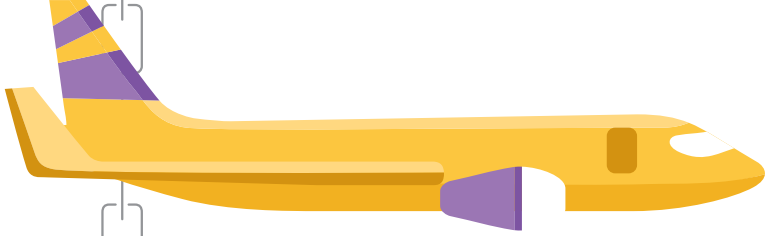


Eliminating the Blind Spot within Vendor & Supply Chain Risk Management

The more things change, the more they stay the same. I had always found practical wisdom in that saying, and for much of life and business it rings true. However, the year 2020 proved that in many very important ways, our world has had to abruptly adapt to significant changes in our personal and professional lives, and for many of these changes things are unlikely to stay the same or return to pre-2020 routines.

Blind Spots Become Blind Trust

Human beings have been engaging in risk management for almost as long as we have been making decisions. This is particularly the case in our relationships. In our personal life, these relationship partners are fundamental to our security, growth and well-being; in business these relationships are also fundamental and for the same reasons. All successful relationships come with the demands for dependability, security, and trust. The challenges of this past year have tested these pillars, causing many businesses to ask important questions of their business partners, and in some cases completely break from prior relationships that seemed once reliable. The uncertainty and risk to human capital only exacerbated the problem of effectively managing the risk to personnel and supply chains.

Blind Spots Become Blind Trust (cont.)

Every major compliance assessment and certification includes risk management as a cornerstone to its control framework. Not surprisingly, many businesses look to compliance assessments for indicators of dependability, security, and trust. Whether you need assurance that your business associate is safe to manage your electronic protected health information, or your cloud provider has appropriate cybersecurity safeguards in place, or if your transaction service provider employs technical safeguards against inaccurate or incomplete transaction processing, there is likely a compliance assessment specifically designed to answer your specific assurance need. However, when was the last time you were able to effectively gain assurance over your supply chain that didn't involve a self-assessment form or questionnaire to your vendors and suppliers? In the event that you did receive a compliance assessment report from those suppliers, they were likely only from larger services providers in the form of an ISO certification, SOC 2 report, PCI Report on Compliance, or similar deliverable not specifically designed for your specific supply chain questions or concerns. Make no mistake, these compliance assessments are well known and regarded for providing assurance in many respects, but often times they are not aligned with the specific information businesses need to assess risk throughout their supply chain. In other instances they are misunderstood or misused entirely. Does your colocation provider's SOC 1 truly satisfy your risk management questions? Has the ISO certification mark from your cloud provider fully addressed your privacy concerns? Are you over relying on the self-assessment questionnaire from your software vendor? What about the suppliers you use for physical devices on your network or your on-premise hardware devices, neither of which are eligible to undergo a SOC 2 examination, as they are goods and not services[1]?

[1] AICPA authoritative guidance and literature limits the scope and applicability of SOC 2 examinations to service providers, and their outsourced systems. Systems that produce, manufacture, or distribute goods are not eligible for SOC 2 examinations and reporting.

Blind Spots Become Blind Trust (cont.)

Blind Spots Become Blind Trust (cont.)

To effectively manage risk, organizations must consider the risks presented by their vendor relationships (dependencies), and if those risks have been mitigated to an acceptable level. Part of this assessment is determining the sufficiency and relevance of the information provided by that vendor.

> In almost every case, a self-assessment is inadequate for mission-critical or key vendor relationships, and independent third-party audits, certifications, and assessments are necessary to increase the reliability of information related to a vendor's controls and processes.

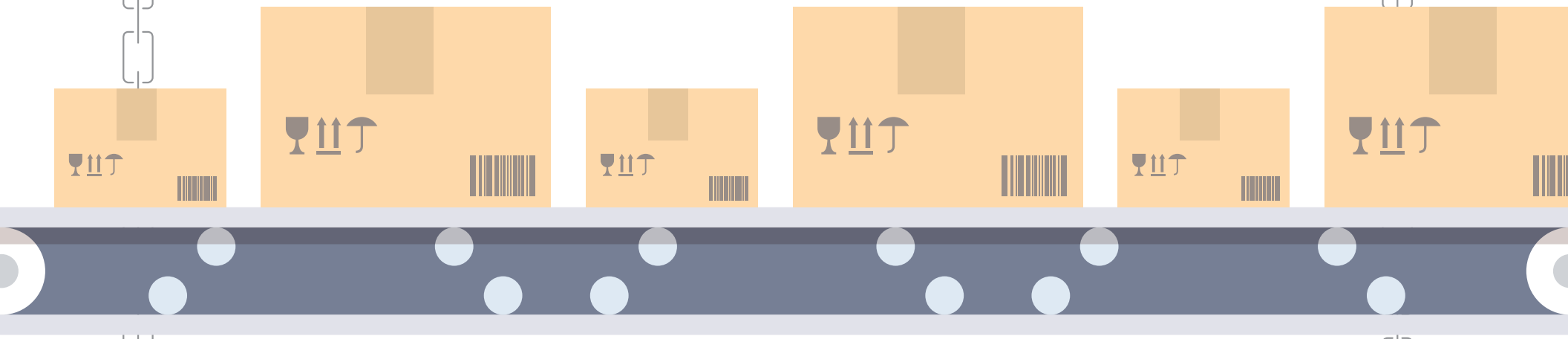
However, what about the commercial off the shelf (COTS) software you deployed into your on-premise environment? How many businesses can confidently know that the cybersecurity practices of the software developer are consistent with security best practices or secure coding techniques? Or that the hardware modules and other physical devices were produced in accordance with agreed upon product specifications? For many organizations, the lack of a well-known and consistent assurance framework for evaluating producers, manufacturers, and distributors of goods (including COTS) has left a blind spot in their vendor risk management programs. Unfortunately, this blind spot has led to blind trust for many organizational vendor risk management programs.

A Clear Solution in Sight

I have performed thousands of control and compliance assessments over my career, that involved the assessment of hundreds of organizations' vendor risk management programs. An important and consistent component of those programs has been a desire for simplicity and efficiency. This has led to a class-based approach where third party vendors are grouped by their size (as a percentage of the budget) or the services they provide, then assessed for risk. Given the need for efficiency, this invariably prompts compliance and risk management teams to find the most efficient solution to their information needs; typically in the form of a well-known request (compliance report, certification, or questionnaire) from a well-known vendor (e.g. cloud provider, SaaS provider, etc.). Given the need for simplicity, risk managers will also commonly rely on the reports, certifications, and questionnaires common and familiar to them (ISO Certification, SOC 2, PCI ROC, etc.). However, a fundamental flaw in this approach, is that it lends itself to a templated set of questions for a limited group of vendors that are overwhelmingly service providers. What about the producers, manufacturers, or distributors of goods in your supply chain? What about the suppliers that provide your on-premise software? Just because a vendor is small doesn't mean they are low risk, and it certainly doesn't mean you should trust their encryption modules, network devices, or on-premise software you download and install in your environment.

A Clear Solution in Sight (cont.)

Organizations should evaluate the risk vectors across all vendors, including software suppliers, then determine the risk management approach for all third-parties, before assessing risks of each third-party vendor. This is an important first step, as it also presents an opportunity for organizations to primarily understand the nature and extent of both the services and goods / software provided by their vendors, then secondarily understand whether or not a common compliance benchmark (seemingly dominated by service provider interest) exists or not. This likely would have the benefit of encouraging compliance and risk managers to ask specific questions based on their specific risk management objectives, then determine the very best form of assurance they should seek from the vendor. Historically, if it was determined that controls assurance was necessary for a supplier of goods, the prevailing only option was to request they complete a questionnaire, or worse yet, blindly accept the risk. This need not be the case any longer.



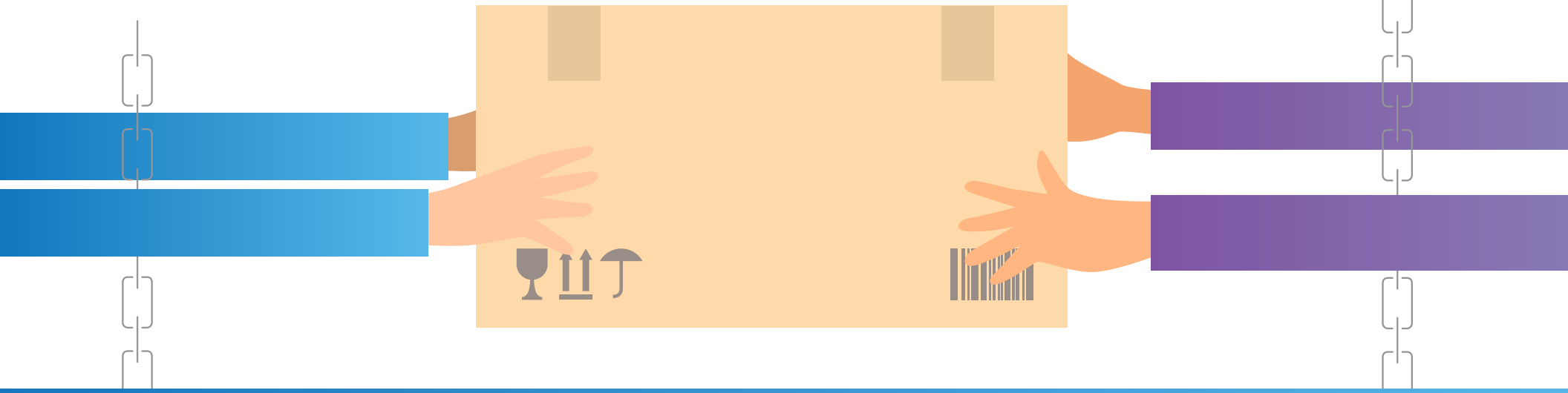
A Clear Solution in Sight (cont.)

SOC for Supply Chain is the most recent SOC reporting option addition to the AICPA's Suite of SOC Services. This report is designed to provide relevant information to organizations up and down their supply chain, and is specifically designed for all industries and stakeholders seeking to manage supply chain risks. The AICPA launched the SOC for Supply Chain in the Spring of 2020, although its design and purpose predated the COVID-19 pandemic. This report is similar to SOC 2 examinations in many ways, but is intended to report specifically on the risk management programs of producers, manufacturers, and distributors of goods. This includes organizations that create commercial off the shelf software for download or on-premises self-managed implementations. This is very important. The SOC for Supply Chain report provides a direct option for organization's that previously relied on vendor questionnaire responses because service provider assessment reports (SOC 1, SOC2, SOC 3, many PCI ROCs, etc.), were unavailable for use by suppliers. This closes a major gap in third party assurance reports in that risk managers can have a more robust look at the process maturity and control effectiveness of suppliers in the same comprehensive way common to service providers. For suppliers, it has the potential to undergo a single examination and provide their SOC for Supply Chain report to their customers, and in doing so find some relief from seemingly limitless vendor / supplier questionnaires. By reducing the dependency on questionnaires, both the organizations that supply (produce, manufacture, or distribute) goods and the organizations the organizations that depend on those suppliers, can reduce the demand for questionnaires and gain independent third party assurance respectively.

A Clear Solution in Sight (cont.)

Whether your organization is a producer, manufacturer, or distributor of goods and software, or if your organization relies on the goods produced by others, the SOC for Supply Chain report is more than just a way to describe your controls and processes, and may very well prove to be the most important SOC report you use to evaluate and manage your vendor supply chain risks.

At a high-level, the SOC for Supply Chain report leverages the very common and almost universally accepted COSO framework and popular Trust Services Categories, both found in SOC 2 examinations. This is important as risk managers will find that the SOC for Supply Chain report they can receive from their suppliers will closely align in form and function, as the SOC 2 reports they receive from their service providers. Third-party SOC report assurance can truly be attained for both service providers and their supplier counterparts.



A Clear Solution in Sight (cont.)

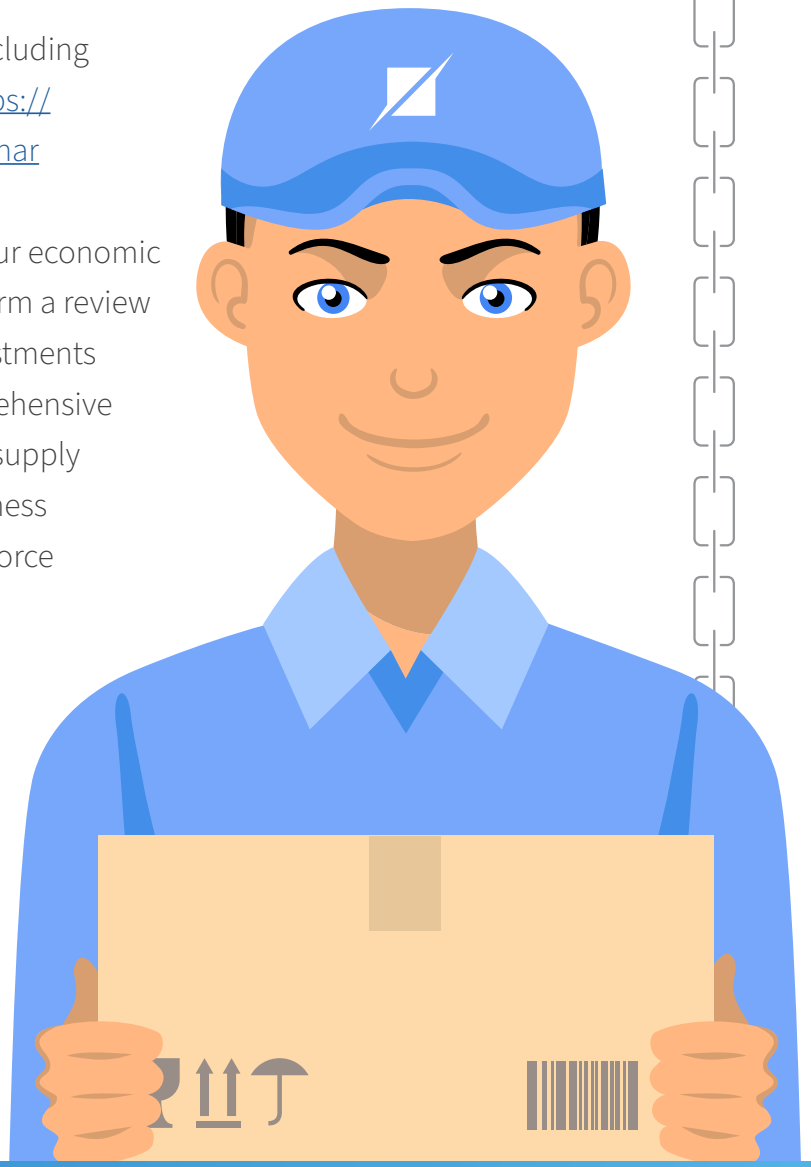
A Clear Solution in Sight (cont.)

SOC for Supply chain focuses on the principal system objectives of the supplier. These closely align with the principal service commitments and requirements, found in SOC 2 reports. A vendor may make commitments about different aspects of the product (including software) or its distribution, including commitments related to a product's performance specifications and availability. In layman's terms, these are the promises your vendor has made to you and its other customers regarding the device, distribution process, or software, for example. Common examples can include product specifications, including digital performance, the performance of firmware updates, conformity with industry standards (e.g. FIPS 140-2) and regulations, the secure storage, distribution, and delivery of products and software, etc. Since these promises are a cornerstone of the SOC for Supply Chain report, they are directly linked to the commitments made to your organization during the vendor selection process and may be reflected in the vendor's agreement, terms of service, or similar arrangement's with your organization. This alignment of expectations and independent third-party assurance over those expectations provides for tremendous advantages over general or templated questions that are completed or partially completed by the vendor itself. For the suppliers and software vendors, this third-party validation promotes trust and competitive market advantages over those suppliers simply completing self-assessments, as well has recouped labor costs through reduced questionnaire demands.

A Clear Solution in Sight (cont.)

For more detailed information related to SOC for Supply Chain, including a comparison of SOC for Supply Chain and SOC 2, please visit: https://hub.schellman.com/soc-examinations/soc-for-supply-chain-webinar

As we look forward to the rest of 2021, we can be optimistic that our economic and healthcare recovery will continue. Organizations should perform a review of their risk assessment methodologies and make necessary adjustments based on lessons learned from this past year. A honest and comprehensive review may reveal inadequate or flawed assumptions about your supply chain vendors, the reliability of their software updates, the robustness of your VPN and other vendors you relied upon for a remote workforce technologies, including software that may have been necessary to download and securely work and collaborate from home, among other changes to your organization. It should be clear that a 2019-style risk assessment and approach proves insufficient for 2021 and beyond. In addition to the challenges from 2020, organizational risk managers and vendors should also consider new and important opportunities to receive and provide more assurance, and improve the effectiveness and efficiency in the vendor risk management process.



About the Author - Ryan Buckner

Ryan Buckner is a Principal at Schellman & Company. Ryan currently serves on Schellman's attestation leadership team and leads the firm-wide research and development for attestation methodology. Ryan is a CIPP, CISSP, CISA, ISO 27001 Lead auditor, and maintains multiple CPA licenses, among other certifications. Ryan is also an AICPA-approved and nationally listed Peer Review Specialist for SOC examinations. Having completed over 1,000 service audits, Ryan is one of the most experienced service auditors in the world.

Certifications

Certified Public Accountant (CPA)
Certified Information Privacy Professional (CIPP)
Certified Information Systems Security Professional (CISSP)
Certified Internal Auditor (CIA)
Certified Information Systems Auditor (CISA)
Certificate of Cloud Security Knowledge (CCSK)
AICPA Advanced SOC
ISO 27001 Lead Auditor

For more information on SOC for Supply Chain
go to www.schellman.com

CLICK FOR MORE INFO

www.schellman.com
4010 W Boy Scout Blvd, Suite 600 / Tampa, FL 33607 / 1.866.254.0000
Outside of the United States, please dial: +1.813.288.8833