The Cloud Landscape: Role of IT Audit

By Angela Mwemezi

Over the past few years, the landscape of IT audit has undergone a profound transformation with the rapid adoption of cloud computing. As organizations migrate their operations to the cloud, the role of IT auditors is becoming increasingly crucial.

According to the International Data Corporation (IDC) Worldwide Software and Public Cloud Services Spending Guide for 2023, it is anticipated that global expenditure on public cloud services will soar to $1.35 trillion by 2027.

With the increasing adoption of public cloud services by businesses, the fundamental roles of IT departments are expected to undergo a transformation, shifting from directly providing the technological backbone of business operations. Instead, the evolution of these solutions is likely to be primarily driven by public cloud vendors rather than internal IT teams. Consequently, IT departments will need to reassess their focus on cybersecurity and resilience, finding ways to seamlessly integrate new applications with existing legacy systems and adapt to collaborative security frameworks.

As organizations store sensitive data in the cloud, ensuring robust measures for data protection and privacy has become paramount. Management must assess encryption methods, access controls, and compliance with data protection regulations such as the Personal Data Protection Act 2022 (PDPA).

From the KPMG global tech report 2023, results show that cybersecurity and privacy concerns were ranked as primary factors that could slow down digital transformation progress. And amid the ongoing migration to cloud infrastructures, 40% of the respondents say that enhancing security has become a key goal in their XaaS (everything as a service) projects.

As much as there are challenges, cloud computing has become a cornerstone of modern business operations, offering scalability, flexibility, and cost-effectiveness. Organizations are leveraging cloud services for storage, processing power, and software applications, leading to a paradigm shift in IT infrastructure.

Technology leaders surveyed in the KPMG global tech report 2023 cite improved data management and integration as the number one benefit of public cloud platforms. Sixty four percent (64%) of respondents to the report say they've increased profitability or performance because of their digital transformation efforts with public cloud and XaaS technologies.

Some stakeholders have proven that the benefits outweigh the challenges when it comes to cloud services. Of course, overall risks and benefits depend on several factors including the type of cloud service models used, nevertheless, it is undeniable that the cloud has become an integral part of modern infrastructure and is here to stay.

Benefits of auditing in the Cloud environment

Since cloud environments come with inherent risks, IT audit practices in the cloud assist organizations in identifying, assessing, and managing these risks effectively and this is where KPMG comes in. We play a pivotal role in ensuring the security, compliance, and efficiency of cloud-based operations, allowing organizations to make informed risk management decisions. As part of our assurance services, we adhere to the standard ISAE 3402, which specifically applies to assurance in cloud computing, providing an internationally recognized framework for evaluating service organizations' controls and processes.

Benefits of auditing in the Cloud environment

- **Risk Identification and Mitigation:** IT audits help cloud providers identify potential risks within their infrastructure, services, and operations. By assessing these risks, providers can implement appropriate mitigation strategies to safeguard their systems and data.
- **Compliance Assurance:** Cloud providers must comply with various industry regulations and standards to ensure the security and privacy of customer data. IT audits help validate compliance with regulations such as Personal Data Protection, and industry standards like ISO 27001. This compliance assurance builds trust with customers and regulatory bodies.
- **Security Enhancement:** Audits help identify vulnerabilities and weaknesses in the cloud infrastructure and services. By addressing these issues promptly, providers can enhance the overall security posture of their offerings, reducing the likelihood of data breaches and unauthorized access.
- **Performance and Cost Optimization:** Audits can also evaluate the performance of cloud services, identifying areas for improvement and optimization. This includes assessing factors such as response times, uptime, scalability, and resource utilization, ensuring that the cloud environment meets the performance expectations of customers. Also, through IT audits, cloud providers can identify inefficiencies and areas of unnecessary expenditure within their infrastructure and operations.

Benefits for cloud service users

- **Addressing Security Concerns:** IT auditors play a vital role in assessing encryption methods, access controls, and compliance with data protection regulations. By conducting thorough security audits, they help organizations identify vulnerabilities and implement robust security measures to protect their data assets in the cloud.
- **Ensuring Compliance:** Compliance with regulatory requirements is another area of focus for IT auditors in the cloud landscape. Stringent regulations impose strict requirements on how organizations handle and protect sensitive data. IT auditors help organizations

navigate these regulatory frameworks, ensuring adherence to legal obligations and safeguarding sensitive information stored in the cloud.

- **Optimizing Resource Utilization:** In addition to security and compliance, IT auditors also play a role in optimizing resource utilization in the cloud. By conducting audits of cloud infrastructure and services, they identify inefficiencies, unused resources, and potential areas of overspending. This allows organizations to optimize their use of cloud resources, reduce costs, and maximize the value of their cloud investments.

Considerations for IT Auditors in the Cloud Landscape

Entities that have established foundational definitions for the cloud landscape include the National Institute of Standards and Technology (NIST), International Organization for Standardization (ISO) and the Cloud Security Alliance® (CSA). NIST defines cloud computing as a model that enables convenient, on-demand access to a shared pool of configurable computing resources. CSA also emphasizes scalability, secure access, and the displacement of data and services from inside to outside the organization. ISO has developed standards related to cloud computing, including ISO/IEC 17788 for cloud computing terminology and ISO/IEC 17789 for cloud computing reference architecture.
Crucial aspects that IT auditors should take into account concerning cloud computing encompass a range of considerations such as:

- Exploring issues surrounding data ownership, data custody, and security administration in connection with diverse cloud deployment models: The Cloud Security Alliance (CSA) offers assessment and guidance documents that ensure compliance with cloud security protocols, these are the Cloud Controls Matrix (CCM) and Consensus Assessments Initiative Questionnaire (CAIQ). Cloud Controls Matrix (CCM) is a cybersecurity control framework for cloud computing, that can be used as a tool for the systematic assessment of a cloud implementation and provides guidance on which security controls should be implemented by which actor within the cloud supply chain.CAIQ provides a set of Yes/No questions that cloud consumers and cloud auditors can ask of a cloud provider to ascertain their compliance to the CCM.

- Navigating legal requirements and addressing unique risks specific to the cloud environment: Stringent regulations can introduce intricate challenges regarding the handling and protection of data stored within cloud infrastructures, demanding meticulous attention and proactive mitigation strategies. This mandates the implementation of robust compliance frameworks tailored to align with the unique regulatory landscape, necessitating comprehensive risk assessments to ensure adherence to legal obligations and the safeguarding of sensitive information.Companies can easily fall out of compliance by not having proper access control and restrictions to comply with compliance standards such as Payment Card Industry-Data Security Standard (PCI-DSS).

- Acknowledging potential constraints on the right-to-audit within a cloud-based framework: Auditors may confront limitations in their ability to conduct physical inspections of a vendor's facilities, necessitating alternative approaches and methodologies to ensure thorough scrutiny and oversight. For instance, auditors may rely on robust documentation reviews and engage in extensive interviews with pertinent stakeholders to ensure regulatory adherence and data protection standards are upheld.

Conclusively, the adoption of cloud computing represents a fundamental shift in how IT services are delivered and consumed. As organizations navigate the complex cloud landscape, the role of IT auditors becomes increasingly critical. By ensuring the security, compliance, and efficiency of cloud-based operations, IT auditors help organizations unlock the full potential of cloud technologies while mitigating risks and building trust among stakeholders. As cloud computing continues to evolve, the role of IT auditors will remain indispensable in navigating the ever-changing landscape of cloud technology.

> **IT auditors help organizations unlock the full potential of cloud technologies while mitigating risks and building trust among stakeholders**

Contact

Angela Mwemezi
IT Advisor
Audit
KPMG East Africa
amwemezi@kpmg.co.tz

The views and opinions are those of the author and do not necessarily represent the views and opinions of KPMG