armanino

Transparency Into Supply Chain Risk

WHY YOU NEED A SOC FOR SUPPLY CHAIN REPORT

AN ARMANINO WHITE PAPER

OVERVIEW

Due to the significant reliance between companies that produce, manufacture or distribute products, there is interconnectedness between suppliers, consumers and business partners. These partnerships constitute the supply chain. Modern supply chains have become increasingly complex because of automation and technological advancements.

Each time an entity does business with a supplier, new supply chain risks arise, many of them not visible and beyond the purview of an individual organization. Although these relationships may be beneficial in terms of increasing revenue and market opportunities and reducing costs, the resulting vulnerabilities may threaten the entity's ability to meet critical deliverables. For example, they may be unable to provide products that adhere to performance specifications. Or, they may fail to satisfy quality and delivery commitments or production, manufacturing or distribution agreements.

For these reasons, companies must have visibility across their supply chain to completely understand and manage the risks that arise from doing business with suppliers, including the controls suppliers have in place to alleviate those risks. If not managed properly, these risks can lead to loss of intellectual property, reputational damage, obstruction of key business operations, fines, litigation, etc.

Due to these high stakes, managing supply chain risk has become an increasingly critical issue for companies and their stakeholders. To provide confidence to the organizations they do business with, suppliers also want to communicate how they are addressing the production and distribution risks in their own systems.

The Impact of COVID-19

Producers, manufacturers and distributers face various vulnerabilities due to the complex network and relationships that exist between them. Some common causes of supply chain disruption are:

- Natural disasters and weather conditions that affect a supplier's facility
- Threat of military action or war in the location of a supplier's plant
- Poor financial condition of a shipper or primary supplier
- Disease (COVID-19, SARS, MERS, etc.)

Businesses worldwide have had to manage disturbances caused by the COVID-19 outbreak. This widespread disruption has brought the criticality of supply chain administration and supply chain vulnerabilities into the limelight. More than ever, it is crucial for companies to get a better understanding of their supply chain — how their suppliers source products, how to alter their material acquisition, etc.

These are some ways organizations can mitigate supply chain risk amid COVID-19 or other disruption:

- Collect data to predict demand risk and plan for other risks that arise by communicating with vendors (the inability to source from vendors in China during the pandemic has led to great inventory concerns).
- Improve visibility in the supply chain by getting an understanding of demand, supply conditions, inventories (upstream and downstream), production and purchasing plans.
- Use advanced analytics to plan ahead and give supply chain executives better visibility and data to make preemptive decisions like buying extra inventory and looking into alternate sourcing options.
- Have multiple sources for products and resources across geographies; do not rely on a single source for important components.
- Better prepare for disruption by performing regular risk assessments, monitoring vendors and developing business continuity plans.

What Is a SOC for Supply Chain Report?

To help organizations, their customers and their business partners identify, assess and address supply chain risks, the American Institute of Certified Public Accountants (AICPA) has developed a voluntary reporting framework to foster greater transparency in the supply chain. A System and Organization Controls (SOC) for Supply Chain Report uses this market-driven, flexible framework to provide information about controls within a service organization's system relevant to security, availability, processing integrity, confidentiality and/or privacy.

A SOC for Supply Chain examination addresses any system used to produce, manufacture, or distribute goods, for example:

- Producers – organizations that make a product. (e.g., companies that extract raw materials or develop software for on-premise installation)
- Manufacturers – organizations that convert raw materials into finished goods for use or sale (e.g., clothes, machine parts)
- Software developers – those who develop and sell software designed for user implementation with minimal to no customization of the underlying computer code
- Distributors – businesses that provide or manage another entity's logistics (e.g., order fulfillment, inventory management)

The Value of a SOC for Supply Chain Report

A SOC for Supply Chain Report is intended to enable users to manage risks arising from business relationships with their supplier and distribution network. Companies can use the SOC for Supply Chain framework to relay information about their supply chain risk management efforts and the controls and processes they have in place to prevent, detect and respond to supply chain vulnerabilities.

CPAs can use the framework to examine and report on management-prepared system information and on the effectiveness of system controls, strengthening stakeholders' trust in the information.

Contents of a SOC for Supply Chain Report

- Section 1 - Assertion of company's management about the description and whether controls stated in the description were effective to provide reasonable assurance that the entity's system objectives were achieved based on the applicable trust services criteria
- Section 2 - Independent accountant's report
- Section 3 - Description of the company's system that includes details about:
    - Manufacturing and distribution system
    - Principal system objectives
    - System components (infrastructure, software, people, procedures, data, materials)
- Section 4 - Description of the testing procedures performed by the practitioner and the results thereof
- Section 5 - Any other information provided by company management that was not covered in the report

Description Criteria	Implementation Guidelines
The description contains the following information applicable to the system and the trust services category or categories addressed by the description:	**When making judgments about the nature and extent of disclosures to include, consider the following:**
DC 1: The types of goods produced, manufactured, or distributed by an entity and, if relevant, the characteristics of the production, manufacturing or distribution processes[1]	The types of goods produced, manufactured, or distributed by an entity and, if relevant, the characteristics of the production, manufacturing, or distribution processes[2]
DC 2: The principal product performance specifications, commitments, and requirements and production, manufacturing, or distribution commitments and requirements (principal system objectives)[3]	The principal product specifications, commitments, and requirements, and production, manufacturing, or distribution commitments and requirements (system objectives)[4]
DC 3: For identified system incidents that were the result of controls that were not effective or otherwise resulted in a significant failure in the achievement of one or more of the entity's principal system objectives during the period addressed by the description, the following information: a. Nature of each incident b. Timing surrounding the incident c. Extent (or effect) of the incident and its mitigation and remediation[5]	For identified system incidents that (a) were the result of controls that were not effective or (b) otherwise resulted in a significant failure in the achievement of one or more of the entity's system objectives during the period of time addressed by the description, the following information: a. Nature of each incident b. Timing surrounding the incident c. Extent (or effect) of the incident and its disposition[6]
DC 4: Risks that may have a significant effect on the entity's ability to achieve its principal system objectives[7]	Significant risks that affect the entity's production, manufacturing, or distribution[8]
DC 5: Relevant information about the system that produces, manufactures, or distributes the products, including the following: a. Components of the system, to include i. infrastructure, ii. software, iii. people, iv. procedures, and v. data b. Significant inputs used by the system (raw materials and other inputs) c. Boundaries of the system, when necessary to prevent users from misunderstanding the system being described[9]	Inputs to the system (raw materials and other inputs) and the components of the system used to produce, manufacture, or distribute the product. Components include the following: a. Infrastructure b. Software c. People d. Procedures e. Data[10]

[1] DC section 300, *2020 Description Criteria for a Description of an Entity's Production, Manufacturing, or Distribution System in a SOC for Supply Chain Report*, issued in March 2020 by the AICPA's Assurance Services Executive Committee

[2] Ibid
[3] Ibid
[4] Ibid
[5] Ibid
[6] Ibid
[7] Ibid
[8] Ibid
[9] Ibid
[10] Ibid

Description Criteria	Implementation Guidelines
DC 6: The applicable trust services criteria and the related controls designed to provide reasonable assurance that the entity's principal system objectives were achieved	The applicable trust services criteria and the related controls designed to provide reasonable assurance that the entity's system objectives were achieved
DC 7: If a customer's controls are necessary, in combination with controls at the entity, to provide reasonable assurance that the entity's principal system objectives would be achieved, those complementary customer controls	If a customer's controls are necessary, in combination with controls at the entity, to provide reasonable assurance that the entity's system objectives would be achieved, those complementary customer controls
DC 8: If a supplier's controls are necessary, in combination with controls at the entity, to provide reasonable assurance that the entity's principal system objectives are achieved and a. the entity is using the carve-out method (most common), the following: i. The nature of the products produced, manufactured, or distributed or the services provided by the supplier ii. Each applicable trust services criterion that is intended to be met by controls at the supplier iii. The types of controls that entity management assumed, in the design of the entity's system, would be implemented by the supplier and are necessary, in combination with controls at the entity, to provide reasonable assurance that the entity's principal system objectives are achieved; such controls are commonly referred to as complementary supplier controls or CSCs[11] b. the entity is using the inclusive method, the following: i. The nature of the products produced, manufactured, or distributed or the services provided by the supplier ii. The portions of the system that are attributable to the supplier iii. Relevant aspects of the supplier's infrastructure, software, people, procedures, and data iv. The controls at the supplier that are necessary, in combination with controls at the entity, to provide reasonable assurance that the entity's principal system objectives are achieved	If a supplier's controls are necessary, in combination with controls at the entity, to provide reasonable assurance that the entity's system objectives are achieved and a. the entity is using the carve-out method (most common), the following: i. The nature of the products produced, manufactured, or distributed or the services provided by the supplier ii. Each of the applicable trust services criteria that are intended to be met by controls at the supplier iii. The types of controls that entity management assumed, in the design of the entity's system, would be implemented by the supplier and are necessary, in combination with controls at the entity, to provide reasonable assurance that the entity's system objectives are achieved (commonly referred to as complementary supplier controls or CSCs) b. the entity is using the inclusive method, the following: i. The nature of the products produced, manufactured, or distributed or the services provided by the supplier ii. The portions of the system that are attributable to the supplier iii. Relevant aspects of the supplier's infrastructure, software, people, procedures, and data iv. The controls at the supplier that are necessary, in combination with controls at the entity, to provide reasonable assurance that the entity's system objectives are achieved[12]

[11] Ibid
[12] Ibid

Description Criteria	Implementation Guidelines
DC 9: Any specific applicable trust services criterion that is not relevant to the system and the reasons why it is not relevant	Any specific applicable trust services criterion that is not relevant to the system and the reasons it is not relevant
DC 10: Significant changes during the period addressed by the description to the entity's system and controls that are relevant to the achievement of the entity's principal system objectives[13]	Significant changes during the period addressed by the description to the entity's system and controls that are relevant to the achievement of the entity's system objectives[14]

Report Criteria

Two sets of different but complementary criteria are used in an engagement:

1. Description criteria for use by a company's management when preparing a description of its system and by the CPA when evaluating management's description.

2. Control criteria for use by a company's 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. Control criteria evaluate the effectiveness of controls to provide reasonable assurance that the company's principal system objectives are met. These are the same control criteria as those in a SOC 2 report – the trust services criteria. The AICPA aims to use the existing *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*, similar to the SOC 2 and SOC for Cybersecurity reports.[15]

- **Security** – Systems and information are protected against unauthorized access, unauthorized disclosure of information and damage to systems that could compromise the availability, integrity, confidentiality, or privacy of information or systems and affect the organization's ability to achieve its objectives.
- **Availability** – Systems and information are available for operation and use to achieve the organization's objectives.
- **Processing integrity** (over the provision of services or the production, manufacturing or distribution of goods) - System processing is complete, valid, accurate, timely and authorized to achieve the organization's objectives (i.e., to produce, manufacture, or distribute goods that meet the products' specifications).
- **Confidentiality** - Information designated as confidential is protected to achieve the organization's objectives.
- **Privacy** (in a production, manufacturing, or distribution system) - Personal information is collected, used, retained, disclosed and disposed of to achieve the organization's objectives.

[13] Ibid
[14] Ibid
[15] Ibid

Inclusive vs. Carve-Out Reports

Carve-out method

When the controls performed by the supplier are necessary, in combination with the entity's controls, to achieve the system objectives, such controls are referred to as complementary supplier controls (CSCs). Since CSCs are important to report users, they are disclosed in the description. The most typical method for presenting CSCs is to include only those processes and controls that the entity is responsible for performing and identify the CSCs that the entity expects suppliers to implement. This is known as the carve-out method.[16]

When using the carve-out method, the description identifies the types of CSCs that the supplier is expected to implement and the trust service criteria they affect. Consideration also may be given to disclosing the identity of the supplier when such information may be useful to customers or business partners. CSCs are usually presented in tabular format near the end of the description, along with the trust service criteria to which each CSC relates. Management may request the practitioner's assistance when determining how to present the CSCs in the description. The practitioner can provide examples of CSC disclosures made by other entities and make recommendations to improve the presentation of the CSCs in the description.[17]

Inclusive method

In some cases, entity management may want to present the relevant processes and controls of the supplier in its description either to meet the common information needs of users or because of the significance of the supplier's role in the process. This is known as the inclusive method of presentation.[18]

Under the inclusive method, the relevant aspects of the supplier's infrastructure, software, people, procedures and data are considered part of the entity's system. Therefore, they are disclosed in the description and subject to the practitioner's examination procedures. The description separately identifies controls at the entity and controls at the supplier. Note that when the inclusive method is used, supplier management is also a responsible party in the examination.[19]

[16] Ibid
[17] Ibid
[18] Ibid
[19] Ibid

	SOC for Supply Chain Examination	SOC 2 Standard Examination	SOC 1 Examination	SOC for Cybersecurity Examination
Type of organization	An entity that produces, manufactures or distributes products	Organization or segment of an organization that provides services to user entities	Organization or segment of an organization that provides services to user entities	Any type of organization
System level or entity-wide?	Entity's system or systems that produce, manufacture or distribute products	System or systems that provide services	System or systems that provide services	Entity-wide cybersecurity risk management program or can be narrowed to specific system
Purpose of the report	To provide users with information about controls within the entity's system relevant to security, availability, processing integrity, confidentiality or privacy to enable users to manage risks arising from business relationships with their supplier and distribution network	To provide users with information about controls at the service organization relevant to security, availability, processing integrity, confidentiality or privacy to support users' evaluation of their own systems of internal control	To provide users with information about controls at the service organization relevant to financial reporting	To provide general users with useful information about an entity's cybersecurity risk management program for making informed decisions
Intended users	Entity management and specified parties who have sufficient knowledge and understanding of the entity and its system	Service organization management and specified parties who have sufficient knowledge and understanding of the service organization and its system	Service organization management and specified parties who have sufficient knowledge and understanding of the service organization and its system	Entity management, directors, and a broad range of general users including analysts, investors, and others whose decisions might be affected by the effectiveness of the entity's cybersecurity risk management program

	SOC for Supply Chain Examination	SOC 2 Standard Examination	SOC 1 Examination	SOC for Cybersecurity Examination
Applicable standard	AT-C section 105, Concepts Common to All Attestation Engagements, and AT-C section 205, Examination Engagements, in AICPA Professional Standards	AT-C section 105 and AT-C section 205 in AICPA Professional Standards	AT-C section 105 and AT-C section 205 in AICPA Professional Standards	AT-C section 105 and AT-C section 205 in AICPA Professional Standards
Scope	Controls relevant to security, availability, processing integrity, confidentiality, or privacy in a production, manufacturing, or distribution system	Controls at a service organization relevant to security, availability, processing integrity, confidentiality, or privacy	Controls at a service organization relevant to transaction processing and supporting IT general controls.	Entity's cybersecurity risk management program and controls
Responsible party	Entity management	Service organization entity management	Service organization entity management	Entity management
Report distribution	Restricted to use of the entity and specified parties	Restricted to use of the service organization and specified parties	Restricted to use of the service organization and specified parties	Appropriate for general use

Considerations for including bundled services in the scope of the examination

Many entities that produce, manufacture, or distribute products bundle services with the sales of those products. In such situations, it may not be practical to perform separate examinations of system controls relevant to the production, manufacturing, or distribution of products and system controls used to provide the bundled services. In that case, the responsible party and the practitioner may agree to include the systems and controls within those bundled services within the scope of the SOC for Supply Chain examination.

More Likely to Include the Bundled Services in a SOC for Supply Chain Examination	More Likely to Include the Bundled Services in a SOC 2 Examination
The services relate to the physical good produced (for example, maintenance services provided in connection with sale of a car).	The services relate to data or intangible goods produced (for example, contract application development).
	The physical good is incidental to the provision of the bundled service. (An independent report on the service might be more useful to the users.)

STRATEGIC INSIGHTS PRACTICAL ACTION

Armanino provides an integrated set of accounting services — audit, tax, consulting and technology solutions — to a wide range of organizations operating both in the U.S. and globally.

You can count on Armanino to think strategically and provide the sound insights that lead to positive action. We address not just your compliance issues, but your underlying business challenges, as well — assessing opportunities, weighing risks, and exploring the practical implications of both your short- and long-term decisions.

When you work with us, we give you options that are fully aligned with your business strategy. If you need to do more with less, we will implement the technology to automate your business processes. If the issue is financial, we can show you proven benchmarks and best practices that can add value companywide. If the challenge is operational, we'll consult with your people about workflow efficiencies. If it is compliance, we'll ensure that you meet the requirements and proactively plan to take full advantage of the changes at hand. At every stage in your company's lifecycle, we'll help you find the right balance of people, processes and technology.

For additional information, contact:

Liam Collins
Partner-In-Charge, SOC Audit Practice
liam.collins@armaninoLLP.com
415 710 4705

Ryan Goodbary
Director, SOC Audit Practice
ryan.goodbary@armaninoLLP.com
415 568 3463

armanino