RSA

RSA RISK FRAMEWORK FOR THIRD-PARTY RISK

HELPS ORGANIZATIONS MATURE CAPABILITIES TO CONTROL RISK ARISING FROM THIRD-PARTY RELATIONSHIPS

Organizations across the globe are undergoing Digital Transformation, with rapid adoption of new technology and increased integration of business processes. Digital Transformation delivers efficiency and flexibility to enable the delivery of better, more innovative products and services. Yet organizations are also realizing that a new class of cyber and digital risks has emerged. While rooted in traditional security, identity and risk challenges, Digital Transformation has caused them to mushroom in scale, complexity and consequence.

To help organizations improve their ability to manage these risks, RSA has developed RSA Risk Frameworks. These are Advisory Engagements for organizations seeking to optimize maturity in a specific area impacted by Digital Transformation, including Cyber Incident Risk and Third-Party Risk, as well as Dynamic Workforce and Multi-cloud Transformation. Delivered by RSA Risk & Cybersecurity Advisory Practice (RCAP), Risk Frameworks engagements leverage advanced assessment tools based on proven best practices for cybersecurity and risk management developed over thousands of previous engagements. They provide customers a view of their current state of cyber risk maturity, with a gap analysis and a roadmap for advancing maturity.

One of the biggest impacts of Digital Transformation is the exploding number of potential interfaces between an enterprise and its partners, including data sources. In today's dynamic environment of interconnections and outsourcing, it is not enough for an enterprise to be focused only on its internal risk. The enterprise must manage risk across the enterprise's entire ecosystem of third parties including partners, cloud providers, software hosting companies, service providers and other data partners.

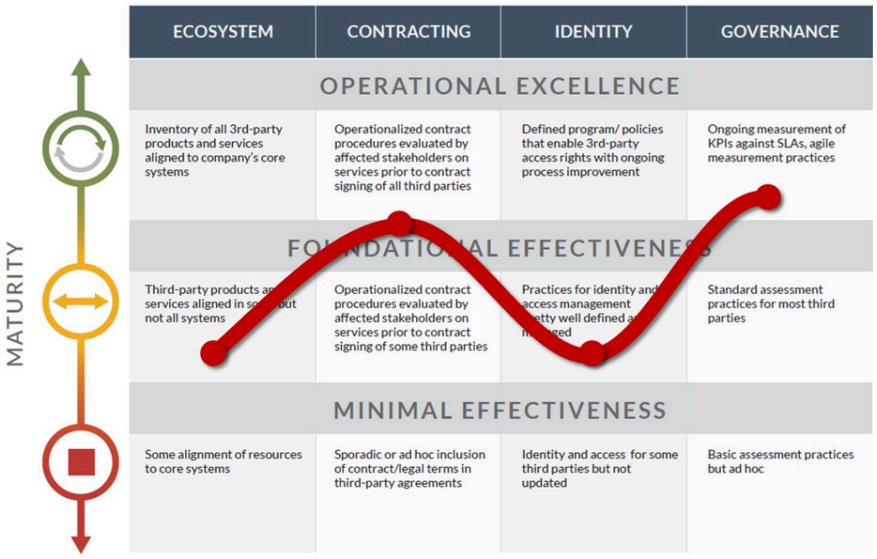

Figure 1: RSA Third Party Risk Framework (simplified)

RSA Risk Framework for Third Party Risk promotes a business-centric model of consultancy to help organizations assess their current readiness for managing risk across the ecosystem—both internal and external. The outcomes can be significant. In its 2018 Data Risk in the Third-Party Ecosystem report, 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.[1]

Based on RSA's unique expertise across the risk and cybersecurity domains, the RSA Third Party Risk Framework targets the difficult but critical task of protecting the enterprise from digital threats that are outside an organization's control, yet central to effective performance. In this commissioned survey, 69% of IT Security and Business Risk professionals indicated agreement or strong agreement that the relationship between business risk and IT security can be difficult to coordinate. Furthermore, over 60% indicated agreement or strong agreement that their organizations have some weaknesses with regard to the IT and business risk management skills necessary for security breach detection and security breach response.[2]

The RSA Risk Framework for Third Party Governance helps organizations assess and improve their maturity across the categories of risk management: Ecosystem, Contracting, Identity and Governance. For each of these areas, RSA will apply its proprietary Third Party Risk Quantification Tool, which produces a profile of an enterprise's maturity in third-party risk, as well as an aspirational profile (long-term goal of third-party governance maturity status across the risk management lifecycle). The comparison between current and aspirational states produces a gap analysis that can help organizations prioritize areas for improvement.

As with all RSA Risk Frameworks, the Cyber Risk practice helps enterprises to assess their current readiness for managing risk with an approach that crosses an organization's traditional functional boundaries, using a maturity model that assumes the perspective of the CEO, COO, CCO, CIO and other executives.

The RSA Third Party Risk Assessment provides the following:

- Interviews and documentation with key business stakeholders to deeply understand the business's goals, objectives and existing risk posture
- Administration of the RSA proprietary Third Party Risk Maturity Quantification Tool to baseline maturity across the enterprise's ecosystem
- Gap analysis of current state posture to desired levels of third-party governance maturity based on industry best practices
- Development of a roadmap that can be utilized to move to a desired level of cyber risk management maturity

ABOUT RSA GLOBAL SERVICES

The RSA Global Services team of 650 cybersecurity business and technical consultants operates in more than 100 countries, and earned "Strong Performer" rating in the Forrester Wave™ for Digital Forensics and Incident Response Service Providers.[3] With over thousands of engagements, RSA Global Services has helped secure many types of organizations, often designing and implementing comprehensive risk and security management programs.

RSA Global Services combines deep business security skills and broad risk management knowledge to help the organization to assess and improve its third-party governance maturity status. Within the RSA Risk and Cybersecurity practice, three groups provide critical security services:

- RSA Risk and Cybersecurity Advisory Practice (RCAP) delivers business-driven cybersecurity services focused on core business analysis, business impact assessment and cyber risk assessment in the areas of cyber incident management, third-party governance, data privacy and digital business resiliency.
- RSA Advanced Cyber Defense (ACD) delivers services to assess breach readiness, security operations center (SOC) or cyber incident response team (CIRT) assessment and design, incident response planning and testing, and "Expert on Demand" services.
- RSA Incident Response (IR) helps customers design, manage and perform incident response functions via both proactive and reactive services. Available on a retainer or ad hoc basis, RSA IR extends the organization's security skills to deal with security incidents of all types and severities.

[1] Ponemon Institute, Data Risk in the Third-Party Ecosystem, November 2018
[2] ESG Custom Research, Cybersecurity and Business Risk Survey, June 2018
[3] The Forrester Wave™: Digital Forensics and Incident Response Service Providers, Q3 2017