AICPA

SOC for Supply Chain Backgrounder

A New Solution for Managing Supply Chain Risks

Background

Manufacturers, producers, and distribution companies (referred to herein as "organizations") must manage a complex network of plants, service providers, and suppliers to operate efficiently and meet commitments to customers. At the same time, the threats to and vulnerabilities of each supplier in the chain have increased significantly. When a supply chain is disrupted, the organization is at risk of failing to meet production or delivery commitments it has made to its customers. Causes of disruption to supply chains include the following:

- Weather and other natural disasters (such as hurricanes or tornadoes) in a geographic area that is home to a supplier's facility
- Threat of war or military action in a geographic area that is home to a supplier's plant
- The lack of financial well-being of a key supplier or shipper
- Wide-spread diseases (such as SARS, MERS, or the COVID-19 coronavirus) that can affect the entire supply chain

For these reasons, an organization's ability to achieve its objectives is increasingly dependent on events, processes, and controls that are not visible to the organization and are often beyond its control, such as controls at the suppliers. Manufacturers, producers, and distribution companies are looking for visibility across their complex supply chain networks to better understand the risks of doing business with suppliers and the controls the suppliers have in place to mitigate those risks. The failure to manage these risks appropriately can result in

- reputational damage,
- loss of intellectual property,
- disruption of key business operations,
- fines and penalties,
- litigation and remediation costs, and
- exclusion from strategic markets.

This is why supply chain risk management has become such a significant issue to many organizations and their stakeholders. Suppliers are also increasingly interested in communicating how they manage the production and distribution risks in their own systems as a way of reassuring the organizations with whom they do business.

In recognition of the needs of commercial customers and business partners of manufacturers, producers, and distribution companies, the AICPA has developed a framework for reporting on the

controls over a manufacturing, production, or distribution system. Organizations can use the reporting framework to communicate to stakeholders relevant information about their supply chain risk-management efforts and the processes and controls they have in place to detect, prevent, and respond to supply chain risks. The reporting framework also enables a CPA to examine and report on management-prepared system information and on the effectiveness of controls within the system, thereby increasing the confidence that stakeholders may place in such information. A report that results from an examination of a manufacturing, production, or distribution system and its controls is referred to as a SOC for Supply Chain report.

Managing supply chain risk of suppliers

Because of their dependence on suppliers, organizations are responsible for understanding the risks of doing business with suppliers and for designing, implementing, and operating controls to mitigate those risks. For that reason, organizations are interested in, among other things,

- obtaining an understanding about the risks identified by a supplier that affect the supplier's production, manufacturing, or distributions of goods.
- comparing the supplier's objectives for the production, manufacturing, or distribution of goods with customers' needs.
- obtaining an understanding of the production, manufacturing, or distribution process of a supplier to better understand the risks to the customer of doing business with the supplier and the controls that the supplier has implemented to mitigate those risks.
- when establishing IT connectivity with a supplier or business partner, understanding the information security controls implemented by the supplier or business partner in order to more effectively integrate the security controls of the two entities.

Currently, organizations interested in the systems and controls of their suppliers have to assemble desired information from many different sources, including the following:

- Supplier-provided information
- Site visits, inspections, and other procedures performed by the supplier's internal audit functions
- Assurance programs (such as International Organization for Standardization [ISO] certifications) performed by third-party assessors

With the introduction of a SOC for Supply Chain framework, however, organizations may find that obtaining a SOC for Supply Chain report from their suppliers is the most efficient way to get the information they need to understand the risks of doing business with suppliers.

A natural extension of the CPA's role and specialized knowledge

The public accounting profession (that is, CPAs) has long been active in assisting organizations in addressing process and information security management.

Beginning in 1974, CPAs were required to consider the effects of information technology on historical financial statements during an audit of those statements. That requirement led to the development of

system and organization control (SOC)[1] reporting for service organizations (SOC 1® and SOC 2®). It also resulted in tremendous growth in the market for information security consulting services. Today, 4 of the leading 13 information security/cybersecurity consultants are CPA firms.

Information security and cybersecurity services that CPA firms offer are shown in the following chart:

Third-party reporting services	Cybersecurity governance advisory services	Information security/cybersecurity program advisory services
SOC for Service organization examination reports (e.g., SOC 1® and SOC 2® reports) • ISO 27001 certification • HITRUST assessment • Federal Information Security Modernization Act of 2014 reporting		
Cloud security advisory services	Information security/cybersecurity regulatory and compliance services	Security training services
Security policy development advisory services	Security threat management services	Security solution design and implementation services
Privacy advisory services	Managed security services	

Objective of the SOC for Supply Chain reporting framework

The objective of the SOC for Supply Chain reporting framework is to provide a means by which manufacturers, producers, and distribution companies can communicate useful information about their systems and the controls within the systems to customers and business partners. CPAs can examine and report on such information, thereby increasing the confidence that customers and business partners can place in the information.

The reporting framework and the CPA's report resulting from its use do the following:

- Provide a set of common criteria for disclosures about a manufacturing, production, or distribution company's system — Through the use of a common set of description criteria that set forth disclosures about the system, the SOC for Supply Chain report reduces the information burden on organizations by providing customers and business partners with

[1] In 2017, the AICPA introduced the term *system and organization controls* (SOC) to refer to the suite of services practitioners may provide relating to system-level controls of a service organization and system- or entity-level controls of other organizations. Formerly, SOC referred to service organization controls. By redefining that acronym, the AICPA enables the introduction of new internal control examinations that may be performed (*a*) for other types of organizations, in addition to service organizations, and (*b*) on either system-level or entity-level controls of such organizations.

useful information about the system and its controls to help users better understand the associated risks and make better decisions.

- Provide a set of common criteria for assessing control effectiveness —The SOC for Supply Chain report provides an independent assessment of the effectiveness of a manufacturer, producer, or distribution company's controls using the AICPA's 2017 trust services criteria for one or more of the following categories: security, availability, processing integrity, confidentiality, or privacy.
- Reduce the communication and compliance burden on organizations — The SOC for Supply Chain report reduces the number of information requests from customers and the amount of information sought if such requests are made.
- Provide useful information to customers and business partners while minimizing the risk of creating vulnerabilities to the organization— Information provided in the SOC for Supply Chain report is designed to meet the needs of customers and business partners without disclosing critical defenses that might be targeted by malicious actors.
- Provide comparability — The SOC for Supply Chain report would provide customers and business partners with information that could be used to track the progress of the organization's supply chain efforts across time and to benchmark those efforts against other organizations.
- Provide scalability and flexibility — The SOC for Supply Chain framework is useful to manufacturers, producers, and distribution companies of varying sizes and across all industries.
- Evolve to meet changes — The SOC for Supply Chain framework will be updated and modified over time based on experience, changes to the environment, and organization and stakeholder needs.

The SOC for Supply Chain framework leverages the core competencies of CPAs as providers of examination services, applying them to an organization's supply chain efforts in accordance with the AICPA's Code of Professional Conduct and attestation standards.

Components of the SOC for Supply Chain reporting framework

The SOC for Supply Chain reporting framework provides three key sets of information that, taken together, are intended to meet the objectives discussed previously. They are as follows:

1. *Management's description*. The first component is a management-prepared narrative description of the manufacturer, producer, or distribution company's system for producing a good or set of related goods. The description is designed to provide system-specific information about the organization's objectives, risks, and the processes and controls implemented and operated to address those risks. The description provides the context needed to enable customers and business partners to understand the conclusions management expresses in its assertion (see item [2]) and by the CPA in the CPA's opinion (see [3]) about the effectiveness of the controls included in the organization's description of its system.
2. *Management's assertion*. Management makes an assertion about whether the description is presented in accordance with the description criteria and whether the controls presented in the description were effective to provide reasonable assurance of achieving the organization's

objectives based on the trust services criteria. Both sets of criteria are discussed further in the next section.

3. *The CPA's opinion*. The final component is a CPA's opinion on the description and on the effectiveness of controls within the system to achieve the organization's objectives.

Two sets of criteria used in the framework

To implement the reporting framework, the AICPA developed two sets of different but complementary criteria to be used in a SOC for Supply Chain engagement:

- Description criteria to be used by management when preparing a description of its system and by the CPA when evaluating management's description. The description criteria were publicly exposed in 2019 and finalized in March 2020.

- Control criteria to be used by management when assessing controls within the system and by the CPA when evaluating the effectiveness of those controls to achieve the organization's system objectives. Since 1997, the AICPA has maintained a set of criteria used to evaluate the security, availability, processing integrity, confidentiality, or privacy of systems. The most recent version of these criteria, the *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, or Privacy* (commonly referred to as the 2017 trust services criteria), are used as control criteria in a SOC for Supply Chain examination.

In addition to the two sets of criteria, the AICPA's Assurance Services Executive Committee Supply Chain Working Group, working in conjunction with the AICPA's Auditing Standards Board, has developed an attestation guide, *SOC for Supply Chain: Reporting on an Examination of Controls Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy in a Production, Manufacturing, or Distribution System* (referred to as the SOC for Supply Chain guide), which provides guidance to CPAs on how to perform a SOC for Supply Chain examination in accordance with the AICPA attestation standards. The guide was published in March 2020.

Related AICPA efforts

In 2011, the AICPA released a reporting framework designed to provide customers of service providers with information useful in managing the risks associated with doing business with a service provider. A SOC 2® — SOC for Service Organizations: Trust Services Criteria report provides information on a service provider's processes and controls to enable customers to (*a*) evaluate the risks of doing business with the service provider and (*b*) understand the controls at the service provider so they can design their own controls to complement the service provider's controls.

Since its inception, this reporting framework has become a widely accepted tool in managing service provider risk. Now, the SOC for Supply Chain reporting framework may be used to address the risks associated with manufacturers, producers, and distribution companies.

The SOC for Supply Chain examination is part of the AICPA's suite of SOC services. Through a SOC engagement, a CPA provides an opinion on a service organization's system controls (in a SOC 1, SOC 2, SOC 3, or SOC for Supply Chain examination) or on entity-wide controls (in a SOC for Cybersecurity examination).

All of these engagements focus on examination-level assurance; in other words, the CPA expresses an opinion on management-prepared information about the organization's system or cybersecurity program and the effectiveness of controls within the system or program. The CPA's opinion increases the credibility of that information and the reliance that users can place on it.

Conclusion

The AICPA believes that a manufacturer, producer, or distributor and its customers and business partners will be best served if there is a defined set of information intended to enhance understanding of controls over manufacturing, production, and distribution systems. The information in the SOC for Supply Chain report is intended to provide useful information to stakeholders while also being

- transparent,
- consistent across time,
- comparable between entities,
- reasonably complete,
- scalable, and
- flexible.

The SOC for Supply Chain examination could go far in meeting the information needs of customers and business partners of manufacturers, producers, or distributors.