ARCHER

EBOOK

5 Tips for Managing Third-Party Risk

Your Third Parties Should Add Value, Not Exposure

Digital Transformation & Third-Party Risk

Across industries and around the world, organizations rely on third-party products and services for a variety of reasons. Whether they are part of the physical supply chain or the digital support infrastructure, vendors, service providers, and external parties have become woven into the fabric of the business.

In today's world, it is easier than ever for an organization to rely on relationships with third parties to provide the services for business operations that were traditionally handled in-house - everything from running internal IT operations to developing products for customers. This strategy not only creates opportunity and value for the business, but can also create emerging risks that must be managed efficiently and effectively.

Third Parties Can Introduce **Unpredictable, Inherited Risks**

Third-Party Risks Are More Complex and Interrelated

It is not unusual today for organizations to rely on third parties for critical strategic operations that were once entrusted only to internal teams. The risks of these relationships are, therefore, more complex and critical than ever before. These risks include data breaches, fraud and theft, business disruption, regulatory compliance violation, and reputational damage. They are often fast-moving, complex and interrelated, and because they are typically hidden within both your organization's activities and your third parties' activities, they can be hard to anticipate.

Third Parties Are Not Managed Consistently

In many organizations, third-party relationships are managed in silos across different business units or functions. Each function may have its own way of identifying, assessing and managing business partners. This not only leads to redundant activity but also inhibits the executive management team's ability to get a complete and accurate view of third-party risk and performance across the organization. And without a firm grasp of their organization's third-party risk exposure, leadership cannot make informed decisions about how much to invest—and where—to protect the business from these risks.

Third Parties Are Mission Critical to Organizations

The more an organization depends on third parties to meet its business objectives, the more rigor it needs to apply to managing these relationships. Unfortunately, few organizations understand the extent of their dependence on third parties and the potential risks this dependence creates. As a result, they are unable to keep up with their organization's changing business landscape, challenges associated with their third parties, growth of third-party engagement, or their business's demand for agility.

1

Know Your Third Parties

A regulation in the financial services industry known as “Know Your Customer” requires financial institutions to verify the identity of their clients and assess potential risks. Ideally, organizations across all sectors should do the same with their external partners, since many organizations lack a clear understanding of their third-party dependencies.

Follow these steps to get started:

Catalog all third-party relationships and engagements, including the individuals responsible for each one.

Associate each third party with the business unit, division, function or business process that it supports.

Identify the data governance controls required for each third party and each of its agents to carry out their contractual obligations.

Determine which performance metrics to track during the course of a third party’s engagement with your company.

2

Understand Their Impact

A typical organization may use hundreds, if not thousands, of third parties. These partners will require varying levels of due diligence and oversight depending on the importance of the products, services or capabilities they provide. The more critical the third party, the more rigorous governance the partner is likely to require.

To understand the nature and scope of your organization's dependence on its third parties, heed the following advice:

Leverage existing business impact analysis studies to determine the criticality of each area of the business and tie that criticality to the third parties supporting each area.

Identify and evaluate risks to determine the level of exposure each third party (and their products or services) poses to the organization.

Design and implement controls commensurate with the third parties' business needs and risk to the organization.

Adjust third-party governance, assessment and monitoring activities basedon each partners' criticality to the business.

3 Evaluate Your Third-Party Risks & Take Action

Many third-party relationships introduce unpredictable, inherited risks that result in losses to an organization. Since it's not possible to transfer all risks to third parties through contractual agreements, a risk management process based on standards and best practices can help your organization identify, assess, treat and monitor these risks. A standards-based risk management process can also ensure that:

- Stakeholders across the enterprise make decisions about third-party risks consistently and in accordance with the organization's risk appetite.
- The executive management team understands third-party risk exposure in its entirety, enabling them to determine how much to invest to protect their business from these risks.
- Regulators requiring rigorous oversight of third-party relationships understand an acceptable risk management approach is in place.

A sound risk management process should encompass the following activities:

Assessing and managing requests from business line managers to initiate new third-party relationships.

Documenting third-party relationships and associated contracts, and establishing business owners within the organization who are responsible for each relationship.

Conducting risk assessments of each third party's control environment; leveraging the assessment results to determine the vendor's residual risk across applicable risk categories; and taking appropriate action to reduce risk to acceptable levels.

Documenting and monitoring performance and service level metrics for each vendor and each product or service they offer.

4

Monitor Your Third Party

Monitoring of third parties is essential because their security and risk profiles can change, along with their ability to perform to the service levels your organization has established. But monitoring can be a challenge, especially when you are trying to keep up with multiple third-party relationships. Automating your initial assessments and ongoing monitoring of third parties' security can provide an accurate picture of third-party security and help ensure you are not caught off guard by changes that could affect the risk to your organization.

Proper oversight should include:

Documenting third-party performance and service-level metrics and monitoring that each engagement is being delivered in accordance with expected outcomes.

Monitoring third-party online access and responding to related risk, compliance and security issues.

Automating initial and ongoing measurement of the effectiveness of third-party security.

Ensure third parties are properly factored into business continuity, disaster recovery and other resiliency preparations.

Adjusting your monitoring activities so that your most critical third parties get the most scrutiny.

5

Coordinate Security, Risk & Business Teams

Because third parties can introduce such a wide range of risks, managing third-party risk and performance in the age of digital transformation requires close collaboration among security, risk and business functions. Together, these teams can ensure that decisions about third-party risks are made consistently across the business, and that risk and security considerations are front and center when new third parties are being assessed and evaluated. Third-party viability, criticality, performance, risk and security must be coordinated together throughout the third-party governance lifecycle.

How Archer Helps You Manage Third-Party Risk

With Archer Third Party Governance, you can capture prospective relationships, engage affected stakeholders and assess contract risk, financial wherewithal, and inherent and residual risks across multiple risk categories. This enforces risk-based selection and establishes performance metrics. Archer Third Party Governance automates and streamlines oversight of your vendor relationships by facilitating key activities necessary to fulfill regulatory obligations and best practices across the entire third-party management lifecycle. Archer Third Party Governance includes several use cases to meet your specific business needs as you mature your third-party risk and performance management program.

How We Help

Understand the relationships you have with third parties to mitigate risk.

Document third-party relationships and associated contracts, plus the business units and named individuals in your organization who are responsible for each relationship.

Use a single repository to aggregate all third-party information.

Build and execute assessments to help manage third-party relationships

Determine your organization's residual risk across several categories by leveraging a series of risk assessment questionnaires to assess third parties' control environments and then analyze the results.

Assess third-party security risks quickly and more accurately with continuous, automated visibility into your vendors' IT landscape.

Perform integrated third-party risk and performance management.

Gain a holistic understanding of your organization's dependency on third parties across all of your business units.

Catalog the products and services third parties deliver to your organization according to each business process and business unit they support.

Document performance metrics and service level agreement metrics for each third-party product and service to ascertain whether each engagement is delivering expected performance.

Manage issues generated by audit, risk, compliance and other teams.

Establish the corporate structure and accountability, and workflow and reporting to manage finding.

Visit Archer online to review resources that will help you take the first step toward strengthening your organization's third-party risk posture.

About Archer

Archer, an RSA company, is a leader in providing integrated risk management solutions that enable customers to improve strategic decision making and operational resiliency. As true pioneers in GRC software, Archer remains solely dedicated to helping customers understand risk holistically by engaging stakeholders, leveraging a modern platform that spans key domains of risk and supports analysis driven by both business and IT impacts. The Archer customer base represents one of the largest pure risk management communities globally, with over 1,500 deployments including more than 90 of the Fortune 100.

1. Salesforce.com, "Digital Transformation: Strategies for Success," July 2018, p. 2

ARCHER