MATURITY MODEL SNAPSHOT

THIRD PARTY GOVERNANCE
You hear it every flu season: Shaking hands with someone means shaking hands with every person that person has shaken hands with. It’s not a bad reminder of the risks of working with third parties: As your exposure to other businesses grows, so does your risk exposure. And it’s not just from third-party vendors; it’s from their vendors, too. How can you possibly track all those relationships to manage your risk?

You won’t get far trying to separately monitor every vendor; no organization has the resources for that. What you need is a clear, consistent view of third-party engagement across the enterprise, and a way to automate and streamline oversight. That’s the most effective context for managing third-party risk.

You can’t avoid dealing with third parties in business any more than you can avoid shaking hands with everyone at the company holiday party. But you can definitely take steps toward reducing risk.

**CAPABILITIES: WHAT IT TAKES TO MATURE THIRD-PARTY MANAGEMENT**

Third-party governance today requires automating and streamlining oversight to:

- Meet regulatory obligations associated with third-party relationships
- Engage stakeholders who are affected by third-party risks
- Standardize processes across the organization to quickly prioritize risks
- Provide a comprehensive view of risk to the executive team

RSA Archer Third Party Governance provides key capabilities to:

*Establish the scope and context for third-party management* by gathering information to understand exactly how the organization relies on third parties.

*Identify and assess third-party risk and performance* and capture changes to relationships that may alter risk profiles.

*Proactively evaluate risk* with efficient methods of assessing risk before onboarding new third parties.

*Monitor third-party risk profiles* and provide accurate and timely reports to stakeholders.

**STAGE BY STAGE: MAPPING THE MATURITY JOURNEY**

RSA Archer Maturity Models guide organizations through the journey from baseline risk management to optimized processes that balance opportunities and risks. There are five stages along the way:
THE SILOED STAGE: MASTERING THE BASICS
Organizations at this stage are preparing to evolve existing approaches to third-party management.

- Multiple records of third-party relationships are maintained by different departments, with no one system of record to tie together the information.
- Discussions are just beginning as to what makes for a high-risk third party and what controls should be in place.

THE TRANSITION STAGE: STABILIZING AND STRENGTHENING
Moving from Siloed to Managed, there’s a more holistic view of third-party risk across the organization.

- Third-party products and services are beginning to be mapped together with IT systems and organizational structures.
- The organization agrees on a consistent method for assessing third-party risk.
- It’s possible to generate a list of key third parties, but with little business context.

THE MANAGED STAGE: STANDING FIRM
The view of third-party risk across the organization becomes more focused and actionable.

- Third-party relationships have been centrally documented and mapped to business units.
- Risk assessments of third-party engagements are based on formal processes.
- Stakeholders regularly receive a list of risks and controls that clearly demonstrates the relationship between their level of risk and their risk tolerance.

THE TRANSFORM STAGE: ASSERTING CONTROL
There’s a greater understanding of the business context of third-party relationships.

- Business objectives and strategies related to third-party management are clearly documented.
- Decisions to proceed with third-party engagements are enforced through technology.
- Monitoring provides early warning signs of changes in risk performance of third parties.
THE ADVANTAGED STAGE: RIDING THE WAVE
Third-party governance is optimized for effective risk management.
• Third-party risk assessment results are as automated as possible and practical.
• Fourth-party risk is evaluated when making risk decisions about third parties.
• Third-party risk monitoring and reporting are most robust, including
dashboards, push technology, on-demand notifications and ad hoc requests.

Organizations ultimately realize the competitive advantages of harnessing risk: getting to market first, launching new products with calculated efficiency, and avoiding major issues that could wreck reputations and ruin bottom lines.

For more detailed information about the RSA Archer Maturity Model for Third Party Governance, visit www.rsa.com/en-us/resources.

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 series outlines the segments of risk management that organizations must address to transform GRC.

ABOUT RSA
RSA offers Business-Driven Security™ solutions that uniquely link business context with security incidents to help organizations manage risk and protect what matters most. RSA solutions are designed to effectively detect and respond to advanced attacks; manage user identities and access; and reduce business risk, fraud and cybercrime. RSA protects millions of users around the world and helps more than 90% of the Fortune 500 companies thrive in an uncertain, high risk world. For more information, visit rsa.com.