ARCHER

EBOOK

Manage Third-Party Risk to Advance Digital Transformation

A Guide to Managing Third-Party Business and Security Risk

Third Party Risk
Takes Many Forms

Third-party risk consists of more than just one type of risk. In this e-book, we'll explore multiple areas of risk introduced by using third parties and discuss ways security and risk management leaders can work together to manage the risks.

Companies are creating increasingly complex ecosystems that use third parties to augment their own business capabilities. A major consideration in this strategy is the balance between the strategic efficiencies and capabilities of these third parties and the potential inherited risk of leveraging external parties. Because of the increasingly intertwined nature of third-party ecosystems, security and risk management leaders and teams must work together...

CISO Objectives

- Set and execute IT and security strategy
- Strengthen security posture and defense
- Control costs while reducing risk to acceptable levels
- Ensure controlled end-user system access
- Maintain data privacy
- Drive IT compliance (PCI, SOX, etc.)

"It's my job to ensure our business teams' 'need for speed' doesn't put the company at undue risk. I know they need to work fast. But they need to know what's really at stake. Our reputation isn't something I can fix once it's broken."

CRO Objectives

- Set and execute risk management strategy
- Control costs while managing risk at acceptable levels
- Run the enterprise risk management program throughout the company
- Lead the enterprise risk committee and report to the CEO and board of directors

"It's my job to know about, understand and facilitate the management of all of the big risks across the enterprise, including those that threaten the organization's strategies and objectives or may be introduced through new products and services, business processes, combinations and reorganizations."

Third-party risk cannot be eliminated, or at least not without forsaking all the benefits. The task is then to identify, mitigate and continuously manage third-party risks, and continuously improve and maintain the maturity of the organization's third-party risk program. This happens most effectively when there is a focus on the following four areas:

Ecosystem

The alignment of business goals/objectives with external information systems, hardware, software and all other products and services delivered by third parties

Contracting

The inclusion of scope, accountabilities and service level agreements (SLAs) in contracts and legal agreements with third (and in some cases, fourth) parties

Governance

The ongoing measurement of adherence to defined scope, accountabilities and SLAs as specified in contracts and legal agreements

Ecosystem

Third-Party Relationships Need Ownership Inside the Organization So the Engagement Proceeds as Expected

The alignment of business goals and objectives with external products and services delivered by third parties is critical for several reasons. The first is third-party relationships need ownership inside the organization so the engagement proceeds as expected and any issues can be quickly resolved. Another reason for this alignment is to prioritize the third party according to the areas, products or services, or IT functions they support. IT and business leaders should collaborate on this process so there's agreement between IT and the business.

The following steps are vital in creating this ownership and defining criticality:

Document the structure of the internal organization and the interdependencies between business processes, IT systems, locations, devices and data.

Determine the criticality of the business processes across the organization through a business impact analysis (BIA).

Inventory all existing third parties, their products and services, and align them with the business and IT infrastructure they are supporting. The BIA results will help determine the criticality of each third party.

Inventory the 4th, 5th and Nth parties the third parties are using and relatetethem to the third parties your organization engaged with.

Contracting

It’s Important that Business and IT Leaders Both Participate in Defining the Rules of Engagement

With any third party, it is vital to define the rules of engagement at the beginning of the relationship or each term of work. This requires including scope, accountabilities and SLAs in contracts and legal agreements with third and (in some cases, fourth) parties. A third party may engage with both business and IT functions, but that support may be very different with varied expectations. That’s why it’s important that business and IT leaders both participate in this up-front process.

Complete contracts, performance expectations and SLAs prior to engaging with third parties.

Set up performance metrics that will be tracked, evaluated and tied to payment schedules and amounts.

Establish penalties for non-conformance to contracts and performance expectations.

Establish contract stipulations for the third parties’ use of 4th, 5th and Nth parties and their accountability for them.

Governance

Managing Third-Party Risk Requires a Programmatic, Coordinated and Risk-Driven Approach

Managing third parties often is the responsibility of a procurement department, which onboards the third party, finalizes contracts and performs other administrative tasks. What is often missing in the process is the ongoing management of risks that might arise during engagement with the third party. Risks can be business or digital, necessitating the involvement of risk and IT security teams. Managing third-party risk requires a programmatic, coordinated and risk-driven approach, and a truly integrated risk management strategy should include a comprehensive third-party governance program that focuses on reducing risk, improving security and improving business performance.

Catalog and manage third-party relationships across the full lifecycle, from initiation of a new or changing third-party relationship to termination of the relationship.

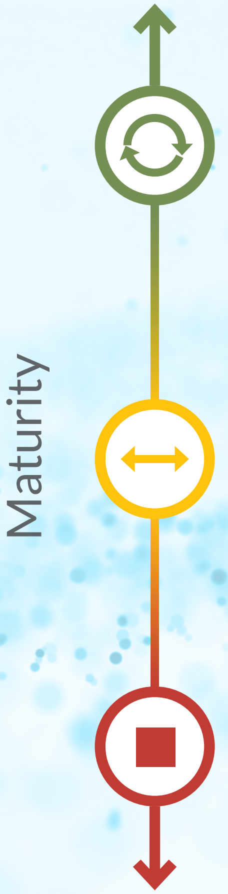
Assess the broad range of risks related to third-party relationships (information security, fraud, litigation and compliance risk, contract risk, financial risk, resiliency, financial viability, reputation, strategic risk, fourth-party risk, etc.).

Use business context to intelligently focus risk management toward the third parties that matter most by tailoring assessment activities based on the inherent risk of each unique third-party relationship.

Evaluate the adequacy of third-party risk treatments, evaluating and monitoring deficiencies until remediated.

Implement third-party performance monitoring for compliance and optimization of resources and to ensure third parties are fulfilling their service-level commitments.

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.



Ecosystem	Contracting	Governance
Operational Excellence		
Inventory of all third-party products and services aligned to a company's core systems	Operationalized contract procedures evaluated by affected stakeholders on services prior to contract signing of all third parties	Ongoing measurement of KPIs against SLAs, agile measure practices
Foundational Effectiveness		
Third-party products and services aligned in some but not all systems	Operationalized contract procedures evaluated by affected stakeholders on services prior to contract signing of some third parties	Standard assessment practices for most third parties
Minimal Effectiveness		
Some alignment of resources to core systems	Sporadic or ad hoc inclusion of contract/legal terms in third-party agreements	Basic assessment practices but ad hoc

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.

ARCHER