J. Inst. Eng. India Ser. B (June 2024) 105(3):733–750
https://doi.org/10.1007/s40031-024-01034-x

REVIEW PAPER

A Unified Approach Toward Security Audit and Compliance in Cloud Computing

Y. S. Rajesh[1,2] · **V. G. Kiran Kumar**[3] · **Asmita Poojari**[4]

Received: 15 March 2023 / Accepted: 26 February 2024 / Published online: 23 March 2024

Abstract The use of cloud computing has become a reliable information technology solution over the past decade by providing numerous services and resources on a pay-as-you-use basis and evolving from concept to reality. Despite increasing demand and popularity, the adoption of the cloud is hindered mainly by security concerns. Successful cloud adoption and uncomplicated operation are possible if users, intermediaries, and service providers act reliably according to regulations by assuring shared responsibility policy. The biggest challenge in the audit and assurance of cloud computing is the lack of a de facto approach to meet an enterprise's requirements. The primary focus is on the challenges and effectiveness of audit and assurance by conducting an exploratory study on industry best practices, auditing standards, required certifications, and regulatory compliance frameworks like GDPR, Sarbanes–Oxley, ENISA, ISO 27001, NIST, EU-SEC, OWASP, BSI C5, CIS, ANSSI, HIPAA, CCM, CSA STAR, PCI DSS, COBIT, and SOC in a cloud environment and classifying on basis of applicability. In this research paper, we provide general guidelines on auditing standards by referring to threads and vulnerabilities analyzed and suggesting a unified approach toward audit considerations in cloud computing environments.

Keywords Audit · Cloud computing · Cloud security · Security auditing

✉ V. G. Kiran Kumar
kiranvgk@gmail.com

Y. S. Rajesh
email@rajeshys.com

Asmita Poojari
asmitapoojari@nitte.edu.in

1 MS UpGrad Education Private Limited, Nishuvi, 75, Dr. Annie Besant Road, Worli, Mumbai 400018, India

2 PSOM Technologies Pvt Ltd, Bengaluru, India

3 Department of Electronics and Communication Engineering, A J Institute of Engineering and Technology, Kottara-Mangalore 575006, India

4 Department of Computer Science and Engineering, N M A M Institute of Engineering and Technology, Karkala, India

Introduction

This study, which is pertinent to the current problem, focuses on two key cloud computing challenges: security audit concerns and audit compliance. When switching from a center (on-site) to a center (cloud), cloud customers must trust that cloud service providers will handle and safeguard their information with due diligence and prevent them from losing control. Cloud service companies need to gain this trust. Only open, law- and user-compliant behavior by service providers will make this possible [1]. Although 80 percent of Fortune 500 IT decision-makers agreed that cloud computing gave their company a competitive edge, security concerns continue to be a major deterrent to cloud adoption. It is more significant than conformity and honesty. Therefore, developing a cloud security audit plan is essential [2]. A strategy to lessening the challenges of cloud-specific security audits is suggested in this study. It is more significant than conformity and honesty.

Our research is driven by the desire to apply a consistent approach to assurance components for cloud computing technology suppliers and users by defining the requirements for audit considerations that need to be verified during audit operations. Therefore, while evaluating cloud computing solutions, audit professionals would be able to gather proof of the sufficiency of control. Professionals will discuss the unified assurance approach with numerous aspects that

would favorably effect cloud adoption based on an assessment of the most recent research. As a result, the insights gained from this study could contribute to a unified approach to assurance aspects of cloud computing and have an impact on academia by making information technology assurance solutions more flexible. Some of the research questions are as follows:

- What standards and legal/regulatory frameworks are suggested to reduce security risks?
- In a multi-framework environment, what audit challenges exist when reviewing critical security controls?
- How can a unification strategy address issues with assurance and auditing?

Background

The theory of computing in the "cloud" originated from the term "utility computing," defined by computer scientist John McCarthy in 1961. Leonard Kleinrock, lead researcher for ARPANET (Advanced Research Projects Agency Network), predicted that as computer networks become more sophisticated, "computer utilities" will likely spread, serving individual homes and offices across the country, similar to the current electric and telephone utilities. The concept of ubiquitous computing is becoming a reality in the twenty-first century cloud computing industry. Computing power used to be a scarce and costly resource. A major paradigm shift from computing scarcity to abundance has occurred due to the advent of cloud computing, which has made computing resources abundant and affordable [3]. For many businesses, cloud services are becoming a necessary part of their information technology infrastructure. In the previous 10 years, the cloud computing business has experienced tremendous growth in revenues as well as improved adoption and acceptance of the technology. IT spending in important market categories is expected to increase by 51% in 2025, reaching about $1.8 trillion [24], according to Gartner. According to Moghadasi et al. [4], the cloud computing industry is made up of cloud service providers, brokers, and customers who can take advantage of low-cost, elastic, scalable, global accessibility, flexible billing, manageable metering, easy monitoring, and cost benefits consolidation that led to lower capital and operating expenses. Cloud computing has brought up new cybersecurity issues as well as raised security and privacy concerns. The quantity and complexity of risks and vulnerabilities, including misconfiguration, unauthorized access, data manipulation, data deletion, unsecured APIs, and compliance infractions. As a result, regulatory measures have increased significantly, necessitating unique strategies and techniques to reduce risks [5]. The most significant problem arises when cloud providers apply privacy and security restrictions that are out-of-sync, leaving customers perplexed when it comes to setting up security guidelines and compliance procedures for their businesses. The main components of information security, regardless of whether the technology is used on- or off-site, are availability, confidentiality, integrity, and non-repudiation [6]. As was already indicated, rigorous adherence to compliance standards and the careful use of industry best practices can help protect against hazards in the cloud environment. These elements are essential in maintaining everyone's sense of security. An extensive audit is necessary to determine whether the cloud service complies with security regulations. The purpose of this audit is to confirm compliance with pertinent rules and regulations and assess how well security procedures are working. Essentially, compliance assurance is a powerful way to deal with cloud computing's security issues [7]. According to Carter [8], ISO 19011 defines auditing as an organized procedure rather than just an idea. Regardless of the service or deployment strategy, auditing cloud computing security requires a wide range of knowledge, abilities, and experience. In addition to using auditing standards, the auditor needs to have a thorough awareness of the relevant compliance frameworks that apply to the particular company sector and technology under evaluation [9]. The traditional information security methodology for auditing on-premises infrastructures entails systematic data collection and analysis to identify areas that require extra care and attention. A great deal of experience has been gained by many organizations in auditing many aspects of technology and operations. They frequently keep up-to-date work schedules and audit plans that can be modified to guarantee consistency, dependability, and the best possible audit efficiency. When it comes to cloud security compliance audits and assurance, it is important to understand that regulations have varying standards and auditor demands, including the level of testing required. Take into consideration the differences between different compliance frameworks to demonstrate this argument. For example, PCI DSS prioritizes strong risk management procedures, whereas ISO/IEC 27001 lays more emphasis on protecting cardholder data. However, compared to CSA STAR, FedRAMP—the U.S. government's strict standard for cloud services—imposes more stringent restrictions. Because of this, the precise controls and actions that must be taken may differ based on whether framework is appropriate in a certain situation [10]. Three big players dominate the cloud services market: Google, Microsoft, and Amazon. Amazon claims Amazon Web Services over 77 availability zones throughout 24 geographic locations, and it holds an impressive 33% of the market, while Google Cloud Platform has substantial global coverage across 22 regions and 61 zones. Microsoft Azure is present in over 60 places worldwide. Most countries in the world struggle with a complicated web of state, industry, and governance norms, which can result in legal conflicts internationally

and compliance issues. In essence, compliance is adhering strictly to the laws and regulations that govern in order to enforce rules and policies. As an illustration, banks must abide by PCI DSS requirements in order to protect customers' sensitive credit card information. Every publicly traded corporation in the US is required to abide by SOX, which was created to support efficient internal controls in financial and information technology procedures. In a similar vein, HIPAA protects personal health information. Breaching these restrictions may result in severe consequences such as fines, legal action, and a tarnished image. These laws, which are typically drafted by politicians, are typically complex, broad in scope, and occasionally interpreted differently. Furthermore, the lack of full, independent, and vendor-neutral cloud architectures exacerbates the complexity of achieving compliance [11]. Due to the global reach and the widespread presence of cloud computing services, auditors have a tough time harmonizing compliance duty in the face of diverse frameworks and legislation, according to a study by Kuyoro et al. [18]. The following describes the way the paper is organized: Literature review section explores into a comprehensive overview of the literature that covers the study's background information as well as an analysis of past research on cloud vulnerability management and cloud computing assurance. Section 2 provides a summary of the research initiatives that have been completed. "Research Methodology" section describes the research approach we used to carry out our investigation. The Section on "Analysis of Cloud Computing Architectural Design, Safety Issues, and Regulatory Requirements," models of cloud computing are examined, and a succinct explanation of its fundamental components—virtualization, storage, networking, databases, regulatory compliance, and related security issues—is provided. We go into great detail about the auditing and assurance aspects of cloud computing in the Section. "Discussion and Challenges on Security Issues," along with a suggested methodology based on the previous research. Our research is concluded in final Section. "Conclusion and Future Work," where we provide a summary of the results, address any limits of the study, and suggest possible directions for future investigation.

Literature Review

In this section, we give an overview of relevant reviews and discuss reviews on cloud management research, cloud security research, and cloud computing assurance research.

Introduction

We offer a concise review of research breakthroughs that reflect the advancements in cloud compliance and business operations, so that readers may have a thorough awareness of the changing landscape of cloud security challenges and their alignment with audit practices. The subject of cloud-related audit and assurance is still in its early stages, and cloud computing technology is a relatively new discovery with only a little over a decade of history; therefore, the body of research that is currently available is not very large. As a result, we have done a thorough analysis of theses, research papers, and periodicals from the last 10 to 12 years. This review categorizes cloud computing management, threats and vulnerabilities, implemented controls, and audit aspects to enhance readability, focusing on various aspects of cloud services and their impact on security.

Optimizing Cloud Infrastructure: A Comprehensive Management Approach

Within the dynamic field of cloud computing, enterprises grapple with a multitude of challenges while also reaping significant opportunities. The practice of audit and assurance is pivotal, as it involves the systematic assessment of operations to pinpoint deficiencies and gauge the efficacy of implementation and management [12]. To begin with this strategy, it is critical to first understand the complexities and challenges inherent in the adoption and maintenance of cloud systems. This necessitates a thorough understanding of how huge hardware infrastructures seamlessly combine with sophisticated software applications to ensure continuous operation in the world of automated and on-demand cloud computing services, a topic well-explored by Cook et al. [13]. Forell et al. [14] thoroughly analyzed notable difficulties such as scalability, the existence of numerous abstractions, federation, dynamism, energy efficiency, and failure management. Open-source collaboration becomes essential during the transitional phase of any growing technology, functioning as a spur for subsequent developments. Ismaeel et al. [15] thoroughly compared and explored the design and properties of popular open-source Infrastructure-as-a-Service systems such as Nimbus, Eucalyptus, OpenNebula, CloudStack, and OpenStack revealing insights into their distinguishing characteristics. These platforms are critical in the hard work of creating and managing IT infrastructures that can scale indefinitely. The studies referenced highlight the problems and considerable promise embedded in the cloud computing industry's evolving ecosystem. Niranjanamurthy et al. [16] discuss the concept of a Virtual Private Cloud (VPC) within the AWS framework. A VPC is allocated to an AWS account and operates as an isolated entity within the AWS cloud, maintaining coherence while remaining distinct from other virtual systems. Amazon EC2 is a key component, enabling users to provision scalable computing capacity in the cloud, thereby contributing to

a flexible and dynamic computing environment within the AWS cloud infrastructure.

Security Risks and Threats in Cloud Environments

A collection of scholarly publications provides profound insights into the problems of managing threats and vulnerabilities in cloud computing as well as the compliance frameworks required to ensure cloud security and assurance. In a notable contribution by Los et al. [17], the Cloud Security Alliance methodically identified and categorized the nine significant security vulnerabilities in cloud computing, aptly dubbed "The Notorious Nine." Ahmed et al. [1] went deeper into security threats and problems, doing a detailed classification of these issues. Kuyoro et al. [18] have added to the discussion by undertaking a detailed data analysis that dissects security issues. Another unique viewpoint, offered by Dutta et al. [19], provides the top 10 risk analysis from the perspective of IT experts, offering insight on risk evaluation methodology for each issue. Tissir et al. [20] conduct a semantic literature evaluation that includes cloud models and pertinent cybersecurity frameworks, clarifying ways for managing risks connected with each cloud model. Following an examination of these contributions, it is clear that cloud computing, like any other domain, is not immune to security flaws, by Chiregi and Jafari Navimipour [21]. Denial-of-Service, data loss, data breach, insecure APIs, account hijacking, insufficient diligence, abuse, illicit misuse, hostile insiders, and problems deriving from shared technology are the key security risks. Effective risk management is dependent on the attentive implementation of suitable controls and regular monitoring of cloud environments.

Audit and Assurance

The realms of cloud audit and cloud-based audit represent two distinct dimensions that significantly depart from traditional IT audit practices. Recent challenges and issues in the domain of audit and assurance have garnered attention from a spectrum of authors, manifesting in doctoral theses and research papers. An evidence-based approach to audit, as advocated by Rübsamen [22], underscores the importance of continuous auditing and the diligent adherence to data policies through automated processes. With regard to Industry 4.0, Simetinger [23] sheds light on the imperativeness of security controls at the infrastructure level, the need for specialized skill sets to assess technical compliance, and the myriad challenges associated with audits in Industry 4.0 environments.

Diving into the niche of cloud auditing, Mateescu and Sgârciu [7] present an approach that suggests quantifying, assessing safety levels, comparing assumed and actual risk tolerance, and validating the effective implementation of cloud services. Brumă [24] introduces a groundbreaking framework focusing on the cybersecurity aspect of cloud audits, elucidating the limitations of traditional audit methodologies and propounding a fresh framework designed to address these shortcomings. The idea of conducting audits during the migration process, as proposed by Ismail et al. [25], empowers end-users to evaluate the compliance programs of service providers.

Exploring emerging methodologies and challenges in cloud security auditing, Ryoo et al. [9] analyze adherence to prescribed standards and the requisite customizations within various business models. In a notable endeavor, the doctoral thesis authored by Doelitzscher in 2014 [26] introduces a prototype named "Security-Audit-as-a-Service." This innovation incorporates features such as the detection of changes in cloud infrastructure, integration of cloud audit policy language, and the inclusion of anomaly detection capabilities.

In summary, the state-of-the art works collectively grapple with diverse challenges and proffer numerous frameworks aimed at equipping auditors with the tools to make informed assertions regarding cloud assurance. It is noteworthy that each paper calls for further research to refine approaches for reconciling the complexities of complying with various frameworks.

Gap Analysis

The gaps observed in the literature review reveal that in this research, including a focus on service regulation and provisioning, there is a lack of investigation into cloud ecosystem interactions and insufficient exploration of audit and assurance risks associated with these services. None of the research publications considered for analysis addressed any particular guidelines to follow while conducting assurance activities; instead, most of them concentrated on quantifying, qualifying, and offering a competitive advantage of the cloud services evaluation.

Research Methodology

In the present study, a mixed-methods strategy was used in the current investigation, integrating both qualitative and descriptive methodologies to highlight a challenge in the cloud auditing process. It primarily involves gathering, documenting, characterizing, and evaluating the relevant facts to determine the current level, movement, and state of affairs of a phenomenon. However, it is dependent on qualitative variables, which can vary. To fulfill this research's objectives, a number of strategies and processes were applied [27].

The research design, which comprises a survey of the literature and an analysis of previous efforts in relevant domains, serves as the conceptual framework for doing

research. The plan outlines the approach and methodology of the study that was selected to meet the goals of the research, find credible and legitimate study materials, and provide answers to the research questions. In order to highlight a thorough contextual investigation of fewer occurrences or situations and their interrelationships, the researcher used an exploratory study design.

Figure 1 depicts the steps in the research process, which are as follows:

- Assessment of the cloud environment using scholarly articles in the related field of study.
- Comparison of best techniques and standards of practices with the requirements for implementation in the pertinent domains.
- Examination and evaluation of the best practices identified.
- The discourse pertains to the exhaustive inventory of crucial elements that auditors will carefully examine.

Analysis of Cloud Computing Architectural Design, Safety Issues, and Regulatory Requirements

Cloud computing refers to complex technology that involves various technologies such as virtualization, storage, networking, databases, and compliance with regulatory requirements. Understanding the concept can be confusing; however, an overview of cloud computing models is given in this section, building blocks, and security challenges. It also discusses the auditing and assurance challenges related to cloud computing and proposes a solution accordingly as described by Ataya [28], Elluri, and Joshi [29].

Cloud Computing Roles

Recognizing the different roles of cloud computing aids in comprehending models of cloud services, deployment strategies, security responsibilities, and various cloud computing aspects [27]. A cloud service user might be a company or a particular individual who purchases cloud services.

- The provider of cloud services is an entity, either a business or organization, responsible for delivering cloud services.
- Cloud service consumers incur a fixed rate for services, provided resource utilization or transaction volumes stay within predefined limits.
- A cloud service partner refers to a third-party entity that provides cloud-based services utilizing the infrastructure of the cloud service provider.
- Comparable to brokers in other industries, a cloud service broker assists businesses in meeting their cloud computing needs by offering broker services.

Cloud Computing Characteristics

The ISO/IEC 17789 and NIST 500–292 architectural reference model for cloud computing define five basic characteristics of cloud computing: on-demand/self-service, resource pooling, network access, quick elasticity, and measurable services. Furthermore, ISO/IEC 17788 adds multi-tenancy as a sixth attribute. This comprehensive framework acknowledges shared resources, immediate service availability,

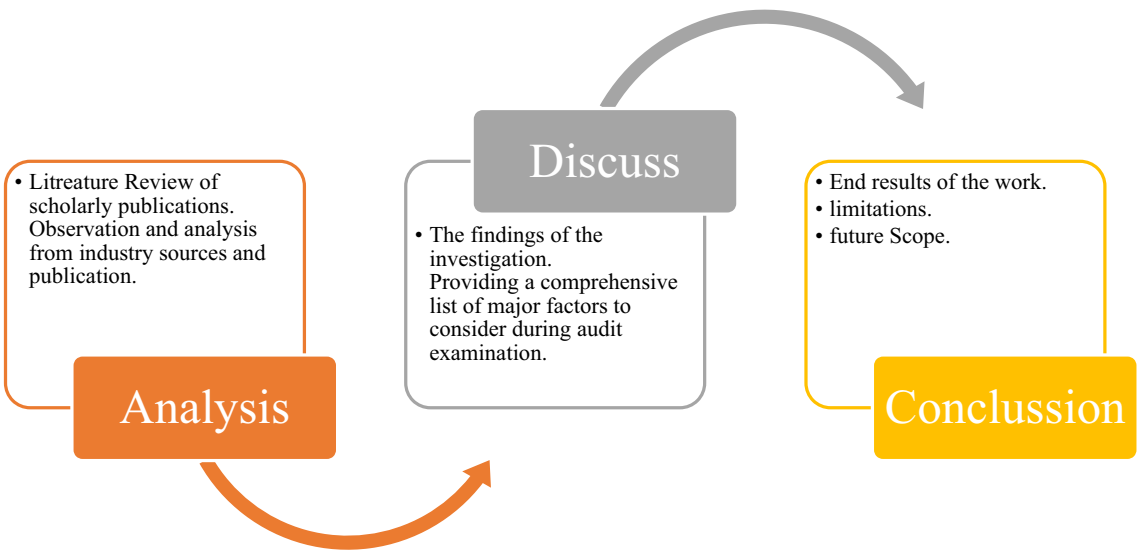

Fig. 1 Research process

Fig. 2 The important characteristics of cloud computing

ubiquitous network access, scalability, measurement of usage, and multi-tenancy, emphasizing the versatility and complexity of cloud deployments. Figure 2 shows the crucial features of cloud computing by Islam et al [30].

Self-Service and On-Demand: Cloud computing offers real-time monitoring of server availability, capacity, and network storage, enabling users to track computer operations in real-time.

Resource Pooling: To allocate computing resources among numerous clients, the cloud service provider uses a multi-tenancy strategy, based on customer demand. Consumers have control over resource location but can choose higher-level abstraction locations.

Measured Service: The cloud service provider uses a measurement and monitoring system to ensure users access only authorized resources and are accurately billed based on usage.

Network Access: Network access refers to the availability of resources over a network without a direct physical connection, often without the network infrastructure being explicitly included in the service offering.

Rapid Elasticity: Allows users to quickly scale-down or raise the amount of resources they take from a common pool—often completely autonomously. They are able to better match resource usage with demand as a result.

Multi-tenancy: A mode of operation where multiple distinct tenants, such as businesses, work together in a common space. In public clouds, this manner of operation is typical. Despite being physically connected, the renters are logically apart from one another.

Cloud Architecture Fundamentals

Cloud computing's structure is well-defined, offering a comprehensive breakdown of its integral components and subcomponents. Its pervasive influence has permeated every facet of modern life, delivering a myriad of advantages, including transformation, storage, collaboration, and sustainability. Cloud-based services and applications [31] such as Google Docs, Skype, and Netflix can be accessed using virtual networks or regular internet connections ensuring seamless user access [32]. The business world is increasingly embracing cloud migration due to the compelling cost-effectiveness it offers, thanks to the substantial storage capacity provided by cloud platforms. The expansive bandwidth within cloud computing architecture empowers users to retrieve cloud-based data from any corner of the globe at any given moment. Furthermore, this architecture promotes sharing, fostering collaboration among client source users and open-source groups, exemplified by industry giants like Microsoft and Red Hat [33].

The cloud computing architecture shown in Fig. 3 consists of two components: the front-end and the back-end.

- **Front-end:** The front-end infrastructure includes everything that an end-user interacts with. Web browsers, web apps, and local networks make up the front-end cloud architecture.
- **Back-end:** The front-end architecture is made possible by the cloud back-end architecture. It is located on a distant server and is made up of hardware and storage. The provider of cloud service is responsible for and oversees this back-end cloud architecture. The main elements of back-end cloud architecture are storage, security, application, management, and service.

Cloud Architectural Design Concepts

The APIs are used by controllers to access pools of computing, network, and storage resources developed, managed, and provided by the service provider [34].

Cloud Computing Service Model

The cloud services depicted in Fig. 4 are commonly categorized into three general models: Infrastructure-as-a-Service, Platform-as-a-Service, and Software-as-a-Service.

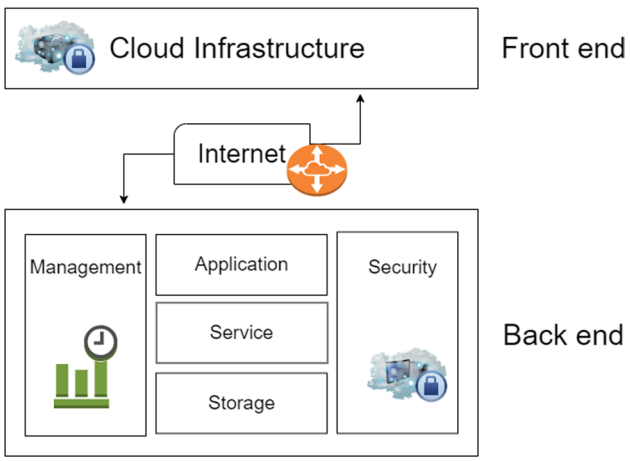

Fig. 3 Front-end and back-end architectures in cloud computing

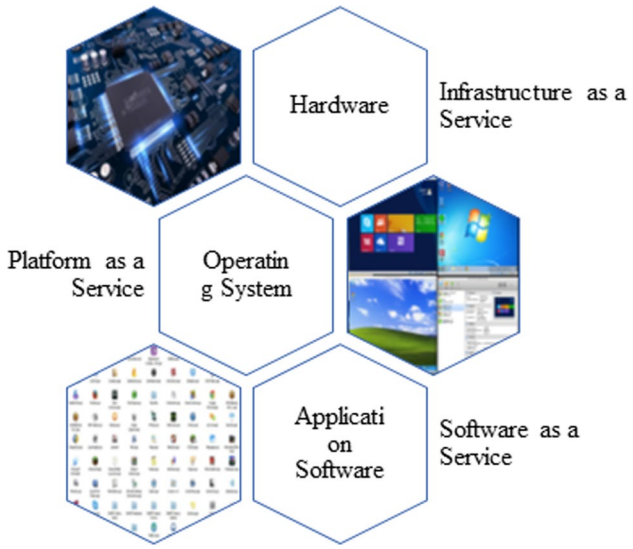

Fig. 4 Showing cloud computing service model

Infrastructure-as-a-Service With Infrastructure-as-a-Service (IaaS), users can install software on managed hardware that is linked to their network. The client is in charge of logical resources like software, while the provider oversees the data center.

Platform-as-a-Service PaaS, also known as Platform-as-a-Service, is a cloud computing model that eliminates the overhead of building and maintaining servers by giving users the environments and tools they need to develop, run, and manage their own applications.

Software-as-a-Service (SaaS) Large organizations can process data on a production setting by renting turnkey applications from suppliers using the SaaS paradigm. However, there are a lot of risks that cloud services have to deal with, like phishing, malware injections, insider threats, and non-compliance with regulations. Shared responsibility serves as the basis for liability for breaches, by Kumar et al. in 2019.

Cloud Computing Deployment Model

Figure 5 shows the deployment model for cloud computing, which includes public, private, hybrid, and communal deployment strategies recognized by NIST and ISO/IEC, by Mitchell [35].

Logical Model

A conceptual model of cloud computing has been demonstrated by the Cloud Security Alliance. It provides four tiers of functionality and associated security standards, and during the implementation, the concept is adhered by both cloud and traditional cloud computing models. The functionalities and security concerns of the logical model are shown in Table 1, by Okour [36], Olajide [37], Piazza, and associates [38].

- Processing, storage, and networking are handled by the infrastructure layer, which is the central part of a cloud computing system.
- Within a virtual environment, the infrastructure layer interacts with various logical layers while being configured and maintained by the metastructure layer.

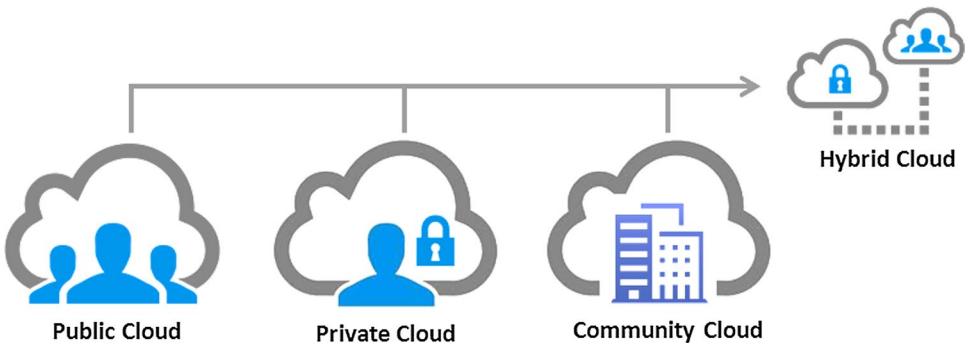

Fig. 5 Showing cloud computing deployment model

Table 1 Logical model functionalities and security concerns

Functionality	Security concern
Infrastructure layer	Ensuring the integrity of the underlying hardware and software
Metastructure layer	Protecting the integrity and isolation of virtual machines
Infostructure layer	Associated with data security
Applistructure layer	Encompass application and operating system security

- The infostructure layer is responsible for handling information storage, access, and management in the data management stack.
- Applications and operating systems are installed at the logical layer known as the application infrastructure.

Shared Responsibility Concept

The shared responsibility model shown in Fig. 6 in cloud computing shifts responsibility from the customer to the service provider, transitioning from infrastructure to Software-as-a-Service, Pugh and Hilley [39]. The data owner owns information but has no control over its handling. The client is responsible for securing data but cannot enforce fundamental protections, by Reid and Miller [40].

Software-as-a-Service: A turnkey application is accessible through the Software-as-a-Service concept. In this case, the application and all of its supporting infrastructure, including physical security, are the provider's responsibility.

Platform-as-a-Service: The cloud service providers often have a thin line between their responsibilities and customer responsibilities, with customers installing applications on their operating systems.

Infrastructure-as-a-Service: An inverted shift of responsibility exists in cloud computing. The cloud service provider maintains physical security and manages the systems of the facility; on the other hand, the cloud customer installs the operating system. The shared responsibility matrix displayed in Table 2 helps to understand this transition, by Eftimie and Racuciu [41].

Cloud Security Architecture

The hardware and software required to safeguard the workloads, systems, and data on cloud platforms are included in cloud security architecture. Planning and design should be the first steps in developing a strategy for cloud security architecture, which should then be integrated into cloud platforms from the bottom-up. All too often, cloud architects try to integrate security last and prioritize performance first, by Rizwan Ahmad [42].

The Significance of Cloud Security Architecture

Cloud computing provides increased agility, performance, and the effectiveness of costs, enabling businesses to respond quickly to market shifts and make data-driven decisions. However, it can also expose businesses and their data to risks. A cloud security architecture, or "security architecture for cloud computing," is crucial for businesses to utilize cloud services while reducing risk and susceptibility to attack. Identity and access management, defense mechanisms, auditing of compliance, and security principles are all integrated into the development and operation of cloud services by the architecture.

Threats to the Cloud Security Architecture

When designing their cloud implementation, customers should be prepared for common threats such as malware and privilege-based attacks. Instead of listing all the

Fig. 6 Showing shared responsibility model

Table 2 Shared responsibility matrix

Responsibility	On-prem.	IaaS	PaaS	SaaS
Classification of data and responsibility risk	Client	Client	Client	Client
Risk due to user and endpoint	Client	Client	Client	Client
Risk due to authentication and access	Client	Client	Client	Client
Application threat	Client	Client	Shared	SP
Network threat	Client	Client	Shared	SP
Threat due to host	Client	Client	SP	SP
Threat due to infrastructure	Client	SP	SP	SP

SP Service Provider

common hazards, this article will provide a brief summary of the top issues that business executives are currently thinking about, by Subashini and Kavitha [43].

- Insider risks include cloud service providers' administrators and employees with access to systems and data. Users entrust their data to these employees, while governmental bodies can access data through subpoenas or other legal procedures. Security professionals focus on these factors.
- DoS attacks, both temporary and permanent, are a significant concern. Temporary attacks bombard systems with repetitive requests, while permanent attacks cause firmware damage, preventing server booting. Security perimeters use network compliance standards and redirect traffic to alternative resources.
- "Cloud edge" refers to server architecture beyond direct control of a cloud service provider, extending services to remote or rural areas, posing hardware integrity and physical attack defense challenges.
- Consumer control affects how consumers evaluate public cloud services. Users are worried about moving sensitive workloads to public clouds from a customer perspective. Major cloud providers typically have more resources and expertise in cloud security than average private cloud companies. Generally, clients find it reassuring to have total control over their most sensitive data, even if their security methods are not as sophisticated.
- The most sophisticated cloud security architecture in the world will not let a user create a better password because of hardware limitations. One among the most prominent attack vectors is passwords. While cloud security architects are focusing on software, firmware, and hardware security, average users will still be responsible for the following recommended practices.

Cloud Architecture Security Breach Incidents

All such famous incidences are explained as in Racuciu et al. [41] and Schubert et al. [44].

Yahoo

Yahoo's 2013 data breach, initially reported to involve one billion compromised accounts, was later revealed to have exceeded three billion. The breach, originating from a spear-phishing email in 2014, led to four charges against two individuals suspected of spying for Russia, underscoring the complexity of cyber threats and urging increased digital security measures.

Alibaba

In November 2019, a hacker infiltrated Alibaba's Taobao, stealing user information like IDs and customer reviews. Alibaba took swift action, notifying law enforcement, highlighting the importance of heightened system and network monitoring to detect and thwart potential cyber threats. This incident underscores the critical role of cybersecurity in safeguarding user data and digital platforms.

LinkedIn

LinkedIn experienced a data scraping attack in 2021, affecting 700 million profiles. The stolen data, including social network details, email addresses, phone numbers, geolocation information, and genders, were posted on a Dark Web forum. LinkedIn claimed no confidential information was compromised but argued it violated its terms of service. The incident highlighted potential data security risks on social media platforms.

Sina Weibo

China's largest social media site, Sina Weibo, has reported a data breach in June 2020, compromising 172 million users' personal information. The hacker sold the data for $250, likely due to lack of passwords. Weibo, a platform rarely sharing uncensored national news, is closely monitored and regulated, putting anonymous users at significant risk.

Facebook

Facebook experienced a data breach in April 2021, revealing personal information, including IDs, account names, and phone numbers. Despite the breach, Facebook claims to have fixed it immediately. Subsequently, Mark Zuckerberg was asked to make an appearance before federal officials to discuss the issue related to private matter with the Federal Trade Commission.

Marriott Corporation

In September 2018, an attack exposed over 500,000 Starwood visitors' personal information. Marriott discovered the network had been compromised before its acquisition in 2014, likely due to outdated hardware. While the organization did not face closure, the incident resulted in significant reputational damage, posing challenges for restoration.

Accenture

Accenture, a leading cybersecurity startup, revealed in its Cyber Risk Report that in 2017, it accidentally exposed

137 GB of data in AWS S3 storage buckets, leading to cybercriminals exploiting it for defamation and extortion. In August 2021, Accenture was targeted by another LockBit ransomware attack, causing a series of client system breaches and demanding a $50 million payment. The accusations were refuted in September.

Verizon

Verizon experienced a data breach in 2017 when NICE Systems exposed customers' protected health information. In 2020, the company detected 29,207 security events, with 5,200 confirmed as breaches. DDoS attacks were orchestrated through social engineering and client-side web application viruses. The pandemic's shift to remote work increased cyberattacks. In 2021, Verizon identified unauthorized credentials in 61% of attacks, with phishing incidents increasing from 25% to 36%.

Cognyte

In May 2021, Cognyte, a cybersecurity analytics company, failed to implement authentication protocols, exposing five billion user records and allowing online thieves to access their database. The exposed data included user credentials, email addresses, passwords, and vulnerability data points. The incident highlighted the vulnerability of attackers to even the smallest faults, emphasizing the importance of prioritizing attack prevention strategies over mitigation techniques. Cognyte secured the data within four days, highlighting the need for cybersecurity organizations to prioritize prevention over mitigation.

Raychat

Iranian chat application Raychat has defended itself against a cyberattack that exposed 267 million user data, including usernames, emails, passwords, and encrypted chats. The breach was caused by a bot attack linked to a MongoDB misconfiguration. Despite paying a ransom, there was no assurance that the stolen data would not be disclosed or sold on illicit platforms. The situation persists, with Iranian hackers consistently targeting civilians in ongoing cyberattacks, posing continuous security concerns.

Common Errors Made by Security Architects in Cloud Design

- Excessive distribution in cloud architectures can lead to poor dependability and delay. Deploying platforms across different clouds and easily connecting them can exacerbate this issue. To ensure good building practices, processing and data storage placement should be based on proximity to the same applications and data repositories, typically within the same cloud or on the same platform.
- In the era of cloud computing, security is paramount as it permeates the application, data stores, platform, and hosting cloud. A cloud project may produce subpar security solutions, posing significant security risks for applications and data storage. Careful security is required at every stage.
- Apps have not been made to adapt to changes over the last 20 years, which has resulted in modernization and expenses. According to service-oriented architecture (SOA), making changes now will pay dividends later. Virtual networks and ordinary internet connections are two ways to access cloud-based services and apps like Netflix, Skype, and Google Docs.

Cloud Computing: Governance, Risk, and Compliance (GRC)

Both risk management and governance are extensive topics of research. This discussion emphasizes how these changes happen within the framework of cloud computing; it is not intended to be, nor should it be, a comprehensive examination of those subjects outside of the cloud computing environment [43].

The important aspects that the cloud computing has an impact are

- Governance
- Information security
- Enterprise risk management
- Information risk management

Conflicting International Legislation

Cloud technologies could allow people to connect from anywhere in the world. In order to provide redundancy and closer service delivery, many clients want to use cloud services globally, while this can also be done on a lesser scale. Nonetheless, this raises the problem of different legal frameworks in different countries. For example, data privacy in the EU is governed by the General Data Protection Regulation.

Regulations and Laws that Affect Cloud Computing

In order to ensure compliance with all applicable requirements, cloud audit professionals should be aware of these potential challenges and seek advice from skilled legal counsel.

- The Organization for Economic Cooperation and Development
- Asia Pacific Economic Cooperation Privacy Framework

- General Data Protection Regulation
- Additional Legal Controls

Regulations and Laws Governing Cloud Computing

Since the cloud is always evolving, it is essential to keep an eye on legal requirements and make sure of compliance. Some common conditions for contractual compliance are as follows:

- **CLOUD SECURITY ALLIANCE'S CLOUD CONTROLS MATRIX (CCM):** A framework providing a set of security controls to help organizations assess and improve their cloud security posture.
- **FINRA (FINANCIAL INDUSTRY REGULATORY AUTHORITY) regulations:** Specifically designed for financial data security; these regulations establish guidelines and requirements for ensuring the security of financial information within cloud environments.
- **SERVICE ORGANIZATION CONTROLS (SOC) standards:** A series of standards and reports developed by the American Institute of CPAs (AICPA) that assess and assure the reliability of service organizations' internal controls.
- **GENERALLY ACCEPTED PRIVACY PRINCIPLES (GAPP):** A set of principles that guide organizations in managing and safeguarding privacy, ensuring compliance with privacy regulations and standards.
- **PAYMENT CARD INDUSTRY DATA SECURITY STANDARD (PCI DSS):** A security standard designed to ensure the protection of sensitive payment card information during storage, processing, and transmission.
- **CENTER FOR INTERNET SECURITY'S CRITICAL SECURITY CONTROLS (CSC):** A set of security best practices aimed at helping organizations enhance their cybersecurity defenses and resilience.

These guidelines evaluate the organizations' and cloud service providers' security posture, guaranteeing the accuracy of financial data stored in the cloud. Compliance with these standards is often required for cloud service providers, while the GAPP provides a framework for managing and protecting personal information. By adhering to these frameworks and standards, organizations can ensure a secure and legally compliant cloud computing environment.

Service-Level Agreement (SLA)

The service-level agreement (SLA) is a mutually agreed-upon performance guarantee between the end-user and the provider of cloud services. Every cloud computing service-level agreement was negotiated directly between a customer and the service user. Until a client becomes a substantial consumer of cloud services, most SLAs are standardized when huge utility-like cloud computing providers appear.

- Customer-based SLA
- Service-based SLA
- Multi-level SLA

Legislation for Cloud Professionals that is frequently referred to…

- The 1996 Health Insurance Portability and Accountability Act
- The Gramm–Leach–Bliley Act (GLBA) of 1999
- The Stored Communication Act of 1986
- The California Consumer Privacy Act of 2018
- Sarbanes–Oxley Act

Cloud Data Security Challenges and Strategy

Data at rest face consistent threats, regardless of their storage location, which can compromise the security triad (Confidentiality, Integrity, and Availability). Unauthorized access threatens confidentiality, whereas unauthorized changes threaten data integrity. Furthermore, the loss of storage devices might cause data availability to be disrupted. Significant risks include virus, ransomware, improper data disposal, jurisdictional complexity, unauthorized provisioning, regulatory non-compliance, Denial-of-Service, data corruption, theft, or loss of media. These threats emphasize the need for comprehensive data security strategies.

Need for Encryption

Securing data created remotely is of utmost importance, particularly in guarding against man-in-the-middle attacks. To mitigate this risk, it is imperative to perform data encryption before uploading it to cloud. Implementing a robust key management system, aligned with FIPS 140-2's approved cryptographic solutions, is vital. Similarly, data generated through remote manipulation should be encrypted right from their inception to thwart unauthorized access. Adhering to industry best practices for key management is highly recommended. Encryption plays a pivotal role in safeguarding data in storage, in transfer, and in operation.

Encryption functions as a shield in the remote user terminal environment, providing secure communication within the cloud consumer's enterprise and preventing inadvertent access to others' data within the cloud provider's data center. The importance of encryption cannot be overstated, as it forms the cornerstone of secure cloud usage. In this discussion, we will delve into two specific aspects of cloud encryption: key management and

a cutting-edge encryption technique that could bring in a new era of cloud security and trust.

Key Security

Encryption keys, which serve as the vital numerical codes for encryption and decryption, must be shielded with a level of protection equal to or greater than the data they safeguard. This stringent safeguarding is a stipulation of the organization's data security regulations, driven by the sensitivity of the data at hand. It is crucial to emphasize that the efficacy of any cryptographic system hinges on the absolute secrecy of these keys.

Key management encompasses several critical aspects:

- **Key Recovery**: Retrieving a user's key should be a formidable challenge for anyone other than the authorized user. However, there are instances in which a company would want access to a user's key, perhaps due to employee termination or lost keys. In such cases, a well-defined technology and procedure for key retrieval should exist, typically involving multiple individuals.
- **Key Distribution**: Securely distributing the keys in a cryptosystem environment can be intricate and precarious. Establishing a secure session without a key in advance can be a challenge. While out-of-band key distribution is a common approach, it can be labor-intensive and costly. Further, the keys must be encrypted while transmitting.
- **Key Revocation**: Organizations require a robust mechanism in order to suspend or revoke cryptographic keys, especially when user access to sensitive information needs termination or a key's security is compromised. This ensures unauthorized access is curtailed, protecting the confidentiality and integrity of sensitive data.
- **Key Escrow**: Maintaining duplicate copies of keys in secure locations, held by a reliable third party, is often advantageous. This practice can aid in various key management processes.
- **Outsourcing Key Management**: Cloud computing typically demands that keys be stored separately from the data center. One approach is for the cloud client to manage keys themselves, necessitating expensive infrastructure and specialized personnel. An alternative is to enlist the services of CASB (Cloud Access Security Broker). CASBs are third-party suppliers that provide cloud customers with identity and access management (IAM) and services of key management. The cost-effectiveness and expertise of CASBs make them a compelling choice, surpassing the challenges of in-house key management.

Hashing

It is a procedure that uses hash functions, which are cryptographic methods, to accept any length of data as input and produce a unique hash result. The main purpose of it is to carry out data integrity checks. After an action, the hashes of the two files are compared to look for changes or corruption in the data. In the cloud, hashing can provide several kinds of security services:

- Check the accuracy of data backups
- Confirm the accuracy of email correspondence
- Assist in identifying system compromises
- Monitor file integrity

Furthermore, it is critical to select a collision-resistant (two functions providing the identical hashes) hash function. SHA-3 is currently the industry standard.

Discussion and Challenges on Security Issues

This section discusses the audit approach, which enables audit experts to investigate security measures, determine compliance requirements, and provide feedback to stakeholders.

Introduction

The paramount advantage of conducting an audit lies in its ability to instill confidence in stakeholders regarding an organization's ethical, financial, and operational well-being. Audits serve this purpose by focusing on the information and systems that form the cornerstone of competitive advantage for most companies and public institutions, as highlighted by Wang et al. [45]. Audits, formal evaluations and examinations of cloud information systems, seek to evaluate their adherence to a particular criterion, such as but not confined to the regulations, laws, and industry norms that are now in existence and are followed by information systems based on cloud computing.

- Compliance with the current rules, regulations, and industry guidelines governing information systems based on cloud computing.
- Adherence of cloud information systems and their associated regulations to governance norms, encompassing relevant regulations and procedures.
- Maintenance of cloud-based data and information storage with the requisite layers of privacy while maintaining integrity and accessibility.
- Ensuring the efficient execution of cloud computing operations, meeting established effectiveness targets.

Viewpoint of this Discussion

Auditing is a process that involves carefully examining and reviewing an entity's processes and procedures to make sure they are accurate, reliable, legitimate, and comprehensive. However, in general, auditing may not be well understood or its relationship to an organization. Over time, it has evolved into a procedure that all businesses need to adhere to in order to meet regulations. When the term "cloud audit" is used, there is a contrast between auditing the cloud and auditing within the cloud.

Understanding the Process, Methodology, and Implementations of Unified Cloud Audits

Everyone finds an audit to be uncomfortable. However, when it involves something as sensitive and private as a person's data or work practices, this can be a laborious procedure, and if the user is careless, they may easily miss something important, even more so in a cloud environment, where upholding compliance poses a special set of challenges. Pros in the cloud computing sector can benefit from this strategy. This strategy incorporates applicable compliance requirements, best practice suggestions, and more.

Audit types are

- Internal audit
- External audit
- Certification/Attestation audit done by a third party
- Governance and Strategy audits
- Configuration and Activity Monitoring
- Access Review
- Compliance and Controls audits

Development of a Cloud Assurance Program

The process of creating a cloud assurance involves three steps in a unified strategy, by Wu et al. [46]. Figure 7 shows the same.

Design an Assurance Program

- **Delineate Stakeholder Roles and Responsibilities**: Establish clarity in the roles and responsibilities of relevant stakeholders. This includes designating a supervisory position responsible for the program's overall success and a program operations role tasked with day-to-day management.
- **Identify and Assess Cloud-Related Risks**: Catalog the potential cloud-related risks an organization anticipates and evaluate the specific cloud service in question. This evaluation should include an analysis of risk likelihood, impact, and tolerance levels.
- **Authorize the Program**: The authorization process should encompass the approval of new services, addressing unique risk scenarios, approving architectural designs, controls, and tools, as well as granting exceptions where necessary.
- **Define Monitoring and Feedback Mechanisms**: Plan how the program will be monitored and how feedback will be received. Monitoring can occur regularly, at predetermined intervals, or in a continuous manner, with flexibility to adapt during the design phase. Continuous improvement and feedback should be fundamental components of a risk-based approach and governance process including continuing monitoring.

Fig. 7 Cloud assurance program

Development of the Assurance Program

- **Develop a Comprehensive Data Classification Program**: Implementing a well-defined data classification program is a foundational pillar of effective risk management. It plays a critical role in guiding the risk management process. When classifying data, it is crucial to account for the data's entire life cycle and remain adaptable to potential changes in data definitions. Evolving laws, regulations, standards, and technologies can alter how datasets are defined in future.
- **Define CSP Needs and Services**: The data classification will often lead to distinct requirements for different groups. This is the juncture to enhance compliance. Third-party certifications and attestations should be used in accordance with international norms. Sensitive information, for example, should only be handed to CSPs who have received third-party evaluations that fulfill high control standards, such as those defined in SOC 2. Each CSP and its services should be thoroughly evaluated since different services, even within the same CSP, may exhibit varying security characteristics.
- **Identify Applicable Laws, Regulations, and Standards**: Determining the legal, regulatory, and standards framework that pertains to various data types depends on several factors. These include data classification (e.g., personal data, business data, or financial data), CSP jurisdiction, industry sector, and the jurisdiction of the cloud customer. Careful consideration of these elements is critical to ensuring compliance and data security in the cloud.

Implement the Assurance Program

In the context of cloud migration, consider the following key steps:

- **Map and Classify Data**: Begin by mapping and classifying data relevant to the migration. This process involves identifying data owners, stewards, administrators, and user categories. Data owners and stewards, often from a business background, are responsible for data governance. Administrators, typically from a technical background, handle tasks like backup and monitoring. Mapping user categories helps determine different access levels to data and services.
- **Define Relevant Processes, Functions, and Systems**: It is critical to identify the processes, functions, and systems that will be involved in the migration. Beyond data, this includes defining data access systems as well as the processes and tasks required for data upgrades, backups, and access controls.
- **Evaluate Sensitivity and Criticality**: Assessing the sensitivity and criticality of cloud applications is a foundational step in ensuring their security and resilience. Various factors, including vulnerability to confidentiality and integrity threats as well as the importance of application availability, must be considered. Additionally, the General Data Protection Regulation (GDPR) emphasizes resilience within the CIA triad, further underlining the need for applications to perform effectively under adverse conditions. The selection of the cloud delivery service level and deployment style should be carefully aligned with the specific requirements and characteristics of each workload, taking into account the organization's overall cloud strategy.
- **Implement Security Requirements and Risk Assessment Processes**: Following an analysis of application sensitivity, technical attributes, and pertinent regulations, organizations should initiate processes for security requirements and risk assessment. This entails the development of security architecture, the implementation of mitigation measures, and addressing specialized security needs to safeguard the migration process effectively.

The Auditing Standards in the Cloud Environment

The auditing criteria for cloud computing under this technique are as follows:

- Conformity Evaluation in accordance with ISO/IEC 17021–1:2015
- ISO/IEC 27006:2015—International Standard for Information Technology—Security Techniques
- ISO 19011:2018—Auditing Management Systems Guidelines
- ISO/IEC 27007:2020—Information and Privacy Protection, as well as Information and Computer Security and Privacy
- ISO/IEC 27701—Security Methodologies
- Information Technology in accordance with ISO/IEC 27018
- International Institute of Internal Auditors (IIA)—Professional Practice Standards

Audit Execution

The most important part of this paper is the audit execution approach suggested, where the key considerations required to be verified by an audit professional are suggested pertaining to every aspect that is analyzed in the previous section in accordance with the standards and regulations**.** The auditor looks at several factors when deciding what kind, when, and how the auditing processes will be conducted during an audit of an entity's cloud environment. The following

section provides audit professionals with guidance regarding the unified approach, which takes into account universally accepted auditing standards.

- Cloud Service and Scoping
- Access Management
- Data Security
- Network
- User Device Management
- Configuration Management
- Vulnerability Management
- Monitor and Logging
- Business Continuity and Contingency Planning
- Governance Risk and Personnel

By following this audit considerations list, an audit professional can cover all the relevant aspects of cloud audit and assurance. Hence, it is called a "unified approach." For detailed discussion, refer to this part of the main report by Weir et al. [47].

GAP Analysis

The audit results ought to indicate the domains in which the business currently complies and those in which it does not. The gap analysis examines the differences in areas where the organization still does not adhere to the given guideline or norm. The goal of the gap analysis is to assist in figuring out how to get to the intended outcome, which is complete compliance.

Best practices state that auditors should generally avoid offering detailed suggestions on how to resolve gaps. In order to achieve compliance, they should not recommend any specific tools, programs, or goods since doing so can put the auditors in a conflict of interest and lessen their objectivity. Furthermore, rather than having the impacted departments within the organization participate in this analysis, externals to the target departments should conduct the analysis so they may offer unbiased opinions and answers. Depending on the industry, gap studies can be conducted against a wide variety of frameworks. For instance, ISO/IEC 27001 is a typical framework in information security. The NIST cybersecurity framework is another often-used benchmark in cybersecurity.

Performing a gap analysis typically involves six essential steps:

- **Define the Analysis Need and Gain Management Approval**: Begin by articulating the significance of the research and securing approval from management.
- **Outline Scope, Objectives, and Relevant Frameworks**: Clearly define the scope and objectives of the analysis while also identifying the pertinent frameworks and benchmarks that will guide the assessment.
- **Assess the Current State**: Investigate and understand the current scenario of the department or area under analysis. This entails research and employee interviews to gain insights into existing practices.
- **Review Evidence and Documentation**: Scrutinize available evidence and supporting documentation, validating statements and data to ensure accuracy and reliability.
- **Identify Gaps**: Identify disparities between the established framework or standards and the actual state of affairs. These gaps highlight potential risks and areas for improvement within the organization.
- **Prepare and Approve Findings**: Compile the analysis findings into a comprehensive report. Present this report to company leaders for their review and approval, ensuring that the insights and recommendations are acknowledged and acted upon.

Conclusion and Future Work

This section outlines research findings while acknowledging the limitations of the research and identifies areas for future investigation.

Achievements in the Field of Research

Concerns over the absence of a security audit plan are developing among companies that entrust a CSP with their information assets. Organizations are becoming more concerned about the transparency offered by cloud services, which also undermines user confidence, which is why cloud security audits are becoming more and more important. A feasible solution that gives organizations systematic access into cloud activities and allows them to closely monitor and look into how important requirements are being met is needed. This article presents a single approach to facilitate security audit completion and perhaps boost business confidence and compliance with cloud service usage. It is hoped that the proposed strategy, methodology, and this assisting tool will significantly progress the current state and area of cloud computing auditing. These days, a company's profitability and information security may be its two most important considerations. These days, finding the best balance between the amount of money spent on security features and their profitability is crucial since they are interdependent and have a direct impact on each other. To guarantee that adopting IT programs contributes the most business value possible, businesses need to have a strong audit procedure that can assess the maturity of the IT strategy, the profitability rate, and the safety of the implemented IT solution. By integrating governance and operational criteria with compliance concerns,

a comprehensive evaluation of cloud systems that evaluates the cloud's overall safety from both operational and compliance standpoint may be provided. This approach provides the following benefits and developments:

- Determines the level of safety by utilizing security measures and controls in an inventive audit method grounded in a sensible and experienced approach.
- Ascertains the level of adherence to the standards that functioned as the main point of reference for the audit framework. Based on considerations, the traditional technique is modified to create the strategy for cloud infrastructures.
- Offers a useful method for carrying out intricate assessments that highlight the advantages and disadvantages of the company.
- Offers decision assistance for possible cloud adoption by assessing the entire range of internal mechanisms, controls, processes, and procedures put in place to ensure an efficient governance and management process, as well as the maturity and adaptability of the company.
- By using an international standard as a reference model, the audit process incorporates the best practices, guiding principles, and sensible recommendations. By using an established framework for the initial implementation-level assessment, we are able to benefit from all the features of a framework that has been proven valuable via experience.

Users may draw the conclusion that this strategy helps the company to obtain visibility on its own IT ecosystem by evaluating the governance, management, and operations maturity levels utilizing a holistic approach.

Research Limitations

While the objectives of the study program were met, a number of decisions had to be made that limited the effort. The main constraints of the research are summarized as follows:

- **Level of Auditor Control:** To the degree that the auditee is capable of responding, the auditor may alter the audit questionnaire. Given limited resources to acquire audit evidence, an auditor may be put off by the constraints caused by this approach because it essentially cedes control over an important component of evidence gathering and depends only on the auditee's cooperation.
- **Technical Constraints:** Given that the auditor has the most extensive knowledge of the fundamental configurations required for conducting an audit, it is logical to use this approach, assuming a basic level of technical proficiency in the runtime environment before beginning a fully developed audit assignment.
- **Reporting Limitation:** To sum up, the recommended method is deficient in systematic processes to create the required reporting pattern that is widely accepted to consider the unification of presenting under numerous laws and regulations.

Recommendations for Future Work

Numerous avenues for cloud security audit research have become possible as a result of this study. It is imperative to delineate the trajectory of forthcoming research and plausible remedies for some constraints mentioned earlier. Future research should focus on evaluating intelligent audit assessment and global reporting framework. The worldwide reporting strategy will also cover the process, ensuring that every audit activity is completed accurately and consistently and reducing the chance of human mistake in the interpretation of audit results. It should be mentioned that when reliability increases, organizations will accept the global security reporting technique more extensively.

Acknowledgments The authors would like to thank PSOM Technologies Private Limited, Bengaluru, India, the Department of Electronics and Communication and Engineering, A J Institute of Engineering and Technology, Department of Computer Science and Engineering, NMAMIT NITTE, and Upgrad Education Private Limited, Nishuvi, 75, Dr. Annie Besant Road, Worli, Mumbai, for the support for carrying out the research work

Funding No funding.

Availability of Data and Material No such data were used.

Declarations

Conflicts of Interest/Competing Interests The authors declare that they have no conflicts of interest.

Consent for Publication Authors give consent for publication in the journal.

References

1. H.A.S. Ahmed, M.H. Ali, L.M. Kadhum, M.F. Zolkipli, Y.A. Alsariera, A review of challenges and security risks of cloud computing. J. Telecommun. Electron. Comput. Eng. **9**(1–2), 87–91 (2017)
2. A.R. Alobaidi, Z.N. Nuimi, Cloud computing security based on OWASP. 2022 5th International Conference on Computing and Informatics (ICCI) (2022), p. 22–28
3. M. Anisetti, C.A. Ardagna, E. Damiani, F. Gaudenzi, A security benchmark for openstack. 2017 IEEE 10th International Conference on Cloud Computing (CLOUD) (2017), p. 294–301

4. M. Moghadasi, S. Majid, G. Fazekas, Cloud computing auditing roadmap and process. Int. J. Adv. Comput. Sci. Appl. **9** (2018). https://doi.org/10.14569/IJACSA.2018.091265
5. R. Kumar, R. Goyal, On cloud security requirements, threats, vulnerabilities and countermeasures: a survey. Comput. Sci. Rev. **33**, 1–48 (2019). https://doi.org/10.1016/j.cosrev.2019.05.002
6. U.M. Ismail, S. Islam, A unified framework for cloud security transparency and audit. J. Inf. Secur. Appl. **54**, 102594 (2020)
7. G. Mateescu, V. Sgârciu, Cloud computing audit. Sci. Bull. UPB Ser. C: Electr. Eng. **77**(3) (2015)
8. N. Carter, *Auditing the ISO 19011 Way* (BSI British Standards Institution, 2003)
9. J. Ryoo, S. Rizvi, W. Aiken, J. Kissell, Cloud security auditing: challenges and emerging approaches. IEEE Secur. Priv. **12**(6), 68–74 (2014). https://doi.org/10.1109/MSP.2013.132
10. X. Kontargyris, *IT Laws in the Era of Cloud-Computing: A Comparative Analysis between EU and US Law on the Case Study of Data Protection and Privacy (Nomos)* (Schriften der Albrecht Mendelssohn Bartholdy Graduate School of Law, 2018)
11. D. Yimam, E.B. Fernandez, A survey of compliance issues in cloud computing. J. Internet Serv. Appl. **7**(1), 1–12 (2016)
12. S. Karkosková, Towards cloud computing management model based on ITIL processes. in *Proceedings of the 2nd International Conference on Business and Information Management* (2018)
13. N. Cook, D. Milojicic, V. Talwar, Cloud management. J. Internet Serv. Appl. **3**(1), 67–75 (2012)
14. T. Forell, D. Milojicic, V. Talwar, Cloud management: challenges and opportunities. 2011 IEEE International Symposium on Parallel and Distributed Processing Workshops and Phd Forum (2011), p. 881–889
15. S. Ismaeel, A. Miri, D. Chourishi, S.M.R. Dibaj, Open source cloud management platforms: a review. 2015 IEEE 2nd International Conference on Cyber Security and Cloud Computing (2015), p. 470–475
16. M. Niranjanamurthy, M.P. Amulya, N.M. Niveditha, P. Dayananda, Creating a custom virtual private cloud and launch an Elastic Compute Cloud (EC2) instance in your virtual private cloud. J. Comput. Theor. Nanosci. (American Scientific publishers), **17**(15), 4565–4570 (2020). https://doi.org/10.1166/jctn.2020.9106
17. R. Los, D. Shackleford, B. Sullivan, The notorious nine cloud computing top threats in 2013. Cloud Secur. Alliance, **2** (2013)
18. S.O. Kuyoro, F. Ibikunle, O. Awodele, Cloud computing security issues and challenges. Int. J. Comput. Netw. **3**(5), 247–255 (2011)
19. A. Dutta, G.C.A. Peng, A. Choudhary, Risks in enterprise cloud computing: the perspective of IT experts. J. Comput. Inf. Syst. **53**(4), 39–48 (2013)
20. N. Tissir, S. el Kafhali, N. Aboutabit, Cybersecurity management in cloud computing: semantic literature review and conceptual framework proposal. J. Reliab. Intell. Environ. **7**(2), 69–84 (2021)
21. M. Chiregi, N. Jafari Navimipour, Cloud computing and trust evaluation: a systematic literature review of the state-of-the-art mechanisms. J. Electr. Syst. Inf. Technol. (2018)
22. T. Rübsamen, Evidence-Based Accountability Audits for Cloud Computing. (Doctoral Dissertation, University of Plymouth, 2016)
23. F. Simetinger, Audit and assurance specifics in cloud-based industry 4.0 environment. J. Syst. Integr. **9**(3), 7–17 (2018). https://doi.org/10.20470/jsi.v9i3.349
24. L. M. Brumă, "Cloud security audit – issues and challenges," 2021 16th International Conference on Computer Science &Education (ICCSE), Lancaster, United Kingdom, pp. 263–266 (2021). https://doi.org/10.1109/ICCSE51940.2021.9569654
25. U.M. Ismail, S. Islam, H. Mouratidis, Cloud Security Audit for Migration and Continuous Monitoring. 2015 IEEE Trustcom/BigDataSE/ISPA, vol. 1 (2015), p. 1081–1087. https://doi.org/10.1109/Trustcom.2015.486
26. F. Doelitzscher, Security audit compliance for cloud computing. University of Plymouth 2014 Phd Thesis., PEARL (2014)
27. A. Nagar, K.P. Joshi, A semantically rich knowledge representation of PCI DSS for cloud services. 6th International IBM Cloud Academy Conference ICACON 2018, Japan (2018)
28. G. Ataya, PCI DSS audit and compliance. Inf. Secur. Tech. Rep. **15**(4), 138–144 (2010)
29. L. Elluri, K.P. Joshi, A knowledge representation of cloud data controls for EU GDPR compliance. 2018 IEEE World Congress on Services (SERVICES) (2018), p. 45–46
30. S. Islam, M. Ouedraogo, C. Kalloniatis, H. Mouratidis, S. Gritzalis, Assurance of security and privacy requirements for cloud deployment models. IEEE Trans. Cloud Comput. **6**(2), 387–400 (2018). https://doi.org/10.1109/TCC.2015.2511719
31. H.M. Melaku, Context-based and adaptive cybersecurity risk management framework. Risks (2023)
32. M. Barati, O. Rana, Checking GDPR compliance for cloud-based services. 2021 IEEE World Congress on Services (SERVICES) (2021), p. 2
33. D. Kim, K.P. Joshi, A semantically rich knowledge graph to automate hipaa regulations for cloud health it services. in 2021 7th IEEE Intl Conference on Big Data Security on Cloud (BigDataSecurity), IEEE Intl Conference on High Performance and Smart Computing (HPSC) and IEEE Intl Conference on Intelligent Data and Security (IDS) (2021), p. 7–12
34. M. Kelly, E. Furey, K. Curran, How to achieve compliance with gdpr article 17 in a hybrid cloud environment. Science **3**(1), 3 (2021)
35. C. Mitchell, Privacy, compliance and the cloud. *Guide to Security Assurance for Cloud Computing* (2015), p. 3–14
36. S. Okour, The impact of the application of IT governance according to (COBIT 5) framework in reduce cloud computing risks. Mod. Appl. Sci. **13**(7), 25 (2019)
37. P. Olajide, PCI DSS compliance validation of different levels of merchants in a multi-tenant private cloud (2013)
38. M. Piazza, J. Fernandes, J. Anderson, A. Olmsted, Cloud payment processing without ritualistic sacrifices reducing PCI-DSS risk surface with thin clients. 2016 International Conference on Information Society (i-Society) (2016), p. 166–168
39. C.E. Pugh, M. Hilley, Regulatory Compliance and Total Cost Influence on the Adoption of Cloud Technology: A Quantitative Study [Doctoral dissertation, Capella University]. In ProQuest Dissertations and Theses. (2021). https://www.proquest.com/dissertations-theses/regulatory-compliance-total-cost-influence-on/docview/2572572997/se-2
40. G.A. Reid, S. Miller, Improving HIPAA Compliance Efforts with Modern Cloud Technologies [(Doctoral dissertation, Capitol Technology University).]. In ProQuest Dissertations and Theses. (2021). https://www.proquest.com/dissertations-theses/improving-hipaa-compliance-efforts-with-modern/docview/2595993643/se-2?accountid=12118
41. C. Racuciu, S. Eftimie, Security threats and risks in cloud computing. Sci. Bull. Mircea Cel Batran Nav. Acad. **18**(1), 105 (2015)
42. R. Ahmad, Cloud Security and Governance. Metropolia University of Applied Sciences, Master's Thesis (Information Technology), (2021)
43. S. Subashini, V. Kavitha, A survey on security issues in service delivery models of cloud computing. J. Netw. Comput. Appl. **34**(1), 1–11 (2011)
44. L. Schubert, Ustutt-Hlrs, K.G. Jeffery, B.K. Neidecker-Lutz, L. Schubert, E. Ustutt-Hlrs, *A Roadmap for Advanced Cloud Technologies Under H 2020 Recommendations by the Cloud Expert Group* (2012)

45. D. Wang, D. Zhong, L. Li, *A Comprehensive Study of the Role of Cloud Computing on the Information Technology Infrastructure Library (ITIL) Processes* (Library Hi Tech, 2021)
46. R. Wu, G.-J. Ahn, H. Hu, Towards HIPAA-compliant healthcare systems in cloud computing. Int. J. Comput. Models Algorithms Med. **3**(2), 1–22 (2012)
47. G. Weir, A. Aßmuth, M. Whittington, B. Duncan, Cloud accounting systems, the audit trail, forensics and the EU GDPR: how hard can it be? British Accounting & Finance Association (BAFA) Annual Conference 2017 (2017)