No. 2020-06
12 March 2020

To the Point

AICPA issues criteria for describing and reporting on controls over a production or manufacturing system

The framework can be used for reporting on a system that produces, manufactures or distributes products.

What you need to know

- The AICPA issued criteria that establish a framework for manufacturers, producers and distributors for describing the controls over a production system in reports used by customers and business partners.
- The AICPA Trust Services Criteria (TSCs) can be used, in conjunction with this framework, for evaluating the effectiveness of the controls as they relate to security, availability or processing integrity of the production system, or the confidentiality or privacy of information used in conjunction with the production of goods.
- The framework also provides the supplier with a basis for engaging an independent certified public accountant to report on the information provided and the effectiveness of supplier controls, increasing the customer's trust and confidence in the supplier and its processes.

Overview

The Assurance Services Executive Committee (ASEC) of the American Institute of Certified Public Accountants (AICPA) issued a set of criteria for preparing and evaluating a description of a system used to manufacture, produce or distribute goods in a System and Organization Controls (SOC) for supply chain report. The criteria are part of a framework used by manufacturers, producers and distributors (collectively, suppliers) to communicate the controls they implemented to manage the risks related to the achievement of their principal system objectives, including commitments to customers.

To increase customer trust and confidence in the supplier and its processes, the supplier's management may engage an independent certified public accountant to evaluate whether management's description is presented in accordance with the new criteria and whether controls were effective to provide reasonable assurance that the supplier's principal system objectives were achieved. Such an engagement is called a SOC for supply chain examination and is performed in accordance with AICPA Attestation Standards. A SOC for supply chain examination report includes the following sections:

- A description of an entity's system for manufacturing, producing or distributing goods, including the controls over that system
- A written assertion by management that its description is presented in accordance with the description criteria established by ASEC and the controls over that system are effective
- An opinion of an independent certified public accountant on the description and either the suitability of design or the effectiveness of the entity's controls
- A description of the accountant's test performed over the operating effectiveness of the controls and the results of those tests, as applicable

The framework for reporting on a system to manufacture, produce or distribute goods is a companion to the SOC 2® framework for reporting on controls at service providers. The SOC 2 framework has been used since 2011 and has become a widely accepted method for obtaining useful information on a service provider's controls over its system.

Key considerations

The ASEC developed the criteria and reporting framework for suppliers to provide relevant information about their risk management efforts and the processes and controls in place to detect, prevent and respond to risks related to the security, availability, processing integrity, confidentiality or privacy of their production processes.

As suppliers adopt the framework and engage independent certified public accountants to report on their systems, their customers and business partners will benefit by having:

- A system description and an assessment of controls over that system based on common sets of criteria used by many different entities, resulting in a reduced need to understand multiple evaluation frameworks
- Reduced communication and compliance burdens on customers and business partners
- Greater comparability with other suppliers and for the same supplier between periods

Suppliers will benefit by using a reporting framework that is consistent between entities of different sizes, but flexible and adaptable to different organization sizes, industries, environments and circumstances. They will also benefit from reduced communication and compliance burdens.

The description criteria identify the information that supplier management should share with customers and business partners about an entity's system and controls, including:

- The types of goods produced, manufactured or distributed by the system
- The principal product specifications, commitments and requirements made by the supplier (principal system objectives)

- Any identified system incidents resulting from controls that were not effective or resulting in a significant failure in the achievement of one or more of the entity's principal system objectives
- Risks that may have a significant effect on the entity's ability to achieve its principal system objectives
- Relevant information about the system, such as:
  - Components of the system, including infrastructure, software, people, procedures and data
  - Significant inputs used by the system (raw materials and other inputs)
  - Boundaries of the system
- The applicable trust services criteria and the related controls designed to provide reasonable assurance that the entity's principal system objectives were achieved
- 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

The description criteria include implementation guidance for each criterion and factors for suppliers to consider when making judgments about the nature and extent of disclosures required.

The framework will help members of the supply chain ecosystem effectively manage risks arising from a supplier.

How we see it

- The SOC for supply chain framework is a useful tool in assessing and managing supplier risk for complex supply chains, including managing risks from technology in both processes and products, and increased cybersecurity risks.
- We expect the use of the supply chain reporting framework by suppliers to increase value to customers and other stakeholders, similar to SOC 2 reports for service organizations' users.
- The criteria and supporting framework are expected to be useful for suppliers in the automotive and transportation, consumer, diversified industrial product, life sciences, mining and metals, oil and gas, and technology sectors.

The following examples illustrate how the criteria may be used.

Illustration 1 — Manufacturer — security only

The IT systems of Manufacturer A are connected through a virtual provider network with the IT systems of a key supplier, Supplier B. Manufacturer A has determined that Supplier B would pose a significant cybersecurity risk to its manufacturing systems if the IT systems of Supplier B are breached. Manufacturer A requests Supplier B to obtain a SOC for supply chain report from an independent certified public accountant so that it can understand and evaluate the effectiveness of controls that Supplier B has implemented to address its cybersecurity risks.

Illustration 2 — Distributor — security, availability and confidentiality

Distributor C provides inventory/order management and fulfillment/shipping services for a regional retailer of consumer goods. Distributor C is responsible for managing store stock levels (availability) and the physical shipment of goods to various retail locations. Distributor C is also responsible for order fulfillment and shipping for the retailer's e-commerce presence.

The retailer is responsible for providing the order details and customer shipping information to Distributor C, which is made possible by providing Distributor C with real-time access (through vendor log-on credentials) to its inventory management system and e-commerce system. The retailer requests Distributor C to obtain a SOC for supply chain report from an independent certified public accountant so that it can understand and evaluate the effectiveness of the controls Distributor C has in place to address its security risks and confidentiality concerns related to the access to customer data.

SCORE No. 08551-201US

ED None

ey.com/us/accountinglink