

# RSA® ARCHER® THIRD PARTY GOVERNANCE

## ソリューション概要

### はじめに

サードパーティとの関係に関するネガティブな記事が、ほぼ毎日のように見出しを飾っています。たとえば、サプライヤーから提供された製品に欠陥があった、クラウドサービスが停止した、サードパーティプロバイダーによるデータ侵害がたび重なっているといったものです。組織が製品やサービスの提供または強化のためにサードパーティサプライヤーを利用する頻度はますます高くなっています。また、これらのサプライヤーでも、サービスを提供するサードパーティを利用しています。

サードパーティの製品やサービスがビジネス活動のために利用されるようになればなるほど、リスクイベントやパフォーマンス低下の発生頻度が高くなり、それらの影響も大きくなります。さらに、リスクの件数、複雑さ、拡大速度も増大します。追跡する関係が非常に多いため、サードパーティガバナンスの複雑さを把握し、管理することは困難です。ほとんどの組織では、こうした複雑さの増大に対処するためのスタッフや利用可能なリソースを用意することはとてもできません。残念ながら、こうしたことが原因で、ビジネスに損害をもたらす不測の事態が発生することも少なくありません。ベンダープロフィールの一部、エンゲージメントの詳細、パフォーマンスデータが組織内のさまざまなチームにばらまかれるといったことが何度も発生しています。これは、ビジネスコンテキストや、サードパーティとの関係の重要性をまったく理解できていないことを意味しています。

サードパーティのリスクおよびパフォーマンスを管理するための一貫性のあるエンタープライズ規模のフレームワークがなければ、すべての業務部門においてサードパーティリスクの特定、評価、処置、監視を一貫性のある方法で行うことはできません。結果として、サードパーティのリスクおよびパフォーマンスを把握するための唯一の信頼できる情報源を見つけることが難しくなります。サードパーティリスクの包括的なエンタープライズビューがなければ、経営陣はビジネス上の意思決定に必要な、明確なイメージを描くことができません。

### TAKE CHARGE OF THIRD PARTY RISK AND PERFORMANCE

サードパーティのリスクおよびパフォーマンスの管理プロセスを企業全体で標準化することにより、共通の語法、測定法、統制、プロセスを確立し、リスクの把握、優先順位付け、管理をすばやく行うことができます。サードパーティリスクを正確に表示するこのRSA Archerにより、経営陣はサードパーティリスクのイメージを正確に描き、リソースを迅速に割り当て、より適正なビジネス上の意思決定を下すことができます。

### RSA ARCHER THIRD PARTY GOVERNANCEのメリット

RSA® Archer® Third Party Governanceにより、ベンダーとの関係の監視を自動化および効率化することができます。また、GRC(ガバナンス、リスク、コンプライアンス)プログラムの一環として、サードパーティ管理のライフサイクル全体を通して規制上の義務を果たし、ベストプラクティスを実行するのに必要な、重要なアクティビティを促進することができます。有望な関係を把握し、影響を受ける利害関係者を招集して、契約に伴うリスク、財力、各種のリスクカテゴリーに存在する固有リスクと残留リスクを評価することができます。これにより、リスクに基づく選択を行い、パフォーマンスメトリックを設定して、サードパーティのライフサイクル全体を通してプログラムを監視および管理できるようになります。

### Understand Your Third Party Relationships

組織全体でサードパーティの利用頻度が高まると、組織が利用しているサードパーティと、それらがもたらすリスクの大きさをカタログ化して評価するための機能が必要になります。この機能は、組織のサードパーティに対する依存度と関連するリスクを把握するうえで重要な役割を果たします。また、サードパーティのパフォーマンスを最適化し、不測の事態や損失の発生を防ぐための最初の一步になります。

サードパーティとの関係が依然として、あらゆる規模の企業において大きな悩みの種になっています。85%もの回答者が、ジョイントベンチャーのパートナー、サプライヤー、ディストリビューター、エージェントなどとのビジネス上のつながりをどうにかして見直していると回答しました。ただしその大半は、サードパーティとの間に発生するリスクを調査するか、それらのリスクの監視を強化するかのいずれかです。

コンプライアンスのトレンドに関する調査  
Deloitte および Compliance Week  
2014年5月

Ponemon Institute が実施した調査では、調査に参加した企業の41%以上でサードパーティによるデータ侵害に悩まされていました。その結果として失われたブランド価値は、多くの場合、1億8,400万ドルから3億3,000万ドルに上りました。

## 意思決定とアクションの実行

組織のリスク選好度とリスク許容度に従って、一貫性のある方法でサードパーティリスクに関する意思決定を行い、必要に応じて適切なリスク対応を実施されるようにしてください。サードパーティリスクを最小限に抑えるには、組織のすべてのマネージャーが一貫性のある方法でリスクを評価し、組織のリスク許容度に基づいて統制とリスク移転手法を適用していることが確認される必要があります。結局、防御の最前線として、マネージャーが適切な措置を講じる責任を果たす必要があります。

## Monitor Third Party Relationships

組織のサードパーティリソースへの依存度はますます高くなっています。そのため、ベンダーとの関係についての最新情報を常に把握し、既存のサードパーティとの関係に生じる重大な変更をモニタリングできるようにする必要があります。サードパーティとの関係は静的なものではなく、リスクは今後も出現および進化し続けるでしょう。最終的には、サードパーティとの関係に重大なリスクが存在しないようにする必要があります。

## RSA ARCHER THIRD PARTY GOVERNANCE

RSA Archer Third Party Governanceであれば、有望な関係を把握し、影響を受ける利害関係者を招集して、契約に伴うリスク、財力、各種のリスクカテゴリーに存在する固有リスクと残留リスクを評価することができます。これにより、リスクに基づく選択を行い、パフォーマンスメトリックを設定できるようになります。RSA Archer Third Party Governanceでは、サードパーティ管理のライフサイクル全体を通して規制上の義務を果たし、ベストプラクティスを実行するのに必要な、重要なアクティビティを促進することにより、ベンダーとの関係の監視を自動化および効率化することができます。

RSA Archer Third Party Governanceには、サードパーティのリスクおよびパフォーマンスの管理プログラムの成熟度に応じて、特定のビジネスニーズを満たすユースケースが複数用意されています。(以下のオプションを選択できます)

### Third Party Catalog

RSA Archerサードパーティカタログを利用すると、サードパーティとの関係/エンゲージメント、関連する契約のほか、各サードパーティとの関係構築に携わっている組織内のビジネスユニットおよび担当者をすべてドキュメント化できます。RSA Archerでは、単一のリポジトリに含まれているすべてのサードパーティ情報(プロフィール、エンゲージメント、サードパーティのビジネス階層、担当者、設備、サードパーティの責任者など)に関するレポートを作成できます。

### Third Party Engagement

RSA Archer Third Party Engagementでは、サードパーティから提供される製品およびサービスに関する情報を詳細に文書化することができます。たとえば、サードパーティがサポートするビジネスプロセスに製品/サービスエンゲージメントを関連づけたり、フォースパーティ、保険契約証書、マスターサービス契約をドキュメント化したりすることができます。これらの情報を通じて、サードパーティへの依存度を包括的に把握することができます。また、契約のレビュー、契約のリスクの評価、サードパーティの財務面の有効性の評価、固有リスクの評価を、複数のリスクカテゴリーにわたって実施することができます。サードパーティエンゲージメントは、サードパーティに対する固有リスクエクスポージャーの量を明確に把握するのに役立ちます。

### Third Party Risk Management

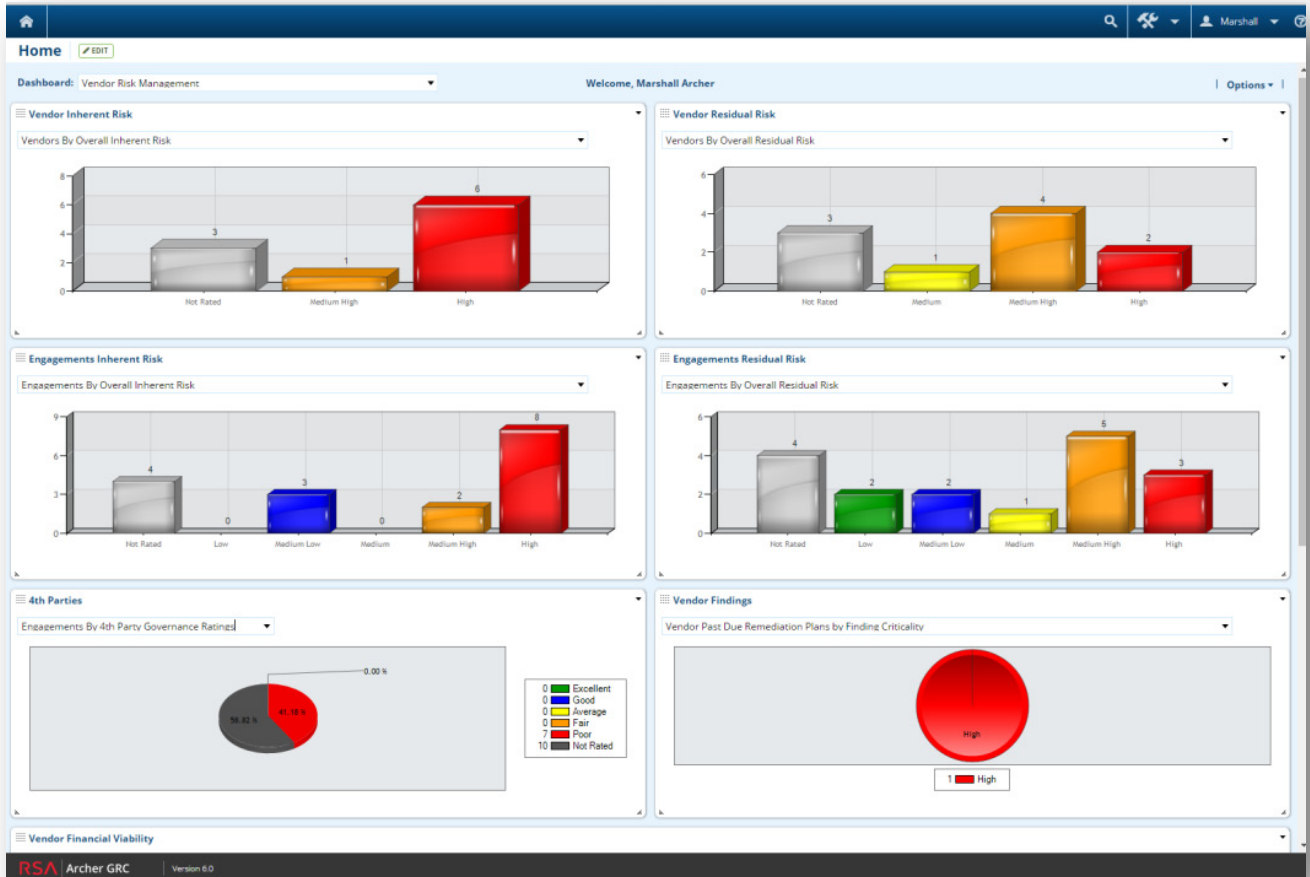
RSA Archerサードパーティリスク管理では、サードパーティが組織に提供するエンゲージメントに関連して導入しているガバナンスと統制を評価することができます。これらの評価によって、財力、契約のリスク、コンプライアンス/訴訟、忠実度、情報セキュリティ、評判、回復性、戦略、サステナビリティ、フォースパーティリスクなどの各種のリスクカテゴリーにおける、サードパーティエンゲージメントの残留リスクスコアが決まります。さらに詳細な分析を行うために、アセスメントアンケートを構成して、関連するサポートドキュメントの収集のために使用することができます。こうしたアンケートの結果は、サードパーティが組織に提供するすべてのエンゲージメントにおいて、サードパーティの全体的な残留リスクプロフィールを特定する際に要因として考慮されます。評価の発見事項を自動的に収集して、例外として管理することができます。また、改善計画を策定して、問題が解決されるまで監視することができます。

### Third Party Governance

RSA Archer Third Party Governanceでは、各サードパーティのパフォーマンスを監視できます。メトリックは、4つのカテゴリー内でエンゲージメントごとに設定できます。そのカテゴリーとは、品質、イノベーション、パフォーマンス、関係です。メトリックはエンゲージメントごとに示されます。また、メトリックを集約してサードパーティに送り、当該サードパーティが提供するすべてのエンゲージメントのパフォーマンスを示すことができます。

## まとめ

RSA Archer Third Party Governanceは組織にとって、サードパーティガバナンスプログラムの一元的な統合、ビジュアル化、管理ポイントになります。RSA Archer Third Party Governanceは、異なるリスクリポジトリから収集したサード/フォースパーティのリスクデータを統合することにより、サードパーティのライフサイクル全体をさらに適正に把握し、優先順位を付け、管理することができます。また、効率的かつ効果的な方法でプログラムを管理しながら、必要なリスク管理のアカウントビリティと文化を強化します。



EMC、EMC、EMCのロゴ、RSA、RSAのロゴ、Archerは、米国およびその他の国におけるEMC Corporationの登録商標または商標です。VMwareは、米国およびその他の地域におけるVMware, Inc.の登録商標または商標です。Copyright © 2016 EMC Corporation. All rights reserved. Published in the USA. 4/16ソリューション概要H14008-2-J

RSAは、この資料に記載される情報が、発行日時点で正確であるとみなしています。この情報は予告なく変更されることがあります。

**RSA**