a definition that is intentionally broad and general because the GDPR is intended to apply to almost any type of information about a particular person. To help clarify, the regulation goes on to say, "an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person."[11]

In simpler terms, personal data is any information that could be used to identify someone. However, deciding whether a given piece of information is actually personal data depends on the context. A good explanation of this distinction can be found in a document published prior to the GDPR by the Information Commissioner's Office (ICO), the independent regulator for data protection in the United Kingdom. The ICO explanation points out:

> A name is the most common means of identifying someone. However, whether any potential identifier actually identifies an individual depends on the context. By itself the name John Smith may not always be personal data because there are many individuals with that name. However, where the name is combined with other information (such as an address, a place of work, or a telephone number) this will usually be sufficient to clearly identify one individual.[12]

Conversely, it is possible to identify an individual without knowing that individual's name. A physical description or some combination of other data – such as age, gender, home address, employment, personal possessions, or online profile – can be used to identify an individual. So even if one piece of data might not appear to be personal data, it could become relevant alongside other data and be used to reasonably establish an individual's identity.

Most organizations collect many different types of information on customers, employees, suppliers, and other stakeholders. Whether these pieces of information should be regarded as personal data depends in part on how they are collected, used, stored, and potentially combined with other information. Ultimately, organizations of all types must be careful with almost any data that they collect or process.

Protection, privacy, and resilience

Data integrity, retention, and availability are all critical features of the overall data security approach. But a security-alone approach to data protection is not adequate.

The cultural issues alluded to earlier – in which personal data is recognized as belonging to the individual rather than to the organizations that acquire or store the data – are now being codified in regulations such as the GDPR, which establish privacy as a fundamental human right. Now, data protection practices must address both keeping data safe and restricting the use of personal data to those areas the data owner (the individual) has specifically allowed.

In other words, organizations are beginning to understand that they essentially borrow this personal data for a specific business purpose and must use it within parameters to which the data subject agreed to in advance.

The concept of data privacy – sometimes defined as "the right to be left alone" – is also changing. Today, data-based personal privacy has become less a matter of invisibility and more a matter of the type of data collected, who has access to it, how data will be used, and how long it will be stored.

Increasingly, individuals are choosing to share their data only with companies that have demonstrated compliance with relevant privacy and data-protection regulations. High-profile data breaches, such as social media sites collecting and sharing users' personally identifiable information with research consortiums and other companies, demonstrate how information can potentially be shared without the data owners' knowledge or consent. They also serve as reminders to consumers of risks associated with the unauthorized use of their personal data.

Employers, too, are finding they must align their operational practices to data protection principles. Because connecting personal devices to company networks can expose employers to a measure of risk, it is becoming increasingly commonplace for organizations to require employees to sign acceptable use policies that either greatly limit or completely eliminate their personal privacy rights while they are using personal mobile computing devices on company networks. At the same time, employers need to consider their employees' privacy-related expectations as afforded to them under the GDPR and other data privacy regulations.

To put it another way, privacy cannot exist without security, but security can exist without privacy, which is not an ideal situation from the perspective of the organization or the employee. With the continued advance of technology, organizations and individuals must increase awareness and knowledge of data protection, data threats, and the steps required to provide security and privacy while still maintaining appropriate and effective business practices and relatable social media interactions.

Privacy and data protection no longer represent just a security challenge. In fact, security alone is not enough. Privacy, like security, must be integral to the organization's culture. The objective is to combine privacy- and security-related thinking into a comprehensive approach that brings security and privacy professionals together for the common goal of overall data protection.

In today's environment, with emerging regulations and standards on the one hand and evolving consumer and stakeholder expectations on the other, a growing number of forward-looking organizations are focusing on the concept of resilience as a critical attribute in their data protection and privacy programs.

"Resilience" might not be the word that first comes to mind when considering how to approach privacy and data protection issues. However, it does address many of the relevant challenges in the sense of being able to absorb and adapt to new requirements without having to start over from scratch or redo compliance efforts.

Dictionary definitions of resilience refer to concepts such as toughness and elasticity as well as the capacity to recover quickly from difficulties. In the context of privacy and data protection practices, toughness is not necessarily the most critical attribute, but the other aspects of resilience – elasticity and fortitude – certainly are. Organizations will need both in order to adapt quickly as regulatory requirements, stakeholder expectations, and technology itself continue to evolve.

Internal audit, for its part, will need to demonstrate those same qualities as it works to validate the effectiveness of resilient data protection measures. Contemporary research by The IIA and related organizations (described in more detail in Section 3 of this report) reveal that internal audit professionals increasingly regard data privacy and related issues as leading risks they must address. At the same time, however, these issues also create valuable opportunities for internal auditors. In addition to providing assurance on the effectiveness of data protection and privacy programs, internal auditors also can take a proactive role in helping to enhance their organizations' ability to be resilient and remain effective as risks continue to evolve.

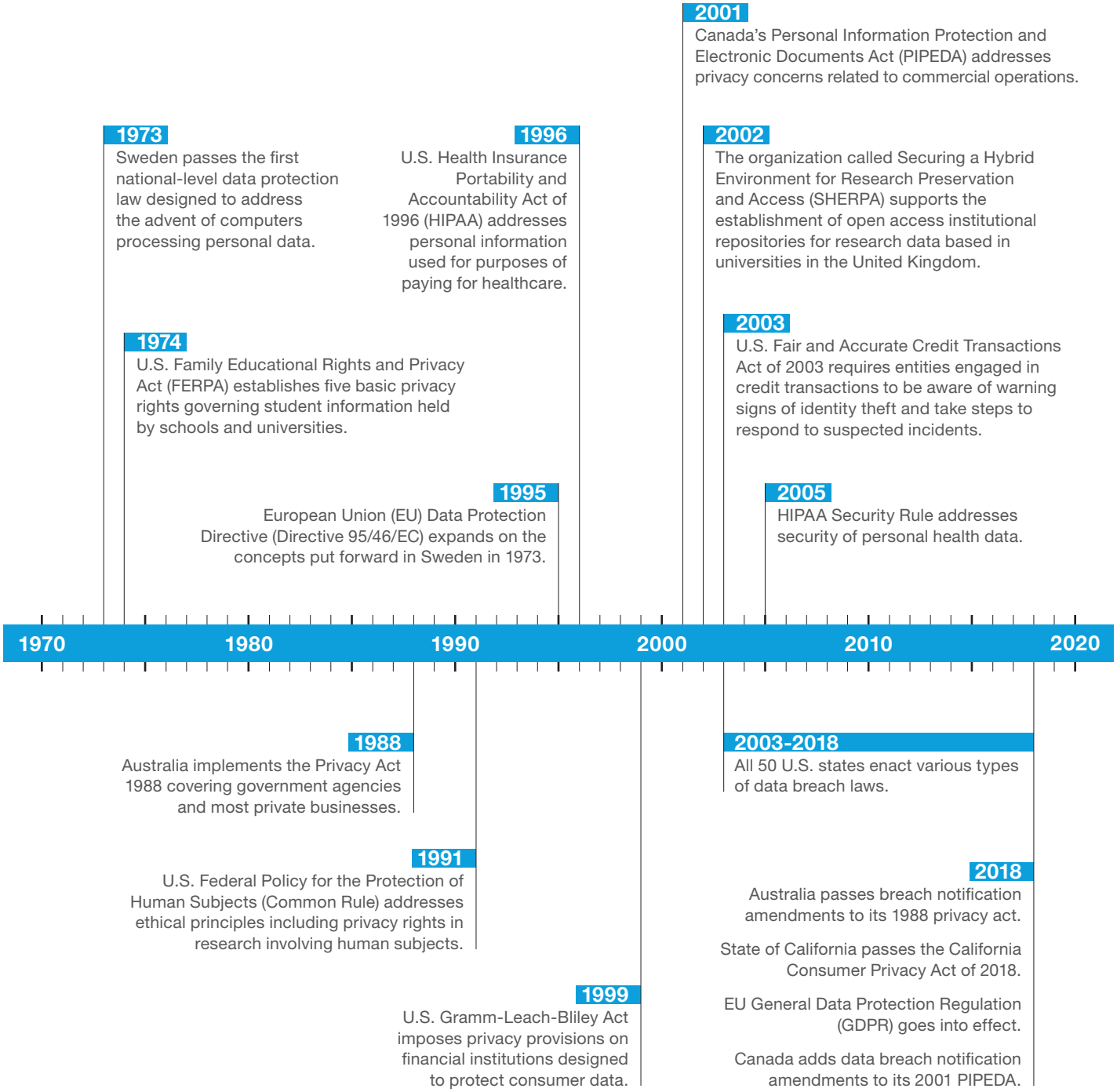
2) Regulatory context, compliance, and other risks

The landscape for privacy and data protection is becoming more complex, as regulatory agencies at various levels of government and in various geographic locations continue to increase their data protection activities in an effort to protect the security and privacy of data subjects. Today, virtually every organization with customers, employees, suppliers, or other third-party relationships in virtually any jurisdiction can find itself subject to a growing array of specific privacy and data protection requirements.

Evolution of the regulatory environment

The high-profile GDPR, discussed later in this section, is only one of many comparable regulatory structures that are either already in effect or currently under consideration. Since the earliest days of digital data, nearly 100 countries and all 50 U.S. states have enacted laws intended to protect personal data (Exhibit 1). Although many states do not yet have privacy-specific regulations, virtually all have implemented regulatory requirements regarding the handling of data breaches. Like the GDPR, many of these are comprehensive laws with effects that are felt far beyond their individual jurisdictional boundaries.

Exhibit 1: Evolution of privacy and data protection



Note: Examples only; not intended as a complete list
Source: Crowe analysis

GDPR: A brave new world?

Among the many new regulatory structures governing the protection and privacy of personal data that have been passed over time, the EU's GDPR clearly is the most prominent in recent years. Replacing the 1995 Data Protection Directive, the GDPR became effective in 2018. It introduced multiple data privacy and security requirements for organizations that process the personal data of citizens of all EU nations.

The GDPR applies to any organization that processes the personal data of EU citizens and residents or to any organization that provides services to individuals while they are in the EU either as residents or visitors. Organizations in any industry or sector, including both for-profit and not-for-profit organizations, are within the scope of the regulation, whether they are physically located or operating in the EU or merely selling goods and services to EU residents. Note, however, that the selling of goods or services to EU residents triggers the GDPR only if that selling is purposeful – that is, if the goods or services are marketed specifically to those individuals. The mere act of someone in the EU making a purchase from a U.S.-based website does not automatically trigger application of the GDPR.

As noted earlier, the GDPR's definition of personal data covers any information about any "identified or identifiable natural person," including factors specific to an individual's "physical, physiological, genetic, mental, economic, cultural, or social identity."[13] This is an important expansion of the previous EU Data Protection Directive.

The GDPR requires organizations to respect an individual's choice regarding how his or her personal data is handled. Consent documentation must be written in language that is easily understood, and it must describe what personal data will be collected, how it will be used, and how and where it will be shared. In addition, a confirmed data breach must be reported to relevant authorities within 72 hours.

To comply, many organizations have had to develop new processes for notification, consent, and data collection, or significantly upgrade their existing processes. It is important to recognize that the GDPR's impacts were felt enterprisewide in the organizations affected, and that they certainly were not restricted to IT departments alone.

Other pending global developments

Outside the EU, many other countries also are restructuring their data privacy regimens. In Brazil, for example, the previous data protection legal framework, which contained conflicting elements for various sectors of the economy, had not been widely enforced. After years of effort, a new General Data Protection Law was passed in 2018 and goes into effect in 2020.

The new law draws many concepts from the EU's GDPR, but it also adds other particulars. Any foreign company that offers services to the Brazilian market and collects any personal data of data subjects located in Brazil will be subject to the new law, regardless of whether it has a physical presence in the country.

While many expect that the new Brazilian data protection law eventually could serve as a model for other Latin American countries, the situation is far from consistent across the entire region. On the South American continent, for example, only two countries – Argentina and Uruguay – have implemented general data protection laws that are accepted by the EU as adequate, so that personal data of EU residents can flow freely between them and EU member states.[14]

Colombia is generally recognized as an evolving data privacy regime with a strong regulator. In fact, two fundamental personal data rights – the right to privacy and the right to data rectification – are written into the country's constitution.[15] Mexico passed comprehensive federal data protection laws in 2010 and 2017, and the government's executive branch has issued four additional regulatory documents or guidelines in recent years.[16] Four other countries have data protection laws covering only certain sectors of the economy, and one country has no data protection law at all.[17]

With such a patchwork of regulatory schemes, organizations that have interests across Latin America find that data protection compliance presents a severe challenge to their security and data teams, as well as to the internal audit groups that review their efforts and results.

The data protection landscape is equally varied in Asia. India, for example, was involved in a contentious debate over its first comprehensive data protection law, filling what many have considered a serious void, particularly in view of the country's very active technology sector. The debate over the bill's particulars lasted for several years, but on Dec. 4, 2019, the Union Cabinet cleared The Personal Data Protection Bill.[18] This longstanding debate is generating challenges for many businesses that wish to move back-office capabilities offshore to India but find that Europeans and many multinationals object to their data processing activities being handled there in the absence of a strong and comprehensive data protection regulatory structure.

Until recently, China's data privacy framework was composed of various laws and sector-specific regulations. In 2017 and 2018, however, Chinese consumers began pressing for more specific privacy rights in response to several high-profile controversies involving the use of personal data by social media and internet companies. In late 2018, China's National People's Congress announced that a new personal data protection law was officially on the agenda for the next term of the legislature. Meanwhile, while the new law is being drafted, the nation's highest administrative internet regulator issued new guidelines that provide some indication of the future direction of the new law.[19]

Japan recently updated its data protection law, bringing it closer to the GDPR standard. In early 2019, the Japanese government adopted certain supplementary rules that apply only to data transferred from EU nations.[20] In South Korea, personal data is protected by a comprehensive general data protection law as well as by several sector-specific laws. Amendments to technology-sector regulations went into effect in 2019, and several bills revising other data protection laws are currently under review.[21]

U.S. data protection regimes

Within the United States, the majority of states have issued data protection regulations over the past 15 years, but most are focused on addressing data breaches. While many states' laws share some common elements, they can best be described as a virtual patchwork of individual regulations. As a practical matter, compliance generally requires analyzing their requirements individually on a state-by-state basis.

Moreover, in addition to requiring businesses to implement data security practices when handling personal information, 11 states go further, requiring businesses to also incorporate data security provisions into their vendor agreements.[22] Similarly, some states have implemented laws that address data privacy issues in specific industries, but only a few have developed broad data privacy initiatives that apply across all sectors of the economy.

California has begun to address privacy on a broad scale with the California Consumer Privacy Act of 2018 (CCPA), which generally is regarded as the most comprehensive approach thus far. The CCPA, which went into effect in January 2020, is sometimes referred to as the GDPR of the United States, primarily because both are comprehensive and far-reaching. But this comparison overlooks many important differences in the two structures.

Like the GDPR, the CCPA requires compliance from many organizations based in other states and countries. In the case of the CCPA, any organization that obtains personal information on 50,000 or more California residents annually, has annual gross revenues in excess of $25 million, or derives the majority of its revenue from selling California resident data must comply.[23]

The GDPR and CCPA differ in many important respects, starting with such fundamentals as basic terms and definitions. Unlike the GDPR's broad and somewhat all-encompassing definition of personal data, the CCPA defines "personal information" (not "personal data") very explicitly, including a lengthy list of specific examples. It also lists information that is explicitly excluded from the term.[24]

Under the CCPA, California residents have the right to request a record of their personal information held by an organization, to have that personal information erased, and to object to the sale of their information. When requested, organizations also are required to provide information on how the data is used and with whom it is shared. In addition, the law outlines a series of proactive steps organizations must take including establishing verification processes, obtaining express opt-in consent, and complying with extensive notification and documentation requirements.[25]

Risks beyond compliance

With potential penalties in the thousands of dollars for each violation, organizations subject to the fast-growing array of data protection and privacy regulations can find themselves facing significant financial risks if they are found to be noncompliant – even if their compliance relates to regulations of which they were not aware. But fines and financial penalties are only one of the potential risks that can result if organizations fail to comply.

In many cases, privacy and data protection regulators can order a halt to the international transfer of data until remedies are made. They also can compel organizations to seek external assistance to comply with their regulatory structures.

In addition, because confirmed violations of these requirements often are announced by a well-publicized press release, the reputational damage associated with noncompliance can be significant and long-lived. Regardless of whether the organization is the perpetrator or merely the victim of a data breach or theft, it faces significant liability if it fails to follow the various notification and mitigation procedures that apply to stakeholders in various jurisdictions.

Looking beyond individual data privacy issues, organizations also must recognize the operational and financial risks associated with data breaches that jeopardize mission-critical or other proprietary business information. The theft or irrevocable loss of research results, proprietary formulas, or critical operational data can expose an organization to existential risk, ultimately raising potential business continuity issues and concerns. These various risks – from financial to existential – all merit careful attention from internal audit.

3) Data protection issues and concerns for internal audit

In view of the vast sweep and broad impact of privacy and data security issues in today's organizations, the risks associated with data protection have become topics of major concern in the internal audit profession.

Internal auditors' views of the issues

Cybersecurity and data privacy were by far the leading concerns of European audit professionals who participated in the newly released "Risk in Focus 2020" survey. The study was published in September 2019 by a consortium of European internal auditor institutes representing professionals in the United Kingdom, Ireland, Germany, Belgium, the Netherlands, Spain, Sweden, France, and Italy.

More than three-quarters (78%) of the European respondents listed cybersecurity and data security among the top five risks their organizations currently face.[26] This was the third year in a row in which data protection-related issues were the auditors' leading concern.[27]

In releasing the data, the report notes that an estimated 59,000 personal data breaches took place across Europe in the first eight months after the introduction of the GDPR. According to the report, cybersecurity is "the perennial risk of the modern era,"[28] and predicts "an ongoing convergence between cybersecurity and data protection/privacy risk."[29]

The European consortium's survey data is consistent with the most recent global findings by The IIA. The organization's new publication, "OnRisk 2020," combined both quantitative and qualitative surveys of internal audit professionals as well as the viewpoints of board members and C-suite executives.

This analysis revealed that cybersecurity, data protection, and data ethics were among the top risks perceived to affect organizations in 2020. The report found that "cybersecurity and data and new technology represent critical knowledge deficits" on the part of those engaged in risk management functions – including internal audit. Further, it stated that "(l)ow reported knowledge and high relevance of these risks suggest risk management players should prioritize building knowledge in these two key risk areas."[30]

Where internal audit and data protection intersect

Internal auditors' efforts to provide insight and assurance on the risks associated with privacy and data protection clearly are complicated by the ever-changing risks and priorities associated with these topics. Today's privacy and data protection programs and the internal audit functions that are charged with monitoring them must be resilient and adaptable. They must be effective in the current environment while also proactively anticipating as-yet-undefined future risks and conditions.

Building an effective privacy program can be daunting. The sheer number of processes involved, the numerous places and ways in which data is used, the nonconvergent regulatory requirements, and the sheer size of the task can be overwhelming. This environment creates risk for the internal audit function as it works to assemble the necessary resources to understand the issues and address its role as the third line of defense. At the same time, however, this environment also opens opportunities for internal audit to add value to the organization by operating in a consultative capacity.

A robust and proactive internal audit program is inherently risk-based, focusing on the organization's perceived highest risks first. In the data protection and privacy arena, organizations must provide a structure to identify the highest-risk data and track how it is used. Focusing on the highest-risk areas first will then enable the organization to confront a broader range of important – and even strategic – questions relating to the use and protection of personal data, such as:

- What are the areas of greatest risk? Looking beyond the proprietary business information that all organizations consider high-risk, what is the highest-risk or most sensitive data held by the organization in terms of users' personal information?
- How can the organization develop a strong privacy program that is proactive, anticipating the potential for privacy failures and working to prevent them in advance, rather than detecting them afterward?
- How can the organization establish a data protection foundation that is strong, resilient, and able to absorb the impact of new regulations without having to redesign the entire data protection program from the beginning?
- How can work processes be revised so that the protection of data subjects' privacy is the default position, rather than an additional step?
- How can privacy protections be built into IT systems?
- What steps can be taken to adopt privacy by design without trading away needed functionality?
- What steps will the organization take when privacy regulations preclude continuing use of a specific functionality?
- How can privacy-by-design requirements be extended throughout the life cycle of a process or system?
- Is there an expectation gap between auditors' and privacy officers' priorities and concerns?

Internal audit departments also should be ready and willing to reflect on their own roles and performance. Critical questions to ask themselves include:

- How can internal audit respond quickly and efficiently without causing undue pressure on the organization or extreme additional cost?
- Beyond verifying compliance with requirements, what else can internal audit do to provide additional accountability and openness?
- What role can internal audit play in helping to create awareness within the organization regarding data privacy, data integrity, and data accessibility issues? How can internal audit help to raise management accountability in these same areas?
- What role should internal audit play in protecting data?
- From a compliance perspective, how much is internal audit itself exposed?

The 10 generally accepted privacy principles

One way organizations can begin to address such questions is to adopt a resilient framework for privacy and data protection. The various general and industry-specific cybersecurity frameworks – such as the NIST Cybersecurity Framework, developed by the U.S. National Institute of Standards and Technology, or ISO/IEC 27000, published by the International Organization for Standardization and the International Electrotechnical Commission, to name only two examples – offer a foundation for quickly responding to and recovering from data leaks, breaches, and other issues. In January 2020, NIST went a step further, releasing Version 1.0 of its new NIST Privacy Framework, which it describes as "a tool for improving privacy through enterprise risk management."[31]

In addition to NIST, a growing number of organizations have come to recognize the importance of going beyond basic data protection protocols and are working to address issues of data privacy specifically. In doing so, many of them look to the 10 generally accepted privacy principles (GAPP) developed by the American Institute of CPAs (AICPA) and other organizations as a model for developing a specific privacy framework (Exhibit 2).

Exhibit 2: AICPA generally accepted privacy principles

1. **Management.** The entity defines, documents, communicates, and assigns accountability for its privacy policies and procedures.
2. **Notice.** The entity provides notice about its privacy policies and procedures and identifies the purposes for which personal information is collected, used, retained, and disclosed.
3. **Choice and consent.** The entity describes the choices available to the individual and obtains implicit or explicit consent with respect to the collection, use, and disclosure of personal information.
4. **Collection.** The entity collects personal information only for the purposes identified in the notice.
5. **Use, retention, and disposal.** The entity limits the use of personal information to the purposes identified in the notice and for which the individual has provided implicit or explicit consent. The entity retains personal information for only as long as necessary to fulfill the stated purposes or as required by law or regulations and thereafter appropriately disposes of such information.
6. **Access.** The entity provides individuals with access to their personal information for review and update.
7. **Disclosure to third parties.** The entity discloses personal information to third parties only for the purposes identified in the notice and with the implicit or explicit consent of the individual.
8. **Security for privacy.** The entity protects personal information against unauthorized access (both physical and logical).
9. **Quality.** The entity maintains accurate, complete, and relevant personal information for the purposes identified in the notice.
10. **Monitoring and enforcement.** The entity monitors compliance with its privacy policies and procedures and has procedures to address privacy related complaints and disputes.

Source: https://iapp.org/media/presentations/11Summit/DeathofSASHO2.pdf

These 10 principles provide a generic foundation on which all risk players can build a resilient privacy and data protection program, including an audit plan framework and methodology that addresses the specific associated risk issues. Compared to the more technical cybersecurity standards, the GAPP structure also provides a simpler, more accessible way to get started on developing a privacy foundation.

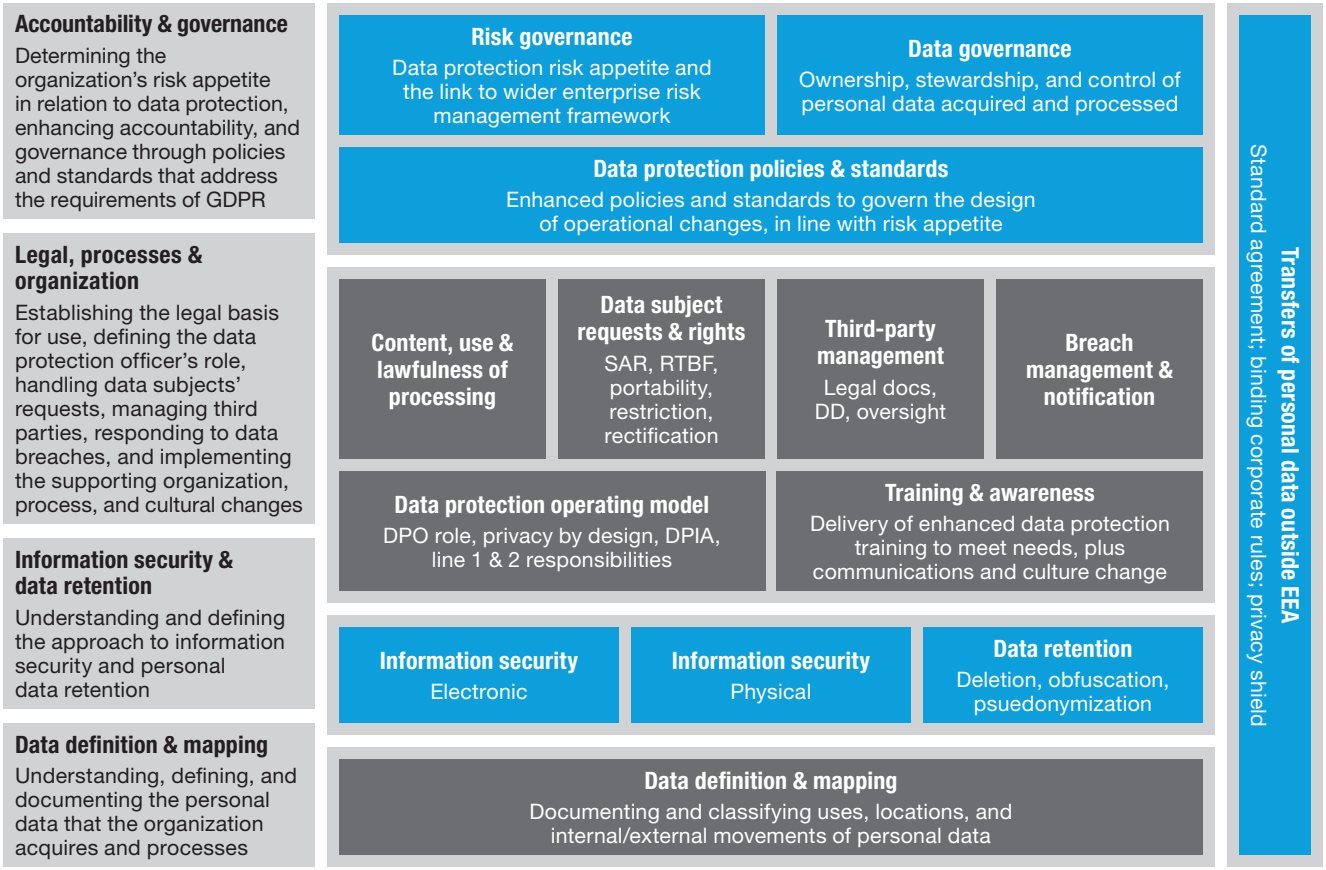
4) A framework for addressing data protection resiliency

As noted earlier, the process of developing and implementing a robust, resilient, risk-based privacy program can be a difficult challenge. The 10 GAPP principles can provide a grounding and foundation, and the various cybersecurity frameworks can serve as a template for development. However, most organizations ultimately find it necessary to deploy a specific privacy and data protection framework to provide structure and direction.

Framework components and structure

Exhibit 3 offers one example of how such a framework could be structured. In this example, the framework is designed to address the critical elements that must be considered as part of an effective privacy and data protection program. This framework includes spelling out the necessary accountability and governance structures, the legal and organizational issues that must be addressed, and the crucial data security and data management functions that are integral elements of an effective privacy and data protection program.

Exhibit 3: Privacy and data protection framework example



Source: Crowe analysis

Internal audit's role: An integrated approach

Internal audit has a critical role to play in helping to develop and apply such a framework. In doing so, internal audit also is likely to encounter important opportunities to add value to the organization.

As is typically the case, the process can be more efficient – and the privacy and data protection program ultimately will be more effective – if internal audit teams with other stakeholders throughout this process. Communication, coordination, and integration among the various stakeholders are particularly important in the early phases of the process, when risks and opportunities are being identified and initially assessed.

5) Implementing the framework and auditing compliance

Developing and implementing a privacy and data protection program – and then auditing compliance and effectiveness – initially can seem like an overwhelmingly complex and intricate process. Like all complex initiatives, however, the effort becomes more manageable when it is broken down into steps.

Suggested implementation and audit methodology

As illustrated in Exhibit 4, the first of these steps is the selection of the privacy and data protection framework itself. Choosing a relevant and appropriate framework, such as the model framework depicted in the preceding section, provides initial structure and organization for the effort, providing a basis for defining the scope and communicating the procedures being executed. Beyond that, it also establishes an assessment and communication format that can be used throughout the initiative, both to link and clarify program requirements and to report audit findings regarding overall implementation effectiveness.

Exhibit 4: Program implementation steps

1 Identify a relevant privacy framework.

- Choose a framework that maps multiple regulations.
- Use the framework to create a common language between internal audit and key stakeholders.
- Link together regulatory requirements, relevant business risks, and accepted privacy procedures and align them to implemented controls.

2 Assess the organization's privacy-related risks.

- Identify the critical types of data collected or maintained by the organization, such as trade secrets and employee data for a manufacturer, or customer and employee data for a financial institution.
- Evaluate where and how the organization does business – domestically, regionally, or globally.
- Highlight areas of highest risk, as identified through the chosen privacy framework.

3 Use the risk assessment results to develop an audit plan.

- Define scope.
- Communicate risks driving the decisions.
- Spell out how the procedures to be executed will help support conclusions and drive impactful recommendations.

4 Execute the defined internal audit plan.

- Communicate findings using the established framework, allowing stakeholders and process owners to see the link between identified risks and mitigating controls.
- Identify exceptions, specifying both conditions and cause.
- Make recommendations for remediation or corrective action.

5 Monitor management's completion of corrective actions.

- Use the framework to develop a picture of the desired state compared to the current state.
- Provide a visual image for stakeholders and process owners to identify relative levels of appropriate control.

Source: Crowe analysis

The second step is to execute the project risk assessment to define the organization's true privacy and data protection risks, recognize stakeholders with whom to collaborate, and identify relevant process owners. Essential questions to be answered include:

- What are the critical types of data collected or maintained by the organization?
- In what jurisdictions does the organization operate?
- Is there a structured approach to data privacy that addresses issues such as training, governance, and ownership?

The results of the risk assessment should highlight the areas defined as higher risk and be used to carry out the third step: developing the audit plan and clearly defining the scope. In some organizations, the first year's assessment is used to identify areas to be enhanced or further developed in future periods. Other organizations might choose to focus primarily on the data mapping procedures in the first year, in order to provide assurance that the approach and results were complete and sustainable. This understanding can then enable the organization to identify relevant data and implement appropriate control activities.

The fourth step is to execute the internal audit plan and communicate results using the chosen framework to provide a clear link between the identified risks and the expected controls. For example, assume for a moment that the initial audit scope was focused on assessing completed data mapping activities, and the audit determined that not all critical processes were included in the organization's data mapping activities. This finding should be clearly communicated in a way that identifies:

- Criteria (all critical processes that were considered)
- Condition (a process that was not considered)
- Cause (why the process was not included)
- Consequence (quantifying the impact in financial terms)
- Corrective action (what and when, including management's agreement to remediation)

An example of such a communication in the audit report might read as follows:

> During execution of procedures, it was noted that process activities relating to warranty management were not included during the execution of the organization's data mapping. Not including this process within the data mapping execution could result in the organization not fully identifying data that is being obtained, maintained, and used. Failure to identify this data limits the organization's ability to determine if data is being maintained per data retention policies, if additional consent controls need to be applied for customer-touching data, if applicable data security measures are being applied, and if personally identifiable data is being obtained. This exposes the organization to increased risk of incurring fines and penalties for regulatory violations, as well as reputational risk as a result of such violations.

The audit report comment also should include a recommendation for corrective action.

The comment's completion would then drive the fifth step of the methodology: monitoring management's completion of defined corrective actions and providing a risk analysis related to privacy and data protection. Applying a simple color-coding scheme to the framework provides a visual image of those areas that are not appropriately controlled (red), those where partial control has been achieved (yellow), and those found to be appropriately controlled (green). Those elements not considered to be relevant areas of risk (such as cross-border transfers in a purely domestic organization, for example) could be coded blue.

In this way, as the organization begins addressing critical elements and moves toward greater resilience, the framework can provide a clear and intuitive method for visualizing, tracking, and communicating progress toward greater program maturity and improved control effectiveness.

Case study: Applying the privacy framework

A company focused on the development and sales of high-end trucking parts (such as specialty lights, custom grilles, and in-cabin sleeping accommodations) had been in business more than 30 years as a B2B-based entity operating across North America. A proposed acquisition by a major over-the-road trucking company was expected to result in a combined entity with an estimated $2 billion in annual revenues.

Management was excited about the combination of these businesses, in large part because of the potential revenue targets in the trucking parts business. But from a long-term perspective, management also saw potential opportunities in combining the customer sales data with other available databases, including typical driver travel routes, other trucking company acquisition targets, and other relevant data.

During a review of the transaction with the board, one of the directors inquired about the privacy-related implications associated with combining information in the way the company had planned. After discussion, the directors recommended that the chief audit executive conduct an audit on the present state of privacy and data protection in the newly combined company.

By using the framework and internal audit approach outlined here, the audit executive was able to establish a clear plan outlining:

- The critical elements to be addressed, such as data governance regarding driver routes and customer sales
- Necessary consent requirements including communication to customers on how data will be used
- A clear reporting mechanism to report results back to the board

Using a risk-based approach aligned to the relevant business goals outlined as part of the acquisition, the chief audit executive was able to help management identify and quantify the relevant risks and develop appropriate risk mitigation efforts that could support and expedite the planned acquisition.

Conclusions and additional research

Today's rapidly evolving regulatory environment, coupled with continued advances in data technology and growing awareness of privacy and data protection issues, poses specific issues for internal auditors. The urgency of these issues is reflected in concerns expressed in recent surveys of the internal audit profession in both the United States and Europe.

In virtually all instances, successfully addressing data protection and privacy concerns will require a cross-functional effort with coordination across various departments and functions within the organization. Internal auditors, for their part, can begin taking a more proactive role in this area by assessing their own level of preparedness within the context of their organizations' current data environment.

The framework and implementation methodology outlined in this report represent one approach that has been successful in helping organizations develop and execute relevant controls for managing and mitigating data privacy-related risks. However, as both the technological and regulatory environments continue to evolve, organizations in general – and internal audit departments in particular – will need to be able to adapt quickly to changes in stakeholder expectations.

In the coming months, the authors of this report will continue assessing the profession's response to these issues. The next phase of this planned research will include a member survey of Internal Audit Foundation members and additional findings from informal case studies and field interviews. The goal of this second phase is to assess how the profession is responding to the ongoing challenges, with a report on the research findings to be published by late 2020.

The third phase of the research project, to be completed early in 2021, will report on how various stakeholders view data privacy issues and, above all, how they perceive internal audit's role and performance in this area. Specific issues, concerns, and examples from current literature will be augmented by relevant comments from field interviews with privacy officers.

The ultimate objectives are to report on how internal audit professionals in various settings have responded successfully to privacy and data protection concerns and to examine how stakeholders' perceptions of privacy and data protection issues align with these efforts to gauge whether the profession has been successful in anticipating and responding to their expectations. In the meantime, as the next phases of research continue, it is hoped the background, framework, and implementation methodology discussed in this report can provide a useful foundation on which internal audit departments can develop and enhance their own responses to this critical area of concern.

[1] Timothy King, "IDC: Data Creation to Reach 163 Zettabytes by 2025," Data Management News, April 11, 2017, https://solutionsreview.com/data-management/idc-data-creation-to-reach-163-zettabytes-by-2025/

[2] "New Policy Prohibits DoD Employees From Using GPS Services in Operational Areas," Defense Logistics Agency Public Affairs Department news release, Aug. 8, 2018, https://www.dla.mil/AboutDLA/News/NewsArticleView/Article/1597116/new-policy-prohibits-dod-employees-from-using-gps-services-in-operational-areas

[3] Alyssa Provazza, "Artificial Intelligence Data Privacy Issues on the Rise," TechTarget Network, May 26, 2017, https://searchmobilecomputing.techtarget.com/news/450419686/Artificial-intelligence-data-privacy-issues-on-the-rise

[4] Ibid.

[5] Matteo Cagnazzo and Chris Wojzechowski, "Security and Privacy in Blockchain Environments," dotmagazine, June 2017, https://www.dotmagazine.online/issues/innovation-in-digital-commerce/what-can-blockchain-do/security-and-privacy-in-blockchain-environments

[6] Kate O'Flaherty, "Facebook Data Breach – What To Do Next," Forbes, Sept. 29, 2018, https://www.forbes.com/sites/kateoflahertyuk/2018/09/29/facebook-data-breach-what-to-do-next/#6779f4f02de3

[7] Karl Utermohlen, "Facebook Data Breach 2019: 540 Million Users' Records Exposed," InvestorPlace, April 4, 2019, https://investorplace.com/2019/04/facebook-data-breach-2019/

[8] Phil Muncaster, "Data Leak Exposes 267 Million Facebook Users," Infosecurity Magazine, Dec. 20, 2019, https://www.infosecurity-magazine.com/news/data-leak-exposes-267-million/

[9] Paul Bischoff, "Which States Have the Most Data Breaches?" Comparitech, June 20, 2019, https://www.comparitech.com/blog/vpn-privacy/data-breaches-by-state/

[10] Regulation (EU) 2016/679 of the European Parliament and of the Council (official text of the GDPR), Article 4, p. 33, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

[11] Ibid.

[12] "Determining What Is Personal Data," U.K. Information Commissioner's Office online guidance, Dec. 12, 2012, p. 7, https://ico.org.uk/media/for-organisations/documents/1554/determining-what-is-personal-data.pdf

[13] GDPR, Article 4, p. 33.

[14] "Adequacy Decisions: How the EU Determines if a Non-EU Country Has an Adequate Level of Data Protection," European Commission website, https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en

[15] "Data Protection Laws of the World" (Colombia), DLA Piper, 2020, https://www.dlapiperdataprotection.com/index.html?t=law&c=CO

[16] "Data Protection Laws of the World" (Mexico), DLA Piper, 2019, https://www.dlapiperdataprotection.com/index.html?t=law&c=MX&c2=

[17] Margareth Kang, "What to Expect From Brazil's General Data Protection Law?" Berkeley Technology Law Journal, University of California, April 22, 2019, http://btlj.org/2019/04/what-to-expect-from-brazils-general-data-protection-law/

[18] Tahira Noor Khan, "India Is Set to Get Its First Data Protection Law," Entrepreneur India, Dec. 9, 2019, https://www.entrepreneur.com/article/343612

[19] Winston Ma Wenyan, "China Is Waking Up to Data Protection and Privacy," World Economic Forum, Nov. 12, 2019, https://www.weforum.org/agenda/2019/11/china-data-privacy-laws-guideline

[20] "EU Japan Adequacy Decision" fact sheet, European Commission website, January 2019, https://ec.europa.eu/info/sites/info/files/research_and_innovation/law_and_regulations/documents/adequacy-japan-factsheet_en_2019_1.pdf

[21] Kwang Bae Park and Hwan Kyoung Ko, "Korea: Data Protection 2019" (Section 18.2), International Comparative Legal Guides, March 7, 2019, https://iclg.com/practice-areas/data-protection-laws-and-regulations/korea

[22] Melissa Krasnow, "Practical Guidance Overview: State Laws Requiring Data Security Practices," Bloomberg Law Privacy and Data Security, November 2018, http://www.vlplawgroup.com/wp-content/uploads/2018/11/Data-Security-Overview-V2.pdf

[23] California Consumer Privacy Act of 2018, Section 1798.140, https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375

[24] Ibid.

[25] California Consumer Privacy Act of 2018, Sections 1798.105, 1798.110, and 1798.115, https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375

[26] "Risk in Focus 2020: Hot Topics For Internal Auditors," European Confederation of Institutes of Internal Auditing, September 2019, p. 7, https://www.iia.nl/SiteFiles/Publicaties/Risk%20in%20Focus%202020%20IIA%20NL%20LR%20def.pdf

[27] Ibid, p. 5

[28] Ibid, p. 11

[29] Ibid, p. 13

[30] "OnRisk 2020: A Guide to Understanding, Aligning, and Optimizing Risk," Institute of Internal Auditors, 2019, p. 5, https://dl.theiia.org/AECPublic/OnRisk-2020-Report.pdf

[31] "NIST Releases Version 1.0 of Privacy Framework," NIST news release, Jan. 16, 2020, https://www.nist.gov/news-events/news/2020/01/nist-releases-version-10-privacy-framework

2020-0163