GUIDE TO MANAGING CLOUD TRANSFORMATION RISK
Realize the Benefits. Mitigate the Risks.
Adoption of cloud computing is at the heart of most organizations’ digital transformation strategies. Organizations today increasingly rely on an expanding array of public, private and hybrid cloud services to move faster and compete more effectively in the market.

But on the way to achieving these benefits, organizations face an array of new security challenges: cloud adoption obscures security teams’ visibility into users and applications; leads to an endless stream of technology changes that security teams must stay on top of; and complicates managing access for the increasingly diverse ecosystem of employees and third parties who need to use these services.
CHECKLIST FOR CLOUD SECURITY

Addressing the security challenges associated with cloud transformation requires a comprehensive security and risk management approach that includes the following activities:

- Extend visibility into users, entities and data across public, private, hybrid and multi-cloud environments.
- Manage cloud access for a dynamic workforce and an expanding third-party ecosystem.
- Authenticate cloud users with a high-level of assurance and minimal friction.
- Govern cloud service provider relationships across the entire third-party management lifecycle.
- Prioritize remediation actions based on the cloud risks that pose the biggest impact to the business.
- Regularly adapt cloud policies and controls based on user engagement with these services and changes in your business.

Knowing how your security and risk management capabilities measure up to industry standards is critical to determining which investments you may need to make and to ensuring the risks associated with your organization's cloud transformation don't undermine the rewards. To assess the maturity of your capabilities, evaluate cloud transformation risk across four key domains: ecosystem, governance, identity and compliance. On the pages that follow, you'll find specific recommendations for each of those domains.

Figure 1: The Importance of Benchmarking

Evaluating your organization's capabilities for securing your cloud transformation against industry standards is critical to ensuring your organization is prepared for these risks.

Source: RSA
An organization’s cloud ecosystem refers to the hardware, software, cloud providers, consultants, integrators and other third-party partners that work together to form an organization’s extended cloud infrastructure.

As organizations move more workloads to the cloud, they grow increasingly dependent on third-party technologies and services to run their businesses. This, of course, increases complexity and risk. But the following actions can help you mitigate ecosystem risks related to your cloud transformation:

- Maintain a record of all the applications and services supplied by cloud providers.
- Classify and prioritize the criticality of both the data “handled” and the services provided by each cloud partner.
- Understand third-, fourth- and nth-party cloud relationships and their importance to your business.
- Define the resiliency requirements and assess the corresponding capabilities of cloud providers that support the delivery of critical services.
- Identify security vulnerabilities in cloud-based software and services and collect cyber threat intelligence on cloud-based attacks.
- Assess the potential business impact of service interruptions or outages for each cloud provider.

86% of organizations describe their cloud strategy as multi-cloud¹
When it comes to cloud security, cloud service providers and their customers frequently have conflicting ideas on who’s responsible for what. For example, one common misconception among organizations procuring cloud services is that responsibility for securing their data shifts completely to the cloud provider. In fact, it does not.

Generally, cloud service providers are responsible for the security “of” the cloud—that is, they’re responsible for the hardware, software and other infrastructure required to provide their services. Cloud customers, on the other hand, are responsible for security “in” the cloud—that is, the actual information stored or processed on the infrastructure used to deliver the cloud provider’s service. They’re also responsible for securing the devices used to access the cloud, for authenticating users, and for managing access rights and entitlements across the user lifecycle.

The following governance controls can help your organization manage security responsibilities with your cloud providers:

- Define a comprehensive set of cybersecurity-related policies and procedures for third-party cloud service providers to follow.
- Establish a process for capturing and managing cloud provider relationships, their importance to the business and potential risks.
- Evaluate your cloud providers’ controls for data retention and disposition and ensure they align with your organization’s policies.
- Assess your cloud providers’ capabilities for monitoring their physical environments, providing visibility into user activity, and integrity-checking hardware, software and data.
- Create a RACI (responsible, accountable, communicated, informed) model for each cloud provider to clarify who is ultimately responsible for different security issues, including declared security incidents.
Passwords and static identity and access management rules don’t provide sufficient defense against attacks that take advantage of cloud vulnerabilities and the myriad of employees and third-parties who need access to cloud applications at any time, from any device. Therefore, secure access to cloud applications requires a high level of assurance that users are who they say they are and that their access is appropriate given their responsibilities and doesn’t put the business in harm’s way.

While managing access has historically revolved around traditional identity and access management tools, today’s new cloud realities require organizations to go well beyond those basic controls to:

- Govern joiner/mover/leaver access rights for employees and third parties and manage credentials and entitlements for authorized devices and processes.
- Apply the principles of least privilege and segregation of duties when granting cloud access permissions and authorizations.
- Correlate data across multi-cloud environments to understand the potential risks associated with authenticating users and assigning rights.
- Authenticate cloud users, devices and other assets commensurate with risk.
- Continuously monitor user behavior and activity related to connections, devices and software.
When it comes to regulatory compliance, organizations struggle to understand what types of data they have in the cloud and where that data resides.

With traditional on-premises systems, IT can literally show auditors where data is stored. IT can also relatively easily restrict or segment data based on attributes like geography, group and data type.

In contrast, cloud computing relies on the ability to host data in multiple locations. Multi-cloud environments complicate data privacy and compliance even more because data simultaneously resides in multiple cloud instances, including public and private clouds, each of which may have different business purposes and may be bound by different contractual relationships. Unless organizations opt for cloud services that lock data into specific regions, they are essentially handing data over to a cloud service provider to store as they see fit.

Implementing the following compliance controls can help your organization meet a variety of internal and external regulatory requirements:

**Classify sensitive data, identify where in the cloud it lives, and assess the potential compliance implications of data location, collection and use.**

**Continuously monitor and assess cloud data usage to ensure adherence to regulatory and corporate privacy standards.**

**Regularly inform employees and customers about cloud data collection practices and the specific data being collected.**

**Evaluate cloud providers’ controls related to audit/log records and how they are documented, implemented and reviewed in accordance with applicable regulations.**

**Train employees and third parties on information security and data privacy regulations; make sure they understand their responsibilities for keeping data safe, including codes of conduct for handling data.**

---

**COMPLIANCE**

A major European airline faces a record $230 million fine after personal details of roughly 500,000 customers were exposed to cybercriminals.⁴
RISK FRAMEWORK

Mitigating the risks associated with moving workloads to the cloud starts with a comprehensive assessment of an organization’s ability to identify, protect, detect and respond to cloud-related risks. The RSA Cloud Risk Framework does just that.

Based on industry-standard guidelines (including the NIST Cyber Security Framework and ISO standards for cybersecurity and risk management), the RSA Cloud Risk Framework is an advisory services offering that assesses the maturity of an organization’s cloud security and risk management capabilities across four areas: ecosystem, governance, identity and compliance. Organizations can use the results of this in-depth assessment to identify gaps, prioritize investments, and adjust their cloud risk management strategies according to the changing needs of the business.
DIGITAL RISK IS EVERYONE’S BUSINESS
HELPING YOU MANAGE IT IS OURS

RSA offers business-driven security solutions that provide organizations with a unified approach to managing digital risk that hinges on integrated visibility, automated insights and coordinated actions. RSA solutions are designed to effectively detect and respond to advanced attacks; manage user access control; and reduce business risk, fraud and cybercrime. RSA protects millions of users around the world and helps more than 90 percent of the Fortune 500 companies thrive and continuously adapt to transformational change.

Find out how to thrive in a dynamic, high-risk digital world at rsa.com

1. Forrester Consulting, Multicloud Arises from Changing Cloud Priorities, July 2018
3. Oracle and KPMG Cloud Threat Report 2019
4. Charles Riley, “British Airways faces $230 million fine. It would be a record under Europe’s tough data privacy law.” CNN.com, July 8, 2019

© 2019 Dell Inc. or its subsidiaries. All Rights Reserved. RSA and the RSA logo are trademarks of Dell Inc. or its subsidiaries in the United States and other countries. All other trademarks are the property of their respective owners. RSA believes the information in this document is accurate. The information is subject to change without notice. Published in the USA, 8/19 eBook H17779 W270438