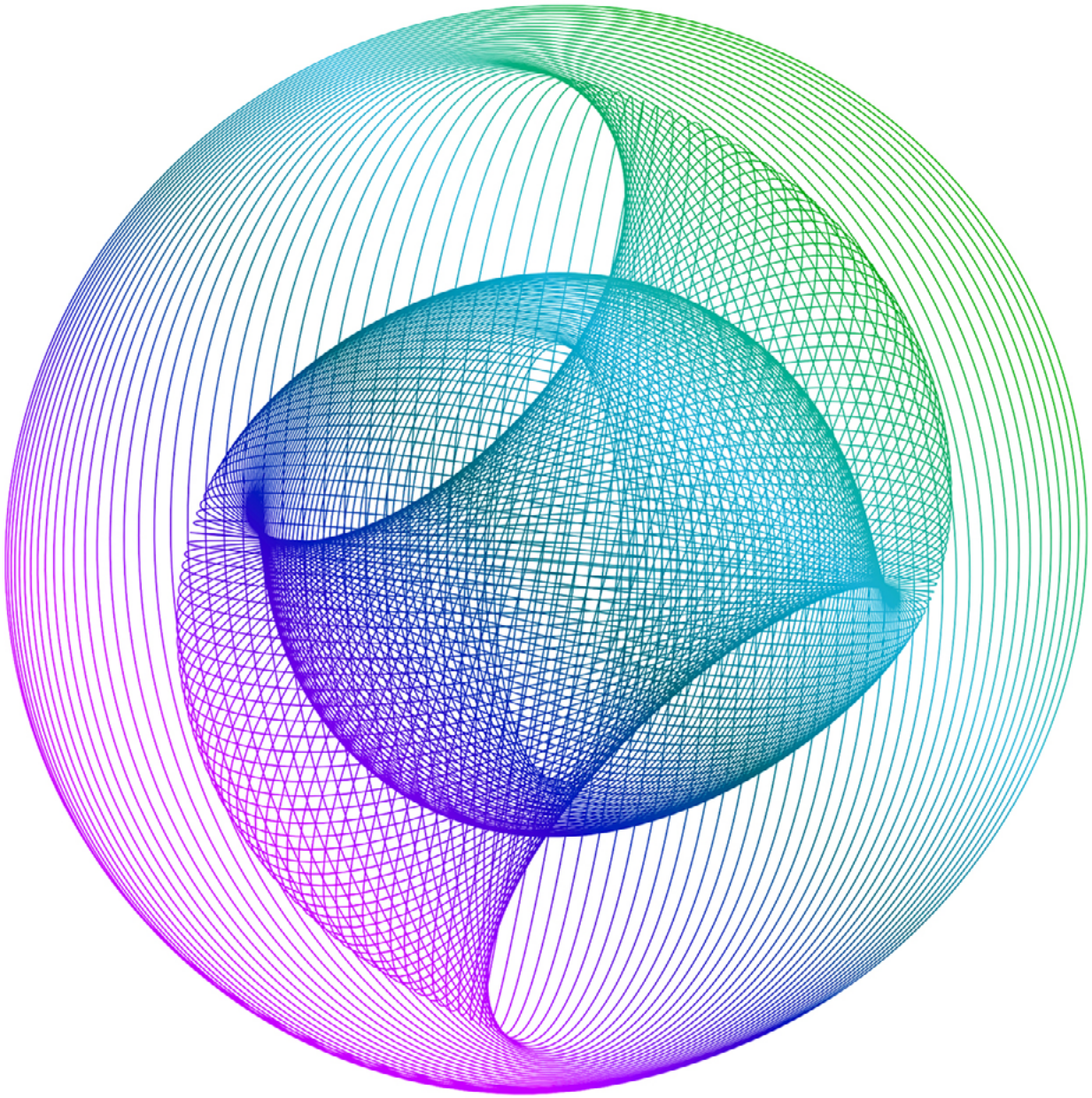
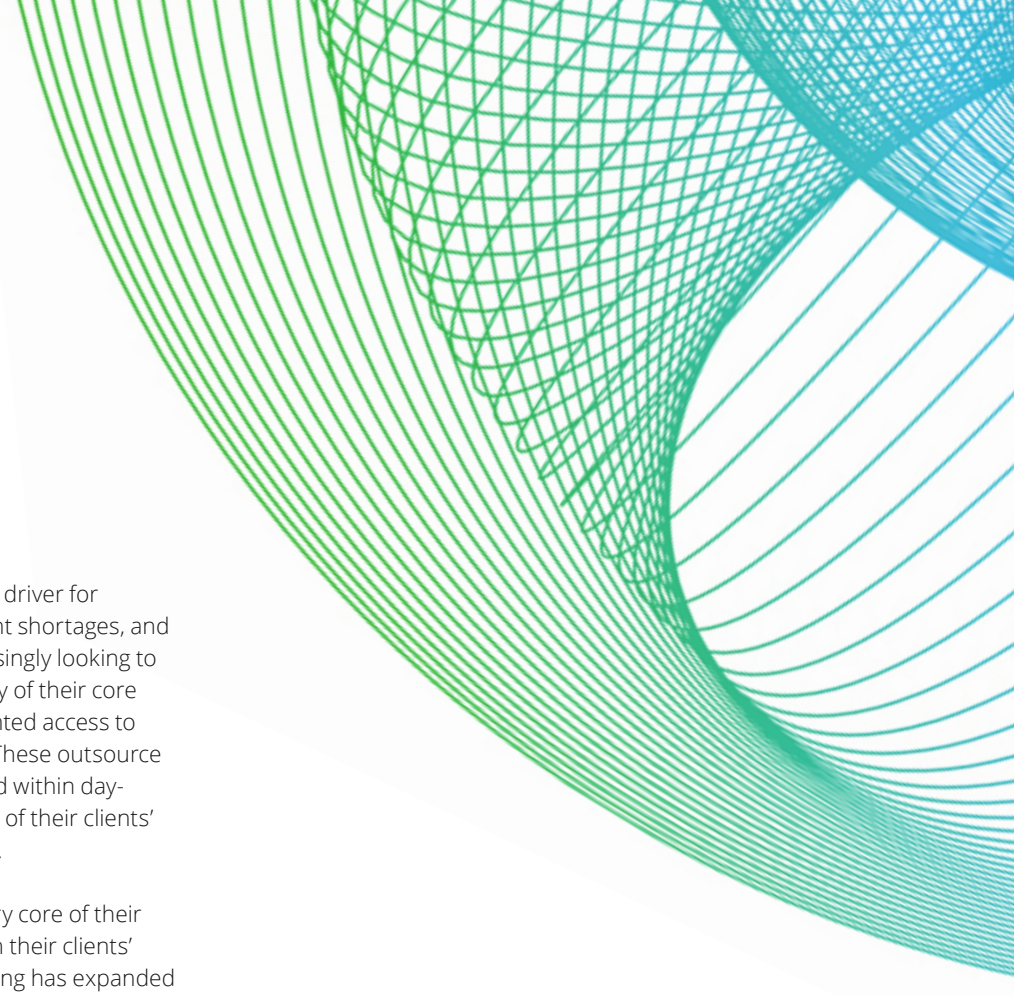
Deloitte.



Third-party assurance optimization

Value-creation strategies for service providers

Introduction



Outsourcing continues to evolve and has become a driver for growth. Today, faced with resource limitations, talent shortages, and competitive pressures, many companies are increasingly looking to third parties to assist with the management of many of their core business and IT processes, giving them unprecedented access to sensitive data and connectivity to critical systems. These outsource service providers (OSPs), which are highly integrated within day-to-day operations, have become a virtual extension of their clients' enterprises and can be a significant source of value.

At the same time, as OSPs' involvement with the very core of their customers' business grows, so does their impact on their clients' internal control environments. The rise in outsourcing has expanded the universe of risks to which organizations are exposed—from financial and operational risk to cyber and business continuity risk to sustainability risk. As a result, many companies are holding their OSPs to the same level of risk monitoring and regulatory compliance that they hold themselves, and demand for third-party assurance (TPA) reports has skyrocketed. Based on the most recent SOC survey results from the AICPA, the total number of SOC 2 reports is increasing on an average 20%–25% every year. Additionally, the once-dominant System and Organization Controls (SOC) 1 report is now sharing a higher percentage of TPA reporting with SOC 2 and other customized TPA reporting options.

Fulfilling customer requests for a wide range of TPA reports and responding to myriad compliance questionnaires can quickly devolve into a set of resource-draining exercises for OSPs that detract from more value-added activities. OSPs need a more streamlined approach to deal with both customer and regulatory requirements. In fact, by efficiently using resources and improving customer satisfaction, TPA optimization can help move an OSP from merely protecting value to actually creating it.

From getting the job done to doing it efficiently

Increased regulation and greater reliance on outsourcing has led to a proliferation of TPA reports, from the workhorse SOC 1 reports to Attestation AT-C Section 205, SOC 2, and agreed-upon procedures (AUP) reports. In addition, there are a wide range of industry-specific reports, such as the Compliance Program Examination Report (CPER) and Financial Intermediary Controls and Compliance Assessment Reports (FICCA) for the financial services industry, Cybersecurity Maturity Model Certification (CMMC) for many governmental contractors, and the Health Information Trust Alliance (HITRUST) Common Security Framework (CSF) for the health care industry. Indications are that in the near future, TPA reports will likely extend to other business-critical areas such as cybersecurity (see the sidebar, "Third-party assurance reporting: Where to next?").

OSPs are also often inundated with security questionnaires from individual clients, requests for customer-specific TPA reports, and demands to arrange for burdensome onsite client auditor visits that well-designed TPA reporting programs should address. Combine this with the need for OSPs to meet their own internal compliance requirements (e.g., complying with Sarbanes-Oxley (SOX) or various industry standards), and it's easy to see why they are looking for ways to ease the burden.

There are significant advantages to optimizing TPA reporting, including:

- **Broad-based assurance:** OSPs can provide assurance to a diverse range of clients with a single report or set of reports.
- **Integrated requirements:** OSPs can "test once" and apply the results across multiple reports. They can also potentially leverage results for internal requirements such as SOX.
- **Time and cost savings:** OSPs can issue their own reports and map or align them more specifically to customer requirements. This saves them from having to respond to multiple "one-off" questionnaires from customers and accommodate audits from customers' auditors.
- **Enhancing trust:** When customers are comfortable with an OSP's reporting process, they are less likely to "second guess" them by requesting additional information about their controls.
- **Rapid tailoring:** OSPs can quickly customize reports for both existing and prospective customers.
- **Customer value creation:** A streamlined TPA process can be a significant competitive differentiator for OSPs who can market their flexibility and ability to quickly meet customer compliance requirements through a variety of TPA reporting vehicles mapped (or tailored) toward specific industry standards and regulations.
- **Improved ability to cross-sell:** With a broad, cross-functional approach to TPA reporting, OSPs can structure reports to communicate to customers the full range of services they offer. This can potentially lead to customer requests for additional services.
- **Business process improvement:** Streamlining TPA reporting also means streamlining controls themselves and identifying where some may no longer be needed. In addition to removing the controls from the reporting framework(s), management may have the opportunity to eliminate the related work activities, and these resources can be redeployed to more value-creating activities.

Ultimately, TPA reporting is a core strategic activity for OSPs, calling for close alignment with business objectives and executive involvement to determine where TPA can have the greatest business impact.

TPA leading practices

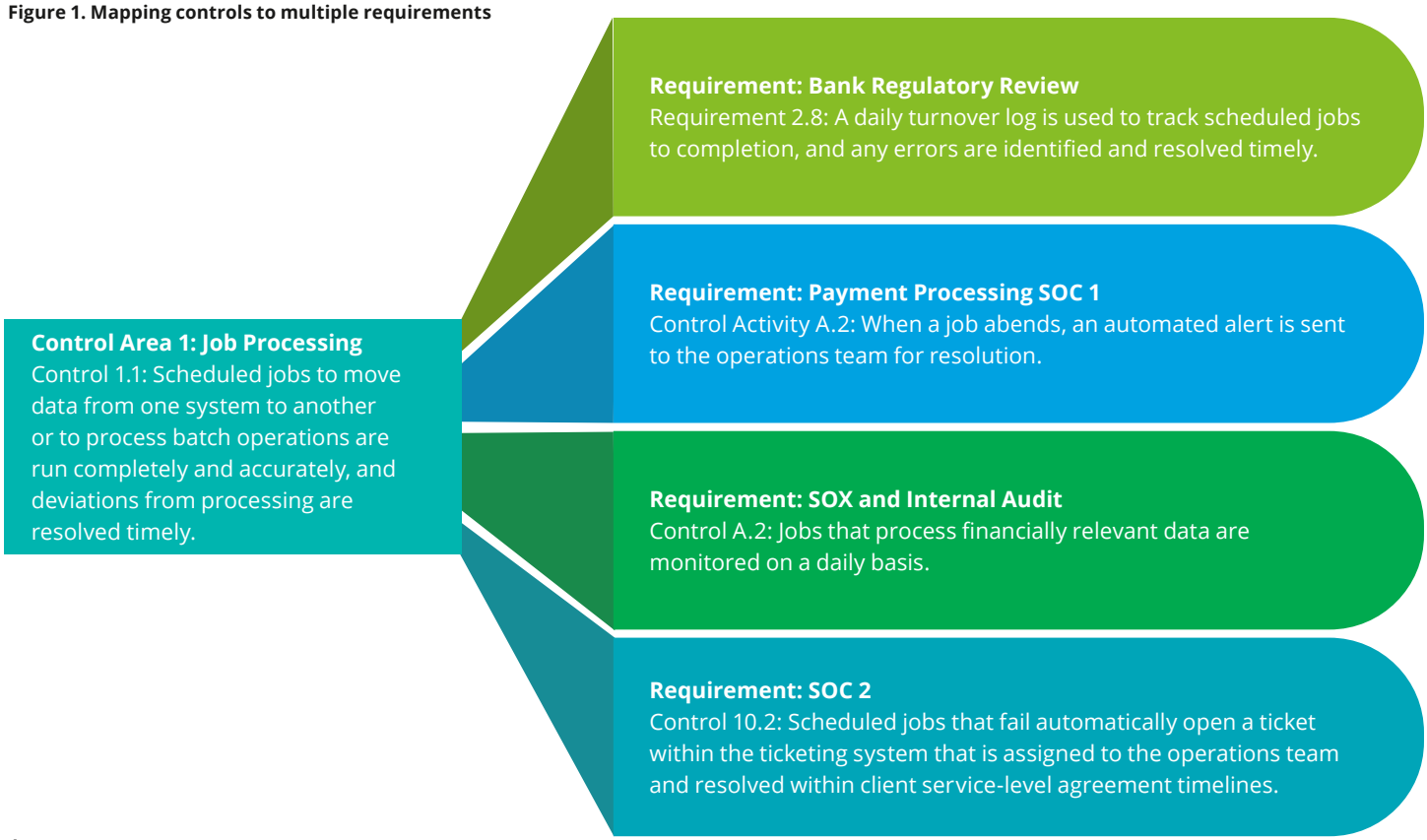
Conquering the problem of TPA report proliferation calls for a comprehensive approach that can streamline efforts and make the best use of an OSP's resources; we have found there are a number of practices that can give OSPs a good head start.

Take stock

Many OSPs are in reactive mode when it comes to managing TPA requests. Part of the problem stems from the fact that they don't have a good handle on all their internal and external control requirements. Creating an inventory of all your control requirements enterprisewide is the first step in both identifying gaps and finding overlaps. The inventory should include internally identified requirements (e.g., SOX control requirements if you are a public company, or others needed for financial reporting), industry requirements, and requirements included in any TPA reports you issue. Finally, the inventory should include requirements covered in any questionnaires or service-level agreements (SLAs) that you respond to on an annual basis.

Once you have an inventory, you can map requirements against the controls that fulfill them and determine which ones you can cover through TPA reports. For example, while you may have a single control that covers the monitoring process for critical jobs/operations, it may align with 20 different requirements, both internal (e.g., SOX) and external (e.g., various TPA reports or specific customer requirements). Noting every requirement that a control fulfills should help enhance efficiency during testing (see figure 1).

Figure 1. Mapping controls to multiple requirements



Get more bang for your buck

If you are handling customer reporting requirements as one-offs, you may be missing important synergies. Once you have a catalog of requirements mapped to enterprisewide controls, you are in a position to realize substantial efficiencies during control testing. Rather than testing each time a requirement comes in from a customer, you may be able to develop a testing strategy that maximizes leveraging each control once—for both internal and external purposes—and then document the results for every requirement to which the control applies.

For example, many TPA reports have common elements. This means that when you test for one report, the results can apply to other reports with similar requirements. You can achieve additional efficiencies 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.

Your catalog of requirements and control tests can be especially useful for rapid compilation of client-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 can enable you to share testing across different reports and yield substantial time savings.

Shout it from the rooftops

Efficient TPA reporting is a valuable asset to customers, who are able to meet their own compliance requirements more quickly based on your rapid turnaround of requests. But if your salesforce is not up to speed on your capability in this area, your customer may never be aware of it. As part of your overall optimization initiative, develop training for your salesforce, management, and other key personnel who interact with those on the client side responsible for reviewing or requesting TPA reports. Training program content should ensure that these individuals are not only conversant in your own practices, but also up to speed on TPA and industry compliance trends. This can position them to promote your TPA capabilities as a value driver for customers.

Practice spring cleaning

TPA requirements are constantly evolving as customer needs change in response to a shifting business and industry landscape. Therefore, consider your requirements inventory a living document that should be revisited on a regular basis. For example, sending out annual TPA reports to customers without reassessing their control requirements can be a wasted effort. You may find you are spending time on issues that are no longer of concern to customers. Their needs could well have changed. And if you don't ask, you may end up with a stack of new questionnaires and requests for client auditor visits—in other words, back where you started. To avoid this pitfall, stay abreast of new compliance developments, adopt a continuous improvement mindset, and be proactive about uncovering—and then meeting—customer needs.

As your TPA reporting evolves, so should your controls landscape. In fact, streamlining TPA provides an opportunity to do something most controls efforts rarely consider: removing certain controls altogether, not just removing them from reports. If controls are redundant or no longer necessary, continuing to execute them is a waste of valuable resources, particularly if they involve manual activities. Look for ways to eliminate these controls so that you can deploy resources elsewhere.

Third-party assurance reporting: Where to next?

Historically, SOC 1 reports, which focus on internal controls over financial reporting (ICFR), were sufficient to meet customer needs. However, increased third-party risk has led to demand for other types of reports (SOC 2, AT-C Section 205, etc.) that focus on controls related to compliance or operations related to specific trust principles (security, availability, processing integrity, confidentiality, and privacy). Privacy, in particular, has become a priority for organizations, leading to increased exploration of SOC 2 reporting. In fact, based on the reports Deloitte issues, SOC 2 reports now comprise approximately one quarter of all TPA reports performed.

New areas of concern continue to emerge, and one of the most critical of these is cybersecurity. Different regulatory bodies have their own sets of requirements along with frameworks, such as the National Institute of Standards and Technology (NIST). In light of high-profile and costly cyberattacks on large corporations, companies are paying greater attention to cyber assurance, and audit committees, boards of directors, and investors are asking more questions than ever before. They are now looking for assurance from a third party as to how the company is managing cyber risk. SOC 2 reports have been at the forefront of providing customers and boards with a level of comfort around organizations' controls that mitigate cyber risks that relate to frameworks such as NIST.

Conclusion

As companies step up their use of outsourcers for the management of mission-critical operations and business processes, demand for TPA reporting is certain to increase. These reports can be complex, and every customer has different requirements. To stay on top of it all and make the best use of limited resources, OSPs need a big-picture view of their control environment. With an enterprisewide inventory of controls mapped to both internal and external requirements, OSPs are better positioned to efficiently and effectively deliver the level of comfort that their customers need from members of their extended enterprise.

Key considerations for optimizing TPA

As you put together your TPA optimization approach, here are some useful questions to ask:

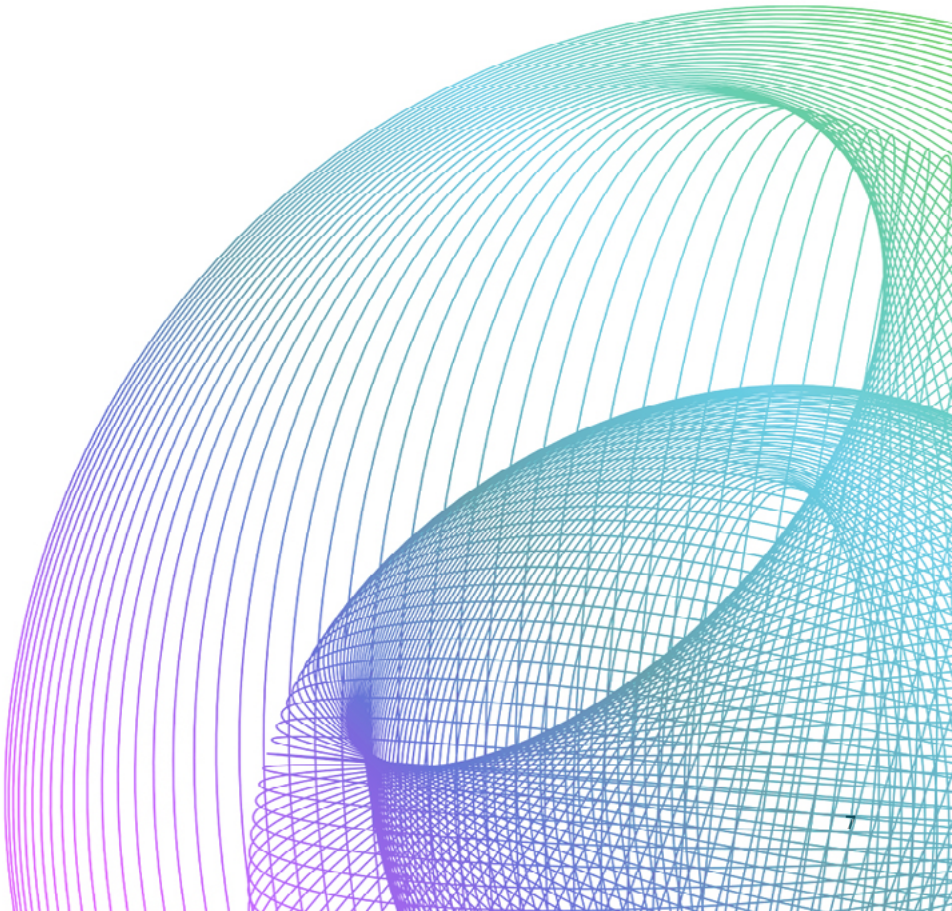
- What reports should we be developing for our customers?
- What are the best reporting methods?
- What are the best reporting vehicles?
- How can we use integrated requirements?
- What synergies can we achieve in our reporting approach?
- How can we synchronize the timing of reports?
- How do we map requirements to customer needs?
- How can we update customer contracts to effectively manage TPA requirements?
- How often should we revisit our approach?
- Is there anything we can stop doing?
- Are we staying abreast of the latest reporting requirements?
- What internal activities can we leverage?

Contact us

Sara Lademan
Advisory Partner | Deloitte Risk & Financial Advisory
Deloitte & Touche LLP
+1 312 486 2981
slademan@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.

About Deloitte

This publication contains general information only and Deloitte is not, by means of this publication, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor. Deloitte shall not be responsible for any loss sustained by any person who relies on this publication.

As used in this document, "Deloitte" means Deloitte & Touche LLP, a subsidiary of Deloitte LLP. Please see www.deloitte.com/us/about for a detailed description of our legal structure. Certain services may not be available to attest clients under the rules and regulations of public accounting.