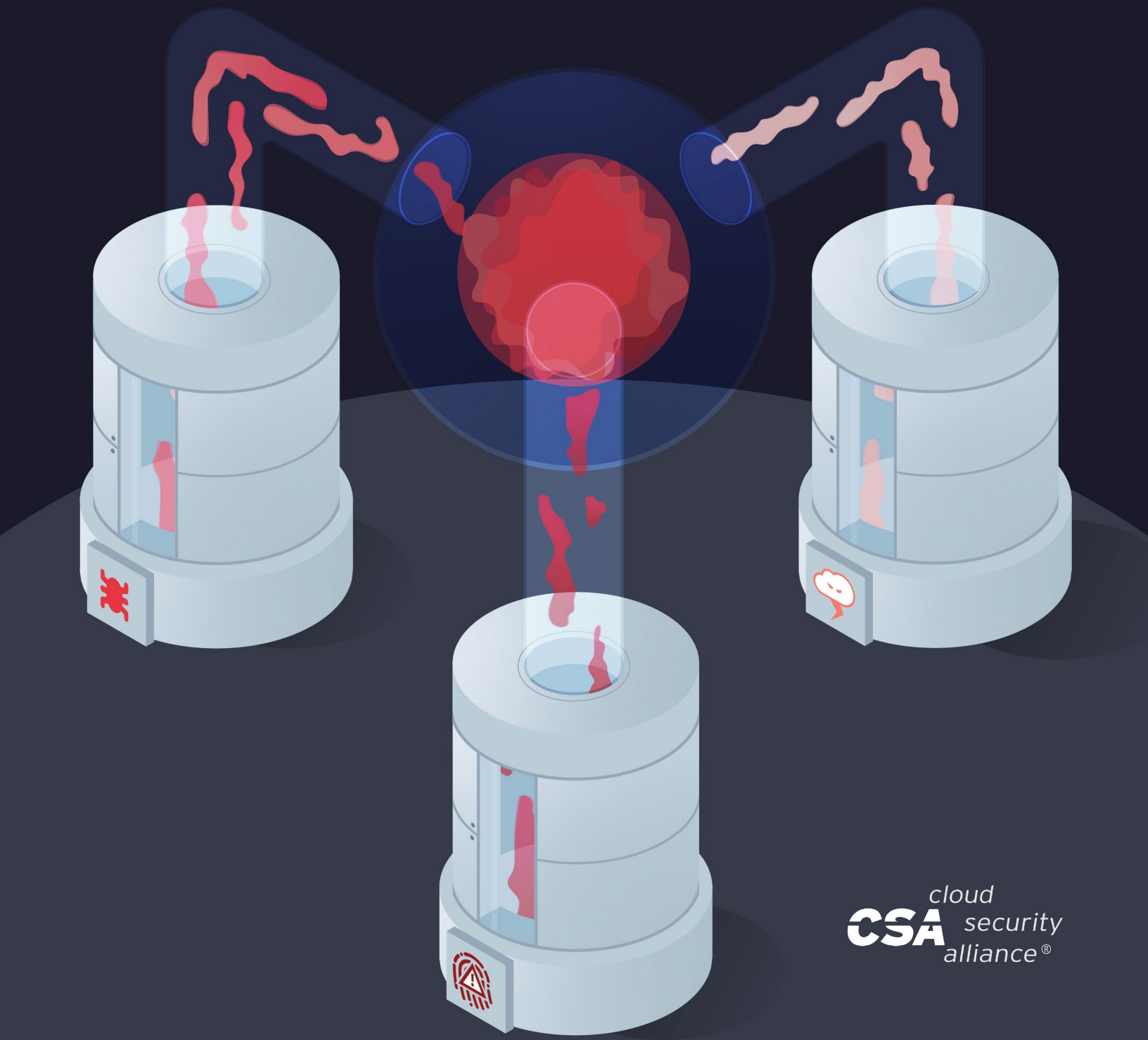
CSA's Perspective on Cloud Risk Management



cloud security alliance®

Acknowledgments

Authors:

Vince Campitelli
Daniele Catteddu
John Di Maria

Contributors:

Ryan Bergsma
Damir Savanovic

Reviewers:

Jon-Michael Brooks
Louis Marinos
Michael Roza
John Yeoh

CSA Staff:

AnnMarie Ulskey (Design)

Table of Contents

1. Introduction

Today, 10 years after the formation of the Cloud Security Alliance (CSA), cloud computing is a proven and globally accepted enterprise delivery and operational technology model. According to a January 2019 IDC report (1), the spending on Cloud IT infrastructure may have reached a tipping point in the third quarter of 2018 by surpassing traditional IT revenues with slightly more than a 50% market share.

Over the same time span, there have been increasing concerns regarding the privacy, security, and compliance challenges associated with this growing market segment. Most recently, there have been several breaches, data privacy, and compliance events associated with various cloud computing service providers that are threatening the goodwill and positive perceptions of the industry. By 2023, IDC expects that traditional non-cloud IT infrastructure will only represent 42.4% of total worldwide IT infrastructure spending (down from 51.9% in 2018).

The rapid growth in both scope and market share, combined with the inherent complexity of cloud computing, appears to be straining the capabilities of existing governance and risk management frameworks. In light of the dramatic growth and apparent onset of harmful events, similar to those hampering non-cloud technology environments, CSA developed this position paper to question the perceived effectiveness of current governance and maturity in the use of risk management frameworks applied to cloud computing.

As users and the uses of cloud computing evolve, so must the supporting governance models -- this includes the maturity of governance and risk management programs designed to review and evaluate the selection, adoption, and migration of traditional operations to Cloud Service Providers (CSPs). In addition, the digitalization of infrastructure, services, and applications fostered by cloud platforms are testing traditional governance and risk management frameworks. Further, as cloud computing platforms are extended to support enterprise-wide business strategies, compared to IT strategies, the executive suite and board of directors become stakeholders.

This prompted the Cloud Security Alliance's following questions:

- Are the risk management methodologies currently available adequate to manage risks in the cloud?
- Are organizations aware of the shared responsibility model introduced by cloud computing, and are the responsibilities appropriately reflected in the risk management processes and programs?
- Are organizations aware of the concepts and implications of indirect/loss of control imposed by cloud computing and the challenges they pose to the design of risk mitigation procedures and their validation?
- Are organizations sufficiently aware of the impact that cloud computing has on the propagation of their supply chains and the difficulty in evaluating and monitoring the consolidated residual risk of third/fourth parties?
- Are the current governance practices adequate to effectively identify, evaluate, and report the relevant cloud risks to relevant stakeholders?

The authors of this paper are fully aware that the answer to some of the proposed questions depends on the level of expertise, knowledge, and experience in the application of the risk management methodologies. Nevertheless, when it comes to using cloud computing technologies, we believe that these are general issues that deserve to be analyzed and investigated.

2. Background

Cloud has the potential to increase awareness that risk management has to be a top-level, enterprise-wide process rather than a siloed or departmental exercise.

According to the Global Association of Risk Professionals, risk management takes on many meanings depending on the industry or framework. Regardless of how it is defined, risk management to address cloud operations plays a vital role in all of an organization's processes and must be part of an overall enterprise business-improvement strategy. The International Organization on Standardization (ISO) has recognized the importance that risk plays and is re-working many of its management system standards to encourage "risk-based thinking," replacing the need for "preventive action" with "actions to address risks and opportunities." When it comes to the cloud, the risk management approach is the same that used on-premises. But when it comes to tactics and implementation, there can be significant differences between traditional and cloud-based IT.

3. Objectives and scope

The purpose of this position paper is to initiate a debate within the cloud and risk management communities on the suitability of existing methodologies and practices to effectively and efficiently assess, treat and mitigate, accept, communicate and monitor cybersecurity risks in the cloud.

We propose five questions that are representative of key elements that should stimulate the debate and support the identification of possible solutions.

The objective of the paper is not to provide definitive answers but rather to contribute food for thought.

3.1 Why should you read this paper?

Once effectively implemented, the organization's governance models will be in alignment with 21st-century business models and technology platforms. This change will meet the market and consumer expectations for safe products and services.

This position paper serves to provide an impartial look at risk by identifying and examining gaps introduced over the last 10 years by the rapid adoption of Cloud Computing. It also deals with how the underlying concepts of effective risk management, when carefully applied, can be integral in managing the broad enterprise risk introduced by cloud computing. Capitalizing on this knowledge and guidance, organizations can attain greater confidence in their cloud risk management programs.

An effective risk management program should be designed to address issues related to economic value, process improvement, compliance, information security, and privacy including:

- New operational security risks created by moving to the cloud
- Costs related to the failure to address cloud compliance
- Risks related to the cloud market growth (the bigger the market, the bigger the risk)
- Mitigation measures

New operational security risk created by moving to the cloud

The cloud brings with it unique risks related to data security, availability, storage, segregation, integrity, and recovery. We will discuss good risk management practices that play a critical role in helping to assure operational security and privacy by identifying all applicable areas of concern, status, and associated risks related to the cloud that previously may not have been addressed.

With the plethora of recent security breaches – both internal and external – instances of unlawful activities and misconduct remain a constant threat to the cloud and public trust.

Costs related to the failure to address cloud compliance

Regulatory compliance is a basic part of doing business. Non-compliance can be an expensive proposition; it diverts the organization's attention from normal operations, attracting scrutiny from regulators that can result in additional fines, repetitive audits, potential legal action, and reputational downturn. The more organized a company can be from an overall risk perspective, the more capital it has available to invest in improving processes and growth activities.

The bigger the market, the bigger the risk

The total size of the global CSP marketplace risk is a function of the depth, breadth, and maturity of the market. The market size of public cloud computing has grown from $58.6B[1] in 2008 to a projected volume of $266.4B in 2020. This growth supports additional investment in innovative new products, services, and market entrants. The impact of serving increasingly sophisticated customers in a market subject to regulatory oversight would tend to raise customer expectations. This places constant stress on the cloud providers to improve key performance indicators such as features and functionality, and security and compliance while lowering storage and processing costs. These represent more intangible risks not easily measured without historical benchmark data.

Mitigation suggestions

Cloud has proven to be one of the more complex technology ecosystems in our modern world. Cloud-specific risk mitigations and/or preventative techniques need to be established to reduce negative organizational impacts. These should be based on continuous assessments of an organization's inputs and outputs. Applying lessons learned and building an intelligent knowledge base, in conjunction with establishing detection techniques to uncover events when preventive

[1] https://www.statista.com/statistics/273818/global-revenue-generated-with-cloud-computing-since-2009/

measures fail or unmitigated risks are realized. The ongoing real-time integrated process of identifying, assessing, and responding to risk is effective risk management. An organization must be able to show they have implemented what the courts call "due diligence" and "standard of care" as part of an organization's governance structure. These techniques comprise best practices and confirm the existence and operation of an effective governance model.

4. Five key questions to explore

4.1 Are the existing risk management methodologies adequate to manage risks in the cloud?

There are numerous risk management frameworks developed over the last 30 years. While some are global in nature, others are related to various industries and can be somewhat specialized, including those related to information technology only.

Applying effective risk management concepts and protocols to the world of cloud computing requires a careful balance among:

- technology-specific risks created by the unique components of cloud computing platforms and technologies,
- business-related risks created by dependence on untrusted third parties, and
- technical and organizational risks introduced by the DevOps philosophy and automation.

The following considerations are fundamental to the creation, operation, and maintenance of cloud computing technologies during the adoption of an enterprise-wide risk management program.

The ascendancy of strategic enterprise risk: Cloud deployment models are being combined in new and unique ways to achieve entire organizational transformations that were not envisioned 10 years ago. Leading-edge businesses rely upon a mixed model of private, public, and hybrid cloud systems to drive organizational transformations, enabling them to compete in an evolving digital marketplace. Hence, the design of their cloud ecosystem becomes just as important as its operational performance. These changes need to be recognized by the risk management process since it can raise both the category and level of risk. At stake is the entire enterprise's ability to meet its strategic objectives, including the ability to survive in the marketplace.

The deployment of innovative and emerging technologies can be critical to organizational success. Over the last five years, the drivers of cloud adoption and consumption changed in ways that impact the inherent risk of the services being consumed. In the early years of cloud consumption, organizations sought key benefits including lower capital cost, reliability, scalability, sustainability, agile deployment, and 24/7 support. During the last 3-5 years, cloud adoption motives expanded dramatically in scope and purpose, focusing more on business enablement and transformation. This spawned a new set of consumption drivers, including:

- Big data solutions and machine learning
- Artificial intelligence

- Device proliferation and Internet of Things (IoT)
- Acceleration of new products and services

As the list of organizational drivers expands and diversifies, the complexity of assessing the individual risks and their cumulative impact on the organization increases at a growing rate. This, in turn, raises the demand for organizational resources and competencies devoted to the Enterprise Risk function, specifically in the organization's ability to manage and exploit the opportunities created by the relevant emerging technologies.

Introduction of new complexities: to create, operate, manage, measure and report upon performance in a cloud-based ecosystem, the organization's risk management system must accommodate a host of new complexities that have dramatically increased the scope and scale of the risk equation:

- Global footprint
- Supply chain expansion
- Device/infrastructure/data explosion
- Introduction of new business models
- Shared responsibilities over security controls/processes
- Diminished visibility of processes, assets, vulnerabilities, incidents
- Data risk is unknown/unmanaged
- Cloud configuration compliance will be an important concern for each CSP
- Continuous assurance and continuous compliance requirements
- Introduction of privacy regulations imposing stronger accountability

Impact on the IT function: it is axiomatic that the larger the financial commitment in cloud computing, the greater the impact is on the IT organization. Many of these impacts have a direct effect on the technical/organizational requirements of the IT organization, including:

- Need for organization redesign
- Reassessment of data governance needs
- Relevant IT, security, and privacy policies
- Design and definition of cloud usage policies
- Skill/competency gaps
- Reassessment of tools/product effectiveness
- Security need for "cloud native" tools
- Reduction of IT staff
- Required continuous monitoring
- Increased third-parties management effort

4.2 Is the shared responsibility model appropriately reflected in the risk management processes and programs?

The achievement of security and compliance in the cloud computing model introduced the concept of "shared controls," known as the Shared Responsibility Model. With it, there is a distinction between

those controls that are the responsibility of the cloud service provider versus the responsibility of the cloud consumer. This reality of the cloud computing model exacerbates the traditional risk management consideration for third-party IT services. It is complicated by the factors of scale due to the automation of processes and procedures which might create issues of mistake propagation, as well as the risk of hidden interdependencies; visibility, due to the absence of evidence (required logs) to support control process operation, and performance; scope, due to the volume of cloud services and service providers in the supply chain; and continuous monitoring, due to the necessity of real-time, inline information consumption and production and alerts. Organizations now share risk identification, assessment, measurement, and control design with their CSP. These are non-trivial exercises and should only be performed by skilled and experienced practitioners. Additionally, consumers unwittingly accept risk when they utilize services without the ability to measure the effectiveness of a CSP's security and control practices. This risk is then owned by the business owner who is responsible for the services provided by the cloud service provider. Under these circumstances, it becomes most important that the organization's governance model appropriately consolidates and reports the magnitude of residual risk to the enterprise stakeholders and the Board.

4.3 Are companies aware of the implications of governance forced by the idea of indirect control?

The public cloud brought with it the idea of loss of direct control over IT service and security capabilities. While using public clouds, users cede direct control over a number of IT, security, and privacy-related features to the cloud service providers.

For instance, CSPs typically prohibit security scanning, penetration testing, and first-party audit by contract. Business continuity and/or disaster recovery testing is often not possible; customer security and privacy policies, including related standards and procedures such as hardening, may conflict with the service provider's efforts; access to key logs and visibility of alerts may be unattainable. Moreover, the key contracting feature of prescriptive SLAs may not be available or measured and reported transparently to the customer if available.

While some have described these issues as loss of governance, we perceive them as a driver for a new governance model over cloud service providers. No more direct access and testing over the physical infrastructure. No more direct information flow between the IT department and the upper management. No more direct auditing of the outsourcer. Rather, a new form of governance founded on an indirect flow of information. Data provided through SLAs, third-party audits, and compliance reports based upon laws and regulations. The effectiveness of this new model will be measured based on its ability to mitigate the unique risks introduced by cloud computing.

To contrast the risks generated by the loss of control, risk management approaches should reinforce the focus on the sources of information used to analyze and assess the cybersecurity risks. Additional emphasis should be given to the variety and accuracy of the SLAs offered, the evidence produced to support the results of third-party audits and certification, the quality and details of the logging services, and other data sources. With this loss of control, it is of paramount importance to reinforce the role of the internal audit function, establish an 'auditor mindset' and an accountability culture within the organization. These are very important issues and concerns in vetting the

effectiveness and quality of an organization's risk management program. The litmus test for the risk management function is the thoroughness of itsrisk identification, assessment, awareness, and measurement of the residual risk communicated to the business owner. This is where the exercise of sound business judgment is crucial in rendering the appropriate cloud selection decision. Selecting the wrong cloud provider, for the wrong reasons, may place the customer in an unjustified position, where risk mitigations are not available, and the risk is "accepted." This can be the risk manager's worst nightmare.

4.4 Is the cloud supply chain complexity factor sufficiently weighed into the risk management practices?

Previously discussed in this paper is the impact of the shared responsibility model on cloud risk management, a theme directly connected to the idea of supply chain management. Cloud security and privacy risk management face challenges related to the complexity of the supply chain. While a customer might have a primary contractual counterpart, for instance a Software as a Service (SaaS) provider, that service provider very often uses someone else's platform or infrastructure. The contractual relationship between the SaaS provider and their cloud usage is not transparent to the customer, creating a problem of information asymmetry.

Building on the concept of indirect control discussed in the previous paragraph, such a lack of visibility into the supply chain raises the simple question of how a cloud customer can perform a proper assessment of the security and privacy risks without having access to complete information -- a typical issue of accountability. Cloud customers are often accountable for security and privacy matters that they are not in a position to evaluate. The issue of supply chain processors and sub-processors came clearly under the spotlight, for instance, with the introduction of the General Data Protection Regulation (GDPR). The duty to protect personal data along the whole supply chain falls on data controllers such as the cloud customer.

A similar emphasis on the issue of accountability and supply chain management can be found in the European Banking Authority's (EBA) "Guidelines on Outsourcing Arrangements." As the guidelines of reference for European financial sector use of cloud computing, it states:

> "Where the outsourcing arrangement includes the possibility that the service provider sub-outsources critical or important functions to other service providers, institutions, and payment institutions should take into account:
>
> a. the risks associated with sub-outsourcing, including the additional risks that may arise if the sub-contractor is located in a different country from the service provider
> b. the risk that long and complex chains of sub-outsourcing reduce the ability of institutions or payment institutions to oversee the outsourced critical or important function and the ability of competent authorities to effectively supervise them."

Such monitoring for risk along the supply chain is not an impossible task, but certainly a resource-intensive one. Resources are the issue with companies often using hundreds, if not thousands, of cloud services, notably SaaS. Many of which have very few users making it economically inefficient to spend too much time and resources in assessing the risk related to them.

Financial inefficiency is not the only problem related to the cloud supply chain risk management. More substantial problems surround identifying responsibility versus accountability, and the lack of information we refer to earlier when analyzing the challenges related to shared responsibility and loss of direct control. Unfortunately, companies often assume that their main contractual counterparts have done their "homework" and performed a proper evaluation of the security and privacy measures implemented by their providers. Would you consider that a safe assumption and proper enforcement of their duty of care? Certainly not.

4.5 Are current practices adequate to effectively communicate risks to the members of the board?

As recent and historically high profile breaches have demonstrated, C-suite executives in many organizations appear to be aware of the threats and risks associated with large-scale data breaches, but lack preparation and a disciplined response when a negative event occurs.
Additionally, board members and senior leaders need to be better informed of the extensive supply chain risk introduced by the mass adoption of numerous cloud-based services. This can greatly expand the threats (both internal and external), as well as the impact of inadvertent mistakes and continuous attempts from nation-states searching for intellectual property. In a recent study (3) on the biggest cloud breaches of 2019, one of the world's leading technology research firms concluded that" ... Through 2025, 99% of cloud security failures will be the customer's fault ...."

Boards need to be better informed of the expanding risks associated with cloud computing and the many ancillary technologies introduced by cloud-based platforms. These risks need to be presented from a business perspective and not through the lens of technology.

Discussions and presentations delivered in overly technical terms can be confusing and distracting to a typical board executive. Boards are seeking knowledge and results that demonstrate that the C-suite executives possess the capability, skills, and leadership to create a strategic plan that wisely invests in innovative technologies, attains operational objectives, and adheres to the governance model and policies of the organization. In today's environment, this almost always includes a cybersecurity plan.

Traditionally, technology aspects of board communication and briefings are the responsibility of the Chief Technology Officer (CTO) and/or Chief Information Officer (CIO). Organizations heavily committed to cloud computing should ensure the entire executive team is well-versed in the business, operational, financial, legal, HR, compliance, security, and privacy impacts of cloud computing. This is especially important in industries or companies, where cloud technologies are the springboard for business or digital transformation.

5. Conclusion and Recommendations

Based upon the examination of the impact of cloud computing on the areas of governance, risk management, compliance, security, and privacy, where relevant, current risk management programs should, at a minimum, be re-examined. To ensure current risk practices are compatible with the current state of the organization's use of cloud computing technologies and platforms it is prudent to assess management's ability to understand and cope with many of the distinguishing characteristics of cloud computing:

Scale and Scope

Major considerations are the focus, scope, and capability of the organization's risk management program. When implemented at scale and pervasively across the enterprise, cloud computing can have a profound impact on the entire company. First, it is imperative that the scope of risk management includes the entire enterprise, including the entire supply chain, the interconnected systems of business partners, links to social media sites, and awareness of geopolitical activity that may be proactive or unwelcome. Moreover, the tendency in larger organizations is for much of the growth in cloud adoption and cloud service provider usage to materialize in the form of numerous Software as a Service (SaaS) providers. These providers typically avoid or evade appropriate risk management and/or due diligence assessments. These service providers are often referred to as Shadow Information Technology (IT) or shadow data services. These entities can present a major risk to the enterprise since by definition they are not identified or evaluated through the normal governance, policies and standards, and procedures and protocols established by the organization. Hence, it is most important that their identification, which in itself requires specialized network software, be established. Once identified, alternative procedures can be developed to complete the risk management and mitigation processes.

Vendor concentration risk

This risk may manifest itself in several different ways. The enterprise may decide to rely upon a few large-scale and global in scope Cloud Service Providers, who provide numerous services related to software services, infrastructure, and platforms. Without the ability to conduct and maintain sophisticated risk assessments and continuous monitoring, an outage at one of the major providers can threaten the operation of significant portions of the enterprise. Further, the traditional concepts of disaster recovery and business continuity may not be achievable. Even if they are, the ability to maintain an ongoing testing program may not be economically viable.

The strengths of the concentration strategy can turn into a significant operational dilemma if the organization, due to business prudence or regulatory mandates, has to maintain a viable exit strategy. This should be considered before establishing a major strategic relationship — in a worst-case scenario, such an arrangement could lead to the analogy of "too big to fail" in the global banking economy.

Resiliency replaces recovery

Traditional business risk assessments rely upon the concepts embedded in business and disaster recovery processes to ensure organizational continuity. The business complexities introduced by

large-scale adoption of cloud computing services warrant an enhanced approach to overall business survival and sustainability. The objective of cyber resilience is to maintain the entity's ability to deliver the intended outcome continuously at all times[2]. The concept also includes the entity's ability to restore regular delivery after adverse cyber events, as well as the ability to continuously change or modify these delivery mechanisms if needed in the face of new risks. While many of the underlying practices and procedures are understood and recognized as being vital to enterprise survival, the absence of a widely adopted and standardized framework to guide design, implementation, and operation does not currently exist. This is an area warranting additional research and development to foster greater adoption and widespread use.

Innovation drives technology, technology drives complexity

Traditional risk management methodologies have focused on identifying risks of adverse events based upon historical data, while the perceived benefits of business and digital transformation have driven the widespread adoption of cloud computing. Organizational success becomes dependent on the positive outcomes of deploying cloud-based technologies. This includes the emerging and explosive use of software-based products and services such as big data, artificial intelligence, and IoT, fostered by dramatic growth in intelligent devices. Moreover, the cadence of progress and success becomes a feature of business success and the benchmark of expectations. These innovations strain the risk management function to adjust their sights on meeting future requirements, increase cycle time to meet business expectations, enhance skill sets and technical competencies, and demonstrate thought leadership and effectiveness.

Shared responsibility model

One of the least understood, but most impactful changes to cloud risk management and governance is the concept of the "shared responsibility" model. While CSPs may employ similar definitions and implementation choices, the techniques and best practices utilized by each CSP may vary widely for establishing, operating, modifying, monitoring, and reporting on controls and configurations.

Awareness alone does not solve the accountability and responsibility requirements. Multi-cloud governance will require mastery of each CSP's configurations and settings. A major short-term challenge for cloud customers is the ability to validate the accuracy and integrity of CSP's configurations and the development of relevant software and tools capable of monitoring their integrity and performance. This was noted in the previous Gartner projection regarding the root cause of cloud security failures.

The desire for information and the auditor mindset

With the introduction of the idea of "indirect control" over IT and security capabilities, the approach to risk management has to evolve to ensure that the risk owners obtain proper information to manage risk. Companies shall demand more transparency concerning the security, privacy, and compliance posture of their cloud service providers. As an organization commences its journey to cloud computing, the risk management function must adjust its focus and protocols to identify those risk and control areas that are no longer under the direct control of the consuming organization. This

[2] https://corpgov.law.harvard.edu/2012/08/23/strategic-risk-management-a-primer-for-directors/

includes the new control and configuration features and options that are necessary to comprehend to optimize the services and capabilities provided by each cloud service provider. The combination of the decreased transparency and loss of direct control warrants:

- the definition of internal SLAs and KPIs that can be used to compare the service level objectives and service qualitative objectives offered by the cloud service providers.
- the replacement of periodic auditing and surveillance with "continuous auditing." This is a relatively new concept as a risk mitigant as it also obviates the reliability and limitation of the point-in-time assurance of the periodic third-party certifications and attestations.
- Change in the approach of internal IT and security and the evolution of the role of IT and security professionals. They will be required to develop auditing skills and apply an auditor mindset in their daily work.

Supply chain architecture and accountability program

The complexity of the cloud supply chain, the proliferation of CSPs (especially SaaS) and chronic lack of resources for performing accurate due diligence, and the need to enforce accountability within the IT service portfolio demands for the definition of "smart" and agile approach to third-party risk management.

Companies should look at defining:

- A map of the inter-dependencies between S-P-IaaS providers to better understand risk concentrations.
- A coherent Lego-like service architecture to allow a quick refactorization of risk every time a block is added or removed.
- A comprehensive accountability program to define responsibility, ownership, and liability under various scenarios, and from this perspective, the ongoing efforts for GDPR compliance that guides companies to contour their approach to data management in a structured way.
- Lightweight solutions specifically dedicated to SaaS, striking the balance between the completeness of the risk evaluation, the amount of resources invested in the assessment, the velocity of the assessment, and the compliance burden that the SaaS provider is capable of delivering. Simplified risk assessment methodologies together with simplified and standardized control frameworks focused on core security requirements become integral to reach the goal.

Board awareness and consciousness

As the most recent and historical high-profile incidents have proven, C-suite executives in many organizations lack the understanding and awareness needed to prioritize cybersecurity. Board members and senior leaders need to move to and understand that cybersecurity goes beyond information technology and can help reduce risk across the enterprise. Communicating risk posture, management, and mitigation recommendations to the highest levels of an organization is a demanding responsibility in a business culture reliant on IT. In a world where threats, breaches, and information risks increase exponentially, every CIO must be skilled in communicating the value of security to the business, keeping away from technical jargon, and making the connection to the business itself.