RSA RISK FRAMEWORK FOR MULTI-CLOUD RISK: MANAGING RISK IN A VIRTUALIZED WORLD
INTRODUCTION

Digital Transformation is a journey underway in organizations across the globe. Defined as an organization's rapid adoption of technology and increased integration of business processes, Digital Transformation creates opportunities to gain strategic efficiencies and capabilities, by providing a technology model that improves continuously and is guided by data. The outcome is smart, actionable insights and the ability to act on those insights faster than the competition, which enables the delivery of better, more innovative products and services.

One important element of Digital Transformation is the shifting of workloads and data to cloud and virtualized infrastructures. This generational change has unleashed a host of benefits in both cost and capability. The speed at which new digital initiatives can be launched, and the ease with which they can be managed—often without IT involvement—has changed the nature of IT forever.

But this transformation is not completely without cost. Using a cloud does not relieve an organization of its obligations and policies. In many regards, cloud computing raises more risks and offers fewer security tools than traditional IT infrastructure. These properties raise concerns that must be addressed with a proactive cloud maturity program.

For example, cloud solutions can introduce blind spots in an organization's threat monitoring program. Virtualized and containerized applications can be provisioned outside of normal IT processes, often by non-IT personnel in line-of-business roles. Different clouds and applications rely on different identity and access systems and may be incompatible with enterprise systems and standards. And many of the same risks of other third-party relationships apply as well: privacy, resiliency, performance and security (both physical and technical) must be considered.

Thus, the benefits received from cloud computing must be balanced against the risks assumed:

<table>
<thead>
<tr>
<th>BENEFITS</th>
<th>RISKS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cost—Opex vs.Capex</td>
<td>Cyber threat exposure</td>
</tr>
<tr>
<td>Speed—Fast provisioning</td>
<td>Compliance with mandates and policies</td>
</tr>
<tr>
<td>Available applications—LOB and IT</td>
<td>Access control</td>
</tr>
<tr>
<td>Reliability—SLAs</td>
<td>Data security and privacy</td>
</tr>
<tr>
<td>Manageability</td>
<td>Resiliency</td>
</tr>
</tbody>
</table>

Like all risks, cloud risk is not binary—you can’t eliminate it completely, or at least not without forsaking all the benefits that cloud computing delivers. The task is then to identify, mitigate and continuously manage cloud risks, and continuously improve and maintain the maturity of your cloud risk program.
To address this need, RSA has created the RSA Risk Framework for Multi-Cloud Risk. Like other RSA Risk Frameworks, it’s based on a maturity model that helps customers fully assess and effectively improve their capabilities. It provides a lens to analyze the full range of cloud risk requirements, using detailed questions and applying expert analysis.

It’s based on established and understood industry risk frameworks, including ISO 31000 and NIST SP 800-161, as well as cybersecurity frameworks, including NIST Cybersecurity Framework (CSF) 1.1 and NIST SP 800-61 Rev. 2, Computer Security Incident Handling Guide (CSRC). However, the RSA Multi-Cloud Risk Framework goes beyond the broad standards to leverage RSA’s deep experience (including industry-specific experience) in helping customers address and manage multi-cloud-related risks of all types.

**Figure 1: RSA Multi-Cloud Risk Framework (simplified)**

### CLOUD RISK CHALLENGES

The fundamental challenge with cloud risk is that, by definition, it involves entities over which you exercise no direct control other than by contract. But you still have the requirement to proactively identify, mitigate and manage those inherited risks over time.

In fact, bad outcomes from cloud risks are in the headlines daily. In 2018, Tesla Motors’ Amazon cloud account was hacked to mine cryptocurrency. ¹ And Google, Amazon and Microsoft (both Office 365 and Azure) were among cloud providers suffering outages in 2018.²

---


Simply put, as businesses use more cloud 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 cloud performance becomes increasingly important to ensure that the quality of products and services delivered continue to meet required standards.

There are three primary drivers of risk, which RSA calls the “3 M’s”: Modernization (Digital Transformation), Mandates (such as GDPR and other privacy laws) and Malice (skilled and well-resourced attackers). Cloud risk is impacted by all three.

Organizations are more frequently using cloud suppliers and often multiple cloud suppliers. The reasons vary, but even companies that standardize on a single vendor find themselves dealing with multiple clouds as a consequence of partner or vendor arrangements. With so many relationships to track, the complexity of cloud governance can be difficult to understand and manage. Many organizations struggle to maintain the staff or resources to cope with this increased complexity.

Often, application and cloud management are spread across different teams within the organization. Cloud risks are not identified, assessed, treated and monitored consistently across all lines of business. 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 cloud risk and performance. Without a consistent enterprise view of cloud risks, the executive team does not have a clear enough picture of risk to make well-informed business decisions about which clouds and application vendors they should do business with, or which ones need to be carefully managed to prevent unwanted surprises from popping up.

THE RSA RISK FRAMEWORK FOR MULTI-CLOUD RISK

The RSA Risk Framework for Multi-Cloud Risk is a professional services offering from RSA Risk & Cybersecurity Advisory Practice (RCAP). Like all RSA Risk Frameworks, this services engagement delivers a business-centric model of consultancy that addresses a specific, major problem facing boards of directors today, including cyber incident risk and third-party risk, as well as risks from the dynamic workforce and multi-cloud environments.
RSA Advisors bring the tools and experience to help organizations assess their current readiness for managing a risk, and to implement a customized strategy for rapid and continual improvement.

Figure 2: RSA Professional Services Overview

Utilizing the RSA Risk Framework for Multi-Cloud Risk, RSA Advisors help organizations advance programs and processes to clearly identify, effectively mitigate and continuously manage cloud risk. This process targets the difficult but critical task of assessing and managing the risks associated with the full range of cloud suppliers with whom your organization has business and/or technical relationships.

These risks grow commensurately with the Digital Transformation and globalization that drives an increasingly interconnected world. Even the best-run organizations face business impacts arising from cloud failures that are outside their control, including regulatory compliance violations, data breaches, fraud, business interruption and reputational damage.

As with all RSA Risk Frameworks, the Multi-Cloud Risk Practice helps assess a company’s current readiness for managing this risk, with an approach that crosses an organization’s traditional functional boundaries, using a maturity model that supports the perspective of the CEO and board members.

The RSA Multi-Cloud Risk Assessment provides the following:

- Interviews with key business stakeholders to deeply understand the business’s goals and objectives relating to cloud deployments
- Gap analysis between current state program posture and desired cloud risk program posture, including comparison to industry best practices
- Identification of types of risks to mitigate and continuously manage, as well as processes to track cloud controls, certifications and risk-management processes
- Administration of the RSA proprietary Multi-Cloud Risk Management Program Quantification Model to baseline current risks arising from potential outcomes due to failures of cloud suppliers
• Evaluation of strengths and weaknesses of cloud risk-management processes as related to customer industry, business goals and risk tolerance

• Development of a roadmap that can be utilized to move to a desired level of cloud risk-management program maturity with time to value as a driver in the roadmap

• Readout of results to stakeholders

At the conclusion of the RSA Multi-Cloud Risk advisory engagement, clients should have a clear understanding of risk-management maturity across the relevant categories and demonstrate the ability to identify, mitigate and manage risk at the highest level of effectiveness. Additionally, clients should have in place a strategic roadmap to both improve maturity in key areas and to sustain capabilities already in place, even in the face of evolving or increasing risks.

In many organizations, RSA can apply its Multi-Cloud Risk Framework and begin making demonstrable impact in 4 to 12 weeks. A typical assessment and gap analysis with interviews and presentation of final deliverable requires a team of two to three RSA Professional Services Advisors, and may vary depending on the complexity and size of the environment as well as the amount of interviews/surveys required. The model presumes 10 to 12 interviews plus an online assessment component.

HOW IT WORKS

Different representations of the RSA Risk Framework for Multi-Cloud Risk highlight different aspects of the model. Figure 2 shows the leading indicators of maturity across four main areas of cloud risk: Ecosystem, Governance, Identity, and Compliance. A detailed scoring system behind these categories and ratings allows organizations to assess maturity for every area and baseline an initial score based on the company’s risk tolerance. This tally can then be used as a reference point from which to prioritize investments, adjust strategy and take other actions that advance cloud risk management.
investments, adjust strategy and take other actions that advance third-party risk management.

![Figure 3: RSA Third Party Risk Framework Categories](image)

- **Ecosystem**—The alignment of business goals/objectives with external information systems, hardware, software and all other products and services delivered by third parties
- **Governance**—The ongoing measurement of adherence to defined scope, accountabilities and service level agreements as specified in cloud contracts and legal agreements
- **Identity**—The management of identity and access (e.g., single-factor, multi-factor, identification) across cloud users, devices and other assets
- **Compliance**—The confirmation of cloud supplier compliance with enterprise security standards, appropriate industry regulations, audits, controls and data control standards, as well as key industry frameworks

Organizations at the most mature level achieve Operational Excellence optimizing cloud security and minimizing business risk. They do this by coordinating and integrating IT and business risk functions across the entire cloud risk-management lifecycle. Other characteristics of maturity include automation of key processes, advanced analysis capabilities and continuous improvement of the incident-management lifecycle.

The RSA Multi-Cloud Risk Framework engagement assesses the types of capabilities that exist at each level of the model. In many cases, maturity progresses from manual processes to siloed digital processes to highly automated, integrated processes. Organizations at intermediate levels of maturity tend to rely on spreadsheets or online tools, coupled with nonintegrated point solutions and open-source or free tools. The problem with this approach is that it rarely provides a holistic view of the risk environment and typically yields a slow and incomplete response. Lacking the insight, visibility and playbooks capable within today's cloud risk programs
puts organizations at a strategic disadvantage, making it more likely that a risk will turn into a problem and that the problem will have a substantial negative impact.

HOW RSA SOLUTIONS MAP TO THE RSA RISK FRAMEWORK FOR MULTI-CLOUD RISK

RSA provides a rich portfolio of products and professional services that enable organizations to unify disparate IT security and business risk functions, advance their maturity model and reduce risk. As shown in Figure 4, the RSA Risk and Cybersecurity Advisory Practice and RSA product suites address every area of mature cloud risk management, across Ecosystem, Governance, Identity and Compliance.

**RSA** Risk and Cybersecurity Advisory Practice (RCAP) is the umbrella practice for the critical components of Digital Risk Management, and it helps customers implement solutions that protect against risk, ensure compliance and accelerate business objectives. Within RCAP are:

- **RSA Risk Management Practice** helps organizations advance their capability for continuous risk improvement and helps ensure that risk programs are well-coordinated and aligned with identified business tolerance levels when it comes to reducing cloud risk.

- **RSA Advanced Cyber Defense (ACD) and RSA Incident Response (IR)** help organizations design and deploy effective cyber defense systems and respond to attacks, respectively. Industry expertise has been earned through thousands of proactive and reactive engagements across the globe.
• **RSA Identity & Assurance Practice** helps organizations resolve the two big challenges related to cloud access to systems. Authentication is the process of continuously validating the identity of a person or resource, while identity governance ensures that access is restricted only to what should be available to any specific identity.

**RSA Product Solutions** are industry-leading software tools that empower organizations to address the critical domains of integrated risk management, threat detection and response, and identity and access management. These include:

• **RSA Archer® Suite**, which delivers integrated risk management (IRM) to increase visibility and insight into true business risks and empowers organizations to make better decisions throughout the risk-management lifecycle

• **RSA NetWitness® Platform**, which is an advanced security information and event management (SIEM) and threat defense solution that aligns business risk context to security risks so that security teams can rapidly detect and understand the full scope of a compromise and its associated risks

• **RSA SecurID® Suite**, which facilitates business by allowing legitimate users to quickly and easily identify themselves, while mitigating the risk of unauthorized users gaining access to the network and other resources

**CONCLUSION**

The RSA Risk Framework for Multi-Cloud Risk provides a maturity model for developing a mature, business-driven strategy that is informed by—and accommodates—both IT and business risk functions across the cloud risk domain. Organizations can apply products and solutions from the RSA portfolio to fully operationalize the model at the highest levels of maturity.

In doing so, they can reduce risks to revenue/mission, reputation and compliance while safely pursuing opportunities that allow them to thrive.

To find out more about using the Risk Frameworks to assess and optimize your organization's risk-management strategy, please visit rsa.com/risk-frameworks.

**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.