Continuous monitoring is required for effective data privacy and security

By Ambler T. Jackson

Ambler T. Jackson, CIPT, CIPM, CIPP US/G, JD, is a privacy subject matter expert located in Washington, DC, USA.

- [linkedin.com/in/amblertjackson/](https://linkedin.com/in/amblertjackson/)

Continuous monitoring is the maintaining of ongoing awareness of information security vulnerabilities and threats to support organizational risk management decisions.[1] One US federal government resource describes continuous monitoring as a risk management approach to cybersecurity that maintains an accurate picture of an agency’s security risk posture, provides visibility into assets, and leverages use of automated data feeds to quantify risk, ensure effectiveness of security controls, and implement prioritized remedies.[2] In the financial industry, continuous monitoring has been described as an “automated, ongoing process that enables management to assess the effectiveness of controls and detect associated risk issues; improve business processes and activities while adhering to ethical and compliance standards; execute more timely quantitative and qualitative risk-related decisions; and increase the cost-effectiveness of controls and monitoring through IT solutions.”[3]

Recent events related to personal data and security have given rise to the increasing need to continuously monitor business processes and the entire data life cycle. As such, it is a best practice—and in the case of federal agencies, it is a long-standing practice—to develop and adhere to a continuous monitoring strategy. Continuous monitoring involves an ongoing process that requires management to continuously review business processes in order to
appropriately mitigate risk associated with collecting, maintaining, and using personal data. Most professionals in a management function or role, or who have management responsibilities, understand that continuous monitoring is an important risk management tool; however, many professionals in management are just now beginning to understand why continuous monitoring is critical and absolutely necessary for business operations across the enterprise.

Continuous monitoring is typically discussed as part of a framework for managing risks. There are several kinds of risks (e.g., strategic, operational, financial, compliance). Within the operational and compliance risk areas, from a data privacy and security perspective, new risks are emerging daily. Without enterprise-wide continuous monitoring, it will be nearly impossible to proactively identify and mitigate new risks. Enterprise-wide risk management allows an entire organization to contribute to mitigating risk; this includes everyone from the frontline employees, technical experts, and management to executive leadership. The approach takes into consideration the mission, objectives, business functions, and processes of the organization as well as the culture and appetite for risk.

What is personal data?

Fundamentally, your personal data is data that identifies you. For example, if I ask you to provide me with your personal information so that I can contact you and ask that you provide feedback on the topic of this article, you may provide me with your email address and phone number. These two data elements are personal to you. No two people share the same email address or telephone number. Upon reading the request, you will immediately understand that I am referring to your data. So, on the one hand, given the context of this example, most people will agree that the term personal data is self-explanatory.

On the other hand, personal data may take on a different meaning and result in a different privacy impact depending on several factors, including, but not limited to, the purpose for which data is collected, how it is used, and by whom. There’s no one global definition for personal data. The legal and regulatory definition and description of personal data may vary according to, for example, the citizenship of the individual to which the data belongs, the type of data collected, the industry to which the data pertains, and other variables.
For example, in the United States, the government describes personal data using the phrase personally identifiable information (PII), and PII is defined as “any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual’s identity, such as name, social security number, date and place of birth, mother’s maiden name, or biometric records; and (2) and information that is linked or linkable to an individual, such as medical, education, financial, and employment information.”

At the state level, at least in California, personal data is expressed as personal information. According to the California Consumer Privacy Act (CCPA), personal information means information that identifies, relates to, describes, references, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or device...." [5] Under the European Union’s General Data Protection Regulation (GDPR), personal data is any information that relates to an identified or identifiable living individual.[6] The Brazilian General Data Protection Law (LGPD) defines personal data as any information related to an identified or identifiable natural person.”

**Manage and protect personal data as an asset**

Data is an asset. Organizations with mature data privacy and security policies and procedures understand that managing their data inventory is just as critical as managing their physical inventory. An organization must proactively protect the personal data that it collects, stores, maintains, or uses as it would any other asset. Legally, in most jurisdictions, across industries, you are required to protect personal data. Ethically, it is imperative that the organization demonstrates a strong commitment to doing the right thing with personal data, data entrusted to them by consumers and employees alike. Failing to exercise an acceptable level of care to protect personal data will certainly ruin the organization’s chances of thriving in the current data-driven economy. Further, data is an asset, and it should be protected as any other physical asset.

As organizations continue to operate in our data-driven economy, there will be new and emerging data privacy and security challenges to contend with. In order to meet these challenges and protect the organization, as well as its
internal and external stakeholders, from vulnerabilities and threats, taking a risk-based approach is a best practice and is highly encouraged. A risk-based approach will help the organization prioritize risks and develop solutions for proactively mitigating those risks. In the broadest terms, risk can be described as any potential for an undesirable outcome.

Privacy professionals have been discussing and dissecting what applying a risk-based approach to protecting data looks like for some time.[7] This is not a new concept; however, the creation of a strategy and implementation of a plan that includes a risk-based approach is challenging due to the coordination, planning, and resources required to be effective. It will require not only buy-in and support by the executive leadership of the organization, but also a shift in attitudes and values as they relate to data privacy. Despite the challenges, it is critical that organizations assess their business processes, determine high-value assets, and manage and mitigate risks. Managing the organization’s data as an asset and continuously monitoring the controls used to secure the data, enterprise-wide, will allow the organization to further its mission and objectives while successfully navigating the regulatory compliance landscape.

A risk-based approach to protect your organization

Protect your organization by managing personal information and mitigating risks inherent in collecting personal data. We live in the Information Age and routinely use technology to perform daily tasks. Similarly, technology is an integral part of organizations’ daily operations. The use of computer software, systems, and networks to store, retrieve, transmit, and process personal data is commonly known as information technology (IT). Advances in IT are certainly helpful and necessary for any business to survive and thrive in this digital era, but the processing of personal data gives rise to cybersecurity threats and data privacy risks. As a result, organizations that collect, maintain, or use personal data must effectively manage the risks associated with such activities by selecting the appropriate privacy and security controls, and continuously monitoring the effectiveness of those controls.

Using a risk-based approach to manage and protect the personal data collected, maintained, or used by an organization requires continuous monitoring of
business processes and IT systems to assess, prioritize, and mitigate the risk associated with collecting, maintaining, or using personal data. It is a proactive and strategic approach, versus reactive and ad hoc. This approach will communicate to stakeholders that the organization values data privacy and the protection of personal data.

The National Institute of Standards and Technology (NIST) developed a Risk Management Framework (RMF) as guidance for different industries, government, and academia. The RMF includes continuous monitoring as a critical part of the RMF process. The RMF includes six areas or steps: categorization of systems, selection of security controls, implementation of security controls, assessment of security controls, authorization of systems, and the monitoring of security controls. The concept of continuous monitoring is essentially the sixth step of the RMF. Many organizations that need to ensure compliance with US requirements for protecting personal data adhere to NIST guidance or some variation thereof.

A continuous monitoring plan helps management assess the effectiveness of privacy and security controls, improve business processes, adhere to ethical and compliance standards, and quickly address any identified risk. Continuous monitoring strategies and plans will vary across industries. For example, the risks for a financial services company will differ from the risks identified by the federal government; therefore, their approach to risk management and selection of controls will also differ. Similarly, an online retailer has unique business processes and risks. As a result, the selection of privacy and security controls will differ, and the monitoring of the effectiveness of those controls may be unique to online retailers. Ultimately, regardless of the industry, if you use IT and you have consumer data that you are legally required—and ethically bound—to protect, you need to have a continuous monitoring strategy that effectively monitors the privacy and security controls for your particular business processes.

Operating without a continuous monitoring strategy is risky

Organizations that do not have a continuous monitoring strategy and haven’t implemented a plan risk exposing themselves and their customers, clients,
employees, contractors, and partners to varying levels of harm. The harm may include consumer identity theft due to a preventable data breach, loss of consumer confidence, loss of investor confidence, and loss of company assets. Failure to implement a continuous monitoring plan may also lead to more threatening outcomes like erosion of shareholder value, reputational harm, and hefty regulatory compliance fines—all of which could end an organization’s ability to stay in business.

**Loss of personal data due to preventable data breaches**

Cyberattacks are becoming increasingly more common for businesses that collect, maintain, and use personal data. Businesses are valuable targets for cybercriminals who hack digital devices, such as computers, tablets, and entire company networks, to obtain personal data to sell on the black market. Hacking, which includes various activities, such as social engineering and phishing, remains the number one type of breach for number of incidents, accounting for 82% of reported breaches.[9] Personal data exposed during or after a cyberattack will require the business to consult breach notification laws and deal with the real possibility that the breach may lead to identity theft. Identity theft is a crime that occurs when an individual’s personal data is used for fraudulent purposes. Data breach response—and adhering to compliance requirements—post-breach is expensive. Continuous monitoring allows organizations to obtain *real-time insight* into vulnerabilities and threats. This ongoing awareness allows management to make informed decisions proactively and, to the extent possible, mitigate the risk associated with cyberattacks.

**Loss of consumer and investor confidence**

In addition to regulatory bodies, investors are also looking very closely at organizations’ risk management efforts. Continuous monitoring strengthens an organization’s ability to prioritize risks and mitigate the risks associated with collecting personal data. Unchecked risk associated with data breaches and evidence of regulatory noncompliance will result in a loss of consumer confidence in the organization, business product, or service. In 2018, Facebook admitted to the unlawful transfer of user data to the data analytics firm Cambridge Analytica.[10] After the scandal, polls showed a 66% drop in consumer confidence.[11] Loss of consumer confidence may lead to a loss of
investor confidence. A loss in investor confidence may negatively affect the organization’s ability to raise capital in the future. A strong continuous monitoring strategy will give management confidence in their data collection and security practices, and the company will be better positioned to communicate information that will improve or restore consumer or investor confidence.

**Loss of the value of shares**

Continuously monitor your organization’s relationship with third-party vendors, because not doing so will prove costly. The Cambridge Analytica scandal caused not only the loss of consumer confidence, but Facebook’s share price dropped significantly in March 2018.\[12\] One of the primary complaints to the Federal Trade Commission is that Facebook disclosed personal user data without users’ consent and that the company did not take appropriate action against Cambridge Analytica until news outlets exposed the scandal. Ultimately, the Federal Trade Commission fined Facebook a whopping record-breaking and history-making $5 billion dollars.\[13\]

**Reputational harm**

As demonstrated by the Cambridge Analytica scandal and the resulting $5 billion fine levied against Facebook, when personal data is compromised, the recovery process can include an overwhelming response from regulators, costly fines, and a loss in confidence in your organization’s data privacy and security program. A company may experience loss of revenue, loss of consumer confidence, loss of investor confidence, loss of company assets, and hefty fines. Of all of the negative consequences associated with an incident that reveals your organization did not appropriately select privacy and security controls to safeguard personal data, and continuously monitor those controls, reputational harm may be the most difficult and time-consuming to overcome.

A March 2019 report from Axios Harris Poll 100, which ranks the reputations of the most visible companies in the United States, found that Facebook’s positive reputation declined over the past year due in part to the data privacy and security controversies.\[14\] Reputational harm alone may not be enough to put a company out of business; however, it is enough to cause concern. For example, according to the Harris Poll, out of 100 companies, Facebook ranked 54, and in
2019, the company fell to 94.[15]

Research and invest in a continuous monitoring tool

Vendors are beginning to develop tools that automate continuous monitoring and produce capabilities that allow the organization to analyze and evaluate the risk identified through monitoring. Many of these tools include testing, auditing, and assessment capabilities. Management, with the input of various stakeholders—including governance, risk, and compliance teams—should thoroughly assess the vendor’s capabilities before diving into the process of selecting an appropriate tool, because risk management is unique to each organization.

The organization must develop a process that enables reliable research and vetting before investing in a continuous monitoring tool to automate the continuous monitoring process. The effort to leverage the expertise of professionals who work on continuous monitoring solutions as part of their job function will have long-lasting benefits in terms of cost savings and resources.

Conclusion

Monitoring data privacy and security compliance is necessary for any organization that collects personal information. Developing a continuous monitoring strategy and implementing a plan will assist management with ongoing awareness of risks, which will help the organization maintain public trust and consumer confidence, and prevent revenue loss and fines associated with noncompliance and data breaches. Additionally, your organization has a legal obligation to comply with the myriad of laws and regulations that provide for the protection of personal data.

Continuously monitoring the organization’s data privacy and security controls and the effectiveness of these controls demonstrates the organization’s commitment to safeguarding personal data to not only the public, but also to regulators as well. Failing to take a risk-based approach to data privacy and security could result in your organization joining the list of companies that
have made the headlines for preventable data breaches that exposed the personal data of their consumers, clients, users, patients, and many others.

**Takeaways**

- Continuous monitoring is a key element of the risk-based approach to data privacy and security.

- Globally, personal data may be defined or described differently than how laypersons describe personal data.

- Organizations can only select and monitor privacy and security controls if they completely understand how all their data is being collected, maintained, stored, or used.

- Organizations must continuously monitor their privacy and security controls to effectively mitigate risk inherent in collecting and processing personal data using information technology.

- Failing to create a continuous monitoring strategy and implement a continuous monitoring plan may result in a loss of public trust and confidence.


2 “Continuous Monitoring,” CIO.gov.


Herb Weisbaum, “Trust in Facebook has dropped by 66 percent since the Cambridge Analytica scandal,” NBC News, April 18, 2018, https://nbcnews.to/2jZON6y.

Salvador Rodriguez, “Here are the scandals and other incidents that have sent Facebook’s share price tanking in 2018,” CNBC, November 20, 2018, https://cnb.cx/2kxkyUU.

