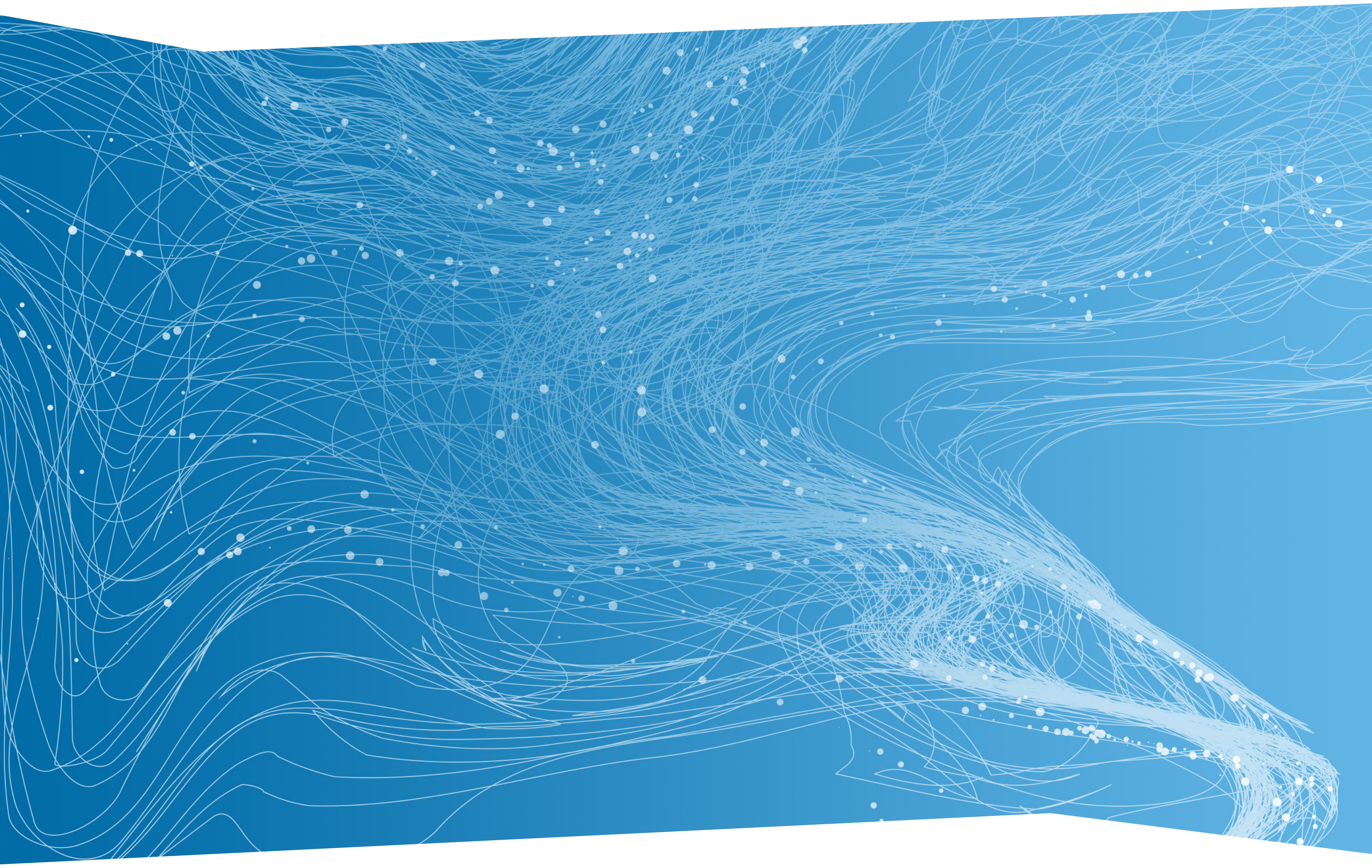


WHITE PAPER

RSA ARCHER® MATURITY MODEL: THIRD PARTY GOVERNANCE

RSA

OVERVIEW

As companies rely more and more on third party products and services to conduct business, the number of risks that these relationships pose to the organization increases and the more important their performance becomes. The RSA Archer Maturity Model for Third Party Governance outlines RSA Archer's role in the critical stages of a company's journey from reactive, compliance driven processes to a risk centric, opportunity focused program managing the risks and performance of third parties that provide a competitive advantage to fuel the enterprise.

CONTENTS

RSA

WHY THIRD PARTY GOVERNANCE?

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. 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 the quality of products and services delivered continue to meet required standards.

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. Most organizations simply do not have 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 supplier risks are not identified, assessed, treated and monitored consistently across all of business lines. 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 picture of risk needed to make business decisions.

KEY CAPABILITIES

RSA Archer GRC Maturity Models focus on key capabilities enabled by the RSA Archer solution. As a technology enabler, RSA Archer provides the critical infrastructure to leverage processes, share data and establish common taxonomies and methodologies.

RSA Archer Third Party Governance automates and streamlines oversight of vendor relationships. The solution facilitates key activities necessary to fulfill regulatory obligations and best practices across the entire third party management lifecycle as part of a governance, risk and compliance (GRC) program. With RSA Archer Third Party Governance, the organization can capture prospective relationships, engage affected stakeholders, assess inherent and residual risks across multiple risk categories, enforce risk-based selection, and establish performance metrics.

By standardizing on third party risk and performance management processes across the enterprise, the organization can establish a common language, measurements, controls and processes to quickly prioritize and manage risks. With this comprehensive view of supplier risks, RSA Archer provides the executive team with an accurate picture of third party risk, enabling them to quickly allocate resources and make better business decisions.

To achieve these goals, RSA Archer's Third Party Governance solution focuses on the following key capabilities:

Establish scope and context for third party management
Catalog business and IT assets, relationships and criticality, establish ownership and accountability, and lay the foundation to better understand exactly where and how your organization relies on third parties and who is responsible.

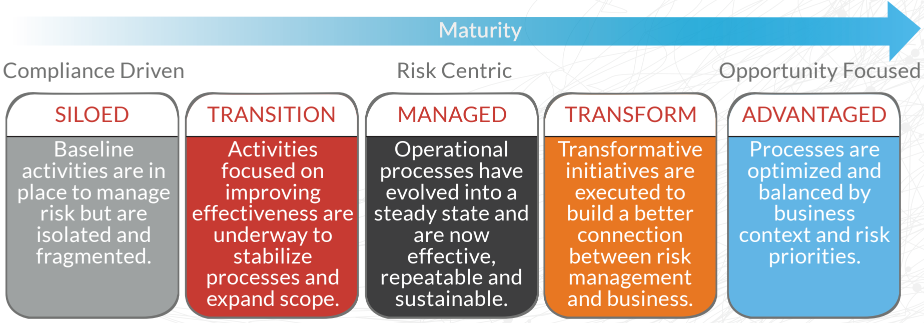
Identify and assess third party risk and performance
Build processes to catalog risk associated with identified third and fourth parties, establish key metrics and indicators of third party performance, and capture changes occurring within the business related to third party relationships and how these changes may alter the third party risk profile.

Decision and treat third party risk
Establish efficient and consistent methods to evaluate inherent and residual risk levels before on-boarding new third parties or expanding existing relationships, and establishing risk treatments, if necessary, through policies, standards and controls.

Report on and monitor third parties
Institute processes to provide accurate and timely reports to all levels of management and other stakeholders to monitor and manage the risk and performance profiles of all of the organization's third party relationships.

THE MATURITY JOURNEY

RSA Archer Maturity Models are segmented into five major stages: Siloed, Transition, Managed, Transform and Advantaged.



SILOED
Baseline activities are in place to manage risk but are isolated and fragmented.

TRANSITION
Activities focused on improving effectiveness are underway to stabilize processes and expand scope.

MANAGED
Operational processes have evolved into a steady state and are now effective, repeatable and sustainable.

TRANSFORM
Transformative initiatives are executed to build a better connection between risk management and business.

ADVANTAGED
Processes are optimized and balanced by business context and risk priorities.

The RSA Archer Maturity Model is designed to be pragmatic and attainable. Elimination of the "Level 0" that typical maturity models include avoids the unnecessary definition of a stage of maturity that will not meet today's third party governance challenges.

- The **Siloed stage** focuses on baseline activities that all organizations need to have in place to effectively manage third party risk and performance

- The **Managed stage** depicts the phase that organizations reach when they achieve a coordinated, sustainable third party risk and performance management program.

- The **Transition stage and Transform stage** help the organization "move to the next level" with initiatives that evolve critical capabilities, setting the stage for advanced capabilities.
- The **Advantaged stage** is designed to be achievable by most organizations, allowing the organization to target an advanced stage of maturity that characterizes an optimized third party risk and performance management program.

The RSA Archer Third Party Governance Maturity Model focuses on building the capabilities outlined above over time, implementing the broad strategy with tactical, intelligently designed processes.

FOUNDATIONS

Foundations are critical elements necessary for the overall success of the Maturity Journey. Without these foundations in place, an organization will face difficulties throughout their journey either due to a lack of focus, commitment, resources and/or strategy. Any organization looking to improve their third party governance maturity should discuss and address these foundations. Without a strong foundation, organizations may not be successful implementing their third party governance program. Foundational elements include:

- **Management commitment –** The degree and level of leadership commitment to third party governance culture, strategy and priorities should be established as maturing risk processes takes time and resources.
- **Performance and acceptable risk -** Defined levels of performance and acceptable risk for third party governance need to be established to set the target state for the program and to ensure the business understands the level of risks involved.
- **Expectations and measurement -** Clear expectations and success criteria defined for the third party governance program must be communicated by management to guide strategies.
- **Stakeholder involvement –** Key business stakeholders and constituents need to agree on the importance of continuous improvement and maturity of third party governance processes.
- **Budget and resources –** Sufficient resources for the third party governance program must be committed to achieve success.

SILOED

Baseline activities are in place to manage risk but are isolated and fragmented.

THE SILOED STAGE: LAYING THE FOUNDATION

In the Siloed stage, the organization has a partial inventory of its people, processes and technology. Inventories reside in different locations, in different formats and may be maintained by different technologies. In some cases, there are multiple overlapping inventories without any one system of record. Inventories that typically exist at this stage include physical facilities, software applications, organizational structure (as depicted through the organization's financial statements) and a listing of human resources.

Various business unit managers, the purchasing department, legal and internal audit have identified what they believe to be key third party relationships, but the lists are maintained separately and may reflect significant differences. There isn't yet a robust formal approach to methodically identify third parties across the organization or to assess third party risk in a consistent manner. However, risk assessments may be performed in certain areas of the organization, for certain types of relationships, and for perceived high-risk third parties.

There is a desire to manage third party risk, but the organization is just beginning to understand what is needed to treat third party risk. The various lists of third parties and any associated risk assessments are beginning to be pooled together for evaluation by senior managers within key functional areas and on an overall basis. However, the list of third parties is incomplete and the risk assessment approaches are inconsistent.

Evaluation of third party risk in the Siloed stage results in an acknowledgement of deficiencies in third party oversight and documentation of agreed upon expectations for third party risk treatment. In other words, discussions are occurring as to what makes for a high risk third party, what kinds of controls a third party should have in place relative to the risk they present, and what other types of risk treatment, including contractual covenants, should be in place to mitigate third party risk.

While the organization is able to produce a list of known third party relationships, the sources of information for the list may be spread across different areas of the organization and in different formats. Information about third parties and the products and services they deliver is inconsistent and often incomplete.

THE TRANSITION STAGE: BUILDING THE CONTEXT FOR THE FUTURE

TRANSITION

Activities focused on improving effectiveness are underway to stabilize processes and expand scope.

As an organization Transitions to the Managed stage, more infrastructure is cataloged and associations between infrastructure elements begin to be documented. In the Transition phase, cataloging of products and services and IT systems and greater detail about the organization's structure begin to be mapped together.

Agreed upon third party risk management terminology, rating scales and a consistent method for identifying and assessing third parties are adopted. Third parties and the engagements they deliver are explicitly identified and centrally cataloged. Internal, external and regulatory examination findings related to third party relationships are captured, and budget versus actual expenditures associated with third party engagements are tracked.

Third party risk tolerance levels are established within which third party relationships are expected to be managed, and authority for making third party risk decisions is explicitly delegated to named individuals.

Expectations regarding third party controls, substantive documentation, standard contract covenants, financial statements and proof of insurance have been formally documented and approved. These expectations have been translated into appropriate internal and third-party facing questionnaires and risk treatment assessment methods.

Sufficient progress has been made in cataloging and assessing third parties so that a list of key third parties can now be generated. While this represents consistent terminology and assessment rating scales, very little business context is available, and responsibility for each relationship is not always clear.

THE MANAGED STAGE: OPERATIONALLY SOUND

MANAGED

Operational processes have evolved into a steady state and are now effective, repeatable and sustainable.

In the Managed stage, the majority of infrastructure elements have been documented in central repositories, with little or no redundancies and overlap. Business processes, IT network devices, third party relationships, regulatory obligations and organizational business units are cataloged. Accountability is established by cross-mapping human resources, organizational structure, business infrastructure, IT infrastructure, third party relationships and regulatory obligations.

The repository of third parties and the engagements they are delivering are mapped to the business units that rely on the engagement, the contracts supporting the engagement, and named individuals in the first and second lines of defense that are accountable for overseeing the engagement. The completeness of the list of engagements is periodically reaffirmed with these stakeholders.

Risk assessments are performed on each third party engagement in accordance with pre-established assessment methodologies across multiple risk categories. Third parties receive assessment questionnaires that reflect the organization's expectations for third party internal control and evidentiary documentation. Assessments include an evaluation of the third party's financial wherewithal; assessment of contracts relative to the organization's pre-established standards for contract risk transfer; and consideration of any third party-related internal, external, and regulatory examination findings. Performance metrics are established for key third party engagements consistent with service level agreements and internal expectations.

The risk treatments in place around every third party engagement are evaluated relative to inherent risk prior to finalizing engagement contracts. These include the results of third party questionnaires, substantive documentation, review of financial statements, and contracts. Remediation plans and commitments received from third parties and internal stakeholders are cataloged and monitored until resolved. Decisions to proceed with engagements are enforced through submitter, reviewer and approver workflow.

In the Managed state, each stakeholder is regularly provided with a list of their risks and controls, depicting risk consistently on an inherent and residual basis so that they can understand the level of risk relative to risk tolerance. Stakeholders also receive regular reports of loss events and outstanding issues and remediation plans. They are able to understand if identified issues are being addressed by accountable individuals in a timely manner. Notifications to stakeholders are automatically generated to assist them in monitoring issues and remediation plans coming due and past due and when residual risk levels fall outside established boundaries.

The second line of defense has the necessary reports to oversee day-to-day administrative functions such as the status of risk assessment campaigns in process, contract reviews and financial statement reviews.

THE TRANSFORM STAGE: PRIORITIZATION AND CONTROL

In the Transform stage, business objectives and strategies are clearly established and documented as the organization's focus becomes more proactive. A complete picture of the interrelationship of IT infrastructure is established, mapping software applications to the systems that support them, databases that store the information, and the networking infrastructure that supports the organization.

TRANSFORM

Transformative initiatives are executed to build a better connection between risk management and business.

The Transform stage is marked by greater understanding of the business context of the third party relationship and how third parties are supporting the organization’s products and services, business processes and IT infrastructure. Further, changes to business, IT and organizational structure and activities are captured to evaluate prospective third parties and changing third party risk profiles prior to finalizing contracts.

The results of risk assessment questionnaires, supplemental documentation from third parties substantiating their control environment, and proof of insurance are all factored into the identification and assessment of third and fourth party risk. Engagement performance metrics are standardized by engagement type, and tailored and weighted according to importance. Exceptions identified through internal and third party-facing questionnaires are automatically escalated to stakeholders for consideration, and the results are reflected in residual risk assessments.

Third parties are required to provide appropriate proof of insurance, which is monitored on an ongoing basis, and exceptions in reported insurance are factored into the adequacy of the third party’s overall risk treatment.

Decisions to proceed with engagements are enforced through technology, based on the level of residual risk and the authorities granted to the individuals making the decisions. Decisions that exceed individual authorities are escalated to senior management and the Board, as appropriate. With mapping of the organization’s business and IT infrastructure, obligations, human resources and third party relationships, risk can be examined and monitored from a broader perspective, including third party risk by product and service, business process, facility, software application, IT system, database and device and regulatory obligation.

Monitoring of key indicators provides early warning of changes in the performance profile of each third party and notifications to stakeholders are automatically generated whenever indicators fall outside of boundaries. This enables stakeholders to respond as quickly as possible when performance begins to deteriorate. In the Managed stage, the second line of defense has confidence that third party management information is accurate and complete because the risk management information system is adequately designed to enforce data integrity.

ADVANTAGED

Processes are optimized and balanced by business context and risk priorities.

THE ADVANTAGED STAGE: OPTIMIZED FOR RISK MANAGEMENT

In the Advantaged stage, mapping of all infrastructure elements is complete, and there is a clear understanding of the “ownership” of strategies and objectives; the products and processes that support the strategies and objectives; the business processes that exist to enable the products and services and strategies and objectives; the IT infrastructure that supports each of the business processes; and the regulatory obligations that the organization must legally comply with. Accountability by named individual and business unit is core to a sound third party management program, reinforcing the desired risk management culture.

Processes exist to identify gaps in known third party relationships and third parties are self-reporting key fourth party relationships and governance processes. Circumstances where fourth parties have multiple relationships across the third party portfolio are documented and factored into fourth party risk assessments based on the quality of reported third party governance and the type and amount of third party risk.

Third party risk assessment results are as automated as is considered practical, and the results of engagement-level inherent and residual risk assessments and performance metrics roll up to the vendor parent level to depict overall risk and performance at the third party parent company level. Third parties with inadequate proof of insurance and those with high risk but poor financial wherewithal are identified.

Decisions to move forward with new and expanding third party relationships are methodically and consistently applied and consider all inputs. In addition, gating processes are enforced through technology to decision third party risk prior to implementing new or materially changed products, processes and activities. Automation triggers risk decisions to be made when the existing level of residual risk increases above tolerance for individual engagements or overall relationships, and documented contingency plans exist to exit significant and high risk third party relationships.

Fourth party risk associated with a third party is evaluated as part of the decision to move forward with a third party, and technology is used to ensure that all deficiencies related to proposed third party engagements are addressed prior to contract signing. Approved exceptions to third party risk are cataloged and periodically reaffirmed.

Third party risk reporting and monitoring is most robust. Stakeholders receive regular reports of third and fourth party risk. Changes that may affect third party risk are reported from wherever they originate across the organization, as are reports to monitor all approved third party risk-related exceptions. Third party risk information is delivered in a variety of ways, including dashboards, push technology, on demand, and ad hoc requests. In each case, stakeholders can dynamically drill into reports to traverse all interrelated records to understand the business context and drivers of risk. The second line of defense can easily configure the organization's third party management information system to tailor taxonomy, assessment methodology, workflow and reporting to align with the unique requirements of the organization and make modifications as the organization grows.

MATURITY MODEL CROSSOVER

Third party governance is an extremely critical part of an overall operational risk management program. For organizations that rely heavily on external parties for products and services risks introduced by external parties can materially impact their overall risk profile.

IT security is dependent on third party security where access to data and/or systems is provided to those parties. Therefore, third party governance can have a significant impact on IT security risk management processes. Additionally, nearly all third party relationships have a role in business operations, which makes third party resilience an important consideration within a holistic business continuity management program. Finally, third parties can introduce significance to regulatory compliance risk to the same extent as if the organization was directly processing affected transactions. Regulatory and corporate compliance management programs must factor in compliance of external parties when determining and managing regulatory compliance.

CONCLUSION

Organizations must mature their third party governance to exploit opportunities.

Companies in the Siloed stage are in the primary stage, addressing individual risks at third parties within a stovepipe strategy. The strategy relies on the individual domains, such as IT, compliance and the business, managing their own set of third party risks driven by snapshot priorities. Within this Siloed stage, there are duplicate efforts, variation in third party risk management processes, and one-off remediation without broadly applied root cause analysis and remediation.

In order to move from the Siloed stage to the Managed stage, organizations Transition through projects that catalog and organize asset information and formalize third party practices. Companies in the Managed stage have established common processes to onboard, manage and monitor third party risks so that individual silos can share information and compile an organized view of inherited risks. As this integration improves, the organization can start getting ahead of the curve on major risks issues involving third parties. The organization has common data and analytical capabilities, effective risk assessment processes, and efficient methods to measure, monitor and report on risk and performance of external entities.

To reach the Advantaged stage, risk processes Transform by focusing on understanding the business context and drivers of third party risk to rationalize controls and strategies, harmonizing across business requirements and reducing administrative overhead and costs. The organization can now manage the full risk lifecycle as it applies to third parties because risk identification, assessment, decision, treatment and monitoring processes for risk are well established and can keep pace with the business. This allows executives to make risk-based decisions to shape the role and use of third parties within business strategies and ensure the organization is prepared for any emerging risk or events.

Organizations in the Advantaged stage are ready to realize the competitive advantage of harnessing risk, such as beating competitors to market, launching new products and services with calculated efficiencies, and avoiding major issues that affect reputation and the bottom line. Risk and business functions in this final phase speak a common language and have built a culture that can identify and respond to emerging business requirements ahead of the curve using common taxonomies, common approaches and well-oiled decision making processes.

ABOUT THE RSA ARCHER MATURITY MODEL SERIES

RSA Archer's vision is to help organizations transform compliance, manage risk and exploit opportunity with Risk Intelligence made possible via an integrated, coordinated GRC program. The RSA Archer Maturity Model white paper series outlines multiple segments of risk management that organizations must address to transform their GRC programs.

ABOUT RSA

RSA's Intelligence Driven Security solutions help organizations reduce the risks of operating in a digital world. Through visibility, analysis, and action, RSA solutions give customers the ability to detect, investigate and respond to advanced threats; confirm and manage identities; and ultimately, prevent IP theft, fraud and cybercrime. For more information on RSA, please visit rsa.com.

Dell Inc. or its subsidiaries believe the information in this document is accurate as of its publication date. The information is subject to change without notice.