RSA RISK FRAMEWORK FOR THIRD PARTY RISK: MANAGING RISK IN AN INTERCONNECTED WORLD
INTRODUCTION

Digital Transformation is a journey underway in organizations across the globe. Defined as an organization's rapid adoption of technology and increased integration of business processes, Digital Transformation creates opportunities to gain strategic efficiencies and capabilities, by providing a technology model that improves continuously and is guided by data. The outcome is smart, actionable insights, and the ability to act on those insights faster than the competition, which enables the delivery of better, more innovative products and services.

One important outcome of Digital Transformation is an explosion of interconnectivity between organizations and the wide availability of third-party capabilities, including:
- Public cloud infrastructures
- Connectivity to partner systems
- Use of outside data sources
- E-commerce networks and platforms
- Sophisticated global supply chains

But this transformation is not completely without cost. Third parties (and even fourth parties) can become dependencies for critical business functions. Third-party risk can result from many common interactions, including with suppliers, distributors, vendors, resellers, cloud partners, B2B partners, outsourcing partners, or through actual or implied contracts.

For example, third parties regularly support the storage, transmission, processing and distribution of critical business and customer data. They participate in integrated supply chains, where the system relies on every third-party link to perform its function, or severe business disruptions may result. And modern third-party relationships often have technical interconnections, where design and control must be maintained and verified on all sides to ensure the accuracy, completeness and availability of all information handled by third parties.

Thus, the benefits received from third parties must be balanced against the risks assumed:

<table>
<thead>
<tr>
<th>BENEFITS</th>
<th>RISKS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Competitive edge</td>
<td>Poor performance</td>
</tr>
<tr>
<td>Leverage vendors’ expertise</td>
<td>Financial exposure</td>
</tr>
<tr>
<td>Resource optimization</td>
<td>Compliance/litigation</td>
</tr>
<tr>
<td>Lower cost/more profitable</td>
<td>Information security</td>
</tr>
<tr>
<td></td>
<td>Resiliency</td>
</tr>
<tr>
<td></td>
<td>Social responsibility</td>
</tr>
<tr>
<td>Expanded market opportunity</td>
<td>Reputational harm</td>
</tr>
<tr>
<td></td>
<td>Strategic failure</td>
</tr>
</tbody>
</table>
Like all risks, third-party risk is not binary—you can’t eliminate it completely, or at least not without forsaking all the benefits of interconnectivity and partnerships. The task is then to identify, mitigate and continuously manage third-party risks, and continuously improve and maintain the maturity of your third-party risk program.

To address this need, RSA has created the RSA Risk Framework for Third Party Risk. Like other RSA Risk Frameworks, it’s based on a maturity model that helps customers fully assess and effectively improve their capabilities. It provides a lens to analyze the full range of third-party risk requirements, using detailed questions and applying expert analysis.

It’s based on established and understood industry risk frameworks, including ISO 31000 and NIST SP 800-161, as well as cybersecurity frameworks including NIST Cybersecurity Framework (CSF) 1.1 and NIST SP 800-61 Rev. 2, Computer Security Incident Handling Guide (CSRC). However, the RSA Third Party Risk Framework goes beyond the broad standards to leverage RSA’s deep experience (including industry-specific experience) in helping customers address and manage third-party-related risks of all types.

---

**Figure 1: RSA Third Party Risk Framework (Simplified)**

**THIRD-PARTY RISK CHALLENGES**

The fundamental challenge with third-party risk is that, by definition, it involves entities over which you exercise no direct control, other than by contract. But you still have the requirement to proactively identify, mitigate and manage those inherited risks over time. As the saying goes, experience is a cruel teacher because the test comes before the lesson. With risk, the only course of action is to anticipate the test and study as hard as you can in case the test happens.
In fact, bad outcomes from third-party risks are in the headlines daily. We witness stories of inferior and defective supplier products, cloud service outages, regulatory violations committed by third parties, and a barrage of third-party provider data breaches. In its 2018 Data Risk in the Third-Party Ecosystem report, 1 42% of Ponemon Institute survey respondents report a data breach due to third parties in the prior 12 months, while an additional 22% did not know if they had suffered such a breach. In another widely reported example, Facebook has repeatedly suffered personal data disclosure through its third parties, including Cambridge Analytica, which shared the information of 87 million users.

Simply put, as businesses use more third-party products and services to conduct business, the risks from these relationships also increase. The number, complexity and velocity of these risks make it difficult to track and respond effectively. Furthermore, the oversight of third-party performance becomes increasingly important to ensure that the quality of products and services delivered continues to meet required standards.

There are three primary drivers of risk, which RSA calls the “3 M’s”: Modernization (Digital Transformation), Mandates (such as GDPR and other privacy laws) and Malice (skilled and well-resourced attackers). Third-party risk is driven by all three.

Organizations are more frequently using third-party suppliers to augment or deliver their products and services, and those suppliers have third parties providing services to them. With so many relationships to track, the complexity of third-party governance can be difficult to understand and manage. Many organizations struggle to maintain the staff or resources to cope with this increased complexity. Organizations are often left wondering where to start and how to prioritize what is most important to the business. Unfortunately, this results in surprises that cause business disruptions.

Often, pockets of vendor profiles, details of engagements and performance data are spread across different teams within the organization. Third-party risks are not identified, assessed, treated and monitored consistently across all lines of business. Each team talks about risk using different language with different measurements, controls and reporting. As a result, it becomes difficult to find a single source of “truth” for third-party risk and performance. Without a consistent enterprise view of third-party risks, the executive team does not have a clear enough picture of risk to make well-informed business decisions about which third parties they should do business with, or which ones need to be carefully managed to prevent unwanted surprises from popping up.

---

1 Ponemon Institute, Data Risk in the Third-Party Ecosystem, November 2018
Organizations are challenged to keep up with the management of so many vendors. Many use traditional spreadsheet-based approaches or other homegrown systems that can’t keep up with the exploding number of interconnections driven by Digital Transformation.

**THE RSA RISK FRAMEWORK FOR THIRD PARTY RISK**

The RSA Risk Framework for Third Party Risk is a professional services offering from RSA Risk & Cybersecurity Advisory Practice (RCAP). Like all RSA Risk Frameworks, this services engagement delivers a business-centric model of consultancy that addresses a specific, major problem facing boards of directors today, including cyber incident risk and third-party risk, as well as risks from the dynamic workforce and multi-cloud environments.

RSA Advisors bring the tools and experience to help organizations assess their current readiness for managing a risk, and to implement a customized strategy for rapid and continual improvement.

Utilizing the RSA Risk Framework for Third Party Risk, RSA Advisors help organizations advance programs and processes to clearly identify, effectively mitigate and continuously manage third-party risk. This process targets the difficult but critical task of assessing and managing the risks associated with the full range of independent organizations with whom your organization has business and/or technical relationships.

These risks grow commensurately with the Digital Transformation and globalization that drives an increasingly interconnected world. Even the best-run organizations face business impacts arising from failures that are outside their control, including regulatory compliance violations, data breaches, fraud, business interruption and reputational damage.

As with all RSA Risk Frameworks, the Third Party Risk practice helps assess a company’s current readiness for managing this risk, with an approach that crosses an organization’s traditional functional boundaries, using a maturity model that supports the perspective of the CEO and board members.
The RSA Third Party Risk Assessment provides the following:

- Conducting of interviews with key business stakeholders to deeply understand the business’s goals and objectives relating to third-party relationships
- Gap analysis between current state program posture and desired third-party risk program posture, including comparison to industry best practices
- Identification of types of risks to mitigate and continuously manage, as well as processes to track third-party controls, certifications and risk-management processes
- Administration of the RSA proprietary Third Party Risk Management Program Quantification Model to baseline current risks arising from potential outcomes due to failures of third parties
- Evaluation of strengths and weaknesses of third-party risk-management processes as related to customer industry, business goals and risk tolerance
- Development of a roadmap that can be utilized to move to a desired level of third-party risk-management program maturity with time to value as a driver in the roadmap
- Readout of results to stakeholders

At the conclusion of RSA Third Party Risk advisory engagement, clients should have a clear understanding of risk-management maturity across the relevant categories, and demonstrate the ability to identify, mitigate and manage risk at the highest level of effectiveness. Additionally, clients should have in place a strategic roadmap to both improve maturity in key areas and to sustain capabilities already in place, even in the face of evolving or increasing risks.

In many organizations, RSA can apply its Third Party Risk Framework and begin making demonstrable impact in one to 12 weeks. A typical Assessment and Gap Analysis with interviews and presentation of final deliverable requires a team of two to three RSA Professional Services Advisors, and may vary depending on the complexity and size of the environment as well as the amount of interviews/surveys required. The model presumes 10 to 12 interviews plus an online assessment component.

**HOW IT WORKS**

Different representations of the RSA Risk Framework for Third Party Risk highlight different aspects of the model. Figure 3 shows the leading indicators of maturity across four main areas of third-party risk: Ecosystem, Contracting, Identity and Governance. A detailed scoring system behind these categories and ratings allows organizations to assess maturity for every area and baseline an initial score based on the company’s risk tolerance. This tally can then be used as a reference point from which to prioritize investments, adjust strategy and take other actions that advance third-party risk management.
• **Ecosystem**—The alignment of business goals/objectives with external information systems, hardware, software and all other product and services delivered by third parties

• **Contracting**—The inclusion of scope, accountabilities and service-level agreements 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 service-level agreements as specified in contracts and legal agreements

Organizations at the most mature level achieve Operational Excellence optimizing third-party security and minimizing business risk. They do this by coordinating and integrating IT and business risk functions across the entire third-party risk-management lifecycle. Other characteristics of maturity include automation of key processes, advanced analysis capabilities and continuous improvement of the incident management lifecycle.

The RSA Third Party Risk Framework engagement assesses the types of capabilities that exist at each level of the model. In many cases, maturity progresses from manual processes to siloed digital processes to highly automated, integrated processes. Organizations at intermediate levels of maturity tend to rely on spreadsheets or online tools, coupled with nonintegrated point solutions, and open source or free tools. The problem with this approach is that it rarely provides a holistic view of the risk environment and typically yields a slow and incomplete response. Lacking the
insight, visibility and playbooks capable within today’s modern third-party risk programs puts organizations at a strategic disadvantage, making it more likely that a risk will turn into a problem, and that the problem will have a substantial negative impact.

**HOW RSA SOLUTIONS MAP TO THE RSA RISK FRAMEWORK FOR THIRD PARTY RISK**

RSA provides a rich portfolio of products and professional services that enable organizations to unify disparate IT security and business risk functions, advance their maturity model, and reduce risk. As shown in Figure 3, the RSA Risk and Cybersecurity Advisory Practice and RSA product suites address every area of mature third-party risk management, across Ecosystem, Contracting, Identity and Governance.

![Image of RSA Solutions Mapping](image)

**RSA Risk and Cybersecurity Advisory Practice (RCAP) is the umbrella practice for the critical components of Digital Risk Management, and helps customers implement solutions that protect against risk, ensure compliance and accelerate business objectives. Within RCAP are:**

- **RSA Risk Management Practice**, which helps organizations advance their capability for continuous risk improvement and helps ensure that risk programs are well-coordinated and aligned with identified business tolerance levels when it comes to reducing third-party risk.

- **RSA Advanced Cyber Defense (ACD) and RSA Incident Response (IR)**, which help organizations design and deploy effective cyber-defense systems, and to respond to attacks, respectively. Industry expertise has been earned through thousands of proactive and reactive engagements across the globe.
• RSA Identity & Assurance Practice, which helps organizations resolve the two big challenges related to third-party access to systems. Authentication is the process of continuously validating the identity of a person or resource, while identity governance ensures that access is restricted only to what should be available to any specific identity.

RSA Product Solutions are industry-leading software tools that empower organizations to address the critical domains of Integrated Risk Management, Threat Detection and Response, and Identity and Access Management. These include:

• RSA Archer® Suite, which delivers Integrated Risk Management (IRM) to increase visibility and insight into true business risks and empower organizations to make better decisions throughout the risk-management lifecycle.

• RSA NetWitness® Platform, which is an advanced security information and event management (SIEM) and threat defense solution that aligns business risk context to security risks so that security teams can rapidly detect and understand the full scope of a compromise and its associated risks.

• RSA SecurID® Suite, which facilitates business by allowing legitimate users to quickly and easily identify themselves, while mitigating the risk of unauthorized users gaining access to the network and other resources.

CONCLUSION
The RSA Risk Framework for Third Party Risk provides a maturity model for developing a mature, business-driven strategy that is informed by—and accommodates—both IT and business risk functions across the third-party risk domain. Organizations can apply products and solutions from the RSA portfolio to fully operationalize the model at the highest levels of maturity. In doing so, they can reduce risks to revenue/mission, reputation and compliance while safely pursuing opportunities that allow them to thrive.

To find out more about using the Risk Frameworks to assess and optimize your organization’s risk management strategy, please visit rsa.com/risk-frameworks.