ARCHER

WHITE PAPER

Four Paths to Managing Third-party Risk in the Digital Era

Third parties play a critical role in organizations undergoing digital transformation. Partnerships with third parties often represent the fastest, most efficient way to deliver new digital technologies an organization is eager to adopt. When a third party becomes part of an organization's operations, its strengths become the larger organization's strengths—but so do its weaknesses, and that's where risk often lies. Will a third party expose a customer's personal data or financial details? Will a third party's underperformance reflect on the overall organization? Will its failure to deliver on a project threaten the project's viability? These are just some examples of the risks of working with third parties. And the more third-party relationships the organization forms in pursuit of digital transformation, the larger the potential risk looms.

Third-party risk is a multifaceted challenge, and successfully managing it requires an integrated, multifaceted approach. This paper describes four aspects of thirdparty relationships that an organization must address in their effort to successfully manage third-party risk.

1. Third-party Catalog: Taking Inventory

For any organization on the path to digital transformation, creating a catalog of third parties with which the organization does business is an essential initial step in managing third-party relationships. A catalog provides a way to inventory third parties and document them according to their organizational structure (parent company, subsidiary, sub-subsidiary). The organization's third-party contacts can be documented there, and accountability for third-party relationships can be mapped based on the person and business unit that own the relationship.

A third-party catalog makes it possible to:

- Gain awareness of all third-party relationships throughout the organization.
- Quickly identify third-party relationships and contracts.
- Establish and document who is accountable for individual supplier relationships.
- Track contract terms, including key events such as renewal and expiration dates.

2. Third-party Engagement: Tracking Activity

An engagement refers to the actual product or service a third party has been contracted to deliver. Being able to document and track engagements gives an organization visibility into the products and services third parties provide, including insights into which business processes those products and services support, the terms of the contracts and agreements associated with them, and other engagement details.

A successful third-party engagement program should:

- Reveal exactly where, how and why third parties are being engaged.
- Identify any inherently high-risk third-party products or services.

- Use notifications and reporting to provide transparency into third-party relationships.
- Reduce third-party-related audit and regulatory findings.
- Establish a basis for a robust third-party risk-management program.

3. Third-party Governance: Monitoring Performance

Being able to monitor and manage the performance of a third party is essential to being able to manage third-party risk. Every organization that enters into a thirdparty relationship to deliver products and services to customers brings into the relationship expectations of how those products and services should perform, and the third party should be prepared to meet those expectations. While those expectations may be formally included in contracts in the form of agreed-upon service levels, contractually establishing expectations is only a first step.

To manage the risk of a third party underperforming or failing to perform to expectations, organizations also need to monitor performance metrics throughout the relationships. Any indication that the third party's performance is in trouble can then be addressed at the earliest opportunity. While litigation and compensation after the fact may provide some recourse, the best outcome is for the third party to meet or exceed expectations in the first place. A formal third-party governance program provides the foundation for that.

Third-party governance should enable an organization to:

- Create and capture performance metrics and associate them with specific engagements.
- Report on performance against those metrics.
- Uncover deteriorating performance and quickly address it.
- Avoid third-party-related losses and spend fewer resources on performance remediation.
- Demonstrate effective third-party performance management to the leadership team and regulators.

4. Third-party Risk Management: Assessing and Managing Risk

There are many risks associated with outsourcing a product or service to a third party, and the more an organization relies on third parties, the more challenging it can become to manage those risks. Many of the risks can be significant, including customer data breaches, regulatory compliance violations, customer or shareholder litigation, financial losses from third-party errors, business interruption and reputational damage. It's important for organizations to be able to understand the risks third-party relationships pose, assess the adequacy of controls third parties have in place to manage their own risk, and fill whatever gap exists between those controls and the organization's own controls.

The process of managing third-party risk should start with working with the third party to identify potential risks, assess the third party's internal control environment and collect relevant supporting documentation. This information can then be factored into a determination of the risk associated with each third-party engagement across various risk categories.

A third-party risk-management program should provide the means to:

- Apply a methodical, standardized approach to assessing third-party risk.
- Manage and mitigate issues that are identified and speed the time to resolution.
- Proactively identify potential or emerging risks.
- Bring down the number of third-party-related incidents and losses.
- Reduce overall third-party risk and third-party-related audit findings.
- Enable a better understanding of the risks third parties pose throughout the organization.

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.