RSA

RSA RISK FRAMEWORK FOR MULTI-CLOUD TRANSFORMATION

HELPS ORGANIZATIONS MAINTAIN CONTROL OF RISK WHEN MOVING TO A MULTI-CLOUD ENVIRONMENT

As innovation drives today's companies to new business models and strategies that increase their market success, they increasingly are looking to cloud-based technology solutions to drive agility, speed to market and access to new enabling technologies that previously eluded them. The compelling cloud business model that leverages corporate OPEX resources, while quickly utilizing existing and affordable vendor resources, creates a compelling business case that can increase time to value and keep competitors at bay. The significant value that cloud providers bring to the general business strategy has raised awareness from the office of the CIO to the entire C-suite. In many organizations, cloud transformation is no longer simply an IT directive but a corporate business strategy, the success of which is measured by the board of directors.

Cloud transformation strategies are pervasive in most organizations today, but few fully understand the complexities of secure adoption and business risk mitigation. As companies speed their adoption of new cloud technologies to meet the demand for increased agility, it remains imperative that they create the associated enabling security measures simultaneously. Cloud transformation provides a promising means of accelerating business strategy but must be accomplished while addressing the complexities of the emerging security challenges it presents.

As companies leverage the cloud, they must maintain ongoing processes and tools that assess and manage cloud-based transformation in the areas of: 1) ecosystem alignment; 2) governance policies, processes and tools; 3) identity and access management; and 4) compliance management.

ECOSYSTEM	GOVERNANCE	IDENTITY	COMPLIANCE
OPERATIONAL EXCELLENCE			
Responsibilities defined between company and cloud provider Cloud services aligned with business goals Processes, procedures, tools defined and integrated KPIs defined with provider	Legal contract review and signoff on all service agreements Responsibilities defined with cloud provider for cyber incident management Mature communications plans and procedures	Fully automated and tested identity management backed by sound access policies All assets authenticate to least required levels leveraging advanced technologies Machine learning-based authentication based on behavioral analytics	Cloud provider fully complies with enterprise security standards Appropriate industry regulations, audits, controls and data control standards Leverages key industry-leading frameworks
FOUNDATIONAL EFFECTIVENESS			
Roles and responsibilities not fully defined between company and cloud provider Cloud services somewhat aligned with business goals and objectives Processes, procedures, tools defined and integrated KPIs defined with provider	Legal contracting somewhat mature Governance processes established based on policy, processes and tools; Ongoing measurement against KPIs Some corporate governance alignment with cloud provider	Some automation and identity management, with foundational processes All assets authenticate to somewhat appropriate levels	Some compliance processes, procedures, tools; Controls that ensure cloud provider adherence to existing corporate standards
BASIC EFFECTIVENESS			
Basic processes and tools, minimally integrated with provider, ad hoc	Basic governance processes and tools, some measurement but ad hoc	Basic roles defined for identity management, basic processes	Basic adherence to controls as specified by enterprise

For each of these areas, RSA will apply its proprietary Cyber Maturity Quantification Tool, which produces a profile of an enterprise's maturity in the management and transformation requirements for moving to a multi-cloud environment, as well as an aspirational profile (long-term goal of multi-cloud maturity status). The comparison between current and aspirational states produces a gap analysis that can help organizations prioritize areas for improvement.

As with all RSA Risk Maturity 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 senior executives.

The RSA Cyber Multi-cloud Maturity Assessment provides the following:

- Interviews and documentation with key business stakeholders to deeply understand business goals, objectives, risk tolerance and existing risk posture
- Administration of the RSA proprietary Cyber Maturity Quantification Tool to baseline risk maturity and readiness for multi-cloud transformation
- Development of a gap analysis and roadmap that can be utilized to close existing gaps and move to a desired level of cyber risk-management maturity

ABOUT RSA GLOBAL SERVICES

The RSA Global Services team of 650 cybersecurity business advisory and technical consultants operates in more than 100 countries and earned the "Strong Performer" rating in the Forrester Wave™ for Digital Forensics and Incident Response Service Providers.[1] 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 advisory and security skills and broad risk-management knowledge to help the organization assess and improve its multi-cloud transformation 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 maturity assessment in the areas of cyber incident management, third-party management, dynamic workforce management and multi-cloud management.
- 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.

ABOUT RSA

RSA® Business-Driven Security™ solutions provide organizations with a unified approach to managing digital risk that hinges on integrated visibility, automated insights and coordinated actions. With solutions for rapid detection and response, user access control, consumer fraud protection, and integrated risk management, RSA customers can thrive and continuously adapt to transformational change. For more information, visit rsa.com.

[1] The Forrester Wave™: Digital Forensics and Incident Response Service Providers, Q3 2017

©2019 Dell Inc. or its subsidiaries. All rights reserved. RSA and the RSA logo, are registered trademarks or trademarks of Dell Inc. or its subsidiaries in the United States and other countries. All other rademarks are the property of their respective owners. RSA believes the information in this document is accurate. The information is subject to change without notice. 02/19, Data Sheet, H17618 W215706.