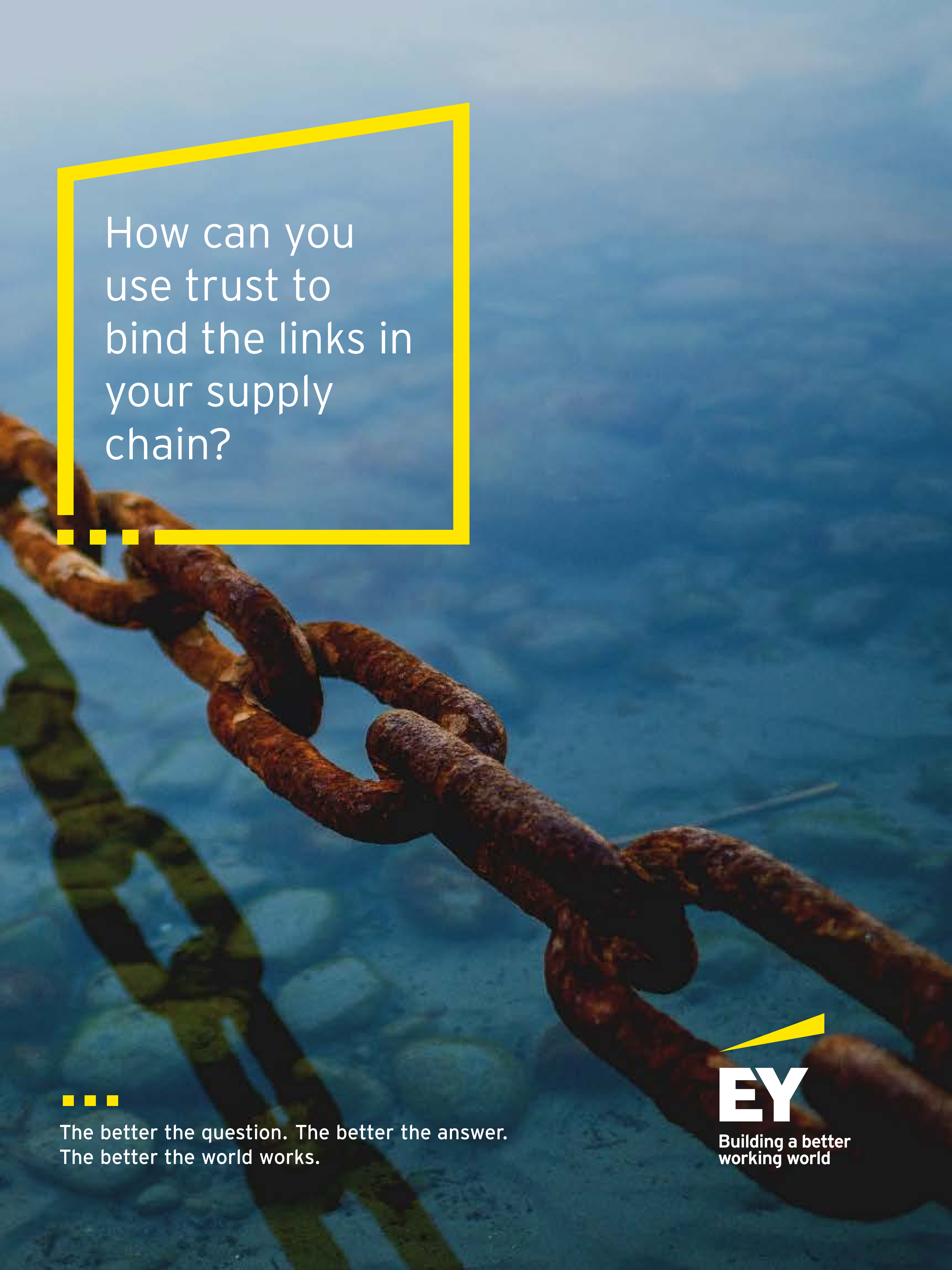


How can you use trust to bind the links in your supply chain?

The better the question. The better the answer.
The better the world works.

EY
Building a better
working world

Establishing trust in the supply chain

Effectively managing risks that arise from dependencies within a supply chain is imperative for members of the supply chain ecosystem to thrive. Having trustworthy supply chain partners helps mitigate these risks. Entities that partner well with their suppliers to build a resilient supply chain, through robust acceptance processes, periodic performance measures, structured supplier decision-making and organized relationship governance, are the ones that thrive.

Historically, trust has been built over time by evaluating the quality of inputs received from a supplier and its performance. However, due to growth in the complexity of supply chains, the evolution of technology in both processes and products, and increased cybersecurity risks, organizations can no longer mitigate supplier risks by simply measuring the quality of inputs and assessing past performance. Instead, organizations need a robust vendor risk management (VRM) program.

A key component of a VRM program is to obtain an understanding of the manufacturing, production and distribution activities of suppliers, and perform an assessment of the controls over those activities in order to evaluate and mitigate the risks arising from the relationship. Currently, organizations assemble this understanding from many different sources. However, the American Institute of Certified Public Accountants (AICPA) has developed a new supply chain reporting framework to permit suppliers to provide relevant information about their risk management efforts to customers to make their processes more efficient and effective.

Supply chain reporting framework – use and benefits

The AICPA's supply chain reporting framework is intended for systems that are used to:

- Produce, manufacture or distribute a single physical product or intangible product
- Operate a production line
- Produce, manufacture or distribute products produced or manufactured within a single facility or physical plant
- Develop and distribute off-the-shelf or packaged software

Suppliers can use this framework to communicate to customers 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 and availability of their production processes. The criteria used to evaluate security and availability are part of a framework, called the Trust Services Criteria (TSC), that includes criteria for evaluating the processing integrity, confidentiality and privacy of a system. The reporting framework also supports a system's processing integrity and its protection of confidential or personal information.

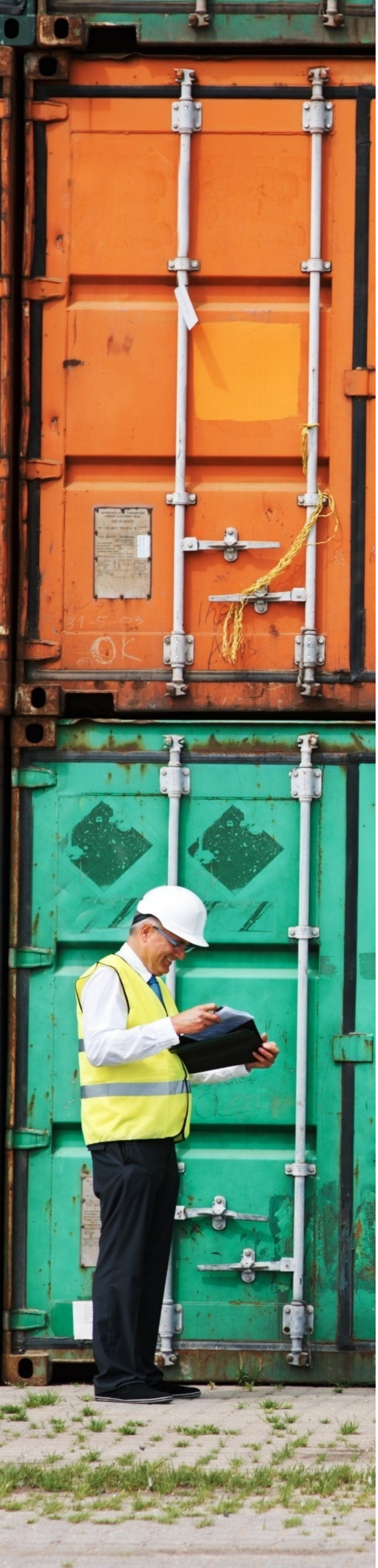
The framework also provides a basis for the supplier to engage an independent CPA to report on the fairness of the information provided and the effectiveness of supplier controls, increasing the customer's trust and confidence in the supplier and its processes. Benefits of adopting the framework, especially when combined with a CPA's opinion, include:

- A set of common criteria for disclosures about an entity's system for manufacturing, producing and/or distributing goods
- Reduced communication and compliance burden on organizations
- Useful information to a wide array of customers, while minimizing the risk of creating vulnerabilities
- Comparability – both with other organizations and for the same organization over time
- Scalability and flexibility – suitable for organizations of all magnitudes and industries
- Adaptability – a framework that is dynamic and will adapt with experiences, the environment and stakeholder needs

Building trust in supply chain relationships

How might a manufacturer, producer or distributor use a System and Organization Controls (SOC) for supply chain report to support their operations? Let's explore a few different use case scenarios.

1	A **manufacturer** wants to demonstrate to its customers the effectiveness of controls relevant to security and product availability.
2	A **software** developer that produces and sells software wants to demonstrate to its customers the effectiveness of controls relevant to (physical and logical) security and confidentiality during the production process.
3	A **distribution and logistics** company, responsible for managing other entities' logistics, including warehousing, inventory management, order fulfillment and distribution, wants to demonstrate to its customers the effectiveness of controls relevant to security, processing integrity (based on customer commitments) and availability.



Steps to building a trusted supply chain

The process of applying the SOC for supply chain framework includes:

Identifying the system used to manufacture, produce or distribute the goods for the customers and the components of the system (i.e., infrastructure, software, people, data and procedures used in the processes)

Selecting the TSC categories of concern to customers and the period of time covered by the description

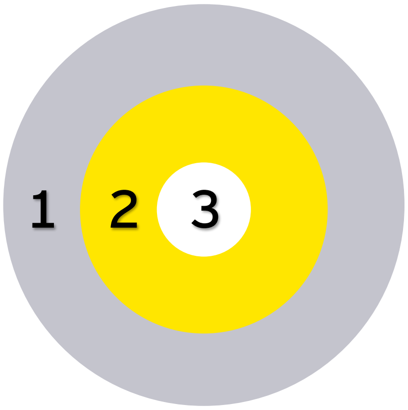
Identifying the risks that are of concern to customers (which may relate to achieving commitments or requirements, such as the NIST CSF)

Identifying the controls that have been implemented to address those risks, based on the category or categories being addressed

Preparing the description based on these items in adequate detail so that readers can comprehend how the system functions and how management and the CPA firm assess the effectiveness of controls (management's description)

Once these measures are established, it is the CPA firm's responsibility to evaluate whether: (1) the entity's system objectives are appropriate, (2) the description presents the system that was designed and implemented in accordance with description criteria, and (3) the controls stated in the description are effective to provide reasonable assurance that the entity's system objectives are achieved based on the applicable TSC (**CPA firm's opinion**).

Given the details presented, who are the intended users likely to benefit most?



1. **Customers** of the supplier who:
   - Use the products of the system as:
     - Inputs to their products
     - Components of their production, manufacturing or distribution systems
   - Rely on a physical distribution system for products used as inputs to products
2. **Business partners** of an entity that:
   - Are dependent on a customer or distributor for their sales
   - License the use of their intellectual property to others
3. **Prospective customers and business partners**

Components of SOC for supply chain reporting

A report prepared using the framework is referred to as a *SOC for supply chain report* and, if it includes a CPA's opinion, will have the following components:

Management's description – a narrative of the system used for manufacturing, producing and/or distributing a good or set of related goods, along with the supplier's objectives, risks and the processes and controls implemented and operated to address those risks

Management's assertion about whether the description is presented in accordance with predefined description criteria and if the controls presented in the description were effective to achieve the supplier's objectives based on the control criteria

CPA firm's opinion on the description and on the effectiveness of controls within the system to achieve the supplier's objectives

Supplier's controls and CPA's description of procedures performed and results of the procedures – supporting information and detail for the CPA firm's opinion and whether there was any failure at the individual control level or for a specific criterion

AICPA Literature

Additional resources are available from the AICPA and can be found on their website, http://www.aicpa.org. Final guidance from the AICPA is anticipated by Q4 2019. For more information, please contact AmericasSOCR@ey.com or your engagement executive.

AICPA Description Criteria	https://www.aicpa.org/content/dam/aicpa/interestareas/frc/assuranceadvisoryservices/downloadabledocuments/exposuredrafts/ed-description-criteria-for-vsc.pdf
AICPA Trust Services Criteria	https://www.aicpa.org/content/dam/aicpa/interestareas/frc/assuranceadvisoryservices/downloadabledocuments/trust-services-criteria.pdf

EY | Assurance | Tax | Transactions | Advisory

About EY

EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. Information about how EY collects and uses personal data and a description of the rights individuals have under data protection legislation are available via ey.com/privacy. For more information about our organization, please visit ey.com.

EYG no. 003822-19Gbl
ED None

This material has been prepared for general informational purposes only and is not intended to be relied upon as accounting, tax or other professional advice. Please refer to your advisors for specific advice.

ey.com