Redefining Enterprise Cloud Technology Governance

Também disponível em português
www.isaca.org/currentissue

Organizations worldwide are rapidly migrating on-premises IT infrastructure, software and other technology to cloud services. Today, organizations spend almost half of their IT budgets on cloud services, and this spending is growing.[1] The benefits of using such services are undeniable, including trading capital expenditure for variable fees (i.e., a pay-as-you-use model) and economies of scale, which cloud hyperscalers typically offer. Cloud technology enables increased speed and agility and access to a global audience in a shorter timeframe compared to on-premises IT infrastructure and services. Furthermore, use of the cloud allows organizations to focus on their core business rather than on maintaining data centers. Cloud services are also constantly enhanced to remain at the forefront of technology.

However, organizations and their governance practices have not been able to match the cloud's pace of change. They lack the required skills and expertise to effectively govern use of the cloud and its associated risk; thus, they are unable to optimize its value. In addition, the adoption of cloud services is often perceived as more expensive when viewed from an operational perspective or as individual cloud services, and this is due to the lack of a definitive or standard integrated framework for cloud governance. At present, industry frameworks do not specifically address the impact of the cloud on IT governance and management processes. Cloud computing is a key enabler of digital transformation and is an important consideration in digital governance. Therefore, it is important that greater emphasis is placed on cloud governance to ensure that it is aligned with future business requirements.

Understanding Cloud Governance Principles

To establish cloud governance principles, two questions should be considered. First, how is cloud governance different from IT governance? Cloud computing converts or abstracts physical IT hardware and software into services, impacting almost all IT management and governance processes. With cloud computing, there is an increased reliance on third parties for critical IT services and infrastructure compared with the traditional on-premises control IT environment. Therefore, governance of IT should also be adapted. Second, why is proper cloud governance so important? Due to the fundamental change in the nature of IT services introduced by cloud adoption (i.e., information security approaches, cost models, required skill), organizations' IT governance processes need to be adapted to the new operating model introduced by the use of cloud services and

DAVID MAZULA | CISA, CISM

Is a partner of the digital trust team at PricewaterhouseCoopers (PwC) South Africa. He has more than 10 years of experience delivering systems audits, internal audits, business process improvements and other consulting services across various industries.

CASPER LAMPRECHT | CISA, CIA

Is a senior manager of the digital trust team at PwC South Africa. He specializes in IT governance and project and program assurance. He has more than 20 years of project management experience and 13 years of experience in IT risk and governance.

infrastructure. Given the notable acceleration of cloud migration worldwide, it is important that executive management and governing boards consider several principles when making the change to the cloud. Fast and flexible practices and controls are key, rather than firm ones. They should centralize policies but decentralize policy execution.[2] **Figure 1** shows such principles.

The outer circle represents the areas of governance. The inner circle is a nonexhaustive representation of the typical IT management processes a cloud migration impacts.[3] Executive management and governing boards should consider the principles of the cloud governance framework to help ensure a well-governed and value-adding cloud environment.

Cloud Governance Components and Risk

There are 14 main governance areas of the suggested cloud governance framework. It is helpful to understand each of these cloud governance framework topics.

Establish a Cloud Strategy and Business Case

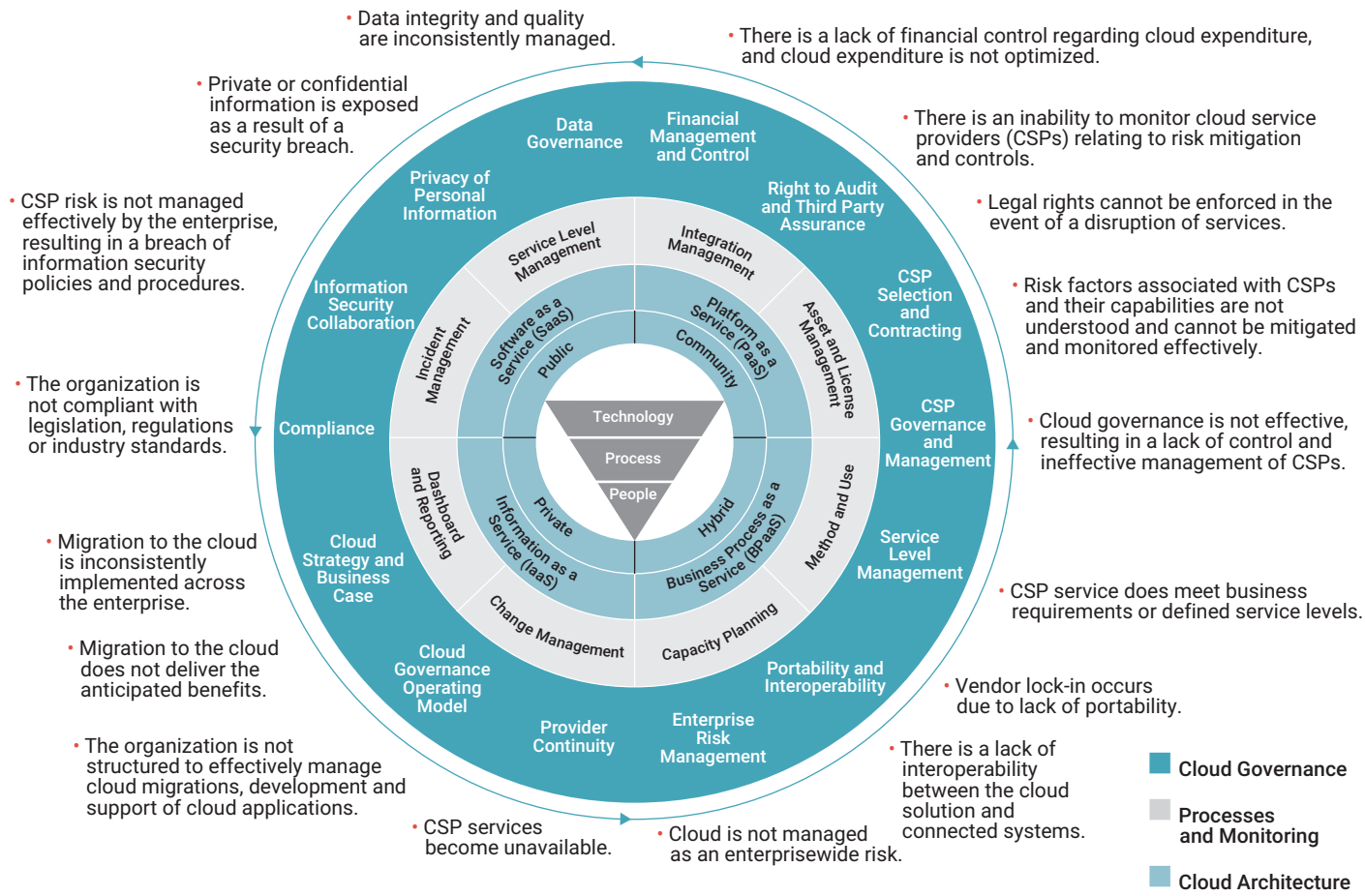
A well-developed cloud strategy that is integrated with an organization's digital business strategy is an important starting point in the cloud adoption journey. Organizations typically opt for a multicloud and cloud-first strategy but do not consider the timing of cloud migration or how the cloud will enable their digital business strategy. Organizations should formulate a business and benefits case that considers cloud strategy and the organization's associated needs and benefits, the total cost of ownership, and strategic factors such as agility and efficiency.

Without a carefully considered and documented cloud strategy, organizations face several sources of risk including:

- A migration to the cloud that is implemented inconsistently across the enterprise. Different organizational divisions or business units may use different approaches to cloud adoption and apply different principles, which may have

FIGURE 1

Cloud Governance Framework



adverse implications for the business in delivering its objectives.

- A migration to the cloud that does not deliver the anticipated benefits and value. Some of the benefits of the cloud, such as agility, may be impeded.
- Unclear and unmanaged third-party reliance risk. This may lead to issues such as system outages, security breaches and noncompliance with regulations.
- Unclear and unmanaged cybersecurity and privacy risk. This can result in cybersecurity breaches and noncompliance with privacy laws and regulations.

Create a Cloud Governance Operating Model

A cloud governance operating model refers to the organizational structure, roles and responsibilities, resources, skills, and business processes that enable cloud services. The cloud supports an organization's digital business strategy and business operating model; therefore, the IT operating model, including the IT governance operating model, should be aligned with the cloud. The IT operating model should be aligned with the business operating model through consultation with the business stakeholders. Once the IT operating model is aligned, the IT governance operating model must be adapted to the risk and challenges posed by the cloud.

Sources of risk that may accompany an inadequate cloud governance operating model include:

- The organization may not be structured in a manner that effectively manages cloud migration, development and application support.
- Cloud activities may not support the business strategy, which could expose the organization to unmanaged risk factors.
- Cloud costs may be excessive, not immediately identifiable (i.e., hidden) or unmanaged.

Seek Compliance With the Cloud

Regulators and other important stakeholders expect compliance with laws, rules, regulations and industry standards.[4] Some of the compliance requirements to which organizations must adhere include the EU General Data Protection Regulation (GDPR), the South African Protection of Personal Information Act (POPIA), South African Consumer Protection Act 68 of 2008, International Organization for Standardization (ISO) standards (e.g., ISO 22316:2017) and Payment Card Industry (PCI) standards. Cloud hyperscalers must also comply with many industry standards, which is why it is important that an organization adopting cloud services integrate the cloud into its compliance processes.

CSPs should be evaluated against organizational privacy policies and monitoring mechanisms should be put in place to ensure continuous compliance with privacy requirements.

Common sources of risk that can arise from failing to integrate cloud into compliance processes include:

- The organization may not be compliant with local or international legislation, regulations or industry standards.
- The organization may lose its license(s) to operate (e.g., loss of the right to process personal information due to the contravention of privacy rules).

Focus on Information Security Collaboration

Using cloud services does not automatically ensure information security.[5] Roles and responsibilities between the cloud service providers (CSPs) and the client should be well-defined for cybersecurity processes and controls. The shared responsibility associated with the types of cloud services being utilized should also be taken into consideration.[6]

Common sources of risk associated with ineffective or inadequate information security collaboration include:

- The organization does not effectively manage CSP risk, resulting in a breach of the organization's information security policies and procedures.
- The entity using the cloud services does not consider and sufficiently implement client-user complementary controls, which may result in gaps in the control environment and elevate the entity's risk exposure.
- Monitoring mechanisms are not in place to ensure that the CSP continues to implement the agreed-on and contracted information security measures.

Protect the Privacy of Personal Information

Management should perform a careful assessment of privacy risk before adopting any cloud services.[7] CSPs should be evaluated against organizational privacy policies and monitoring mechanisms should

LOOKING FOR MORE?

- Read *Continuous Oversight in the Cloud. https://www.isaca.org/continuous-oversight*
- Learn more about, discuss and collaborate on governance in ISACA's Online Forums. *https://engage.isaca.org/onlineforums*

Organizations must adopt and implement an appropriate data governance framework and data management processes such as data quality management while also covering cloud data.

be put in place to ensure continuous compliance with privacy requirements. In addition, proper incident management processes should be established to ensure that there are guardrails in place to deal with incidents when they occur.

Possible risk associated with failing to protect personal information includes:

- Potential private or confidential information exposure due to a security breach
- Potential noncompliance with rules and regulations that can have adverse impacts such as sanctions, financial losses or reputational damage to the organization

Ensure Data Governance to Enable Digitization

Data governance is a key enabler for data-driven organizations and digitization. Organizations can take advantage of multiple cloud data-related services for predictive analytics, competitive advantage and business benefits. Management should establish controls to ensure the integrity, accuracy, confidentiality, availability and completeness of information stored and processed in the cloud.

The inconsistent management of data integrity and quality is a key risk associated with data governance. Organizations must adopt and implement an appropriate data governance framework and data management processes such as data quality management while also covering cloud data.

Monitor Financial Management

To prevent uncontrolled growth and the escalation of cloud expenditure, it is essential to prioritize centralized monitoring and reporting of cloud costs, as well as continuous evaluation, optimization, and forecasting of cloud expenditure. Management should establish processes and controls such as tagging, reporting and allocating costs. Tagging is important for the correct allocation of costs within the organization as cloud use grows.

Common sources of risk associated with cloud financial management include:

- A lack of financial control of cloud expenditure may result in organizations not optimizing cloud use or delivering expected value.
- A siloed approach to cloud computing cost management may not be optimal. It may slow or halt cloud adoption, cripple innovation or decrease the quality of the service offering.
- Cloud sprawl (uncontrolled growth) or the underutilization of cloud resources can result in higher associated expenditure.

Consider the Right to Audit and Third-Party Assurance

Assurance continues to be a challenge, especially in the cases of relatively small CSPs whose processes and governance structures are not formalized. Smaller CSPs may not be able to afford independent assurance providers to issue service organization reports. They may also be unable to cope with multiple requests to audit or perform risk self-assessments of varying degrees of detail. Organizations should consider including the right to audit and the submission of third-party assurance reports in CSP contracts. This is especially important with respect to Software-as-a-Service (SaaS) vendors because SaaS often creates a black box in which the vendor's risk and control environment is not visible to the customer.

Unfortunately, failing to monitor CSPs for risk mitigation and controls is a common source of enterprise risk. This may result in unknown and unmanaged risk, leading to the disruption of day-to-day business operations.

Carefully Select and Contract CSPs

Vendor due diligence, selection and contracting are important to ensure that organizations protect their legal rights. CSP contracts are often standard high-level documents that are one-sided, offering little recourse to customers. Special attention should be given to ownership, particularly in the case of a SaaS contract in which users may invest significant amounts of resources customizing the cloud solution for their purposes.[8]

Common risk factors include:

- Organizations may not be able to enforce legal rights in the event of disruption of services or disputes over matters such as ownership or moving CSPs. This may lead to financial losses or long legal battles for organizations.
- Organizations may not be able to understand the risk factors associated with CSPs and their capabilities to address them and, thus, may not be able to mitigate and monitor them effectively.

Achieve Effective CSP Governance and Management

Governance arrangements and the management of CSPs, whether Information as a Service (IaaS), Platform as a Service (PaaS) or SaaS are used, are important parts of countering the black box effect typical of service providers. Organizations should always retain responsibility for governance.[9] They cannot delegate governance to CSPs. Organizations should proactively manage cloud vendors and have strong internal governance structures that align with the business strategies, especially with overarching digital transformation plans or road maps.

If organizations cannot effectively govern cloud vendors, the result may be lack of control and ineffective management of CSPs.

Pay Attention to Service-Level Management

Organizations should actively monitor and manage CSP service levels. Periodic service-level meetings and reports are essential to ensure that service providers meet the organization's requirements. This is not a new concept for most IT teams; however, organizations should consider taking advantage of modern and cloud-specific tools for monitoring the agreed-on service levels. Without such tools, organizations risk CSP services failing to meet business requirements or defined service levels.

Ensure Portability and Interoperability

Organizations should take into consideration potential migration from the CSP when the provider is appointed to ensure that vendor lock-in does not take place due to a lack of portability. Organizations should include migration assistance in vendor contracts and consider tiering the cloud services they consume to determine the necessary speed of portability. Otherwise, they may face a lack of interoperability between the cloud solution and connected systems, creating islands of information and integration problems.

Prioritize Enterprise Risk Management

Organizations should integrate cloud risk into enterprise risk management processes and report on risk periodically. Management should clearly define roles and responsibilities regarding cloud risk management.[10]

If an organization fails to treat the cloud as an organizationwide risk, cloud adoption may fail and present more problems than progress for the organization.

Consider CSP Continuity

Organizations should architect disaster recovery and continuity in the cloud as part of their cloud solutions and should not assume that automatic recovery will take place. If they fail to do this, it is possible that CSP services will become unavailable.[11]

Organizations should include migration assistance in vendor contracts and consider tiering the cloud services they consume to determine the necessary speed of portability.

Conclusion

Cloud governance is emerging. The use of the cloud changes standard on-premises IT governance processes (e.g., SaaS and IaaS influence the nature of vendor governance and management processes). Cloud has a fundamental impact on IT services, which changes the risk profile. Existing IT governance processes designed for on-premises IT services are not aligned with challenges and risk posed by cloud adoption and migration. The proposed cloud governance framework offers an integrated model of the more important aspects of cloud governance and contributes to effective cloud governance.

Endnotes

1 FutureCIO, "Half of IT Budgets Will Go to the Cloud," 16 February 2022, *https://futurecio.tech/half-of-it-budgets-will-go-to-the-cloud*

2 Wood, T.; D. Bartoletti; *Adapt Your Governance Framework for Cloud*, Forrester, USA, 2018

3 ITIL and Office of Government Commerce (OGC), *Service Operation*, p33–78, The Stationery Office (TSO), UK, 2007, *http://www.teraits.com/pitagoras/marcio/itil/OGC_ITIL_v3_5_Service_Operation.pdf*

4 Heyink, M.; *An Introduction to Cloud Computing: Legal Implications for South African Firms*, Version 2, Law Society of South Africa, South Africa, 2014, *https://www.lssa.org.za/wp-content/uploads/2019/12/LSSA-Guidelines_Introduction-to-Cloud-Computing-Legal-Implications-2012.pdf*

5 Neely, M.; "Securing an Evolving Cloud Environment," *ISACA® Journal*, vol. 3, 2014, *https://www.isaca.org/archives*

6 Vohradsky, D.; "Cloud Risk—10 Principles and a Framework for Assessment," *ISACA Journal*, vol. 5, 2012, *https://www.isaca.org/archives*

7 Woo, T.; D. Bartoletti; *Adapt Your Governance Framework for Cloud*, Forrester, USA, 2018

8 *Op cit* Heyink

9 Kirkpatrick, J.; "Governance in the Cloud," *ISACA Journal*, vol. 5, 2011, *https://www.isaca.org/archives*

10 Raval, V.; "Risk Landscape of Cloud Computing," *ISACA Journal*, vol. 1, 2010, *https://www.isaca.org/archives*

11 Shacklett, M.; "Rethinking Disaster Recovery for the Cloud," *CIO Magazine*, 6 December 2018