THOUGHT LEADERSHIP Article

GIPF
Government Institutions Pension Fund
To guard, and to grow.

21 November 2022

The Challenges of Auditing the Cloud Technology

Recent advances in data storage, communication, and information processing technologies have enabled many companies to utilise business processes that are being supported by IT-enabled applications. Many companies now see a tremendous increase in their capital budgets for IT, which always raises questions on the return of these investments and to what extent emerging and innovative solutions can free up much-needed capital resources. With modern technologies becoming more widespread but at the same time more complex, it is thus important for auditors to understand not only the nature and potential benefits of new technologies, but also the risks they present and the impact they may have on the performance of the audit.

Cloud computing is a convenient, on-demand network access to a shared pool of resources that can be rapidly provisioned and released with minimal management effort or service provider interaction. It allows access to your business data or systems from anywhere 24/7/365 as long as you have internet access, enabling a remote workforce.

Life before the cloud environment was characterized by limited access to certain devices and networks, incorporated defensive layers to protect internal applications and data, and relied on a known and manageable security perimeter to prevent unauthorized access. Life in the cloud can be less secure, due to new risks to be managed.

Auditing the Cloud: Top six challenges

With an understanding of how the cloud differs from traditional IT, and an appreciation of the threat landscape, the following are the top questions that an auditor should be concerned with?

1. **The shared responsibility of the stakeholders:**

   Are the responsibilities of each stakeholder in the supply chain clear, documented and communicated? One of the biggest risks in the cloud environment is lack of transparency. It is therefore important that each stakeholder knows their responsibility. This should be documented and included in the contract.

2. **Laws and regulations**:

   What is the location of the cloud? Which local laws and regulations are applicable? Are there controls in place to identify the applicable jurisdictions and regulations? How is compliance to this identified and managed? Ideally, the cloud location, applicable jurisdiction and regulations should be included in the contract.

3. **Cloud usage:**

   Is there a list of cloud solutions currently in use? Can you identify shadow IT cloud usage? Are controls in place to identify shadow IT cloud solutions? To what extent are the cloud computing activities across the origination coordinated? Identifying the use of cloud computing is important in understanding the cloud computing risks that are relevant to your environment to ensure appropriate controls are in place and operating effectively.

4. **Risk management:**

   Are cloud solutions and the associated risks identified and evaluated as part of the Enterprise Risk Management (ERM) process? Is there a defined risk appetite and risk tolerance for cloud solutions, or were these risks accepted? Was this risk accepted by the appropriate authority within the organization?

5. **Do you have the right to audit?**

   Do the contracts you have with cloud providers include a right to audit clause? The larger the cloud computing provider, the less likely they will allow the inclusion of such a clause, so it’s important to understand your rights and to request access to the cloud provider’s System and Organization Controls (SOC) reports to confirm appropriate controls are in place and operating effectively to ensure your data is secured.

6. **Is your audit team equipped to audit the cloud?**

   To audit and oversee the cloud, your audit team must possess the appropriate skills and expertise. The Cloud Security Alliance and ISACA jointly developed a Certificate of Cloud Auditing Knowledge (CCAK) credential, which includes a risk-based approach to cloud migration and auditing strategies.

To ensure your organisation selects secure cloud platforms, your institutions internal audit department should be involved in the procurement, design and adoption of a cloud solution.

Lamek Lamek Tangeni
Is the Acting Chief Audit Executive at the Government Institutions Pension Fund, the views expressed in this article are his own and do not represent those of her employer.