CONNOR
GROUP

BUSINESS GUIDE

Mastering Vendor Risk:

Outsourced processes don't mean outsourced responsibility. Learn how to effectively manage third-party risks and ensure the integrity of your financial data.

You can outsource your processes, but you can't outsource your risk.

You may be confident you have the right people, processes, and tools to produce accurate financial reporting, but have you considered the impact of third-party resources and systems your team uses to produce its financial data? While your team may execute all tasks accurately and on time as part of your close process, it probably relies on financial data from external organizations like outsourced support, software vendors, or third-party specialists.

Inadequate data control compromises the reliability of your financial reporting. The data quality and how well you manage associated risks limits its accuracy. High-quality data drives effective team processes and actively managing outsourced activities mitigates associated risks.

Below are some best practices to manage risk and ensure your team has reliable data for your close processes:

Service Organizations

What is a service organization, and what is the risk to your financial reporting process?

A service organization is an outsourced company providing relevant services to your company's financial reporting process. Examples include:

- Software providers for tools used either directly (e.g., an ERP or consolidation tool) or indirectly (e.g., a single sign-on tool governing access to financial applications) in your financial reporting process and related internal controls.
- Third-party logistics (3PL) providers
- Payroll providers

If your company relies on data from a service organization, you rely on their processes and controls to guarantee that the data is accurate.

If they were to experience a failure in their internal controls, it could impact the services and data provided by those organizations, including reports generated from software licensed by third parties.

What steps can you take to assess the risk associated with service organizations affecting your financial reporting process?

Navigating service organization risk presents more complexity than navigating other third parties used in the financial reporting process. This stems from service organizations' extensive involvement in subprocesses and the inherent reliance on the data they produce. System and Organization Controls (SOC) reports, issued by service auditors who test a service organization's internal controls, offer varying levels of assurance that the service organization maintains a reliable system of internal controls.

Below is a summary of the different types of SOC reports commonly offered by vendors:

SOC 1 Report: This report centers on evaluating and reporting on a service organization's controls relevant to its customers' financial reporting processes. It's primarily used by organizations relying on the services of third-party providers. SOC 1 reports typically offer the greatest assurance over the completeness and accuracy of financial data produced by the service organization and its systems. The controls tested by service auditors are geared towards user entity financial reporting.

SOC 2 Report: This report evaluates and provides assurance about a service organization's systems and controls that align with Trust Services Criteria (TSC), focusing on non-financial aspects rather than financial reporting. It's tailored for organizations responsible for handling sensitive data and is designed to address data security and privacy risks. A SOC 2 report may or may not be sufficient to address financial reporting risks associated with the service organization; the controls tested, and the results outlined in a SOC 2 report must be evaluated to determine if the scope covers the financial reporting risks posed by that organization.

SOC 3 Report: This report covers a scope and purpose like a SOC 2 report but offers fewer details. It doesn't specify the controls included in its scope or offer details on the results of individual controls tests. For this reason, a SOC 3 report may ensure data confidentiality, but it often won't provide sufficient comfort over the completeness and accuracy of financial data produced by the service organization and its systems.

Type 1 vs. Type 2 reports: A Type 1 report assesses service organization control design but doesn't assess control effectiveness throughout the reporting period. A Type 2 report covers the design and operating effectiveness throughout the reporting period. Accordingly, Type 2 reports typically provide greater reliance than Type 1 reports. SOC 1, SOC 2, and SOC 3 reports may be Type 1 or Type 2 reports.

Provided your relevant service organizations offer SOC reports on their internal controls, management should review those reports at least once a year.

Reviews should focus on two key areas:

- Assessing the impact of any gaps in coverage discovered in the review
    - Inadequate report type or missing report
    - A gap in report period coverage for your fiscal year (e.g., report coverage through Nov 30, but your fiscal year ends on Dec 31).
    - Deficiencies or qualifications noted within the report. Deficiencies identified by the service auditor may impact your organization's ability to rely on the service organization. These deficiencies should be identified and assessed for the impact on your financial reporting. If necessary, address them through the design of compensating procedures/controls.
- Ensuring that any relevant end-user controls outlined in the report (Complementary User Entity Controls, or CUEC) are implemented within management's internal control framework, and subsequently, assessing the impact of any missing CUEC.

Documentation of the review and analysis is typically required for all financially relevant service organizations at publicly traded companies. It is critical for all organizations, regardless of registration status, to review key service organizations to ensure the reliability of key reports generated by systems, automated controls present within systems, and/or data produced related to outsourced processes like inventory/warehouse management, etc.

Third-Party Specialists

What is a third-party specialist concerning your financial reporting process?

Simply put, a third-party specialist is an external individual or organization with expertise in a specific area contracted to provide specialized services or solutions to your organization.

For example:

- Experts in valuation, tax, or technical accounting matters, engaged on an ad-hoc basis to assist in complex analyses

- Outsourced HR contractors who manage the onboarding of employees and create employee master data in your HR system
- Billing specialists
- Contractors hired to support your engineering team

If management relies on third-party experts to produce analyses that materially impact financial statements, it should implement safeguards to ensure data reliability.

How can management design procedures to mitigate the risk associated with reliance on third-party specialists?

Companies should conduct periodic assessments and detailed reviews of deliverables provided and/or transactions processed throughout the reporting process. At a minimum, these reviews should ensure the completeness and accuracy of input data and verify that the outputs of any analysis align materially with expectations. While these tasks are recommended as best practice for all companies regardless of registration status, public companies often need to document them to satisfy Sarbanes-Oxley Section 404(b) audit requirements.

How Connor Group Can Help

Do you know how to perform or document these procedures? What controls should you implement when you can't rely on third parties? Connor Group has advised hundreds of companies on managing financial reporting risk, including risk posed by vendors and third-party specialists. We help organizations design, implement, and/or perform the processes necessary to mitigate risk and satisfy audit requirements.

About Connor Group

Connor Group is built for breakthroughs.

We're a professional services firm focused on the most critical opportunities and challenges facing ambitious companies. We're leaders in accounting, compliance, M&A, IPOs, and digital solutions, including strategy, selection, implementation, automation, analytics, and AI. Serving the offices of the CFO, CIO/CTO, and CHRO, we're trusted by over 2,000 of the most exciting brands on earth to deliver results that last.

Founded in 2006, Connor Group quickly became the leading IPO advisory firm. Helping over 250 companies go public built our pragmatic, delivery-oriented approach and $3.3 trillion in client valuation. It also created elite-level pattern recognition and listening skills to identify problems quickly and solve them efficiently.

The majority of Connor Group has industry experience. We know how to get things done. Our expert teams are fluent in function, technology, and world-class communication. Unlike others, we're independently owned and fully in control of how we deliver. We never compromise on quality.

Neither should you.

connorgp.com

For more information please contact:

Matt Basile
Connor Group
Sr. Manager, FinOps
matt.basile@connorgp.com

Lee Berliner
Connor Group
Director, Transformation and Risk
lee.berliner@connorgp.com