Deloitte.

Managing Risk from Every Direction

Take control of third-party risk with a strong third-party assurance program

How do companies today manage all of the risks associated with using third-party vendors? It's a balancing act. As an Outsourced Service Provider (OSP), it's critical to know what risks may affect your clients — and the best ways to manage those risks — to ensure you are meeting your clients' control needs and requirements.

As a user of outsourced services, it's critical to manage any potential risk to your company and to have proper assurances that your vendors are managing and processing your data in a safe, well-controlled environment.

When you feel like risk is coming at you from every direction, a well-planned third-party assurance program can help provide the control you need.

Third-Party Assurance

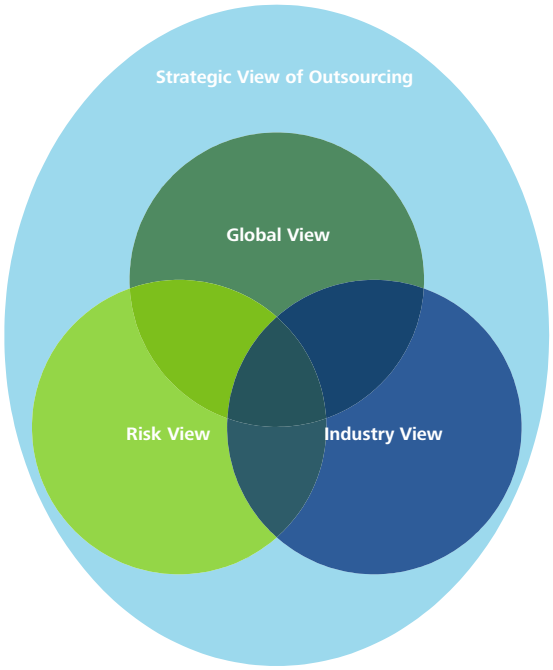
Increasingly, outsourcing of core and non-core functions to outside service providers is playing a vital role in helping companies increase their efficiency and profitability. As a result, outsourcing has evolved into a strategic business practice.

As OSPs are becoming more integrated with their clients' day-to-day operations, they can have more of an impact on their clients' internal control framework, including their financial reporting and compliance requirements.

This increased reliance on OSPs — and the critical role that they can play in their clients' business — has led to an increase in demand for third-party assurance programs.

A strategic view of outsourcing

It's important for companies to take a high level look, or a strategic view, at their existing outsourcing programs and vendors. This strategic overview should help companies identify potential issues and be better equipped to take advantage of available third-party assurance programs, including attestation reporting.



The strategic view of outsourcing is generally comprised of three distinct views — global, risk, and industry views — and can help companies anticipate and mitigate the variety of risks that come with using third-party vendors associated with existing outsourcing programs.

Global view of outsourcing

Today, the reasons for outsourcing extend far beyond Information Technology (IT) processing or the need to find the lowest-cost alternative to in-house operations. Companies are seeking cost and competitive advantages by outsourcing at global levels, as the need for OSPs has evolved over the years from single process outsourcers and hosts to providers of fully integrated cross-border solutions. With global integration comes an added layer of risk — how does a company understand and evaluate OSP risk from a global perspective? Implementing globally accepted reporting standards and controls can help OSPs provide the assurances that their customers expect.

You can outsource a process, but you can't outsource the risk…

Risk view of outsourcing

It is important for companies to be aware of all of the risks that may be typically associated with outsourcing, including, but not limited to reputational, control, compliance, privacy, financial, and operational risks.

Outsourcing any component of a company's business to a service organization can introduce any or all of these risks — either directly or indirectly. Direct risks are typically associated with the actual processing or hosting of data. Indirect risks, which can be equally as critical, are normally associated with how the data is managed (or mismanaged) and the clients' perception of the relationship between the provider and users of outsourced services. To effectively manage these risks, executives rely on specific reports (see the "Attestation Reporting Options" section on page 3) from their service organizations.

Industry view of outsourcing

Outsourcing practices and controls are unique to each industry and as the awareness of vendor risk management has increased across industries, the role of third-party assurance has become more important than ever.

Compliance with industry, government, and other regulations has become more challenging as companies manage increasingly complex reporting requirements. At the same time, many companies are vying for new business and demanding that their OSPs meet certain requirements as a condition of their outsourcing relationship.

A robust control and assurance program, tailored and integrated to address specific industry standards including the Health Insurance Portability and Accountability Act (HIPAA), Health Information Technology for Economic and Clinical Health (HITECH) Act, Federal Information Security Management Act (FISMA), National Institute of Standards and Technology (NIST), Payment Card Industry (PCI) Data Security Standard, to name a few, can help provide companies with the industry perspective that they need.

Once the company has compiled their strategic view of outsourcing — and identified areas of potential risk to the organization — they can establish a plan to begin managing risk from these different directions. Attestation reporting is the first step in the right direction.

Benefits of attestation reporting

Third-party attestation reporting provides a range of benefits for users and providers of outsourced services.

User benefits include
- Ensuring that the expectations of the third-party vendor relationship are met
- Ensuring that the company's multi-purpose reporting requirements — including operational and financial — are met
- Maintaining compliance with industry, governmental, and other relevant regulatory requirements

Provider benefits include
- Broad assurance — the ability to provide assurance to a broad range of clients with a single report or set of reports
- Integrated requirements — provide the option to 'test once' and then apply results across multiple reports
- Cost savings — providing reports issued by the service auditor rather than customer audits
- Competitive advantages through use of prospective user reports
- Savings on answering questionnaires

Attestation reporting options

Leading edge professional service organizations understand the challenges that integrated, outsourcing relationships can present. These organizations can help their clients effectively and efficiently meet existing and growing demands for third-party assurance reporting by incorporating multiple views — global, risk, compliance, industry, and customer views — into their approach.

As indicated in the following table, most professional service organizations offer a range of third-party assurance reporting services including AT101, Agreed-Upon Procedures (AUP) AT201 and AT601 reports, Service Organization Control (SOC) 1, 2 and 3 reports, and readiness assessments.

Third-Party Assurance Reporting Type	Description (as defined by the American Institute of Certified Public Accountants)
AT101	General attestation report
AT201	Report on Agreed-Upon Procedures (AUP)
AT601	Compliance attestation report
SOC 1	Report on Controls at a Service Organization Relevant to User Entities' Internal Control over Financial Reporting (SSAE 16)
SOC 2	Report on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality and/or Privacy
SOC 3	Trust Services Report for Service Organizations

Readiness assessments

In addition to providing reporting services, professional service organizations can also help their clients gauge their readiness needs.

Readiness assessments explore how ready companies are to address risks or needs associated with their OSP programs. The readiness assessment reports can be transferrable across all third-party assurance report types (like the ones mentioned in the previous chart) and typically incorporate a three-phased approach:

Phase 1: Planning

- Conducting scoping discussions and kick-off meetings
- Establishing timing and resource allocations for the readiness assessment

Phase 2: Execution

- Documenting a description of the system and the inherent risks associated with existing controls
- Conducting gap assessments to identify areas of immediate and future focus

Phase 3: Concluding/Reporting

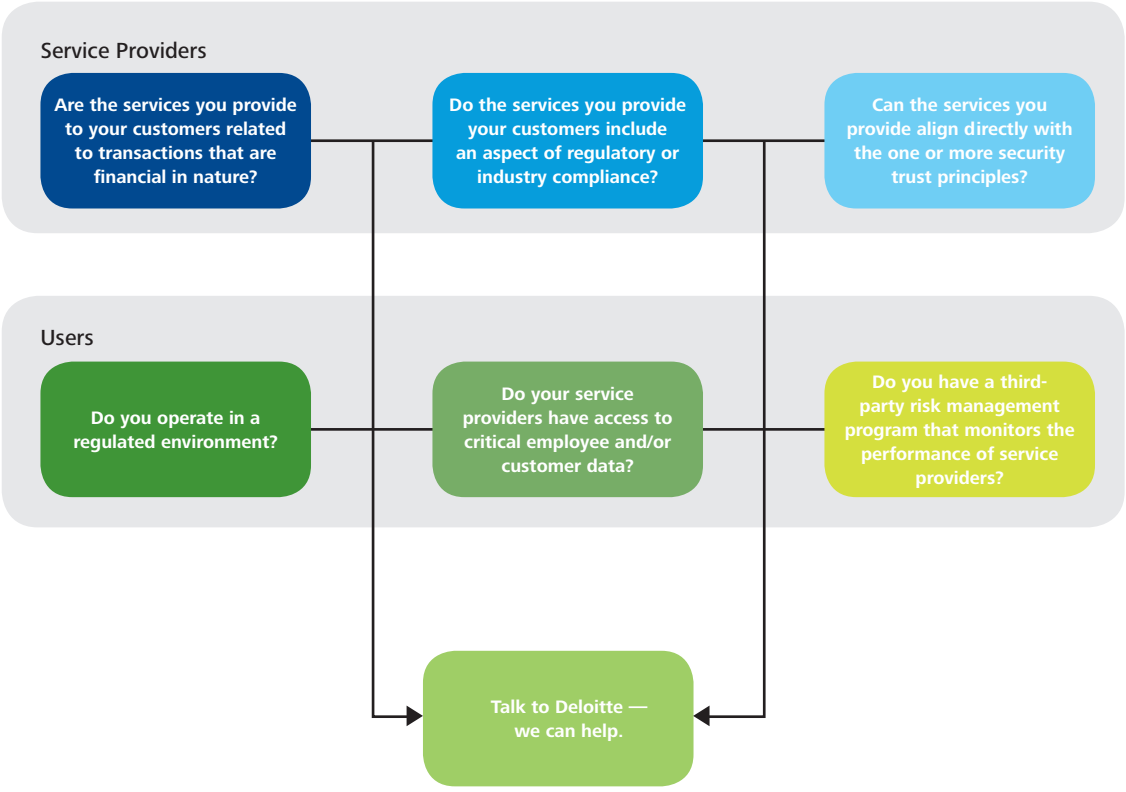
- Communicating advice and recommendations
- Providing the final readiness assessment report

This approach incorporates a risk-centric focus, while also identifying the effective and efficient methods for identifying scope, testing controls, and executing the tasks and activities associated with third-party assurance reporting.

Steps to consider

Attestation reports — questions to consider

Below are questions that service providers and users of third-party services should consider when determining their options when it comes to selecting the most relevant solution for third-party attestation reports:



The other side of the coin — users of outsourced services

Both providers and users of outsourced services are seeking the same end goal — assurance that the risks associated with their business are being managed effectively. While third-party assurance reporting provides a vehicle for OSPs to communicate that assurance to their customers, the users of outsourced services also have a responsibility to manage the risks associated with outsourcing components of their business to other companies through a third-party risk management program.

An effective third-party risk management program addresses compliance, regulatory, and industry risks. Components of such programs include:

- **Governance and oversight** — the organizational structure, committees, roles, and responsibilities for managing third parties
- **Policies and standards** — management expectations for the management of third parties and related risks
- **Management processes** — processes to manage risks across the third-party lifecycle
- **Tools and technologies** — tools and technologies that support risk management processes
- **Risk metrics and reporting** — reports identifying risks and performance associated with third parties, tailored toward multiple levels of management (including third-party assurance reporting)
- **Risk culture** — tone at the top on risk appetite, appropriate training, and awareness to provide positive risk culture

The strategic view of outsourcing not only requires an effective use of third-party assurance reporting, it also requires an effective third-party risk management program to address risks from a 360 degree view.

Conclusion

The outsourcing of key components of a business — in order to meet cost, competitive, and operational demands — has become a strategic imperative within many industries. A multidirectional approach is required to manage these complex relationships because of the global nature, risks, and industry regulations associated with outsourcing. Third-party assurance reporting can help OSPs clearly define, assess, and communicate their approach to their clients.

Since the circumstances around each OSP relationship are unique, a leading OSP process leverages a tailored reporting approach that uses multiple reporting methods. By taking the necessary steps to identify the need for third-party assurance reporting and the appropriate reporting type, the OSP (and the associated users) will help ensure that their risk and compliance needs are addressed. Anticipating and managing these multiple risks is vital to effective third-party relationships.

About the authors

Dan Kinsella is a partner with Deloitte & Touche LLP and works with clients to help them address third-party assurance challenges. He leads Deloitte's Third-party Assurance practice group and is a member of Deloitte's national SOC task force, which works to assist companies in SOC and other third-party assurance matters.

Dan Zychinski is a senior manager with Deloitte & Touche LLP and assists clients in preparing for and complying with third-party assurance requirements. He specializes in delivering information technology and business process governance, security, and risk-related services related to third-party assurance requirements.