Cloud Shift: IT Audit

Shravan Reddy[1], Sid Swarupananda[1]

[1]Master of Science in Data Science
Southern Methodist University
Dallas, Texas USA
skreddy@smu.edu, sswarupananda@smu.edu

Abstract. This paper focuses on cloud computing governance and audit issues by presenting research questions informed by both practice and research. The growing organizational preference of cloud first infrastructure has caused an increased utilization of cloud services for new initiatives to replace existing services. This cloud first approach prioritizes cloud adoption which has resulted in an enterprise shift to the cloud. The pace of these initiatives, along with customer expectations have led to a rapid adoption of cloud services. Especially adjusting to the pandemic, the cloud has not only reduced IT costs and increased flexibility and efficiency but also increased the required level of trust with an outside vendor to secure the business' data. It is in the best interest of an organization to incorporate continuous audits to identify any non-compliance issues related to agreements with cloud providers.

1 Introduction

Today's clouds environments are becoming more and more complex with the goal of delivering reliable and efficient infrastructure to meet their market needs with minimal effort. The need to secure network access to data and business continuity has increased the need for cloud auditing. Cloud auditors monitor the many risks associated with an organization's adoption of cloud services. Some of the risks include: loss of governance, compliance risks, security incident management, and malicious inside behavior. In general, security assurance and decreased risk of data breach are two significant benefits of cloud auditing.

2 Literature Review

Below are some of the articles explored for business in cloud to research questions on Governance, Audit, and Assurance

2.1 The Audit Implications of Cloud Computing

Rajiv D. Banker; Xiaorong Li; Steven A. Maex; Wenyun Shi Retrieved from link

This article discusses if cloud computing allows for increased audit efficiency through reliance on service organization control reports or introduces additional complexity and risk to the audit.

3 Cloud Shift Migration

Cloud migration is the process of moving data, applications or other business elements to a cloud-computing environment. There are various types of cloud migrations. The most common being the transfer of data from local on premise to the public cloud. Most organizations are leveraging the benefit of computing clouding; cloud migration is becoming a popular IT infrastructure practice. It provides solutions to most of the issues IT organizations have to worry about in the past such as disaster recovery plans, cost of hosting a database infrastructure in-house (locally), data availability, and scalability. Migrating to cloud reduces companies operational costs, fulfill their daily data needs, and gain seamless operations flexibility

All the popular cloud services are model around infrastructure, platform and software.

Infrastructure as a Service (IaaS):
IaaS is the lowest level of cloud solutions and refers to cloud-based computing infrastructure as a fully outsourced service. An IaaS provider will deliver pre-installed and configured hardware or software through a virtualized interface. What the customers accessing the cloud services do with the service is up to them.

Platform as a Service (PaaS):
Apart from simply providing infrastructure, PaaS also offers a computing platform and solution stack as a service. The IT infrastructure may come with a graphic user interface, run-time system libraries, programming languages, or an operating system.

Software as a Service (SaaS):
SaaS providers provide fully functionally web-based applications on-demand to customers. The applications mainly target business users and can include web conferencing, ERP, CRM, email, time management, and project tracking among others.

As organizations' need for data security and stability increases, cloud auditing is gaining traction. Cloud auditors explore the potential of given cloud services and evaluate significant cloud capabilities that indicate their reliance on its security protocols, technical performance, and cost optimization.

3.1 Whats is Cloud Auditing

A cloud audit is a process of estimation to improve data availability and consider crucial cloud security aspects. The process involves a technical investigation and presentation along with a detailed report on the performance of your current cloud infrastructure. Depending on the scope and client's specifications, cloud

auditors or cloud auditing companies can conduct the audit of cloud systems.

In a cloud computing audit, there are multiple steps to form an opinion on the operational effectiveness and design of controls identified in different areas. Risk management, data management, network security, system development, communication, vulnerability, and remediation management are some of these areas.

3.2 The need for cloud auditing

A cloud audit offers insights into the current state of an organization's cloud infrastructure. It also helps with optimization, compliance, and potential improvements. Compliance with industry regulations or vulnerabilities to virus attacks are other areas that can be helped.

Cloud auditing is much more complicated than regular IT auditing as it can be internal or external as a standard IT audit.

Many businesses are negligent when it comes to monitoring fluctuating costs or un-managed expenses. Your cloud environment hosts some of the critical aspects of your business, from customer data or future road maps to business processes. By performing a cloud audit at regular intervals, you can understand your cloud environment in a much better way and optimize it well while focusing on both assets and spending. Given that the cloud computing industry is relatively new and evolving fast, it is generally hard for regulators to keep up with the pace of innovation in the cloud space, which is usually why meeting regulatory compliance is not enough to protect your business against breaches. It is better to be safe than sorry. Hence, a company must leave no stone left to find vulnerabilities when performing a cloud audit.

4 Types of Cloud Audit

4.1 Vulnerability Scanning

Security is one of the most important factors to be considered while performing a cloud audit. Failure to meet security compliance guidelines can hinder your business's growth and make it impossible to scale without an array of security breaches. Vulnerability scanning is an auditing procedure that offers a complete rundown of potential points of attack found within the computer software. A vulnerability scanning cloud audit includes a checkup of the following things:

- Systems
- Networks
- Cloud infrastructures
- Web applications

– Network service apps
– Docker containers

Managing vulnerabilities includes patching systems regularly while securing network traffic between components by detecting attacks from within the cloud. In addition, a review of end user systems that interact with cloud-based applications is necessary to ensure system security.

Audit teams need to assess availability by reviewing service level agreements regarding uptime and other related disclaimers. It's important to take a look at the resiliency (clusters, redundancy, and failover) and perform tests especially after changes or system updates. Data backup locations, incident response plans, and peak demand handling are also important aspects that need review.

4.2 SDLC Pipeline Audit

You can use software development life cycle (SDLC) methodologies like V-Model, waterfall, spiral, and prototyping. Proper SDLC pipeline configuration is vital as it underlies the creation of working software. On the other hand, if your CI/CD pipeline is not secure, then chances are there it may expose sensitive data to outside sources.

Specialists can detect cloud security vulnerabilities and verify your CI/CD resiliency that they can control. Also, they will ensure that your SDLC environment configuration is secure and no secrets are exposed. So that your SDLC architecture will be in line with the prevalent security standards.

This audit area will ensure security, privacy, and regulatory compliance. Security will include identifying and monitoring for vulnerabilities that may target your application and reviewing source code and data to find security weaknesses.

4.3 Configuration Audit

Configuration hardening checks guard systems proactively by reducing the attack surface and having sound system fortification. The essential goal of configuration hardening is to prevent potential cloud threats. But at times, it becomes challenging for enterprises to see whether their configurations are correct.

Cloud audit teams assess critical service configurations and systems to solidify them against vendor-neutral standards. Additionally, they ensure that the operating system software is updated to stay ahead of new exploits and that this process runs seamlessly.

It's important to analyze the data environment by reviewing data center locations and determine if the service provider can commit to specific requirements. Within the data centers, application and operating systems need to be reviewed to determine how often components are updated.

4.4 Infrastructure Audit

Cloud infrastructure security, performance, and cost assessment audit detect infrastructure misconfiguration's, vulnerabilities, and threats within the cloud environment. Also, it can check whether a cloud has sufficient monitoring capabilities and verify the access and security policies to improve risk.

Cloud auditors assess infrastructures against CIS benchmarks to detect misconfiguration's to optimize financial resources, time and effort needed to maintain the infrastructure. All these activities can improve the overall configurable computing resource utilization.

While auditing a cloud service providers configuration, restricted access, internal and third party, to data needs to be ensured along with continuous monitoring. A check must be done for the presence of logs and audit trails. Access and security policies improve risk management and having these logs allow a trail to investigate any possible threats that may have occurred. These logs also must have a dedicated storage that also ensure that the logs are tamper-proof.

Another aspect is information encryption. The overall end to end data pipeline, to and from the data with encryption for data in transit, at rest, needs to be understood. The Cloud Service Provider must have an encryption certificate that should provide at least 128-bit encryption and needs to be audited annually by a third party.

5 How To Audit

Cloud audits ensure that the specifics of the cloud environment are delivered according to specific controls regarding security and risk.

Let's take an AWS audit as a popular example. During the audit, we analyze AWS accounts, network configurations, data encryption, security incident response, and more. We use top-ranked sources such as CIS AWS Foundations, security policies based on HIPAA, the FedRAMP, etc.

AWS Audit Plan

- Identifying assets in AWS.
- AWS account analysis.
- Governance audit. Understand what AWS services and resources are in use and ensure that the Customer's security or risk management program has taken into account the use of the public cloud environment.
- Network configuration management audit. Verifying missing or inappropriately configured security controls related to external access and network security, which could result in a security exposure.
- Asset configuration and management audit. The management of the Customer's operating systems and security applications is verified to protect the security, stability, and integrity of the assets.

- Logical access control audit. Focuses on identifying how users and permissions are set up for the services in AWS, ensuring that the Customer securely manages the credentials associated with all AWS accounts.
- Data encryption audit. Understand where the data resides, and validate the methods that are used for protecting the data at rest and in transit (also referred to as "data in flight").
- Security logging and monitoring audit. Validating if audit logging is performed on the guest OS and critical applications installed on Amazon EC2 instances and that the implementation is in alignment with your policies and procedures. Special attention is paid to the log storage, security, and analysis.
- Disaster recovery audit. Disaster recovery controls are checked for operational effectiveness.
- Security incident response audit. Incident management controls are checked for operational effectiveness.

6 Conclusion

Today's cloud environment supports some of the most integral parts of the business like customer data. By reviewing, auditing and optimizing the cloud infrastructure, businesses can pin-point assets that are causing unnecessary expenditure. This allows businesses to gain better financial control and achieve greater visibility over their cloud infrastructure. Cloud audits are essential with the rise in data breaches to assure and lower the risk of losing information.

7 Acknowledgements

The researchers would like to thank the Professor for the templates and structure, supporting the development of the efforts

8 References

1. Rajiv D. Banker; Xiaorong Li; Steven A. Maex; Wenyun Shi. The Audit Implications of Cloud Computing. Retrieved from link
2. Cloud Audit in a Nutshell - Why, How, and with Whom link
3. Cloud Security Audit: Techniques, Trends, and Tools link
4. Cloud Compliance Audits: What You Need to Know link
5. What is Auditing in Cloud Computing? link