COSMOS
Navigate the Compliance Universe

CEP Magazine - January 2020
Budgeting considerations for continuous monitoring of data privacy and security

By Ambler T. Jackson, CIPT, CIPM, CIPP US/G, JD

Ambler T. Jackson (amblertjackson@gmail.com) is a privacy subject matter expert located in Washington, DC, USA.

- linkedin.com/in/amblertjackson/

Businesses traditionally continuously monitor performance. In the digital age that we live in—and considering the amounts of personal data collected, used, and shared by businesses, organizations, and governments—monitoring performance is no longer enough. Businesses and organizations must also monitor data-driven business practices (e.g., collecting and sharing personal data) and information technology (IT) systems that process personal data. Cyberattacks involving the compromise or loss of personal data are becoming increasingly more common for organizations and businesses that collect, maintain, and use personal data. Compromised personal data may lead to identity theft of the data subject, embarrassment, or reputational harm to the compromised company. Therefore, continuous monitoring of business practices and IT systems is not only the appropriate, and in some cases mandated, course of action—it is simply the right thing to do.

Today, many organizations have a cybersecurity program. Depending on the size and the industry, a privacy program may fall within the organization's larger cybersecurity program. Perhaps both privacy and security fall under the broader cybersecurity program. Some organizations may only have a privacy program, and no cybersecurity program at all. Others may simply have an IT department that focuses on security, but considers data privacy when necessary to meet a business need. Regardless of how data privacy and security is embedded in the organization, it will be necessary to continuously monitor activities that may pose a risk to data privacy and securing data assets. Continuously monitoring business practices and IT systems that collect personal information is required to appropriately manage risk. Implementing such a program requires resources, and a budget is required to obtain those resources.

Budgets for continuous monitoring activities will vary. The budget for a Big Tech company and the United States government will not be the same. Similarly, the budget for a new start-up in the online retail space and a new healthcare service will not be the same. In September 2018, the White House released the National Cyber Strategy, which reinforces ongoing work and provides strategic direction for the federal government to act on short- and long-term improvements to cybersecurity for the government, private sector, and individuals. The National Cyber Strategy: (1) recognizes that private and public entities have struggled to secure their systems as adversaries have increased the frequency and sophistication of their malicious cyberactivities, and (2) directs the federal government to do its part to ensure a secure cyber environment for our country. The FY 2020 President's Budget includes $17.4 billion of budget authority for cybersecurity-related activities, a $790 million (5%) increase above the FY 2019 estimate.[1]

Challenges to requests for a budget

Requesting budget approval for continuous monitoring activities may be new for many organizations, and a

how-to reference does not exist. Traditionally, organizations did not have a budget line item for cybersecurity or privacy programs. With the emphasis placed on the importance of data privacy and security in both the private and public sector, the risk management discussions related to budgeting for activities that will mitigate risks associated with collecting, processing, and securing personal data are increasing. Although there appears to be greater importance placed on data privacy as of late, there are still many challenges related to obtaining approval for a budget that supports continuous monitoring activities. Smaller companies often do not have the budget to engage in adequate continuous monitoring activities. Depending on their data practices and industry, leadership may not see the value in having a budget for continuous monitoring activities. Larger organizations may not include a budget line item for the programs that require continuous monitoring because they are currently paralyzed with the arduous task of identifying all of their data assets, systems, and associated risks. An organization cannot continuously monitor what they do not know about.

Additionally, challenges include the fact that, initially, it may be difficult to place a dollar amount on managing risks from a data privacy and security perspective. Depending on the size of the organization and the types of data involved, it may be labor intensive and costly to fully identify and understand the business practices and IT systems that involve personal data and the associated risks. Finally, there is no one-size-fits-all budget for these activities, and every organization will need to take a tailored approach to creating their continuous monitoring budget. Consider that Joe's online bicycle shop in Florida will not be able to use the budget that Sally's online retail shop in the European Union uses. The two shops will have different continuous monitoring needs based on their data collection practices, business processes, and location.

What is continuous monitoring

Through continuous monitoring activities, management can continuously review business processes in order to appropriately mitigate risk associated with collecting, maintaining, and using personal data. Continuous monitoring is typically discussed as part of a framework for managing risks, and new risks are emerging daily. Specifically, continuous monitoring is the maintaining of ongoing awareness of information security vulnerabilities and threats to support organizational risk management decisions.[2],[3] 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."[4]

The approach to continuous monitoring should include the entire organization. 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 frontline employees, technical experts, and management to the executive leadership. The approach takes into consideration the mission, objectives, business functions, and processes of the organization as well as its culture and appetite for risk.

Budget constraints and cybersecurity programs

A cybersecurity program will not always have its own budget line item. Similarly, it is unlikely that continuous monitoring will have its own line item. Those requesting a budget for cybersecurity program activities, which may include privacy, security, and continuous monitoring of risks associated with collecting personal data and IT systems that process personal data, dream of having a line item that is separate and distinct from all other line items in the budget. Instead, these activities are typically lumped in with IT or risk management.

Once the organization's leadership identifies the program that will require continuous monitoring activities,

whether it is a cybersecurity program or a privacy program, the organization will need to fund the activities. It is not unheard of for a request to fund an initiative of any size to face scrutiny or opposition. Responses to requests for funding continuous monitoring activities will vary depending on the size of the organization, attitudes about continuously monitoring data protection and security practices, the priority ascribed to the privacy and security risks identified, and the impact of regulatory compliance requirements for the industry in which the organization belongs. An individual or group requesting a budget to support continuous monitoring activities may love to see continuous monitoring on the organization's budget as a separate line item, indicating its separate and distinct value and weight. This kind of demonstrated financial commitment is rare and may only come with a significant amount of effort, and perhaps fierce protest and advocacy, as funds for cybersecurity—including data privacy and continuous monitoring activities in many organizations—are shared.

Back in August 2019, Kate Brew, AT&T Cybersecurity, tweeted, "Cybersecurity budgets come in many sizes. How does your company determine yours?"[5] Responses included:

- "They keep me far away from budget/financial decisions at my company but I'd like to think a d20 is involved somehow…" (I love Dungeons & Dragons references!)
- "Yeah. They most often range in size from 'miniscule,' to 'barely visible to the unaided eye.'"
- "Pick a number and subtract that number from itself. That's your budget."
- "What is this 'budget' of which you speak?"
- Someone posted an image of a dart board. (Perhaps a roulette wheel would've been more appropriate?)
- Of course, someone else posted a GIF of a Magic 8 Ball. (All signs point to yes?)

To overcome similar responses, in a relatively small organization, the organization's leadership may not consider data privacy and security a priority and a best practice for the organization's business operations. The request for an initial budget or an increased budget in a smaller organization may be met with comments or responses that indicate that the company places more weight on everything except data privacy and security; that they just don't see the value of continuous monitoring activities given the size of the company, their business practices, and data assets; or that there's no justification for the budget requested. In this situation, the requests for a budget that supports continuous monitoring activities may require several meetings, evidence demonstrating the business need, case studies supporting the business need, a report that identifies the risks associated with not monitoring data-driven business practices, and the costs associated with mitigating such risks.

In a larger organization, overcoming negative responses to budget requests may require much more. Consider first identifying stakeholders who see the value in continuous monitoring activities associated with data protection and security, and who will actually support a budget for such activities. Their buy-in and support will be critical. Form a budget committee and hold workshops that focus on the best strategy for requesting a budget. Ensure that the strategy aligns with the organization's overall risk management strategy.

Identify continuous monitoring tools and activities

The organization may already engage in the following continuous monitoring activities:

- Audits
- Compliance documentation reviews

- Risk assessments
- Vulnerability assessments
- Patching

To ensure that the request for a budget that includes continuous monitoring activities is logical, and that any approved budget will not result in monies spent duplicating efforts, it will be critical to meet with the relevant stakeholders and identify all of the technologies and tools that currently support continuous monitoring activities. This is important because many organizations may already perform continuous monitoring activities, but their efforts may be siloed. Leverage the expertise of the organization's IT professionals who may have worked in the past to procure these tools or who are currently maintaining or operating these tools. These individuals have information related to the dollar amount necessary to obtain such tools, as they've likely had to go through the research and vetting process related to selecting the vendor. In addition to identifying the current activities and tools, identify the current resources and stakeholders associated with the activities and tools. (e.g., staff members, consultants, third-party vendors).

In identifying the activities required for the continuous monitoring program, take the appropriate time and measures, and consult the relevant stakeholders, to thoroughly understand the risks to the organization. If the organization does not understand the risks associated with their business practices involving personal data, the request for a budget for continuous monitoring activities may be shortsighted. Consider, for example, a business process or data asset identified as low risk may not require the same continuous monitoring activity as a high-value asset. As a result, it may make sense to plan to seek budget approval for continuous monitoring activities that focus on high-value assets. In this situation, perhaps leadership will make a business decision to accept the risk associated with fewer continuous monitoring activities for low-risk business practices and assets.

Ask intelligently and with the relevant audience in mind

Individuals submitting budget proposals or asking for funding for cybersecurity programs that include continuous monitoring activities should consider whether the budget meets the strategic goals of the organization, whether it is defensible, and whether the audience on the receiving end perceives it as realistic and practical. Determine whether the continuous monitoring activities for which you are requesting funding align with the organization's strategic priorities.[6]

Identify who your "ask" audience is. Who controls the budget, and who is the authorizing official for the budget? In other words, who do you need to convince? Identify the individuals in the organization who have overall responsibility for the review, monitoring, and control of the operating budget. Identify what individuals and what groups of individuals have responsibility for planning, management, organization, direction, supervision, and performance of budgeting activities.

Approach the budget for continuous monitoring activities strategically. Draft a proposal that is appropriately detailed for the audience. Keep in mind that the budget approving official (e.g., CIO, CFO, CTO, or CISO) will appreciate the value of continuous monitoring activities if the information is presented in a manner that demonstrates value to the organization and, specifically, the function they oversee. Present the continuous monitoring activities for which you are requesting funding in a manner that prioritizes needs based on the risks that the organization has described as high. Remember that every organization has a different risk profile, and the continuous monitoring activities should align with the risk profile.

As you draft your proposal and communicate the type of budget you desire, think about the variables that you need to be cognizant of as you determine the best budget for your organization. There's no one-size-fits-all

budget. The type of budget will depend on many variables. There are some budgets that are less desirable for continuous monitoring activities. For example, given the nature of continuous monitoring activities and the ever-changing threat and regulatory compliance landscape, a static budget may not be the best option. Perhaps a continuous or flexible budget may be more appropriate.

Continuous budgets allow organizations to make changes and updates, and have resources to change and adapt to the ever-changing threat landscape. A continuous monitoring strategy will change and, as such, so will the budget for the continuous monitoring program. Expect that the resources required to operate a continuous monitoring program will also change.

Change management considerations

Receiving budget approval for continuous monitoring activities may be met with a flat out nonapproval. A proposed budget may not receive approval for many reasons, some of which include:

- Continuous monitoring activities may fluctuate, and the organization needs prompting that these activities may change, making it difficult to quantify the activities for a given period.
- Continuous monitoring activities are sometimes technical in nature, and budget decision-makers may not understand the technology or the value of the technology that supports the continuous monitoring activity.
- Continuous monitoring activities related to data privacy and security often fall under the organization's cybersecurity program; budget decision-makers may not place significant value on cybersecurity programs.

If it appears that the organization does not value data privacy and security, perhaps a change in culture is necessary. Approval of continuous monitoring activities may come after there has been a shift in attitudes and values related to cybersecurity in general and, more specifically, continuous monitoring activities related to data protection and security. If calls for resources necessary to protect data assets go unanswered after making the business case for a budget that supports continuing monitoring activities, it may be time to consult a professional with change management expertise.

Change management is the discipline that guides how we prepare, equip, and support individuals to successfully adopt change in order to drive organizational success and outcomes.[7] Managing the organization's data as an asset—including continuously monitoring the controls used to safeguard and secure the data—will allow the organization to reach its strategic goals while successfully navigating the regulatory compliance landscape. Continuous monitoring activities 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.

Conclusion

Monitoring business practices that involve personal data requires resources. A budget is required to obtain those resources. In many cases, requests for budget approval will be met with challenges. These challenges may be overcome through demonstrating the value of continuous monitoring activities, aligning the activities with the strategic goals of the organization, and prioritizing the risks that will assist with prioritizing the continuous monitoring activity. This will require coordination and collaboration with staff members, leadership, and all business functions within the organization in order to compile the most accurate, valuable information for the budget-approving individual.

After there is an approved budget for the continuous monitoring activities, tailored for the organization's data-driven processes, and aligned with the organization's strategic goals and risk appetite, actually securing the funding will be the next hurdle to overcome.

Takeaways

- Continuous monitoring is a risk-based approach that provides ongoing visibility into the organization's business practices, data assets, and associated risks.
- Engage in a thorough planning session that includes identifying the organization's risks, risk appetite, current continuous monitoring activities, tools, and resources.
- Tailor continuous monitoring activities according to the risks ascribed to the business practice or data asset.
- Align continuous monitoring activities with the strategic goals of the organization to help demonstrate the value of the continuous monitoring activities.
- There is no one-size-fits-all budget for continuous monitoring activities, and all budget requests should be a collaborative effort, coordinated with the appropriate stakeholders.

1 White House, "Cybersecurity Funding," *A Budget for a Better America* (U.S. Government Publishing Office, 2019), 305, .
2 National Institute of Science and Technology, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*, Special Publication 800-37, Rev. 2, December 2018, .
3 "Continuous Monitoring," , accessed September 6, 2019, .
4 Michael P. Cangemi and Bill Sinnett, *The Benefits of Continuous Monitoring,* Financial Executives Research Foundation, August 2011, .
5 Kate Brew (@securitybrew), Twitter, August 3, 2019, .
6 Staff, "The Right Way to Prepare Your Budget," *Harvard Business Review*, July 20, 105, .
7 Prosci, *What is Change Management?*, accessed November 11, 2019, .