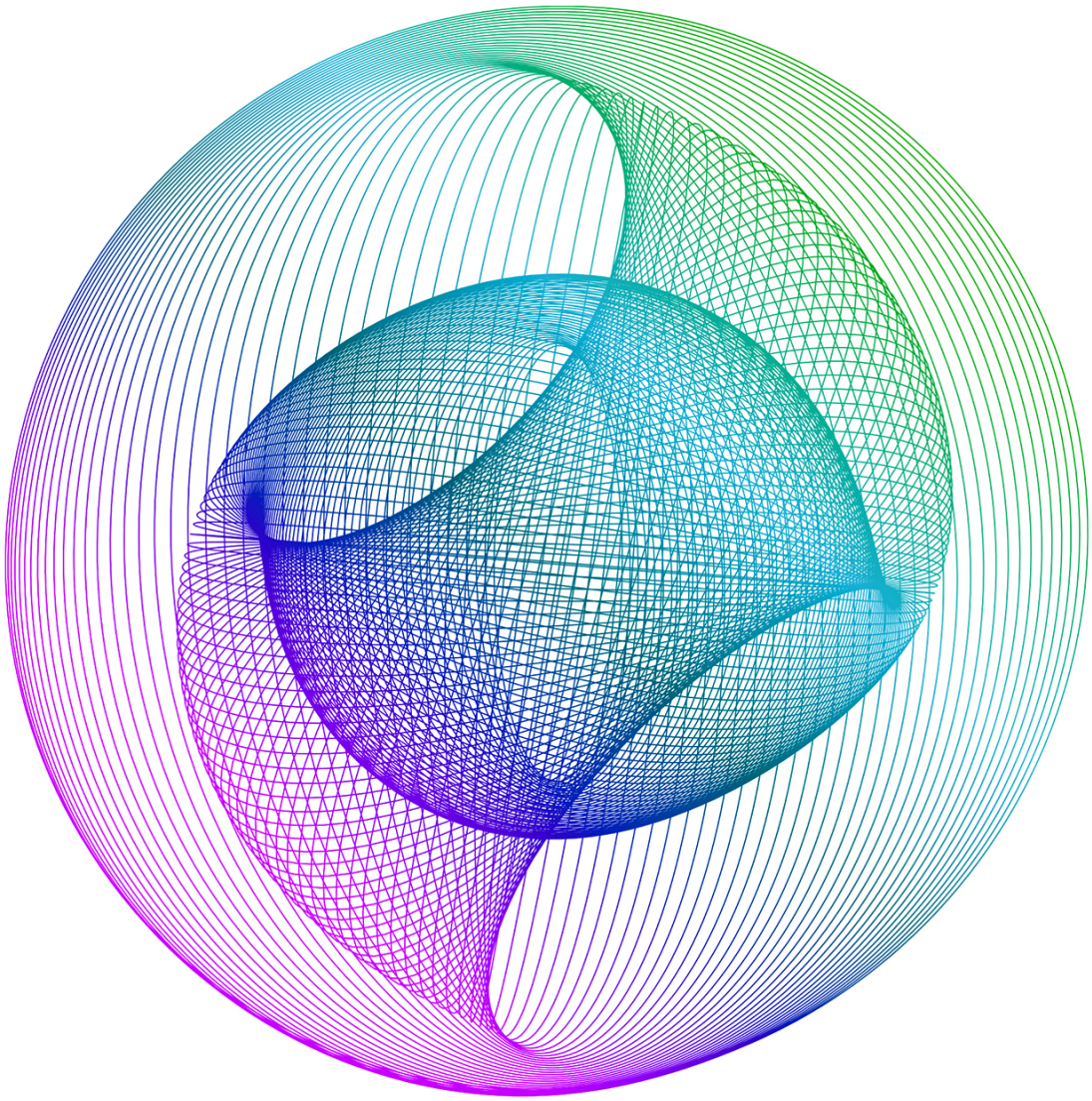
Deloitte.



Top five considerations for TPA governance

Guiding principles for optimizing third-party assurance reporting

MAKING AN IMPACT THAT MATTERS since 1845

Fulfilling customer requests for a wide range of third-party assurance (TPA) reports and numerous compliance questionnaires can quickly become unwieldy, draining valuable internal resources and inflating external costs.

As the number and frequency of these requests escalates, service organizations increasingly need a way to enhance their TPA portfolios. While there is no definitive “right” way for service organizations to structure their efforts to comply with their customers’ demands for assurance, there are some guiding principles that are often helpful in streamlining TPA reporting processes.

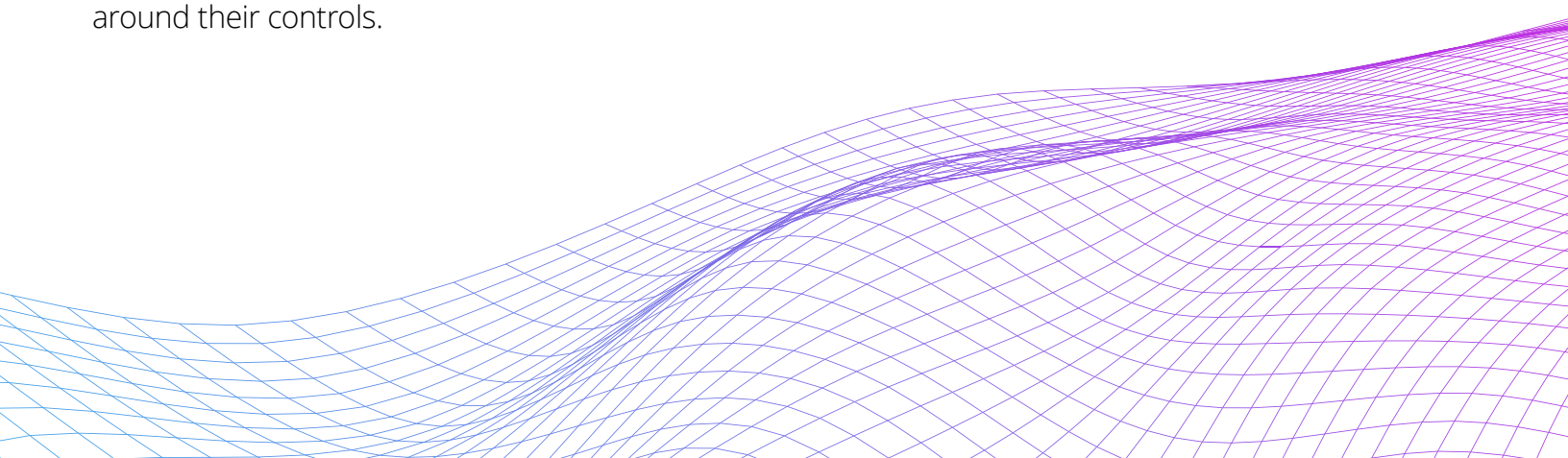
Introduction

Outsourcing is no longer a question; it's a given. With specialized services routinely being delivered through cost-effective centers of excellence, service organizations are woven into the fabric of most enterprises. Service organizations often find themselves serving many industries across multiple geographies, which expands the range of compliance and regulatory requirements they must meet. Meanwhile, companies that heavily rely on outsourcing are being exposed to an expanded universe of risks. These risks now include financial, operational, cyber, privacy, and business continuity, along with the overarching potential for reputational damage should a service organization act irresponsibly or fail to deliver.

Under increasing compliance pressures themselves, companies are asking service organizations to demonstrate the efficacy of their controls to higher and higher degrees. Consequently, the demand for TPA reports is on the rise. Based on annual service auditor reports issued by Deloitte, the total number of reports is increasing by about 5% per year. Enhanced, customizable SOC 2 reports, also called SOC 2+ reports, are in particular demand.

The landscape

The market is still coming to terms with the escalating TPA demands being placed on service organizations. The American Institute of Certified Public Accountants (AICPA) and other industry organizations have been evolving their frameworks both to provide a greater level of assurance and to streamline reporting processes. To this end, the AICPA created SOC 2+, an extensible framework that allows service auditors to incorporate various industry standards into a SOC 2 report. The AICPA also created a new cybersecurity attestation reporting framework in 2017, also known as SOC for Cybersecurity. Depending on the type of customer, TPA-related requests of service organizations may also include any number of industry-specific frameworks, such as those put forth by the Health Insurance Trust Alliance (HITRUST), the National Institute for Standards and Technology (NIST), the Cloud Security Alliance (CSA), and the Payment Card Industry Data Security Standard (PCI DSS). For service organizations that process, handle, or host customer data relevant to financial reporting, a SOC 1 report continues to be necessary, regardless of what other types of reports are required. Amid this complex and rapidly evolving compliance landscape, it is easy to see why service organizations are being challenged to rein in the costs of TPA reporting while still providing their customers with the required level of assurance around their controls.



Top five guiding principles

The proliferation of TPA reports, combined with regulatory and compliance requirements, demands a more efficient approach to TPA governance. Though each organization is unique, we have assembled a list of the top five broadly applicable principles for better managing a complex TPA portfolio, based on our observations in performing independent, third-party examinations for service organizations, from startups to multinational organizations across every major industry.

1 Establish a TPA steering committee.

- This should be a group of people who don't have day-to-day TPA responsibilities, but who have the right experience, expertise, and background to help guide the entire portfolio. A well-balanced steering committee will often include leaders from the TPA project management office (PMO) that is directing the TPA portfolio, the risk and compliance organization, legal, internal audit, sales and business development, IT leadership (i.e., CIO, CISO, etc.), and finance (i.e., often the CFO or controller). It is vital to include the PMO leader, whether that person is from internal audit, compliance, or some other group.
- The role of the steering committee is to:
  - Counsel people throughout the organization on efficient use of TPA resources;
  - Define and disseminate an overall TPA road map for the organization;
  - Empower people to make well-informed contracting decisions through a better understanding of how TPA reports are used;
  - Share leading practices across the organization;
  - Identify and eliminate redundant efforts; and
  - Assist in communicating with customers regarding why certain reporting decisions are made.
- Without a coordinating mechanism, it is difficult to get everyone on the same page. This incongruity breeds ill-informed actions, inconsistent messaging, and duplicative efforts. Establishing a steering committee offers a path to aligning and streamlining TPA obligations across the entire organization. When done well, it can be the single most important action an organization can take to curb the escalating cost of compliance.

2 Institute a check in the contracting process to ensure that the company's commitments to TPA reporting are appropriate.

Once a contract is finalized, organizations have no choice but to deliver the type of report that has been promised. That's why it's important to flag any concerns before signing on the dotted line. Prior to being finalized, contracts should be reviewed by a sanctioned gatekeeper, possibly someone in the TPA PMO, who can check to see if the SOC obligations specified in the contract are appropriate for the type of customer and aligned with the kind of work the company will be doing. This both helps mitigate the risk of overpromising and underdelivering and can reduce duplicative effort. It also aids the sales organization in understanding the true costs of additional compliance requirements. Taking this concept one step further, organizations should consider Salesforce training to prevent representatives from making inappropriate commitments prior to the contracting phase.

3 Align TPA governance to other risk and compliance efforts within the organization.

- Many service organizations are in reactive mode when it comes to managing TPA requests, mainly because they don't have a complete view of their internal and external reporting requirements. Creating a library of all enterprisewide requirements is the first step in identifying both gaps and overlaps (see "Risk and controls optimization summary" on pp. 8–9). Compiled and managed by the TPA PMO, the library should include internally identified requirements, such as SOC 1; other related compliance obligations, such as Sarbanes-Oxley (SOX) and the Federal Deposit Insurance Corporation Improvement Act (FDICIA); industry requirements (e.g., HITRUST, NIST, CSA, PCI DSS); and requirements included in any TPA reports the organization issues. The inventory should also include requirements covered in any questionnaires or service-level agreements that the organization responds to periodically. Finally, the library should be periodically updated through an established process with clear lines of responsibility.
- Once an enterprisewide library of requirements has been constructed, individual requirements can be mapped against the corresponding controls to determine which ones can be covered through TPA reports. For example, an organization may only have one control for regulating physical access to its data center, but this single control may align with 20 different requirements, both internal (e.g., SOX and SOC 1) and external (e.g., various TPA reports or specific customer requirements).
- Noting every requirement that a control fulfills paves the way for more efficient control testing. For instance, many TPA reports have common elements. When testing for one report, the results can often be applied to other reports with similar requirements. This also helps to identify single points of failure that could affect multiple compliance efforts so that management knows where to focus its attention. Additional efficiencies can be achieved by issuing TPA reports under multiple standards (e.g., US, global, or country-specific). The ability to issue these reports outside the United States is an important benefit for global providers.
- An integrated library of requirements and control tests can be especially useful for rapidly compiling customer-centric reports, since the results of each test are already mapped to all relevant requirements. Another way to gain efficiencies is by aligning the reporting periods covered by the various TPA reports so that they overlap as much as possible. This allows testing to be shared across different reports, thus saving a great deal of time.

4 Use SOC 2+ reports as much as possible.

- Created by the AICPA, SOC 2+ is an extensible framework that allows service auditors to incorporate various industry standards into a SOC 2 report. SOC 2+ reports are highly flexible tools that can incorporate multiple frameworks and industry standards into TPA reporting.
- By providing a standardized format for meeting a broad range of regulatory and industry control requirements, SOC 2+ reports eliminate the need for redundant activities and one-off responses. Through a single examination based on the AICPA Trust Services Criteria and one or more integrated frameworks, they allow service organizations to demonstrate to their customers and other stakeholders that effective internal controls are in place. SOC 2+ reports can also be tailored to meet the ever-growing list of security questionnaires by mapping to a suitable and available criterion, such as the standardized information gathering (SIG) questionnaire.

5

Proactively manage the full costs of TPA responsibilities.

- Many service organizations are starting to view costs through a broader lens (i.e., going beyond the hard costs of auditors' fees to encompass the soft costs of tying up internal resources). A complete analysis of TPA costs should include not only auditors' fees, but also the time that dedicated employees spend in managing the TPA portfolio, as well as the time control that owners spend in addressing requests. Service organizations are often inundated with security questionnaires from individual clients, requests for customer-specific TPA reports, and demands to arrange for burdensome onsite client auditor visits. When overwhelmed, some companies have a tendency to "throw people at the problem," so they build out large teams for supporting TPA governance and execution. While this is appropriate in some instances, we've found that one or two full-time employees is typically sufficient for administering a well-designed TPA reporting program.
- Beyond streamlining TPA processes and optimizing resource allocation, some companies are exploring another avenue for proactively managing the complete costs of fulfilling their TPA responsibilities. Though it's not commonplace, a few companies have started to charge their customers fees for reports, particularly those requiring extra effort. As costs escalate, this is something that companies should consider doing more frequently. The idea that customers and service organizations should share the cost of compliance must gain traction if service organizations are to keep up with the mounting number of requests for TPA reports without suffering financially. By writing these fees into their contracts, service organizations can start to level-set expectations regarding the costs that are involved, and it's only fair to share them.

Risk and controls optimization summary

What can organizations do?

As mentioned in consideration 3 in the previous section, the market is still coming to terms with the escalating TPA demands being placed on service organizations. The American Institute of Certified Public Accountants (AICPA) and other industry organizations have been evolving their frameworks both to provide a greater level of assurance and to streamline reporting processes. To this end, the AICPA created SOC 2+, an extensible framework that allows service auditors to incorporate various industry standards into a SOC 2 report. The AICPA also created a new cybersecurity attestation reporting framework in 2017, also known as SOC for Cybersecurity. Depending on the type of customer, TPA-related requests of service organizations may also include any number of industry-specific frameworks, such as those put forth by the Health Insurance Trust Alliance (HITRUST), the National Institute for Standards and Technology (NIST), the Cloud Security Alliance (CSA), and the Payment Card Industry Data Security Standard (PCI DSS). For service organizations that process, handle, or host customer data relevant to financial reporting, a SOC 1 report continues to be necessary, regardless of what other types of reports are required. Amid this complex and rapidly evolving compliance landscape, it is easy to see why service organizations are being challenged to rein in the costs of TPA reporting while still providing their customers with the required level of assurance around their controls. In order to achieve optimizations, service organizations need to do the following three steps:

1

Inventory compliance needs

Understand the risk domains of interest for compliance and the associated regulating bodies and timelines.

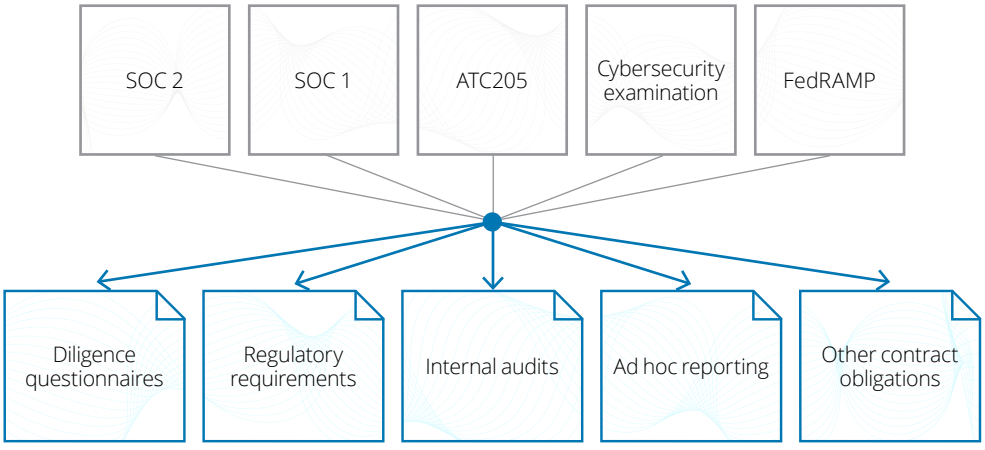
- Information security and data protection
- Third-party risk management and oversight
- Continuity and disaster recovery
- Cyber risk
- Legal and compliance risk
- Incident management
- HR policies and practices
- Performance and quality management
- Fraud risk
- Key person identification and practices
- Stability and reputational risk
- Geopolitical risk

2 Connect the compliance dots

Identify existing frameworks and controls within the organization. Map controls to the internal risk domains, and measure the ability to meet compliance requirement against an established baseline.

3 Optimize reporting

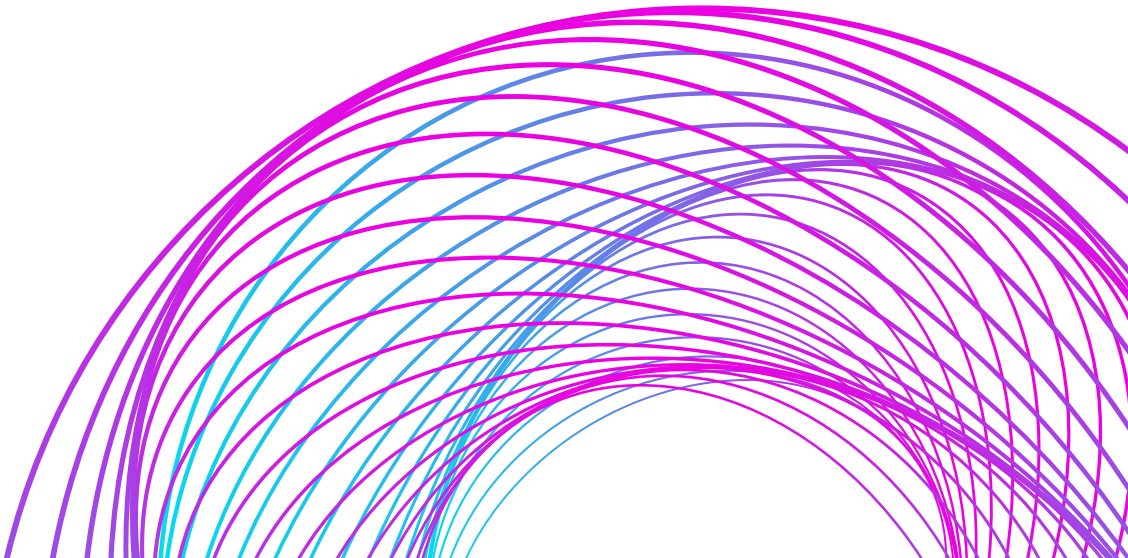
Identify reporting mechanisms that can be delivered utilizing the integrated risk and controls framework and testing mechanisms to satisfy multiple compliance requirements.



Final thoughts

With the risks of outsourcing coming under increased scrutiny, demand for TPA reporting is ballooning. Similarly, the cost of meeting this increasingly complex web of TPA requirements is expanding. Taking a proactive approach to TPA governance is a key step to containing both costs and demands. To be effective, this approach should be inclusive of managing not only external expenditures, but also internal costs in keeping the TPA portfolio up and running. Fortunately, organizations don't need to change everything at once in order to see results.

Building a solid foundation by establishing a TPA steering committee and creating consistent governance processes, enforced by the TPA PMO, is often a good place to start. Considering TPA costs and obligations during the contracting process is another area that can yield rapid improvements. The idea is to step forward, rather than being taken aback. Those who act to reduce the burdens of TPA reporting, instead of just reacting to them, should be better positioned to deliver the heightened level of comfort their customers need while creating significant value for their organizations.



Contact us

Curtis Stewart
Managing director
Deloitte Risk & Financial Advisory
Deloitte & Touche LLP
+1 703 251 1782
custewart@deloitte.com

Dan Zychinski
Managing director
Deloitte Risk & Financial Advisory
Deloitte & Touche LLP
+1 404 220 1169
dzychinski@deloitte.com

Alan West
Senior manager
Deloitte Risk & Financial Advisory
Deloitte & Touche LLP
+1 402 444 1807
alwest@deloitte.com

Deloitte.