MANAGE THIRD-PARTY RISK TO ADVANCE DIGITAL TRANSFORMATION
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.
Digital transformation is creating increasingly complex ecosystems for companies that use third parties to augment their own digital and business capabilities. Companies can gain strategic efficiencies and capabilities by using third parties, but they might also inherit new and unknown digital and business risks from them. Because of the increasingly digital nature of third-party ecosystems, security and risk management leaders and teams must work together to manage third-party risks and reduce their business impacts. This has traditionally been a challenge because these two functions typically have very different objectives and perspectives.

**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.

**Identity**
The management of identity and access (e.g., single-factor, multi-factor identification) across third-party users, devices and other assets.

**Governance**
The ongoing measurement of adherence to defined scope, accountabilities and SLAs as specified in contracts and legal agreements.
The alignment of business goals/objectives with external information systems, hardware, software and all other product 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:

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

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

3. **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.**

4. **Inventory the 4th, 5th and Nth parties the third parties are using and relate them to the third parties your organization engaged with.**
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.
Cyber threats represent one of the most critical risks that third parties can introduce into an organization's IT environment. Many times, external users—including consumers, third and fourth parties and their employees, and IoT devices—are granted access to sensitive information or to roles inconsistent with their purposes. This is sometimes due to business teams anticipating the third party's needs and wanting to grant them more system access than is needed, “just in case.”

To manage the risk of cyber threats, it is critical to secure third-party access to critical resources and ensure that third-party identities are properly governed.

Implement a business-driven identity assurance strategy that affords users the freedom to efficiently and effortlessly access only those systems and data they need for their roles, without sacrificing the organization’s information security posture or compliance obligations.

Protect critical resources with risk-based multi-factor authentication.

Govern access with an automated, analytics-driven approach that simplifies access approvals and certifications, and also speeds provisioning and deprovisioning, while managing gaps like overprivilege, segregation-of-duties violations or other requests that need extra attention.
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.**
RSA is dedicated to helping organizations better manage third-party risk and reduce their business impact, especially as they deal with interrelated business and digital risk stemming from digital transformation. We help security and risk management leaders implement a coordinated approach, so they are aligned with their organization’s strategic objectives; govern their third parties efficiently; identify and mitigate the right risks swiftly and effectively; and continually improve their capabilities while supporting their dynamic businesses.

<table>
<thead>
<tr>
<th>ECOSYSTEM</th>
<th>CONTRACTING</th>
<th>IDENTITY</th>
<th>GOVERNANCE</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>OPERATIONAL EXCELLENCE</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Inventory of all third-party</td>
<td>Operationalized contract</td>
<td>Defined program/policies</td>
<td>Ongoing measurement of KPIs against SLAs,</td>
</tr>
<tr>
<td>products and services aligned to</td>
<td>procedures evaluated by affected</td>
<td>that enable third-party</td>
<td>agile measure practices</td>
</tr>
<tr>
<td>a company’s core systems</td>
<td>stakeholders on services prior to</td>
<td>access rights with ongoing</td>
<td></td>
</tr>
<tr>
<td></td>
<td>contract signing of all third</td>
<td>process improvement</td>
<td></td>
</tr>
<tr>
<td></td>
<td>parties</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>FOUNDATIONAL EFFECTIVENESS</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Third-party products and</td>
<td>Operationalized contract</td>
<td>Practices for identity and</td>
<td>Standard assessment practices for most</td>
</tr>
<tr>
<td>services aligned in some but not</td>
<td>procedures evaluated by affected</td>
<td>access management pretty</td>
<td>third parties</td>
</tr>
<tr>
<td>all systems</td>
<td>stakeholders on services prior to</td>
<td>well defines and managed</td>
<td></td>
</tr>
<tr>
<td></td>
<td>contract signing of some third</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>parties</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>MINIMAL EFFECTIVENESS</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Some alignment of resources</td>
<td>Sporadic or ad hoc inclusion of</td>
<td>Identity and access for some</td>
<td>Basic assessment practices but ad hoc</td>
</tr>
<tr>
<td>to core systems</td>
<td>contract/legal terms in third-party</td>
<td>third parties but not updated</td>
<td></td>
</tr>
<tr>
<td></td>
<td>agreements</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
DIGITAL RISK IS EVERYONE’S BUSINESS
HELPING YOU MANAGE IT IS OURS

RSA offers business-driven security solutions that provide organizations with a unified approach to managing digital risk that hinges on integrated visibility, automated insights and coordinated actions. RSA solutions are designed to effectively detect and respond to advanced attacks; manage user access control; and reduce business risk, fraud and cybercrime. RSA protects millions of users around the world and helps more than 90 percent of the Fortune 500 companies thrive and continuously adapt to transformational change.

Find out how to thrive in a dynamic, high-risk digital world at rsa.com