Chapter 7
Multi-Cloud Environments:
Auditing for Security, Compliance, and Risk Mitigation

Varanasi Rahul
https://orcid.org/0000-0003-2407-7654
Jain University, India

N. Sathyanarayana
https://orcid.org/0000-0002-4185-7751
Jain University, India

L. B. Muralidhar
https://orcid.org/0000-0003-3453-613X
Jain University, India

Y. Fathima
https://orcid.org/0000-0002-0045-1421
Jain University, India

R. Shilpa
https://orcid.org/0009-0002-9805-1481
RJS Institute of Management Studies, India

ABSTRACT

The proliferation of multi-cloud environments, driven by the need for flexibility, redundancy, and cost efficiency, has introduced new challenges in managing security, compliance, and risk. This chapter explores integrative approaches to auditing within multi-cloud infrastructures, highlighting frameworks, tools, and methodol-

DOI: 10.4018/979-8-3373-3078-5.ch007

ogies necessary to ensure robust security and regulatory alignment. It examines key components such as identity and access management, data encryption, network security, and continuous monitoring. Additionally, the chapter outlines auditing practices for security and compliance, referencing international standards like NIST and GDPR. Risk mitigation strategies are discussed through real-world case studies, including risk assessment models and continuity planning. The discussion underscores the need for cohesive auditing mechanisms to address the complexity and fragmentation inherent in multi-cloud systems. By adopting a holistic audit perspective, organizations can safeguard critical assets, meet compliance demands, and build resilient digital ecosystems.

1. INTRODUCTION

1.1 The Rise of Multi-Cloud Environments

Over the past ten years, the technology landscape has evolved with cloud computing being the backbone of contemporary digital infrastructure. While organizations pursue the goal of being scalable, agile, and cost-effective, they embrace multi-cloud strategies—the use of two or more cloud computing offerings from various vendors, more and more. Unlike the use of both public and private clouds to create a so-called hybrid cloud environment, multi-cloud configurations use multiple public clouds (such as AWS, Microsoft Azure, Google Cloud) or a blend of public and private offerings to diversify workloads, avoid vendor lock-in, and improve the reliability of the services concerned. (Majumdar et al., 2022)

Multi-cloud setups have developed from being a tactical decision to a strategic necessity. Enterprises use such setups' flexibility to align various workloads to the most optimal cloud platforms, leverage region-based capabilities, and achieve competitive pricing models. The advantage of multi-cloud deployment is compounded by many complicating factors, especially in security, regulatory compliance, and risk management. Each cloud provider has unique architectures, tools, configurations, and security models with multiple complicating factors in providing visibility, control, and auditability across the IT ecosystem.

1.2 Security and Governance Issues

Security in multi-cloud is hardly a matter of defending a defined perimeter but rather of protecting several platforms with varied access control, audit trails, and threat models. Heterogeneity brings blind spots with it that can be exploited by an adversary. On top of this, cloud assets are inherently temporary in nature—ephemeral