IT Auditing and Compliance in Cloud Computing Environments

Bronte Hodson

Davenport University

IAAS332: Authentication & Audit

Tony McCutchen

Due Date: 09/21/2025

IT Auditing and Compliance in Cloud Computing Environments

Cloud computing has significantly changed the IT landscape, evolving beyond simple online storage to encompass IT infrastructure, platforms, and software as a service. Organizations now demonstrate versatility in how they adopt, manage, and utilize IT resources (Stein et al., 2020). However, this shift from on-premises IT to multi-tenant and globally distributed cloud environments introduces substantial new risks to IT governance, security, compliance, and regulatory oversight that cannot be overlooked (Gupta, 2022). As a result, cloud computing has transformed the nature of IT risk and the organization's response to these risks, along with regulatory compliance and IT auditing in a complex and dynamic environment. Effective management of IT cloud risks and compliance can be achieved through a solid understanding of the Shared Responsibility Model, the implementation of effective governance frameworks and standards, and ongoing regulatory and threat monitoring in the cloud environment (Kumar & Sandbrink, 2024). In this context, the role of IT auditors becomes crucial in helping organizations achieve compliance.

A critical part of understanding security and compliance challenges in cloud computing is the Shared Responsibility Model. This model defines and outlines the cloud service provider (CSP) and customer responsibilities. CSPs typically secure the base IT infrastructure while the customer owns security and compliance over the applications, user access, and their data (Amazon Web Services, n.d.). Therefore, regarding security and compliance in cloud computing environments, it is important to understand what cloud-based services are being provided, and what risks are shared. Generalist cloud service providers (CSPs) such as Amazon Web Services, Microsoft Azure, and Google Cloud Platform offer a variety of services, which include the IT infrastructure, platforms, and software as a service. Specialized CSPs offer software such as file transfer and collaboration software (Gupta, 2022). Knowing these service boundaries is critical, as they help establish security

responsibilities. However, the continuation of cloud breaches occurring shows that organizations can misunderstand their responsibilities, or there are security gaps occurring in either or both the CPS's and customers IT risk management systems, resulting in cloud incidents and compliance breaches occurring.

Considering reported cloud incidents, it is noted that most cloud security incidents are customer mistakes and not CSP flaws. Verizon Inc. (2024) states, "68% of all cloud breaches are attributed to customer misconfigurations or human errors, while only 11% are due to CSP issues." Other incidents may be due to third-party or supply chain incidents. The most common customer mistakes are that they leave their storage buckets public, use weak or reused passwords, do not have multi-factor authentication, encrypt their stored data and data in transit poorly, and do not monitor systems, which may extend the timeframe of breach detection (Verizon, 2024). These breach statistics suggest that some organizations overlook or misunderstand their own responsibilities within the shared services model. Also, the statistics emphasize the need for strong IT risk governance to mitigate these risks. They illustrate the importance of understanding the cybersecurity posture of CSPs, and to integrate cloud risks into the organization's own information risk management systems to keep organizations compliant. Further an important step in managing IT risks in cloud computing is documenting shared responsibilities between CSP and customer. Furthermore, organizations and IT auditors should vet CSPs for security and compliance controls, as well as service agreements (Amazon Web Services, n.d.).

Real-life examples illustrate how a security breach can occur in cloud computing environments. For example, the 2024 Snowflake breach occurred when attackers gained access to Snowflake's customer data using reused credentials, and multi-factor authentication was not enabled on customer accounts. This breach was due to poor access security by the customer, and then Snowflake as the CSP did not have secure default settings and had limited

monitoring. Snowflake's shared responsibility model wasn't fully understood, and the customer and Snowflake did not adopt adequate security measures (Cloud Security Alliance, 2024). Additionally, in the case of the AWS Outage (2023), a technical fault in the Amazon AWS infrastructure caused the outage to multiple websites and businesses, causing downtime. Users of AWS had risks to availability of service and the compliance impacts caused by this (The Washington Post, 2023). Redundancy, disaster and business recovery remain critical in all environments, including cloud computing to ensure compliance.

Considering a broader framework, cloud computing introduces further complexity and challenges for an organization and IT auditor. The distributed nature of cloud computing means data can be processed, stored or backed up anywhere in the world resulting in increased data privacy, security and availability risks. Organizations and IT auditors need to understand complex, evolving regulations in multiple countries to manage the confidentiality, integrity and availability of data to avoid compliance breaches, fines, disruptions, and reputational harm. For example, regulations like GDPR require organizations to put in place strong controls around personal data, including data location, access by users, encryption, and breach notifications (Wolford, 2025). Also, other industry-based regulations require organizations to understand where data is located, processed and how it moves through IT networks. These laws include the Health Insurance Portability and Accountability Act (HIPAA), which requires strict data privacy and security measures to safeguard sensitive patient records, the Sarbanes-Oxley Act (SOX) which regulates financial reporting and internal controls of public companies, and the Payment Card Industry Data Security Standard (PCI DSS) that requires credit card information to be protected in secure locations. These occur in cloud environments, so robust IT risk management systems and IT audits are needed to help achieve compliance and avoid fines and loss of stakeholder trust (Johnson et al., 2022, Chapter 2).

Another complex issue for the organization's risk management and IT auditors is the mix of dedicated, multi-cloud, and hybrid cloud operations. This introduces significant complexity to organizations and auditors. Many organizations, for example, develop redundancy and backup strategies by mixing AWS, Azure, Google Cloud, and a private cloud (Gupta, 2022). The complexity arises from the fact that each CSP controls the implementation of controls differently, complicating compliance and audit processes. Auditors will need to assess how security controls are integrated across each platform and how data is transmitted from one platform to another. While CSPs can provide accepted certification, such as SOC 2 and ISO/IEC 27001/27017, it is up to the organization to secure its own configuration, data, and compliance (National Security Agency, 2024). Complexity and shared responsibilities reinforce the need for organizations to fully understand the risks in hybrid or multi cloud environments and for IT auditors to consider this unique risk when preparing an audit IT.

According to Johnson et al. (2022, Chapter 4), to address the multi-faceted and dynamic risks of cloud computing, auditors are required to use comprehensive industry frameworks and standards as audit baselines for the audit of regulatory compliance. These frameworks and standards can either be used by themselves or in hybrid or collective forms. NIST SP 800-53 has expansive controls used in traditional IT and cloud computers, though mainly through federal information systems controls such as access control, incident response, risk assessment, system and communications protection. ISO/IEC 27001 focuses on establishing, implementing, and maintaining information security management systems (ISMS), while ISO/IEC 27017 provides supplementary security for cloud computing services, and ISO/IEC 27018 seeks the protection of personal data in cloud environments. Furthermore, COBIT is a framework that offers governance and management for IT risk and compliance, creating an alignment of IT goals to business objectives and documentation for

various regulatory compliance such as SOX. According to the PCI Security Standards Council (2022), PCI DSS is a standard designed for worldwide protection of cardholder data via controls such as encryption algorithms, logical network and system compartmentalization, user access limitations, ongoing regular testing of security systems, and surveillance. IT governance frameworks and standards play an important role in managing risks and compliance in cloud computing. These provide actionable programs to implement and audit for consistent regulatory compliance as well as a baseline for IT compliance audits and improved risk management.

With the nature of the cloud computing landscape changing, IT auditors need risk-based auditing. Not every control should be assigned the same amount of risk assessment. Rather, organizations and auditors should evaluate cloud controls based on the highest risk (Franklin, 2025). This would entail planning and testing in terms of targeted audit plans around higher-level frameworks, like NIST, ISO/IEC, and COBIT. Accordingly, this will focus an auditor's energy and resources to the higher-level risk concern areas.

Also, the complex nature of change in cloud computing as well as the rapid provisioning, changing, or decommissioning of resources will create even greater complexity. Continuous monitoring has become necessary and required by IT risk management. Compliance automation tools will decrease the need for manual monitoring and reporting, while continuous monitoring enables quicker identification and remediation of incidents (Kumar & Sandbrink, 2024). Manual auditing has become impracticable with the large scale and complexity of cloud computing. This gap in resourcing could be filled with automation tools, scanning, and security configuration management systems that collect, analyze logs, detect anomalies and remediate incidents (Johnson et al., 2022, pp.227-228, 234-239).

Cloud computing has revolutionized IT infrastructure and has resulted in a dramatic increase in the complexity, scope and skills required for an IT compliance audit. A number

of these complexities have been raised earlier and present unique challenges to organization and IT audits. While compliance frameworks and standards provide a baseline security, compliance doesn't always mean protection. This is because of frameworks and standards don't always consider emerging or zero-day threats. Cloud technology and laws are constantly evolving as are new threats, risks and challenges. Consequently, the IT auditor's role will also be required to evolve to address these unique challenges, requiring skills in cloud tools, and cloud system architecture (Ayu et al., 2024). Auditors should leverage data analytics, AI, and other automation technologies to enhance risk assessment and auditing efficiency (Ayu et al., 2024). Proactive auditing approaches, combined with traditional methods and incident management activities, are crucial for identifying and mitigating cloud-specific risks and ensuring compliance is a continual ongoing process (Kumar & Sandbrink, 2024).

Cloud computing has changed IT infrastructure and increased the complexity of IT compliance audits. Organizations are dealing with shared security responsibilities and changing regulations. Understanding the shared responsibility model, using strong governance structures and standards and through continuous monitoring, organizations and auditors can deal with these threats. IT auditors are critical in helping organizations meet regulatory requirements to stay secure and compliant.

References

Amazon Web Services. (n.d.). Shared responsibility model. https://docs.aws.amazon.com/whitepapers/latest/aws-risk-and-compliance/shared-responsibility-model.html

Ayu, P., Rizki, N., Samosir, S., Muda, I., & Author, C. (2024). *MRS Journal of Accounting and Business Management.* Impact of Cloud Computing on IT Audit Practices: Challenges and Opportunities. https://www.mrspublisher.com/assets/articles/1734515958.pdf

Cloud Security Alliance. (2024). *Unpacking the 2024 Snowflake Data Breach* | CSA. https://cloudsecurityalliance.org/blog/2025/05/07/unpacking-the-2024-snowflake-data-breach

Franklin, E. (2025, September 17). *What Is Risk-Based IT Auditing? | High-Impact IT Areas*. McKonly & Asbury. https://macpas.com/risk-based-it-auditing-prioritizing-key-areas-of-risk-and-concern/

Gupta, G. (2022). *Managing Compliance and Auditing in Cloud.* https://www.theseus.fi/bitstream/handle/10024/749769/Thesis_gupta_gunjan.pdf

Johnson, R., Weiss, M., & Solomon, M. G. (2022). *Auditing IT infrastructures for compliance* (3rd ed.). Jones & Bartlett Learning.

Kumar, A., & Sandbrink, C. (2024). *Security and compliance in cloud environments.* CORP. https://www.corp.at/archive/CORP2024_65.pdf

National Security Agency. (2024). *Uphold the Cloud Shared Responsibility Model*. https://media.defense.gov/2024/Mar/07/2003407863/-1/-1/0/CSI-CloudTop10-Shared-Responsibility-Model.PDF

References

PCI Security Standards Council. (2022). *Payment Card Industry Data Security Standard: Requirements and Security Assessment Procedures* (version 4.0). https://docs-prv.pcisecuritystandards.org/PCI%20DSS/Supporting%20Document/PCI-DSS-v4_x-QRG.pdf

Stein, M., Campitelli, V., & Mezzio, S. (2020). Managing the Impact of Cloud Computing. *The CPA Journal.* https://www.cpajournal.com/2020/07/13/managing-the-impact-of-cloud-computing/

Verizon. (2024). *2024 Data Breach Investigations Report.* https://www.verizon.com/business/resources/reports/2024-dbir-data-breach-investigations-report.pdf

The Washington Post. (2023, June 14). *Amazon's cloud computing service experiences regional outage*. Data Center Knowledge. https://www.datacenterknowledge.com/outages/amazon-s-cloud-computing-service-experiences-regional-outage

Wolford, B. (2025). *What is GDPR, the EU's new data protection law?* GDPR.EU. https://gdpr.eu/what-is-gdpr/