Option #1: The Impact Of Cloud Computing On IT Auditing

Liam Bergerson

CSU - Global

ITS462-1

N. Braun

6/11/23

Option #1: The Impact Of Cloud Computing On IT Auditing

Organizations need a place to store their data. Traditional data centers that are typically on-premises are used to do so. However, traditional data centers are expensive and are difficult to manage. The concept of cloud computing was created fairly recently to address the issues of traditional data centers. Cloud computing allows organizations to subscribe to a provider and use their data storage services. Instead of using on-premise equipment to store data, the organization is using the cloud provider's equipment to store their data. In an audit process, cloud computing can be troublesome as there are more restrictions in place. There are currently certifications available that address security concerns associated with cloud computing that will be discussed. There are many cloud security and auditing issues that are present in the field of IT auditing and cloud computing, however, some issues are more daunting than others.

Cloud Computing and How It Impacts the Audit Process

As stated before, conducting an IT audit on a cloud computing service provider imposes more restrictions than conducting an IT audit on the auditee's equipment. This is because the auditee doesn't actually own the equipment of the cloud provider. In cloud computing, there are three main cloud models that are available: Software as a Service (SaaS), Infrastructure as a Service (IaaS), and Platform as a Service (PaaS). Each one of these service models pose a different set of risks and controls depending on the specific deployment of a

service model the auditee chooses to deploy. Going back to the increased amount of restrictions with cloud computing, certain cloud providers can have more or fewer restrictions that organizations should consider. Some cloud providers completely restrict the act of auditing their service altogether. This can be extremely troublesome for organizations that wish to have the cloud service they use audited. Some cloud providers will allow audits, but will require the client to obtain specific approvals before any audit activities can commence (Rittle, et al., 2016). When choosing a cloud provider, this needs to be considered if the organizations using it wishes to be audited in the future.

Auditing practices defined by the CISA certification and other sources, in my opinion, do not successfully address the issues defined above related with cloud services. Since auditees that are using cloud services are completely at the mercy of the provider, audits can be severely impacted based on the restrictions imposed by the cloud provider. One such auditing practice is to comply with organization security policies. If the cloud provider has policies in place that make auditing extremely difficult or impossible, there is nothing that the organization that is using the cloud provider can do if they wish to be audited. This is why it's crucial that organizations that wish to use a cloud provider that they verify that the cloud provider accepts IT audits with moderate restrictions.

Audit Certifications and Cloud Security

Cloud Security is paramount in order to keep sensitive data confidential. There are certain certifications available that will address cloud security concerns

by teaching users how to secure cloud platforms. The cloud security certification that will be discussed is the Certificate of Cloud Security Knowledge (CCSK). The CCSK is a widely renowned certificate developed by the Cloud Security Alliance (CSA). This certification represents the standard of knowledge required to work in cloud security and teaches users data encryption, cloud incident response, application security, and best practices for Identity and Access Management (Coursera, 2023). I don't necessarily think it's required for IT auditors to have the CCSK certification in addition to the CISA certification. However, I do think it will greatly complement their skillset and is highly recommended in order to work with cloud security during IT audits. Rather than starting from scratch and learning about cloud security while doing IT audits, a course for this certification will teach IT auditors all they will need to know about securing cloud platforms. That way, during IT audits, they will already have knowledge about cloud security. Employers also greatly appreciate a candidate that has actual proof of knowledge of securing cloud platforms.

Cloud Security and IT Auditing Issues

There are multiple cloud security and IT auditing issues that are present when conducting IT audits or securing cloud platforms. However, some issues are more concerning than others. Regarding IT auditing, there have been concerns about audits being used to cover up and hide vulnerabilities within an organization's infrastructure, which is defeating the purpose of an IT audit. This is partly due to the fact that some organizations simply do not wish for the weak

status of their infrastructure to be exposed to the public. So they hide behind the facade of an IT audit to cover up their vulnerable infrastructure. This is a breach of trust towards the clients willing to put their sensitive information in the hands of this organization. They should be doing their part in securing their infrastructure, not keeping it vulnerable and hiding it.

Regarding cloud security, misconfiguration can be a severe issue if not addressed properly. Cloud misconfigurations are a leading cause of security breaches towards organizations using cloud services. If the cloud platform is not configured properly, this will leave many doors for threat actors to use to breach the organizations. Misconfigurations can also lead to data leaks. Since the data center that the cloud provider uses contains other organizations' data, there is a possibility for data leaks. This can leave other organizations' sensitive data vulnerable if one organization suffers a data breach. However, depending on the security measures of the cloud provider, this most likely will not happen.

Conclusion

As more organizations implement cloud computing into their infrastructure, they need to be included in IT audits. Cloud platforms are just as vulnerable as traditional data centers if they are not configured properly. It’s crucial that cloud platforms are audited just as traditional data centers are audited. However, it is more difficult to do so since the cloud platform is owned by the cloud provider. The cloud provider may have restrictions in place that make it extremely difficult or impossible to audit. To help IT auditors with cloud security, the CCSK

certificate will give them the knowledge they need. Many issues are present with IT auditing and cloud security. IT audit facades and cloud misconfiguration are, however, among the most concerning issues present.

References

Coursera. (2023). What Is CCSK? A 2023 Guide for Cloud Security Professionals. *Coursera*. https://www.coursera.org/articles/ccsk

Rittle, J., Czerwinski, J., Sullivan, M. (2016). Auditing the cloud. Internal Auditor, 73(4), 43.