By Neha S. Patel, CPA, CISA

Enhancing the Value of
SOC REPORTS
DURING A PANDEMIC

As CFO of a retail hardware chain, Isabel has just completed a presentation at the company's quarterly board meeting. Board members had plenty of questions about how Isabel and her team had maintained internal controls and monitoring key processes during the global pandemic. She was already compiling a mental list of new risks that would need to be added to an updated risk assessment.

Isabel's first move was to work with Daniel, the company's director of internal audit, to conduct a thorough review of the company's current risk assessment and update the list of critical knowledge components.

A primary area of concern was the company's dependencies on critical third parties. These service organizations include business partners that manufacture and distribute products, as well as vendors that provide cloud-based inventory management systems.

Questions included: *How had the pandemic changed the ability of these vendors to deliver critical services?*

Was it time to conduct a review? What information did Isabel and Daniel need from these third parties to ensure their company's ability to continue operations?

Scenes like this one have taken place in countless organizations as businesses have adapted to changes brought about by the pandemic. What steps have these companies taken to shore up their operations and maintain strong internal controls?

As in any successful relationship, communication is key. Businesses and the companies that provide their outsourced services need to be able to effectively communicate with each other so that there is a shared understanding of how changes in the marketplace may impact risk management, expected commitments and overall operations.

As businesses and their service organizations adapt to the realities of the pandemic, they can use a System and Organization Controls, or SOC, report as a critical communications tool to maintain and strengthen overall operations.

A SOC audit is not a certification. There is no pass or fail rating that comes with any audit. The SOC audit provides transparency about the internal control structure and assurance that the design and operating controls are effective.

A SOC report is a published audit report that includes a detailed description of the service organization's control environment and control activities that have been implemented to meet customer expectations, as well as an auditor's judgment and test of procedures to validate that those expectations have been achieved.

All SOC examinations must conform to the Statement on Standards for Attestation Engagements (SSAE) issued by the Auditing Standards Board. The current SSAE No. 18 offers these five different reporting options, which are designed for different audiences.

1. **SOC 1** reports focus on evaluating internal controls over *financial reporting* related to the outsourced service offering. This information can be crucial for companies that

need to comply with Sarbanes-Oxley, FDICIA or FFIEC. The boundaries of the scope are determined by (a) the types of services delivered to customers and (b) the risks that are pertinent to users of these services.

SOC 1, Type 1 reports are intended to provide auditors with information about the design of controls at a service organization as of a *specific date*.

SOC 1, Type 2 reports are intended to provide information about the design of controls at a service organization and the results of tests of effectiveness for *a period of time*.

2. **SOC 2** reports focus on evaluating compliance with prescribed requirements, such as contract compliance, HIPAA and more commonly, the Trust Services Principles (TSPs). The examination can provide transparency over a company's internal controls as it relates to security, availability, processing integrity, confidentiality and privacy.

SOC 2, Type 1 reports are intended to provide auditors with information about the design of controls at a service organization as of a specific date.

SOC 2, Type 2 reports are intended to provide information about the design of controls at a service organization and the results of tests of effectiveness for a period of time.

3. **SOC 3** reports are used for the same purpose as a SOC 2, but are an abridged version for the reader.

4. **SOC for Cybersecurity** is designed for management to evaluate

their own internal cybersecurity posture.

5. **SOC for Supply Chain** provides insight into internal controls in systems used to produce, manufacture or distribute products.

Why Would a Service Organization's Internal Controls Matter?

For companies that outsource critical functions like payroll processing, claims processing, cloud services and data hosting, a SOC report gives assurance of the service organization's internal control environment. It provides management and internal auditors with transparency about a service organization's processes and gives assurance regarding the design and

> **A primary area of concern was the company's dependencies on critical third parties.**

operating effectiveness of the control activities a service organization has in place.

For organizations that provide outsourced services, an updated SOC audit offers the opportunity to provide their customers with up-to-date information about any changes resulting from the pandemic or other recent circumstances. Used effectively, a SOC report can be a valuable tool that allows a company and its outsourced service

organizations to fully understand how each works symbiotically to address mutual risk management goals.

For example, for a company that outsources transactional processing, like payroll services, a SOC report would include information related to relevant processes and internal controls that relate to the payroll services provided. The updated SOC report allows the company to stay abreast of any changes that could impact its payroll dependencies.

Putting the Pieces Together

A SOC audit or report isn't just a check-the-box service to be placed on a shelf once it is completed. Used effectively, it can provide valuable insight into the service provider's operations, which can in turn improve a company's performance.

Because each SOC audit is tailored based on a service organization's environment, each report is customized to a particular service offering. By focusing on Risk Assessment, Monitoring, Controls Assessment and Reporting, management may gain a more accurate picture of the service organization's current operations post-pandemic.

Risk Assessment

First and foremost, every organization should perform a risk assessment to evaluate the impact of the current environment on operations. At a minimum, the risk assessment should identify specific threats to achieving entity objectives, service commitments, system requirements and business objectives, as well as controls in place to mitigate the risk of those threats.

Some companies needed to downsize their operations or reduce their

workforce during the pandemic, which may have impacted how they performed internal control processes. Controls may be modified and require more time, training or resources to operate. A thorough risk assessment will help identify truly vulnerable areas and guide decision making for how to mitigate them.

For users of services, the focus should be on the organization and identifying critical outsourced services. Assess the impact of those dependencies on the company.

For service organizations, the focus should be on how COVID impacted the delivery of services to customers. Assess the impact to existing processes, including how controls may have been modified during the pandemic.

Here are a few questions to ask:
- What has changed in the operation (i.e., organization structure, remote work, new service, new tools) since COVID-19?
- Which controls (i.e., automated system controls, configurations, alert monitoring) will continue to operate as previously designed regardless of new COVID-19 operations?
- Which controls (i.e., manual, physical) do not operate as designed?

Similarly, when there are significant changes to outsourced services, the service auditor, an independent CPA firm that performs a SOC audit, may also need to design and perform different procedures, vary the timing of planned procedures or perform further procedures in response to the reassessed risks.

Monitoring

Surveys of businesses throughout the country are documenting the negative impact of COVID-19. For example, the US Census Bureau's Small Business Pulse Survey revealed

that three-quarters of small business respondents across the country experienced a large or moderate negative effect as a result of the pandemic. This makes monitoring activities to ensure services are meeting expectations even more critical.

If obtaining a type 2 SOC report, a company should be able to evaluate whether the service organization effectively performed control activities during the period covered by the
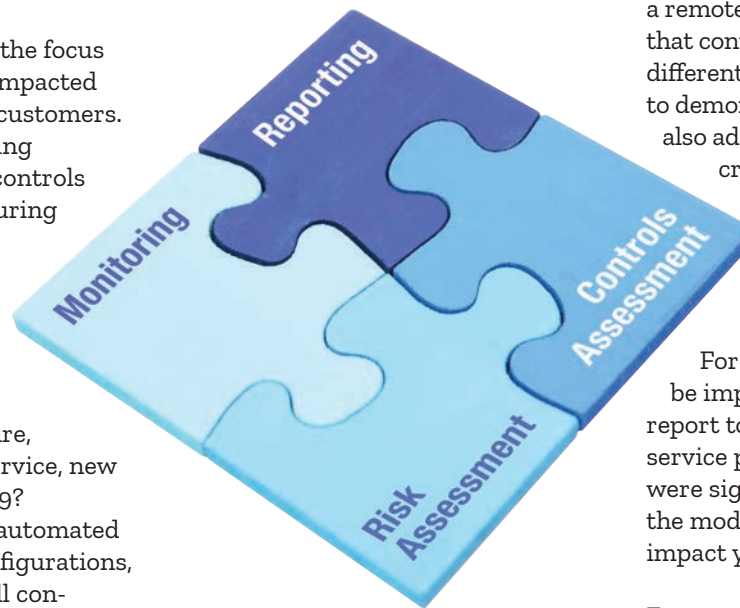
examination. A type 1 report can provide insights on the design of controls, but not the operating effectiveness of those controls.

For users of services, it may be important to identify independent procedures to monitor critical dependencies, especially if a report will not be issued near-term. This can enable the company to have timely oversight to assess risk management vulnerabilities and to determine whether additional controls will need to be implemented within their own organization in the meantime.

For service organizations, additional monitoring procedures may need to be implemented, especially if there are differences in control ownership or operation. New policy and/or procedure documents may need to be

created to help control owners and operators understand their roles and responsibilities for the new control operation. Initially, the control operation should be spot-checked frequently to ensure the new control is up and running effectively.

Controls Assessment

Even though it may not be possible to meet in person, the service auditor still needs to have access to all relevant information and to appropriate personnel. Navigating a remote workforce may mean that control activities are executed differently and that documentation to demonstrate those activities are also adapted. Travel restrictions may create challenges for service auditors who perform audit procedures using physical inspection or observations.

For users of services, it will be important to review the audit report to understand whether your service provider's control processes were significantly modified and how the modified control activities may impact your risk management.

For service organizations, the service auditor will evaluate whether the information is sufficiently reliable for the examination, including the completeness and accuracy of that information. Although the nature, timing and extent of procedures may vary depending on the importance of the information or the related control, the service auditor's procedures may include observing controls as they are performed, inspecting relevant reports or lists, and conducting walkthroughs of related processes and controls.

The service auditor needs to carefully document all procedures to demonstrate that the requirements of the attestation standards were met, particularly since the procedures may differ from those performed before social distancing and other restrictions were in place.

Reporting

With over a year into the pandemic, leadership changes, layoffs or other disruptions in service may all warrant an additional disclosure to help customers understand the impact to their risk. Acknowledging significant changes in the internal control environment and instances of controls not operating are critical to evaluating alternative risk management strategies. It may seem obvious, but reporting these findings is a critical step in identifying problem areas and addressing them with meaningful changes.

For users of services, reviewing the audit report will again be important. Just as in the controls assessment, businesses will need to understand whether their service provider's control processes were significantly modified and how the modified control activities may impact their risk management.

Service organizations need to consider whether changes to their operations represent a significant disclosure during the examination period.

The service organization may want to work with its service auditor to decide whether the examination period should be revised to account for significant changes in the environment. Non-operation of controls should be disclosed if mitigating controls have been designed, developed and implemented, and whether an 'emphasis of matter' paragraph should be added to describe actions taken during the impacted period.

A Finished Puzzle

By focusing on these four pieces of the puzzle, a business will be able to better understand its own control environment and the impact of critical services on which it relies.

Attention to these areas will help a service organization continue to deliver transparency and showcase its commitment to its customers.

Over time, these steps should be repeated as companies and their service organizations navigate the path to new normal operations. In doing so, they may find that disruptions as a result of the pandemic led to new and better ways to operate. The pieces may be shaped differently than before, but the puzzle is stronger than ever.

About the Author: Neha S. Patel, CPA, CISA, is a partner in charge of IT advisory services at Weaver, a national accounting firm. An AICPA System and Organization Control (SOC) Specialist, she focuses on delivering SOC audits, Sarbanes-Oxley compliance and other technology consulting services. She can be contacted at neha.patel@weaver.com.