RSA

# RSA Risk Framework für Drittanbieterrisiken

## Unterstützt Unternehmen bei der Entwicklung ausgereifter Funktionen zur Steuerung von Risiken aus Beziehungen zu Drittanbietern

Unternehmen auf der ganzen Welt durchlaufen die digitale Transformation – mit der schnellen Einführung neuer Technologien und einer verbesserten Integration von Geschäftsprozessen. Die digitale Transformation bietet Effizienz und Flexibilität, damit bessere und innovativere Produkte und Services bereitgestellt werden können. Den Unternehmen ist jedoch auch bewusst, dass eine neue Klasse an Cyber- und digitalen Risiken entstanden ist. Die digitale Transformation ist zwar mit den herkömmlichen Sicherheits-, Identitäts- und Risikoherausforderungen verwurzelt, hat aber zu einer explosionsartigen Zunahme bei Skalierung, Komplexität und Konsequenz geführt.

Um Unternehmen zu helfen, ihre Fähigkeit zum Managen dieser Risiken zu verbessern, hat RSA die RSA Risk Frameworks entwickelt. Dabei handelt es sich um Beratungsprojekte für Unternehmen, die den Reifegrad in einem bestimmten Bereich, der von der digitalen Transformation beeinflusst wird, optimieren möchten. Dazu zählen auch Cyber-Incident-Risiken und Drittanbieterrisiken sowie dynamische Mitarbeiter und Multi-Cloud-Transformation. Die von RSA Risk & Cybersecurity Advisory Practice (RCAP) bereitgestellten Risk-Framework-Projekte nutzen erweiterte Bewertungstools, die auf bewährten Best Practices für Cybersicherheit und Risikomanagement basieren und im Laufe von Tausenden bisheriger Projekte entwickelt wurden. Sie bieten Kunden einen Überblick über den aktuellen Stand zum Reifegrad von Cyberrisiken, zusammen mit einer Gap-Analyse und einer Roadmap für die Reifegradentwicklung.

Eine der größten Auswirkungen der digitalen Transformation ist die explosionsartig steigende Anzahl potenzieller Schnittstellen zwischen einem Unternehmen und seinen Partnern, dazu zählen auch Datenquellen. In der heutigen dynamischen Umgebung mit gegenseitigen Verflechtungen und Outsourcing reicht es nicht mehr aus, wenn sich ein Unternehmen nur auf eigene interne Risiken konzentriert. Das Unternehmen muss Risiken im gesamten Ökosystem von Drittanbietern managen, einschließlich Partnern, Cloud-Anbietern, Software-Hosting-Unternehmen, Serviceanbietern und anderen Datenpartnern.

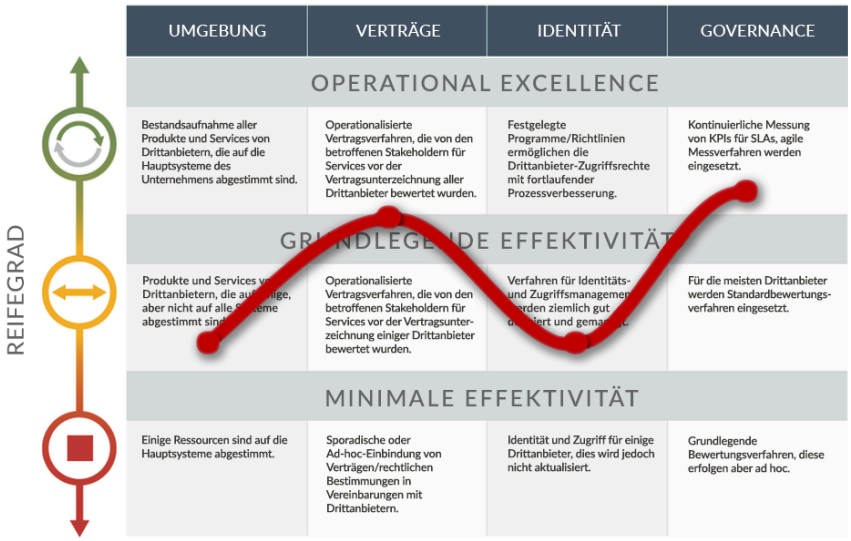


*Abbildung 1: RSA Third Party Risk Framework (vereinfacht)*

Das RSA Risk Framework für Drittanbieterrisiken fördert ein geschäftsorientiertes Beratungsmodell, das Unternehmen dabei hilft, ihre aktuelle Bereitschaft für das Risikomanagement im gesamten Ökosystem – sowohl intern als auch extern – zu bewerten. Die Vorteile können signifikant sein. Im Bericht „Data Risk in the Third-Party Ecosystem“ von 2018 vom Ponemon Institute gaben 42 % der Umfrageteilnehmer an, dass in den letzten 12 Monaten eine Datenschutzverletzung durch einen Drittanbieter erfolgte; weitere 22 % konnten keine Angabe machen, ob eine solche Verletzung stattfand.[1]

Basierend auf dem einzigartigen Know-how von RSA im Bereich der Risiko- und Cybersicherheit zielt das RSA Third Party Risk Framework auf die schwierige, aber entscheidende Aufgabe ab, das Unternehmen vor digitalen Bedrohungen zu schützen, die zwar nicht der Kontrolle des Unternehmens unterliegen, aber dennoch zentral für effektive Leistung sind. In der beauftragten Umfrage stimmten 69 % der Geschäftsrisiko- und IT-Sicherheitsexperten zu oder sehr zu, dass die Beziehung zwischen Geschäftsrisiko und IT-Sicherheit schwer zu koordinieren sein kann. Darüber hinaus stimmten über 60 % zu oder sehr zu, dass ihre Unternehmen einige Schwächen bei den Geschäftsrisiko- und IT-Managementfähigkeiten aufweisen, die für die Erkennung von und Reaktion auf Sicherheitsverletzungen erforderlich sind.[2]

Das RSA Risk Framework für Drittanbieter-Governance unterstützt Unternehmen dabei, den Reifegrad für die verschiedenen Kategorien des Risikomanagements zu beurteilen und zu verbessern: Umgebung, Verträge, Identität und Governance. In jedem dieser Bereiche setzt RSA das proprietäre Tool „Third Party Risk Quantification“ ein, mit dem ein Reifegradprofil des Unternehmens für Drittanbieterrisiken sowie ein angestrebtes Profil (langfristiges Ziel des Reifegradstatus für die Drittanbieter-Governance im Risikomanagement-Lebenszyklus) erstellt werden. Der Vergleich zwischen aktuellem und angestrebtem Status bringt eine Gap-Analyse hervor, mit deren Hilfe Unternehmen die Bereiche, in denen Verbesserungen erforderlich sind, priorisieren können.

Wie bei allen RSA Risk Frameworks unterstützt auch die RSA Cyber Risk Practice Unternehmen dabei, ihre aktuelle Bereitschaft für das Risikomanagement anhand eines Ansatzes zu bewerten, der die traditionellen Funktionsgrenzen eines Unternehmens überschreitet. Dabei wird ein Reifegradmodell verwendet, das die Perspektive von CEO, COO, CCO, CIO und anderen Führungskräften annimmt.

Die Drittanbieter-Risikobewertung von RSA bietet Folgendes:

- Interviews und Dokumentationen mit wichtigen geschäftlichen Stakeholdern, um ein gutes Verständnis der Unternehmensziele, der Zielsetzungen und der vorhandenen Risikoposition des Unternehmens zu entwickeln
- Administration des proprietären Tools „Third Party Risk Maturity Quantification“ von RSA für den Baseline-Reifegrad in der gesamten Umgebung des Unternehmens
- Gap-Analyse vom aktuellen Status bis zum gewünschten Reifegradlevel der Drittanbieter-Governance basierend auf Best Practices der Branche
- Entwicklung einer Roadmap, anhand der das gewünschte Reifegradlevel im Cyberrisikomanagement erreicht werden kann

## Informationen über RSA Global Services

Das Team von RSA Global Services aus 650 Business- und technischen Beratern für Cybersicherheit ist in über 100 Ländern tätig und hat von Forrester Wave™ die Auszeichnung „Strong Performer“ im Bereich „Digital Forensics and Incident Response Service Providers“ erhalten.[3] In Tausenden von Projekten hat RSA Global Services zahlreichen Unternehmenstypen bei der Sicherung geholfen und dabei häufig umfangreiche Programme für das Risiko- und Sicherheitsmanagement entwickelt und implementiert.

RSA Global Services kombiniert fundierte Kenntnisse der Unternehmenssicherheit und umfassendes Know-how im Risikomanagement und kann so Unternehmen bei der Bewertung und Verbesserung des Reifegradstatus der Drittanbieter-Governance unterstützen. Im Rahmen der RSA Risk and Cybersecurity Practice stellen drei Gruppen wichtige Sicherheitsservices bereit:

- RSA Risk and Cybersecurity Advisory Practice (RCAP) bietet geschäftsorientierte Services für Cybersicherheit, deren Schwerpunkt auf der Analyse des Hauptgeschäfts, der Bewertung der geschäftlichen Auswirkungen und der Bewertung von Cyberrisiken in den Bereichen Cyber-Incident-Management, Drittanbieter-Governance, Datenschutz und digitale Geschäftsstabilität liegt.
- RSA Advanced Cyber Defense (ACD) bietet Services zur Bewertung der Sicherheitsverletzungsbereitschaft, zur Beurteilung und Gestaltung des SOC-Teams (Security Operations Center) oder des CIRT-Teams (Cyber Incident Response Team), Incident-Response-Planung und -Tests sowie „Expert on Demand“-Services.
- RSA Incident Response (IR) unterstützt Kunden mithilfe von proaktiven und reaktiven Services bei der Entwicklung, dem Management und der Ausführung von Incident-Response-Funktionen. RSA IR ist auf Retainer- oder Ad-hoc-Basis verfügbar und erweitert die Sicherheitsfähigkeiten der Unternehmen, damit diese Sicherheits-Incidents aller Arten und Schweregrade bewältigen können.

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


09/20, Datenblatt, H17618-1 W386667.