jamk

Managing Compliance and Auditing in Cloud

Gunjan Gupta

Master's thesis
April 2022
Cyber Security
Master of Engineering in Cybersecurity

jamk | Jyväskylän ammattikorkeakoulu
University of Applied Sciences

jamk

Description

Gupta, Gunjan

Managing compliance and auditing in the cloud

Jyväskylä: JAMK University of Applied Sciences, September 2020, 71 pages

The degree program in Technology. Master's thesis.

Permission for web publication: Yes

Language of publication: English

Abstract

Cloud services have emerged as an essential and promising IT solution to many organizations to enable cost efficiency, flexibility, resiliency, agility, and speed. Cloud service providers are implementing and adhering to many cybersecurity measures to ensure the security and confidentiality of users' data. However, organizations' security risks have increased with the arrival of new security challenges like widespread adoption of remote work, constantly changing network security vulnerabilities, and changes in the legal and geopolitical landscape. To build trust and compliance in the cloud environment, it is of paramount importance to have a proper audit to better understand the security posture of their applications and ensure sufficient measures are implemented during the adoption of the cloud. The objective was to research and analyze areas where traditional audits and compliance need to be changed to address cloud-specific attributes and recommendations.

A combination of qualitative and constructive research methodology was used. Once the general and comprehensive knowledge was gathered through 'document analysis/literature review' and 'un-structured interview' methods of qualitative research methodology, constructive research methodology together with the semi-structured interview was used to develop a 'cloud audit checklist'.

The research demonstrates that auditors should know cloud-specific areas, its delivery and service model, key risks, division of roles and responsibilities, and cloud-specific auditing frameworks to move from traditional IT auditing to cloud-specific auditing. Organizations should always understand the security and compliance risks of overall business opportunity and appetite for risk before adopting the cloud. The desired outcome was achieved by developing a cloud audit checklist using a comprehensive study of literature material and having feedback from participants during interviews.

Keywords/tags (subjects)

Cloud computing audit, cloud auditing, cloud compliance, cloud security, compliance in the cloud, cloud audit approach, security in the cloud, securing cloud services, cloud security auditing

Miscellaneous (Confidential information)

Confidential information: No

Contents

Figures

Tables

List of abbreviations

AICPA: American Institute of Certified Public Accountants

API: Application Platform Interface

BAA: Business Associate Agreement

BCP: Business Continuity Planning

CIA: Confidentiality, Integrity, and Availability

CMM: Cloud Control Matrix

COBIT: Control Objectives for Information and related Technology

CSA: Cloud Security Alliance

CSC: Cloud service customer

CSP: Cloud service provider

CSU: Cloud Service Users

DDOS: Distributed Denial of service

DLP: Data Loss Prevention

DRP: Disaster Recovery Planning

ERM: Enterprise Risk Management

ENISA: European Network and Information Security Agency

ePHI: electronic Protected Health Information

GDPR: Global Data Protection Regulation

HIPAA: Health Insurance Portability and Accountability Act

IaaS: Infrastructure as a Service

IAM: Identity Access Management

ISMS: Information Security Management System

ISO: International Organization for Standardization

NIST: National Institute of Standards and Technology

PaaS: Platform as a Service

PCI DSS: Payment Card Industry Data Security Standards

PII: Personally Identifiable Information

RPO: Recovery Point Objective

RTO: Recovery Time Objective

SaaS: Software as a Service

SIEM: Security Information and Event Management

SEC: Security and Exchange Commission

TPA: Third-Party Auditor

1 Introduction

1.1 Background and objective of the study

Over the last decade, the use of cloud services has been widespread. Organizations can move faster by utilizing potential benefits in flexibility, resiliency, agility, speed, and economy. Cloud service providers have many cybersecurity measures in place to provide economic reasons to protect customers. However, with the arrival of remote labor, constantly changing network security vulnerabilities, and changing legal landscape, security risks are increasing exponentially.

According to the Data Breach Investigations Report (Bassett et al., 2021), *"in 2020, 73% of cyberattacks involved cloud assets, compared to only 27% in the previous year".* Migrating to the cloud without implementing needed security, exposes an organization to a rapidly growing threat landscape. An organization faces new security challenges to safeguard data in the cloud as it can be accessed from anywhere and hackers have more vulnerabilities to target. From a cybersecurity point of view, the cloud's benefits of flexibility, resiliency, and economy are both a friend and a foe.

Panetta (2019) predicts, through 2025, 99 percent of security failures in the cloud will be caused by the customers. It is a relentless effort for organizations to maintain security and compliance in the cloud. With new security challenges, many organizations are wondering whether the cloud is the best option. According to a Forbes report (Columbus, 2018), 66% of IT professionals are concerned about the state of security while adopting a cloud strategy.

Due to loss of control of infrastructure provisioning and not having full visibility on security aspects, cloud consumers have difficulty trusting the environment. To build trust and compliance in a cloud environment, internal auditors and the compliance team need to know their environment and cloud-specific risks, characteristics, and key components. Internal auditors need to have an in-depth assessment of the security and management of vital assets in cloud services (Ames and Brown, 2011).

Being different than traditional IT Security and having more pervasive threats than ever, cloud security auditors and compliance teams need to have vast knowledge in cloud-specific areas, and division of roles and responsibilities between cloud service consumers and cloud service providers together with traditional IT auditing knowledge.

Cloud services are bringing new security risks, along with essential and promising IT benefits. Internal auditors need to perform an in-depth assessment to better understand the security posture of these new risks and re-evaluation of traditional IT risks. Fundamental assumptions about security do not comply with the openness and public availability of cloud services (Ames and Brown, 2011). The objective of this thesis is to research and analyze areas where traditional audits and compliance need to be changed to address cloud-specific attributes.

1.2 Motivation for the choice of subject

According to Halpert (2011), organizations can better understand compliance and security risks of the information within the system through IT audits. Understanding both concerns help an organization reduce cost, comply with regulations, improve security, ensure the system is not vulnerable to attacks and make cloud computing successful. The motivation for the research came from a need to identify adjustments regulators and auditors need to do in the modern era of cloud services. It is necessary for a cloud service provider, customer, auditor, and regulator to consider cross-border and legal jurisdictional issues and compliance responsibilities divided between the service provider and customer before adopting cloud computing.

Cloud audit depends a lot on Service (Software as a Service [SaaS], Infrastructure as a Service [IaaS], Platform as a Service [PaaS]) and delivery (private, public, community, or hybrid) model chosen by the organization for cloud computing outsourcing. There is a big difference between auditing public cloud vs auditing hybrid cloud. Cloud audit largely depends on agreements, contracts, and compliance with those agreements. There is no standard fit cloud operating model and controls for every organization. It varies as per the organization's resources, corporate network, and criteria to deliver value to its customers. Cloud auditors should understand and consider organization-specific cloud operating models during the planning and execution of a cloud audit (Halpert, 2011).

The outcome of this thesis work was to provide an audit checklist, listing key domain areas to be audited and provide suggestions on the responsibility of those areas (provider/customer). Hopefully, internal auditors, compliance analysts, and cyber resilience team members will use the information provided. This can also be used as a tracking cloud security implementation status and assessing maturity level. This tool can be used as a basis (requirements specification) to decide and select cloud service providers.

2 Research methods

2.1 Research question

The research question was, what are the changes required in traditional audit and compliance management to address cloud-specific attributes and recommendations? The following research tasks were performed to answer the research question:

- determine the cloud system's constitution,
- assess the cloud compliance responsibilities division between provider and customer, and
- evaluate key risk areas in cloud computing.

The Outcome of this thesis was to provide a checklist to assist customers, auditors, and compliance analysts to perform value-added cloud audits. This checklist provides key domain areas to be audited on the responsibility of those areas (provider/customer). The research question guided the researcher during the research process. Research tasks contributed to defining the attributes to be added to the checklist tool.

2.2 Research methodology

The objective of the thesis was to understand the changes in compliance and audit of cloud services and create a checklist to help the organization's compliance and auditors' team. To achieve the objective, a variety of research methods could be used, and each method had its pros and cons along with an investigative approach. According to Yin (2018), doing case study active research is a largely iterative and step-by-step process. Hence mixed-method – a combination of qualitative and constructive research methodology was used.

The research was first conducted using 'document analysis/literature review' and 'interview' methods of qualitative research methodology. General and comprehensive information was gathered by compiling and analyzing existing material on the topic. The rationale to opt for the qualitative research method was that the qualitative approach typically focuses on the qualities of entities and dynamic processes compare to the quantitative approach focusing on measurement and analysis (May, 2002). Furthermore, according to Portney (2019), qualitative research has its importance in gaining a deeper understanding, of findings by cyber security environment experts, goals, and implications with a wide analytical focus.

Once the general and comprehensive knowledge was gathered through the qualitative research method, constructive research methodology was used to develop an 'audit checklist'. As per Kasanen, Lukka, and Siitonen (1993), the method used for solving a problem through the construction of models, organizations, flow charts, etc. can be defined as the constructive approach. Technical sciences, clinical medicine, and operations analysis have used mostly constructive research approaches. In this research mode, a solution to a particular problem was found by focusing on creating construction.

Furthermore, Kasanen, Lukka, and Siitonen (1993), explained that a constructive approach starts with a relevant problem having research potential. The next step is to understand the research topic by gathering background knowledge on the topic. A construction is created after collecting all the necessary general and comprehensive information on the topic (see Figure 1).

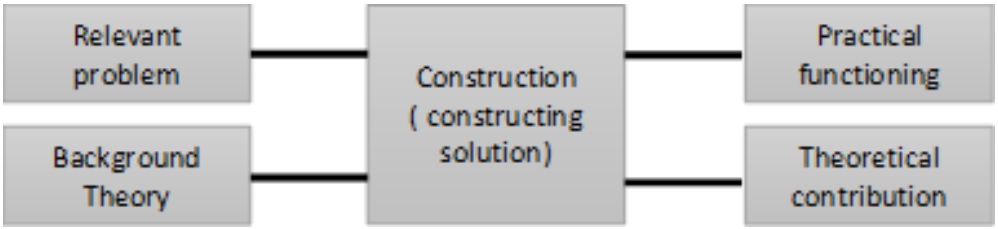

Figure 1: The constructive research process steps (adapted from Kasanen, Lukka, and Siitonen 1993).

The construction should be easy and simple to implement and relevant to the research topic. The constructive approach research process can be divided into the following phases, the order of steps can vary from case to case:

1. Discover and perceive a relevant problem having research potential.
2. Gather the background knowledge on the topic.
3. Innovate, i.e., create a solution based on collected general and comprehensive information
4. Demonstrate that the solution works.
5. Present the solution concept having theoretical connections and contributions to the research.
6. Assess the solution's applicability to the scope.

2.3 Interview process

In qualitative research, method interviews help to get a deeper understanding of the topic and specific subject by understanding the experience, views, or beliefs of an individual. Hence, interviews were helpful in this thesis work where the author had basic knowledge about the research topic and wanted to establish a deeper understanding of it. In this research work, interviews served dual goals, firstly interviews helped in gaining detailed knowledge, legitimize the initial findings as per literature review, and define key concepts, secondly, they aimed to provide feedback in assessing and validating solution implementation that is a checklist development.

People for semi-structured interviews were selected based on their competence level. Idea was to interview individuals working in auditing, compliance, risk management, program, and project management area. Altogether 10 people were shortlisted. Most of them were aware of the background of the research being conducted as these were part of the interview conducted in an unstructured manner to get detailed insight. Interviews were conducted using Microsoft Teams as in-person meetings were not possible due to Covid-19 restrictions. An email invitation along with a team meeting link was sent to the invitees. A list of questions was ready before the interview meeting. The list of questions was not shared before the interview as idea was to facilitate and understand the emergence of new viewpoints.

2.4 Interview questions

The list of questions was created. Although participants were aware of the background, however, a brief introduction was given at the start of the meeting.

Introduction

- Short background about myself on my Job profile and experience,
- Objective of the research,

Requirement and solution analysis phase

- Did you or your organization performed an assessment before moving to the cloud?
- What kind of assessment was done?

Risk assessment and management

- Did your organization perform asset classification and risk identification analysis?
- Are you aware of the threat and vulnerability analysis?
- How are the risks handled and documented?
- Do you know the risk management process? How are the results utilized?

Framework and standards

- Do you use any standards or framework to comply?
- Are there some standards that are currently not used, but should be?

Planning phase

- Have you participated or performed in cloud audit planning or execution?
- What are the steps you take during audit planning? How do you identify cloud auditing scope and objective?
- What kind of security-related documents are analyzed?
- What could be possible steps to improve the planning phase?

Security controls

- What all domains or process areas have you assessed for cloud security auditing?
- What kind of security controls are implemented, or do you test, or do you look for evidence?
- What inputs influence these?
- Do you map security controls with the framework you need to comply with?
- How regularly do you test your security controls?

Audit execution tool / Audit checklist

- Here is the audit checklist in excel, what areas you would like to add or delete?
- Would you like to test or use it for some time and provide me feedback on this?

2.5 Data collection, analysis, and management

Data collection is a systematic process of gathering and measuring reliable information from various sources to provide answers and insights to questions. It was necessary to ensure that data is gathered from reliable and relevant resources. As the research method used was the 'Qualitative research method', there was a need to collect qualitative data. As per Kananen (2015), in qualitative research, there are three methods of collecting and measuring data. These are documents, observations, and interviews. The author used the following sources to collect qualitative data:

- e-books,
- online articles,
- interviews,
- government frameworks, and
- white papers.

Data were collected in two phases. For the first phase, data were collected to gain detailed insights, and understand experiences, government frameworks, and reports. During this phase, literature review and unstructured interview methods were used. For the second phase, data were collected to test and verify the 'audit checklist'. During this phase, observation and semi-structured interview methods were used. Search terms were used like cloud security, cloud computing, cloud auditing, cloud compliance, privacy, and security in the cloud, securing cloud services, cloud audit approach, compliance in the cloud, cloud security auditing, cloud service provider (CSP), third party auditor (TPA), data security, NIST standards, and ISO Standards.

According to Valcheva (2018), in qualitative data analysis processes and procedures are used to analyze the data and provide an explanation, interpretation of patterns, and themes. Qualitative data was analyzed using the content analysis method to interpret the meaning and draw conclusions. According to Bengtsson (2016), content analysis is not a counting process but a research tool to determine the relationship of the results to their context.

In this study, the only possibility to collect personal data was during 'interviews'. While taking notes during interviews, the author did not write any personal information into notes for example name, age, or occupation. The author did not have any intention to collect any personal data during information seeking. All data collected during interviews were anonymized. Interview data was stored in an encrypted format during the thesis writing process and will be deleted once the

research project is completed. The author will not share or release any data with third parties. When the author will publish the result there will be no personal data in the published material. Before the interview, all participants were informed about the data collection and management methods, possible risks, the reason for choosing them, and ways to disseminate the results. This provided information to participants to self-determine whether to engage in the study or not. All data was stored in 'one drive' to prevent loss of data. Data were recorded systematically so that author can access the data easily when needed. All data were erased after the project completed.

2.6 Ethicality and reliability of the development work or research

While conducting research and writing the thesis, the author followed the Ethical Principles for Jyväskylä University of Applied Sciences (JAMK, 2018). Authors have read the chapter 'The Centrality of Ethics in Qualitative Research', in 'The Oxford handbook of qualitative research' given in detail by Leavy (2014). According to Leavy (2014), the main important ethical values to be considered in research development are respect for individual autonomy, protecting their privacy, and minimizing harm.

The author ensured that credit to sources is given by giving references to their work with the proper citation method. There is no intentional violation regarding references and the use of software and applications. As mentioned in section 2.5, the author did not collect any personal data to protect people's privacy.

3 Cloud system's constitution and delivery method

The solution analysis and design phase were conducted using a literature review and unstructured interviews with colleagues and friends working in IT and cyber security areas. Most of the people interviewed in an unstructured manner were working as an IT-auditor, CISO, compliance, and risk management professionals. This phase aimed to gain detailed knowledge and further understanding of the research problem to define key concepts. The purpose of the unstructured interviews was also to find out the knowledge of the IT-auditors, compliance, and risk management experts on cloud computing auditing, and the changes they have made in moving from traditional IT auditing to cloud auditing.

A lot of literature was reviewed and understood. Literature was selected from the various quality and legal sources provided by JAMK (e-books on Skillport, IEEE, ProQuest, and Theseus), available online through government and standards organizations (ENISA, ISACA, CSA, NIST, ISO, KPMG, Deloitte, etc.). The literature and theories that were most relevant to this research were collected, reviewed, discussed, and evaluated in this chapter. This part of the study laid the foundation that supported the analysis and design of this research.

3.1 Cloud services and systems

Cloud services and the system is the on-demand access and availability of computer system resources like networks, data storage, servers, databases, and software through the internet with minimal interaction between customers and providers. ISO/IEC defined cloud computing as " *Paradigm for enabling network access to a scalable and elastic pool of shareable physical or virtual resources with self-service provisioning and administration on-demand*" (ISO/IEC, 2014).

The National Institute of Standards and Technology (NIST) defines cloud computing in a similar way "*Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics, three service models, and four deployment models*" (Mell & Grance, 2011).

There are five fundamental aspects of cloud computing defined by NIST (see figure 2).

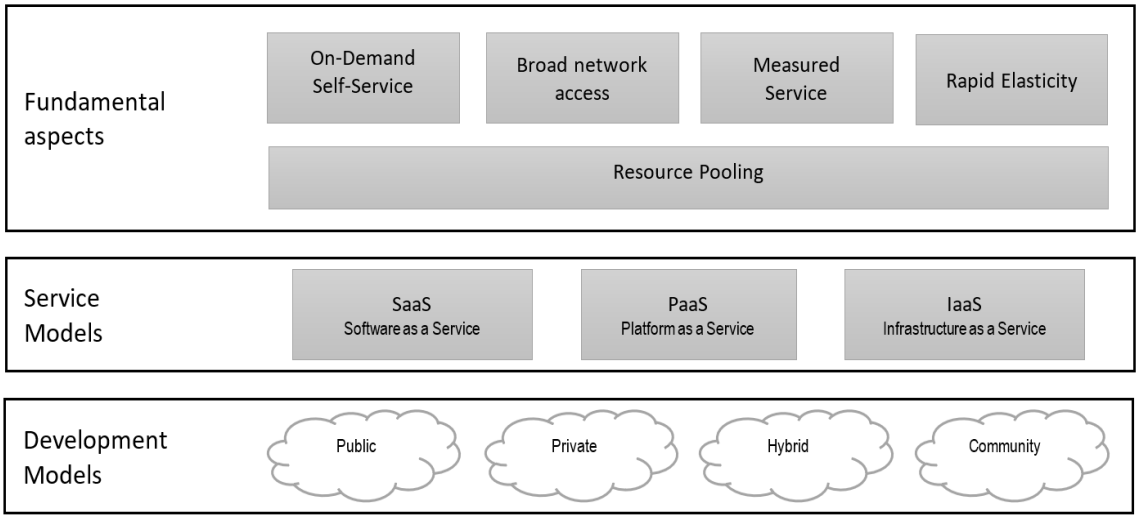

Figure 2: Visual depiction of cloud service and deployments model (Adapted from NIST, 2011)

On-demand self-service This service enables cloud customers to use cloud computing services such as network storage and server time as required without having human contacts between CSP and CSU.

Broad network access: This service provides availability of resources in a private cloud network, which can be accessed through a wide range of devices like smartphones, PCs, and tablets.

Resource pooling: Cloud service provider offers a resource pool of scalable services, serving multiple customers at one time. CSP uses a multi-tenant model. Depending on the customer's demand and consumption, different resources can be assigned and reassigned dynamically. Resources could be memory, network bandwidth, and storage processing. In this case, the customer does not have any knowledge or control over the exact location of the provided resources. A customer can define location at a higher level of abstraction.

Rapid elasticity: This service provides cloud customers an elasticity to add or reduce cloud resources as per their needs. Resources like storage capacities, RAM, CPU processing, etc. Customers can dynamically scale the services. Customers can scale up the resources when they need more and release the resources when they no longer need them. Often it is an automatic process and any quantity at any time.

Measured service: It is a billing model used by the cloud service provider to charge the fees from cloud customers based on the consumption of resources. It is a transparent provision in which both cloud service providers and consumers can monitor, report, and control resource usage (NIST, 2011). There could be two possible payments method:

- Pay as you go.
- fixed monthly plans.

3.2 Cloud service models

Cloud computing is offered mainly in three service models, which can be chosen by customers based on their requirements. However, these models are useful from a description point of view, these are not a rigid framework.

Infrastructure as a Service (IaaS): The consumer can use virtual and physical hardware over the internet provider provides computing resources like networking, servers, storage, and virtualization hosted in a public cloud, private cloud, or hybrid cloud. In this model, the customer has more security controls. For example, the IaaS cloud service provider will only secure the provided infrastructure but it is the full responsibility of the consumer to secure a virtual network, based on the tools available on the service (CSA, 2017).

Platform as a Service (PaaS): In this model, hardware and software tools are provided to consumers over the internet to develop the application to deploy onto the cloud infrastructure. Underlying cloud infrastructure including operating systems, networks, programming languages, libraries, and tools are hosted, managed, and controlled by the cloud service provider. Deployed application and application hosting environment configuration settings are managed and controlled by cloud customers (NIST, 2011).

Software as a Service (SaaS): Consumers can connect and use the provider's hosted application over the internet on a subscription basis. Security management and control is mainly the provider's responsibility including logging, monitoring, auditing, network, operating systems, storage, servers, and application security. Consumers can only manage limited application configuration settings and authorization. Figure 3 provides a cloud service model depiction with shared responsibilities in each cloud service model.

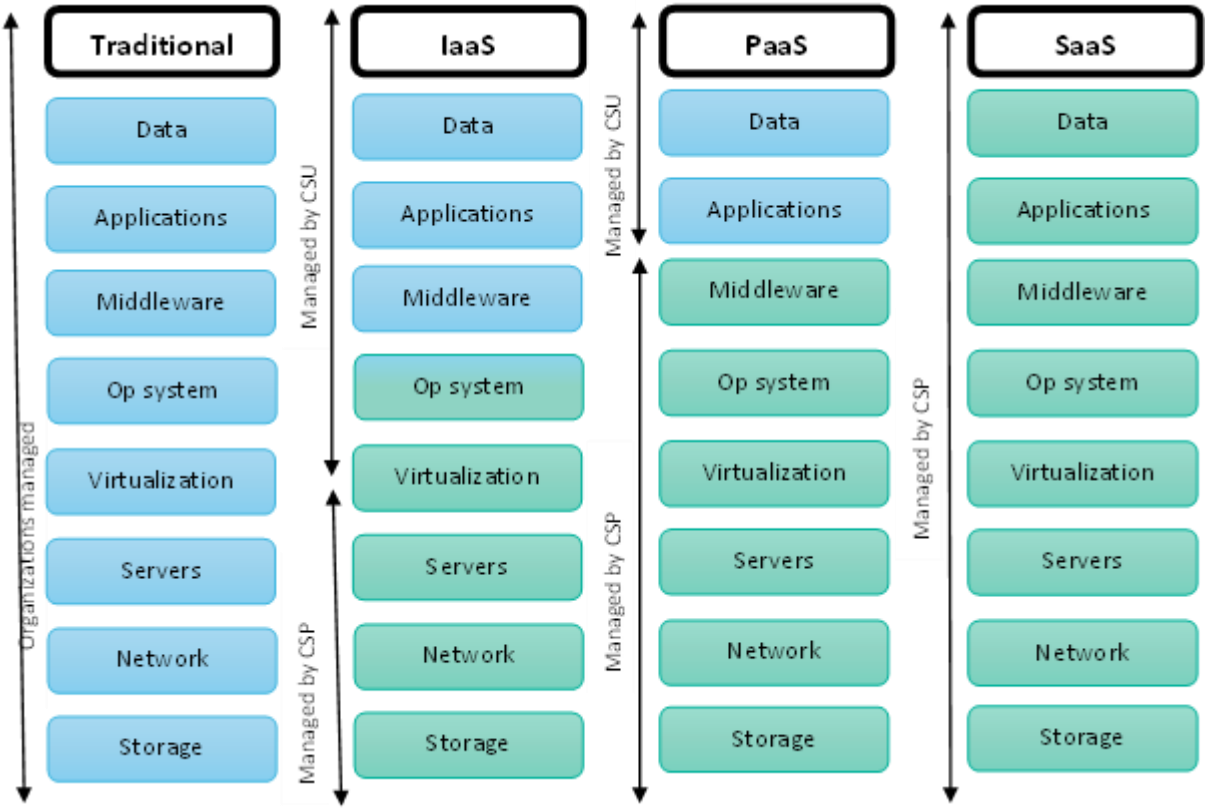

Figure 3: Cloud service model with shared responsibilities (adapted from Cloud Computing and the Microsoft Platform, 2009)

3.3 Cloud deployment models

NIST and ISO/IEC both define four cloud deployment models. These models specify how cloud services are made available and consumed. There are different attributes and implications for the end-users. A cloud deployment model depends on who is hosting the infrastructure for deployment and who is controlling this infrastructure. The most important decision for an organization is to decide on the deployment model to go (Rountree & Castrillo, 2014).

Private cloud: It is a cloud service and infrastructure exclusively provided to one organization to support its various user's group (e.g., business units). An organization itself, a third party, or some combination of them can own, operate, and manage. It may exist on or off premises (NIST, 2011). This model is most expensive as organizations need to acquire and maintain a private cloud. However, security and privacy concerns can be addressed better in this model.

Community cloud: A shared cloud computing infrastructure accessible to a specific community of organizations or employees having shared interests such as security requirements, policies, and compliance considerations. One or more of the organizations in the community, a third party, or a combination of them can own, operate, and manage community cloud services and infrastructure. It can be located on-premises or off-premises (NIST, 2011). As community cloud infrastructure is accessible to only consumers with the same cause, it offers better security than a public cloud and consumers can influence the quality of service. Compare to the public cloud it is more customizable and the community can configure it according to its needs. As the cloud infrastructure maintenance and controlling cost is divided among all the users, it is a lot cheaper than the private cloud. The ultimate decision usually applies to the majority and/or veto members (Halpert, 2011)

Public cloud: It is a widely used cloud model and is available to use by the public. It is owned and managed by a third-party cloud provider which can be a government organization, business, academic, or some combination of them. The infrastructure of the public cloud exists on the premises of the cloud provider (NIST, 2011). Public cloud services are frequently used for online application development and testing, web-based email, and file-sharing (Rountree & Castrillo, 2014). Microsoft Azure, Google App Engine, Blue Cloud by IBM, and Amazon EC2 are the most used public clouds.

The usage of public cloud services in some countries has been prevented due to concerns regarding security issues, such as data residency requirements. Before moving to cloud services, consumers should perform due diligence and in-depth assessment to make sure cloud service user does not violate legislative, regulatory, or business requirements (Halpert, 2011).

Hybrid cloud: It is a computing environment composed of two or more distinct cloud infrastructures (private, community, or public) connected as seamlessly as possible. This interconnectivity enables workloads movement, data, and application portability (NIST, 2011).

3.4 Traditional IT systems Vs cloud computing systems

For an auditor, it is crucial to distinguish between traditional IT systems and cloud computing. It is key for organizations to understand the pros and cons of each of these types of systems. In the traditional IT systems, Organizations purchase, install and maintain IT devices, servers, and data

on-premises. When organizations create their IT infrastructure plan, organizations have the freedom to decide data security implementation plan. Organizations can decide about security devices, network controls, storage, user access management, etc. Organizations are responsible for maintaining business continuity and disaster recovery plan and incident management plan. As organizations are having full control of IT infrastructure, the cost of installing and maintaining becomes very expensive.

In cloud computing, it is possible to have networks, software, storage, servers, and hardware hosted in the cloud enabling cost-effective scaling. In this case, organizations rely mostly on the cloud service provider's security controls and management.

According to Bharadwaj, Bhattacharya, and Chakkaravarthy (2018), there is a need for a paradigm shift in application development and architecture to embrace and leverage scalability, geo availability, failure resiliency, and dynamic provisioning features of cloud computing. More and more organizations are becoming cloud-native and picking up on the adoption of service-oriented and serverless architecture. The traditional endpoint-focused security tools can not be used with cloud services as the perimeter and security move to cloud security controls.

Cloud service features enabling widespread adoption and cost efficiency are different from traditional technologies. Traditional security methods and audit methodologies cannot be fully applied to cloud services. Thus, the shared responsibility concept, resource virtualization, and the inability to audit the infrastructure under the service provider's responsibility require new methods and processes to audit cloud services (Brumă, 2021).

The audit is an independent assurance done by an organization's employees, evaluating organizational processes and controls having focused on risk management and optimization. An external audit examines from an outside perspective an organization's ability to comply with various laws and regulations. Traditional IT audits have been used by organizations to assess confidentiality, Integrity, and availability in data storage and transmission to its authorized users. But when an organization moves to cloud computing its exposes to new cloud-specific security concerns as cloud computing allows multiple users across a large domain (Ryoo, Rizvi, Aiken, & Kissell, 2014).

3.5 Challenges with securing cloud

The security audit of cloud computing becomes challenging due to the associated complexity of this system such as differences in cloud deployment and service models, and thin perimeter between the organization's system and cloud. In most cloud-specific standards recommendations provided are very high level while in existing cloud infrastructure logging information is at a low level. In practice, CSC administrators can perform a limited audit with few available compliance tools having several major limitations (Majumdar et al., 2019).

In traditional IT security auditors identify, evaluate, and test an organization's controls, procedures, and operations to assess those controls are sufficient and being used to safeguard the organization's information assets and data to achieve the objectives and business goals of the organization. To perform this, IT auditors need information and data from both internal and external resources. According to Brumă (2021), the most used security model in the cloud is the shared security responsibility model, in which the provider and customer both share security and compliance responsibility without sharing the database of information regarding the mechanisms implemented by both. These models become difficult in performing a cyber security audit, necessary in selecting the right solutions for securing cloud resources (See figure 4).

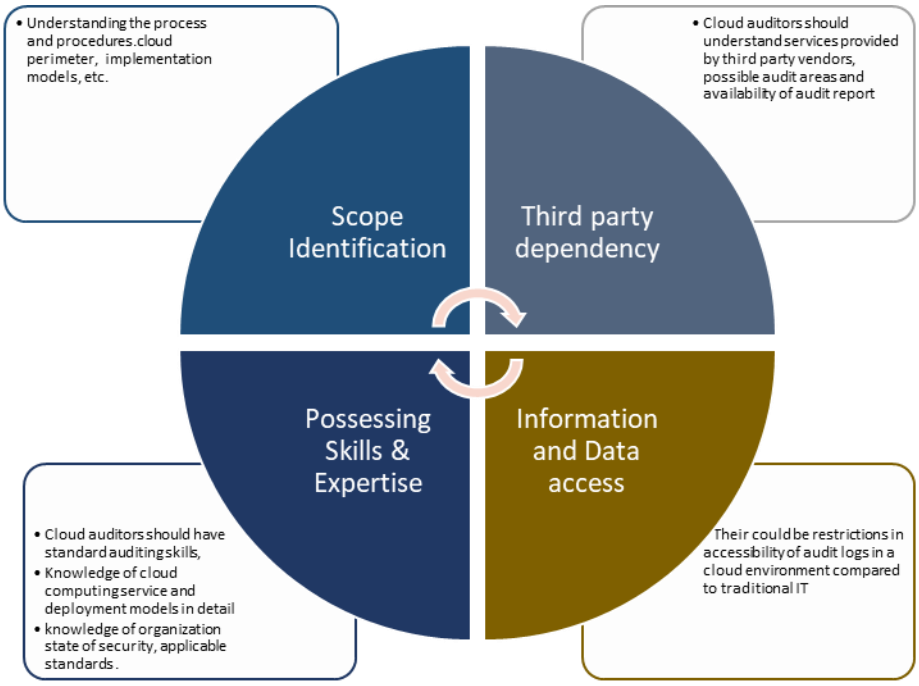

Figure 4: Internal audit challenges (adapted from Bruma, 2021)

For an effective cloud security audit, auditors should have familiarity with the terminology of cloud computing and know a cloud computing delivery method and constitution. This knowledge and familiarity make auditors pay attention to important security aspects like encryption, scope, transparency, colocation, and scale during cloud security auditing processes.

3.6 Key risk and security issues in the cloud

There are many unique security issues and risk areas in cloud computing. To better prepare, and develop strategies and solutions, it is important for an organization to understand what 'threat' means to them and the various risks or threats that the organization can face. According to ENISA (2014), a threat is," *Any circumstance or event with the potential to adversely impact an asset through unauthorized access, destruction, disclosure, modification of data, and/or denial of service*".

Organizations should always analyze and understand the risk to the overall business and its risk appetite. Comparative analysis should be performed to compare the risks of storing data in the cloud instead of premises vs risks when entire data is stored on-premises only. The risks of moving to cloud services compared to the risks of continuing with traditional IT should be considered carefully. Risks should be considered against the type of architecture being considered. Organizations need to find out the possibility of transferring risks to cloud service providers and consider risk against the cost-benefit received from the services (ENISA, 2012). To understand all aspects of security threats and risk areas, the author has gone through several widely published resources. The author has analyzed the security threat and risk areas identified in NIST,2018 and ENISA,2012 and other widely published resources. The key risks to cloud security are:

3.6.1 Lock-IN

Ko and Choo (2015) describe lock-in as the "Hotel-California" syndrome where one can check in, but one can never leave. A cloud service provider produces the service using its standards, protocols, and policies. Due to this migrating from one cloud provider to another becomes extremely difficult, leading to a situation where a customer is tied to their current service provider, i.e., the customer cannot take their business elsewhere, or the costs of doing so would become too high.

To mitigate the risk, customers should carefully check cloud service providers' policies on data moving and the impact on support available, if the customer decided to move to another CSP.

Customers can adopt multi-cloud and hybrid cloud deployments, which have several benefits. Multi-cloud adds redundancy and security as the customer is not dependent on one CSP. With this approach, customers can select a cloud service provider whose add-on services are the best fit for the organization. Customers can also adopt the strategy to build an application on openly available language rather than building on one CSP.

3.6.2 Loss of governance

When an organization accidentally migrates from an on-premises IT infrastructure to cloud services without having a proper governance policy in place, it can lead to a loss of governance and control. In the cloud there are no ring-fenced boundaries like in traditional IT, therefore traditional governance elements like risk and performance management, strategic alignment, and value delivery are ineffective for having the same policies in the cloud. An organization's strategy and capacity to meet its mission and objective can be severely impacted due to the loss of cloud governance and control. Without proper governance and control its very challenging for the organization to comply with the security requirements, maintain good performance and quality of service, and confidentiality, integrity, and availability (CIA) of data (ENISA, 2012).

To mitigate the risk, the organization should identify and implement organizational structure, policies, procedures, and controls so that effective risk management, security governance, and applicable compliance could be possibly achieved. While defining the governance, it is important to consider the complexity, priorities of the enterprise, the company culture, and the parts of IT management, business processes, and applications moving into cloud service providers' control. To ensure security requirement enforcement risk management, metrics for measuring risk management, and service level agreement should be implemented by an organization.

3.6.3 Data protection

One of the biggest security risks when using cloud services is losing confidential and critical data, trade secrets, and intellectual property. Processing or storing of data in another country could lead to data protection legislation difficulties or responsible data protection authority could consider this unlawful. In traditional IT, the organization has full control of the location of data and processing applications. On a contrary, organizations should consider the high probability of movement of their data and processing applications between data centers located in different geographical locations even without informing the organization (ENISA, 2012).

The organizations which handle personally identifiable information (PII) and fall under regulatory compliance laws, need to perform a detailed due diligence and risk analysis when using third parties to deploy PII. For this, the United Kingdom has documented the Data Protection Law, which demands that the end customer (or data controller) is ultimately responsible for data protection. The end customer undertakes the appropriate due diligence and makes sure that needed controls are in place to protect the data.

During due diligence, organizations should evaluate the cloud vendors to understand and evaluate how cloud providers meet the scope of the organization's requirements, protect their assets, and implement best practices. For the end customer, it is important to evaluate data backup procedures – where and how often data is backed up, what are their versioning capabilities and retention procedures. Identity management and access control procedures, administrators' rights and privileges, and business continuity plans are the important aspects to be evaluated by the end customer during due diligence.

3.6.4 Data loss or incomplete data deletion

Data loss is a cloud security risk in which data is stolen, deleted, corrupted, and unavailable to a user, software, or application. According to Linthicum (2013), the main cause of data loss was power loss (See figure 5). Though these reasons for potential risk of data loss can be mitigated by installing a secondary server or platform, however, it is important to make sure that the cloud provider is deploying sufficient business continuity procedures and the cost is included in the price.

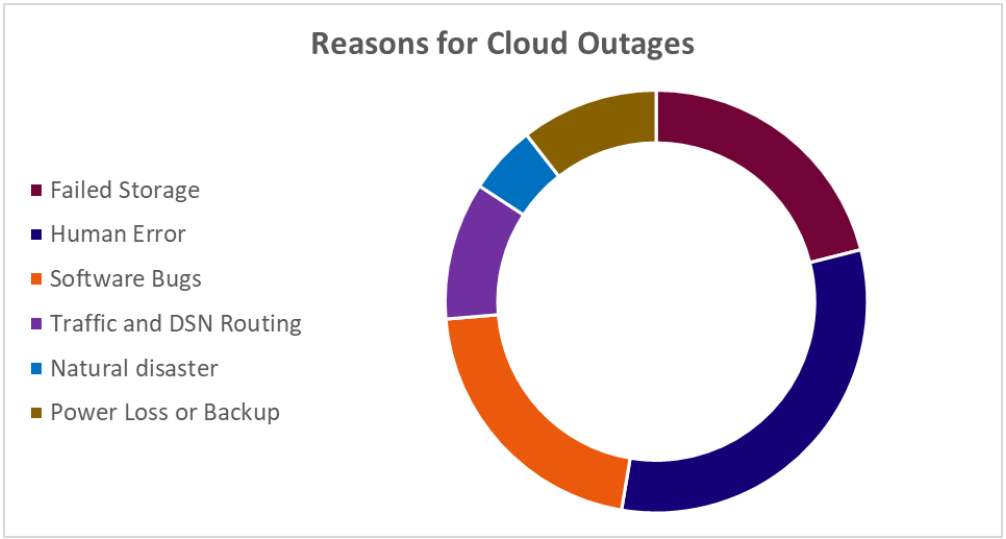

Figure 4: Reason for cloud outages (adapted from Linthicum, 2013)

It is challenging to ensure the complete and effective deletion of a customer's critical and sensitive data, when cloud storage is shared among multiple clients. There is a risk of cloud service providers receiving data that is not collected lawfully by its customer and do not inform if customer data security breaches. As per law, responsibility for the processing of personal data lies with the end customer, even when CSP carried out such processing in its role as an external processor. In case a data controller fails to comply with data protection law, it can face criminal, civil, and administrative sanctions, which are different from country to country (ENISA, 2012). When new software is developed over a cloud in models such as PaaS and IaaS, it is important to implement effective processes and procedures to secure intellectual property on a publicly shared interface. Hence, data and information must be managed consistently to protect the confidentiality, integrity, and availability of the information system.

To lessen the risk of data leakage within the cloud, organizations must evaluate the process for administrating encryption to help prevent accidental disclosure. The customer should select the encryption algorithm based on the actual need to comply with regulations. Encryption highlights the importance of managing the encryption keys in an efficient manner and customers should implement a standardized method of using key management and distribution methods so that they can utilize the encryption and securely manage data (Sun, Pan & Bertino, 2018).

Complex encryption algorithms and a set of cryptography need to be applied to secure the data and information deployed through cloud services in case data is placed in unauthorized hands (Dharmakeerthi, 2020). Organizations can deploy data loss prevention (DLP) software to monitor and detect data security threats. This DLP software should be chosen based on the technology used in the organization. Organizations can perform regular audits to prevent data losses and breaches.

3.6.5 Supply chain Failure

The supply chain is a commonly known risk factor as it is important to keep hardware, software, and installations secure and available with a decent delivery time in all possible situations to

ensure the availability of the service. In cloud computing, the cloud provider can outsource certain production tasks to a third party or can use another cloud provider as a backend. In such a situation, the potential for cascading failures is created as the security level of cloud service depends on the security level of each one of the links and the level of CSP dependency on the third party. In case roles and responsibilities are not clear between all the parties involved in the supply chain or there is an interruption or lack of coordination, this can lead to inventory theft, unavailability of services, loss of personal identifiable data, no clarity on SLA, and economic and reputational losses due to failure to meet customer demand (ENISA, 2012).

The supply chain is likely to be longer in cloud services and customers do not have many options, organizations should consider the potential impact of supply chain failures higher than in classic IT setups. Hence, an organization needs to define and implement the processes to identify, assess and manage supply chain risks in the cloud. During cloud supply chain risk assessment, identify and assess cloud service providers, all third-party partners, services, and components. Based on supply chain risk assessment, design and implement appropriate measures to manage the supply chain risks, agree on contracts and SLA with a cloud provider and third-party partners, to meet the objective of organization (NIST, 2018).

3.6.6 Insecure interfaces and application programming interfaces (APIs)

Users access cloud services through an application programming interface. Therefore, the security of the interface determines cloud security. Insecure APIs can lead to data exposure, break-in function-level authorization, and other security risks. Secure access control, encryption, and authentication mechanism must be implemented in API. In addition, penetration testing can be executed by the organization from time to time to find out the vulnerabilities and fix them. Organizations can implement encryption for data transfer and multi-factor authentication using OTPs or biometrics.

3.6.7 Identity management and access control

Cloud computing brings several changes to identity and access management compared to traditionally managed IAM for internal systems. It is possible that some roles on the cloud service provider side have administrative privilege access to view and misuse customer-sensitive data and information. It is possible that provider's employees misuse their administrative privilege access without getting noticed by customers, which can lead to significant customer loyalty and

reputational risks (Ames, B., & Brown, F., 2011). Fundamental change in cloud computing is that identity and access management are managed by several organizations. To manage the risk, it is important that only authorized users, devices, and processes are having access to logical and physical assets and are managed consistently. Physical and remote access to assets and network integrity is managed and protected. Cloud providers should use multi-factor authentication for all external accounts.

3.6.8 Distributed Denial of service

In cloud computing resources are shared by many users, therefore DDOS is a major risk. On average there are 14% DoS attacks out of all attacks, in a cloud environment. Many big companies' websites like yahoo, AWS, Mirai Krebs, and Github were affected by DDoS. Distributed Denial of Service is a malicious attack targeting to disrupt the normal traffic by flooding a server, service, or network with superfluous internet requests from many sources distributed across a wide geographical area so that legitimate requests are unable to be fulfilled. Organizations need to secure the server and network infrastructure by minimizing the possible points of attack, implementing a web application firewall, content filtering, and using load balancing to identify potential traffic inconsistencies.

As per Patrick & Satyanarayana (2020), it is important to properly analyze and agree on the cloud service provider's SLA on DDoS defense to create tight configuration and protocol to help mitigating the distributed denial of service attack. SLA should clearly define attack types, which layers, duration it covers, and response time taken by the cloud service provider. In types of attack, it is important to understand if it covers attacks matching the vendor's pre-configured signatures, or it also covers unknown attack vectors.

3.6.9 Insider threat

Although this threat exists in the traditional IT environment as well, the probability of an incident is higher in the cloud computing environment as cloud administrator is a highly privileged insider role exists in all three cloud deployment models. Costa (2017), defines malicious insider as an individual who uses his privileged access to an organization's critical information and assets, either maliciously or unintentionally which negatively impact the organization business, reputation and legal regulations. To manage the risk, it is important to understand the process and mechanism

for maintaining access restrictions and mitigation controls placed by the cloud provider. Organizations should identify operational and monitoring controls they can impose to reduce the risk.

3.6.10 Shared technology vulnerabilities

In cloud computing, storage memory, network, routing, and computing capacity are shared between several users. Although one big benefit of cloud computing is due to shared technology, however, it comes with the associated risk of failure of resource (routing, memory, storage) separating mechanism, thus exposing the organization's sensitive information. According to ENISA (2014), the risk of shared technology vulnerability depends on the chosen model of the cloud. This risk is low in private clouds higher in the case of public clouds. This can lead to reputation damage, loss of valuable or sensitive data, and service interruption for CSPs and their customers.

3.6.11 Social engineering attacks

Social engineering term is typically used for a variety of malicious activities to psychologically manipulate people to make them perform some actions or divulge sensitive information. While it is like a simple fraud or trick, it is predominantly fooling unsuspecting users to hand over confidential information, or computer system access. Most victims are contacted through emails, phone calls, or other communication channels to invoke fear or urgency which makes the victim hastily click a malicious link. Most common social engineering attacks are pretesting, quid pro quo, phishing, tailgating, and baiting. Social engineering attacks are a highly common cyber-attack technique. The reason for this is the greater attack surface created by the interaction between two different entities (ENISA, 2014).

3.6.12 Compromise of Service Engine

The service engine is an essential part of Cloud computing. An attacker can access all the customer data through compromise of the service engine leading to a denial of service or complete loss of data. Cloud service providers and customers should articulate a clear division of roles and responsibilities and the minimum actions each party will undertake.

3.6.13 Subpoena and e-discovery (Compliance challenge)

In cloud services, a subpoena is a mandatory compliance to secure the data or information exchange via the internet when an encryption key was not shared between parties in the

communication. Cloud service user, involved in litigation is legally required to respond to the subpoena. The contract between CSP and CSU should state cloud service provider's action in case they're slapped with a civil discovery request or subpoena. As per the stored communication act, customer (data owner) should be informed anytime its data is subpoenaed but having written in contract. This will provide 10-14 days to customer to file a response in the court. Figure 6 provides risks associated with different types of cloud services

Risk Associated With Different Types of Cloud Service			
Risks	**SaaS**	**PaaS**	**IaaS**
Lock-IN	Medium	Medium	Medium
Loss of governance	High	High	High
Data protection	Medium	High	High
Incomplete Data Deletion	High	High	High
Supply chain failure	Medium	Medium	Medium
Insecure interfaces and application programming interfaces	High	High	High
Identity management and access control	Medium	High	High
Distributed Denial of service	High	High	High
Insider threat	High	High	High
Shared technology vulnerabilities	Low	Medium	High
Social engineering attacks	High	High	High
Compromise of Service Engine	Medium	High	High
Subpoena and e-discovery (Compliance challenge	Low	Medium	High

Figure 5: Risk associated with a different type of cloud services model (adapted from ENISA, 2014)

3.7 Cloud security auditing standards and frameworks

Cloud service customers are responsible to always ensure the protection of valuable information in the cloud. As the threat landscape is evolving constantly, this can be a challenging complex task that requires a layering of tools, a strong foundation of policies, guiding principles, and approaches. There are security frameworks specific to different industries that aid in providing organizations with a holistic approach to protecting their valuable information. The security frameworks benefit from protecting vital processes and the infrastructure providing those operations. Other business benefits are achieving regulatory compliance, setting up information handling governance, and controlling data and financial losses resulting from a security breach. A security

framework is for establishing end-to-end security by monitoring data and transactions with the use of coordinated system of tools and behaviors (Vahradsky, 2012).

Cloud service customers should consider the standard and framework carefully based on their operations and requirements. In most cases. CSC needs to comply with more than one standard and framework. The leading security frameworks and guidelines to meet regulatory requirements and have a significant impact on cloud computing security are as follows:

ISO-27001 / ISO-27002 is the international standard for information security, which helps organizations define, implement, manage, continually monitor, and improve their Information Security Management System (ISMS). An ISMS consists of policies, procedures, technology, and controls to secure confidentiality, integrity, and availability of an organization's information assets. ISO-27002 defines controls and implementation guidelines to put in place for compliance with the ISO-27001 standard.

The Payment Card Industry Data Security Standard (PCI DSS) is specific to organizations handling cardholder information. This standard provides technical and operations guidelines to protect cardholder data. PCI DSS-compliant helps developers and cloud service providers to develop and build applications with having a secure credit card payment system. In this case, they need not use a third-party merchant account provider. PCI DSS is a worldwide credit card payment security standard. This standard applies to all the organizations dealing with credit card payment data, which means holding, processing, or exchanging cardholder information. Cardholder data includes personal identifiable information like primary account number, name as it appears on the card, card verification value (CVV), expiration date, CVV2, and magnetic stripe. PCI standard has increased controls around data and its exposure to compromise, which prevents fraud through credit card (Chen, Takabi, & Nhien-An, 2019).

The Health Insurance Portability and Accountability Act (HIPAA) is for organizations handling medical information. It imposes strict information security guidelines on every organization and healthcare provider dealing and handling with protected healthcare information (PHI) to assure the protection of patient's privacy. As per the US Department of Health and Human Services (HSS), HIPAA complaint organizations can process and store electronic protected health information (ePHI) in cloud computing, there is a are allowed to use cloud a Business Associate Agreement

(BAA) between organization and cloud service provider. With BAA in place, cloud service provider is responsible to secure ePHI as per the HIPAA security rules.

Service Organization Control 2 (SOC 2) The main concept of SOC 2 framework to conduct an assessment to report that customer data is managed based on five Trust Services Criteria – Security, availability, processing integrity, confidentiality, and privacy. This framework is developed by American Institute of Certified Public Accountants (AICPA). SOC 2 report is a predefined guideline for privacy and security to provide customers with an overview of privacy and security measures in place. It enables organizations to establish confidence and trust in their services, processes, and controls.

The NIST Special Publication 800–53 is a special framework part of the 800-series. It describes federal agencies, guidelines, and standards to build and maintain information security systems and risk management effectively. It provides common information security rules for all information systems and coherent and repeatable guidelines for selecting and defining standard security processes and controls. These standards and guidelines can be effectively used by private enterprises as well.

Control Objectives for Information and related Technology (COBIT) is developed by Information Systems Audit and Control Association (ISACA). It is an information technology management and governance model (framework). COBIT helps organizations achieve their business and operational challenges in the areas of aligning IT strategy with organizational goals, risk management, and regulatory compliance.

The Cloud Security Alliance Cloud Controls Matrix (CSA CCM) is a cybersecurity control framework for cloud service that consists of a list of controls gathered from various international Information Security Management System (ISMS) standards. It is composed of 197 control objectives covering all key attributes of cloud technology.

3.8 Compliance in cloud computing

Cloud compliance management is the process by which organizations assess, remediate, and prove it is complying with regulatory requirements and internal policies per industry guidelines, and national, and international laws. According to CSA (2017), compliance validates awareness of and adherence to corporate obligations. The compliance process assesses adherence to

requirements, risks, and impact on the cost of non-compliance compared to the cost of achieving compliance, hence recommending, and prioritizing any corrective actions deemed necessary.

Cloud compliance is the responsibility of both customer and the cloud service provider, but the ultimate responsibility of compliance lies with the customer. Customers should understand and define clear roles and responsibilities through contracts and audits with the cloud provider. In the case of the public cloud, the provider must mostly rely on third-party reports and attestations to evaluate their compliance requirements as providers do not allow individual customers to perform audits. Most cloud providers are having various regulatory certifications and take the responsibility to maintain these certifications. However, customers should clearly understand the scope and limitations of these certifications. Customer needs to take the compliance responsibility for whatever applications and services it is built on the cloud. The ultimate responsibility always lies with the customer to decide and manage data and services deployment location and remain compliant with legal and national and international jurisdictions (CSA, 2017).

3.9 Audit process in cloud computing

ISO defines the audit as "*a systematic and independent examination to determine whether quality activities and related results comply with planned arrangements and whether these arrangements are implemented effectively and are suitable to achieve objectives*". Audit is an independent review and evaluation to ensure organization's adherence to applicable processes, internal and external guidelines, and regulations. Audits are a key tool for proving (or disproving) organization's compliance with applicable framework. The cloud audit process can be classified as public, private, internal, or external based on security objectives and requirements. An audit can be performed with or without the support of a third-party auditor.

Internal audit: Cloud service customer uses their processes and procedures and executes the whole process. Cloud service customer does not take the support of any other third party. The internal auditor needs to assure management that all security risks are identified (Brumă, 2021).

Cloud provider auditing: Cloud service providers perform the auditing and specific audit reports are available via their websites. These reports certify their compliance with various regulatory international standards.

Public audit-TPA: Cloud audit is performed by a third-party auditor, independent of the cloud service provider and cloud service customer. The use of a third-party auditor (TPA) provides transparency and efficiency in performing the required auditing tasks and it serves as a bridge between the customer and the cloud service provider.

Current cloud auditing approaches can be classified as retroactive, intercept-and-check, and proactive auditing.

Retroactive audit approach: this is the traditional approach to detect the violation only after they occur as it is conducted periodically with a defined frequency. Due to its after-the-incident nature, it exposes the system to high risk and attackers can exploit the vulnerabilities of systems without getting noticed for a considerable amount of time (Wang, Ou, & Xun, 2019).

Intercept-and-check auditing approach: This approach verifies the compliance of each user request before granting or denying it at runtime. As this approach keep holding the event instances blocked, while performing the major verification, this can lead to a significant delay (Wang, Ou, Xun, 2019).

Proactive auditing approach: This auditing approach combines traditional audit approaches (above two) and incident management activities. It starts proactively auditing before critical events happen resulting in reducing the response time in the cloud.

4 Conducted research evaluation and implementation

During interviews, the researcher found that most of the organization's decision to move to the cloud is mainly driven by the desire for cost-benefit and not as part of their business or IT services roadmap. In this case, when economic benefits drive an organization's decision, often full understanding of needed changes in IT infrastructure and consideration of audit, risk, and compliance management become an afterthought. Organizations need to understand the perspective of IT audit about compliance and security risk before moving to the cloud as it can improve cost and make cloud computing successful. Regarding cloud security auditing standardization, most auditors found that it is better to keep the technology-neutral nature of the commonly used IT security auditing standards and add some uniquely important cloud computing-specific areas. Also, it is necessary to eliminate the controls which are no longer relevant or appropriate.

Auditing for the cloud depends a lot on the deployment model (private, public, community, or hybrid) and service model (SaaS, IaaS, PaaS). Hence, to move from traditional IT to cloud computing audits and compliance management is very important for an auditor to understand the scope of the cloud computing environment, a strong understanding of network scope, dependencies on third parties, and new controls or enhanced reliance on core security services. Cloud auditors should be very well familiar with an internal auditor role in cloud computing and the steps to follow during the audit program. This chapter describes all the above-needed changes in detail here along with a high-level audit checklist based on selected key points. Feedback has been taken in a semi-structured interview on the audit checklist and description of needed changes.

4.1 The internal audit role and skills in cloud computing

Internal audit and compliance have a key role as assurance providers to assist management as well as the board to identify and manage key risks areas related to the cloud. As companies navigate change, the IT Internal Audit function must make sure IT risk is both assessed and addressed. Through internal audit business and management can determine if those risks are appropriately mitigated.

Internal auditors need to act like a "trusted advisor" as the organization takes on new risks moving to cloud computing and:

- proactively provide consultative and assurance support and service;

- inform, train, and engage with the audit Committee/management/board; and
- have the knowledge and forward-looking mindset to have continuous compliance with all relevant regulations.

Internal audit must understand and keep updating the knowledge on cloud computing risks and provide recommendations to mitigate risks. Internal audits should participate and coordinate with cross-functional departments to identify risks, implications, vulnerabilities, and mitigation plans. IA should evaluate the adequacy and effectiveness of processes and control in product/project implementation across functions and recognize the absence of any authoritative control baseline.

In addition to audit skills, cloud auditors need to have good knowledge of cyber security, system architecture, cloud deployments, and service models. They should have knowledge of the operation and fundamental business processes along with organization relationship knowledge.

4.2 Information security audit planning

In performing effective cloud audits necessary first step is to do adequate planning. During the planning of a cloud security and compliance audit, it is important to have a clear understanding of audit objectives and scope. In the planning phase, auditors should form an overview of the organization and the processes. Auditors need to have a clear understanding of the organization's business model, information, and technology resources. It allows for more strategic compliance. Organizations should align their business objectives with the cloud auditing objective to ensure achieving a strong internal control environment and reducing the risk of a qualified opinion. Auditors should understand and collect information from all audited areas to understand the policies, procedures, and applicable standards and regulations. Objectives are used by auditors as a way of concluding the collected evidence.

Scope of auditing is another factor to consider. The scope factor becomes very important mainly due to new technology types of audits in cloud computing. During identifying the scope, the auditor should identify all components like personnel, processes, and systems included in the process. An auditor needs to know the cloud service and deployment model used. All the elements like databases, applications, and infrastructure are included or not included in the service model. The scope should be clearly defined the systems hosted on the cloud and the systems hosted internally. The scope should state the dependencies on third parties – services provided by the third

parties and the areas controlled by them. Some CSPs, particularly large cloud providers provide third-party audit reports to confirm their infrastructure meets compliance standards.

4.3 Risk assessment

It is important to perform a risk analysis before audit planning. Ideally, decisions related to compliance and security auditing should always be backed by risks. For an auditor, it is essential to have a clear understanding of the risks one is ascertaining. Risk could be defined as the possibility of suffering loss, destruction, or damage to an asset because of a threat exploiting a vulnerability. An asset's value could be determined based on the time and resources required to rebuild or restore the asset to its former state. Vulnerability is a known weakness in a particular asset that could lead to the exploitation of the asset in question. All of this can be put into a form of an equation: risk = threat x vulnerability + asset value (Bejtlich, 2004).

In practice, the auditor should know key assets, the risks these assets may pose, and the risk tolerance. Risk tolerance is the level of risk that an organization's leadership and stakeholders are prepared to accept in pursuit of its objectives. It usually varies based on the asset. Moving to the cloud does not change an asset's risk tolerance, it only changes how risk is managed. Cloud computing risk management is based on the shared responsibilities model. The CSPs take responsibility for certain risks, and the CSC is responsible for other remaining risks. This also varies based on the cloud service model, for example, CSP manages more risks in SaaS and the CSC more in IaaS. But, irrespective of the service model, the ultimate responsibility of risk lies with CSC (CSA, 2017).

4.4 Types of control

After assessing and understanding information security risks, threats, and vulnerabilities, the next step in auditing is to make sure that there are the right safeguards and control in place. Controls help to mitigate various types of threats to the organization. These safeguards or protection measures are the first line' of defense to reduce information security risks such as unauthorized updates and deletion of digital information, data and information systems theft, and breaches. An effective cybersecurity control is a mechanism that prevents, detects, and mitigates an attack and enables recovery from a risk event. Depending on the nature of what an organization wants to protect, there could be many ways to apply controls. Controls are generally composed of policies, procedures, organizational structures, physical, logical, and operational access limitations implemented to reduce risk to the organization. Efficient internal controls should be able to provide

reasonable assurance to management that the organization's risk events will be prevented, mitigated, detected, or corrected to achieve business objectives. The controls should address two key aspects. A well-designed information system is comprised of controls built-in for all its critical, and sensitive functional areas. There are three categories of information system controls - preventive, detective, or corrective.

- Preventive security controls, intended to prevent cyber security incidents from occurring. These are effective before the event

- Detective security controls, intended to detect a cyber security breach attempt and characterize an incident in progress by sending an alert to cyber security personnel or sounding the intruder alarm

- Corrective security controls, intended to use after a cyber security incident to reduce the loss of sensitive and critical data and damage to the system or network. These controls are also meant to recover critical business application, systems, and processes as quickly and efficiently as possible.

Security controls can also be classified according to their characteristics,

- Procedural or administrative controls such as incident response plans and procedures, management oversight, security awareness and training, Systems development methodologies and change control, operations procedures, Quality assurance (QA) procedures.

- Access controls such as restriction on physical access - fences, doors, locks, and fire extinguishers.

- Technical or logical controls such as multi-factor user authentication (login) and logical access controls including data and programs, antivirus software, firewalls.

- Legal and regulatory or compliance controls such as national and international laws, policies, cyber security frameworks, and standards.

4.5 Information security audit execution

In this section, based on the literature review and interview author listed the key domain areas and their security controls which should be audited by a cloud auditor. The author created this checklist using a constructive approach. Regular feedback was collected and incorporated into the development of this checklist.

4.6 Audit checklist and assessment tool

In this section, the author developed a cloud audit checklist using the comprehensive study of literary material from several sources and interviews, including checklist from ISACA, the NIST framework and cloud control matrix from CSA (See table 1). The author explained and took feedback from participants during interviews. The author incorporated all feedback in the following checklist which can assist customers, auditors, and compliance analysts to perform value-added cloud audits.

Table 1: Cloud Audit Assessment and Checklist

This table continues till page 61.

Area	Control Description	Control Type
Governance	An organization has defined and implemented a formal governance structure to manage and guide ongoing operations with a cloud deployment program Information security roles and responsibilities are clearly defined, implemented, and coordinated with internal and external stakeholders. Roles and responsibilities are defined in the job descriptions, RACI charts, policies, contracts, and agreements Governance personnel is separate from the daily operational personnel. Governance	Preventive

	personnel report and consult regularly with the top management – board of directors, key business stakeholders, audit & risk committee For the critical function, there is sufficient segregation of duties to provide independence in performing the role The Cloud program steering committee is regularly meeting operational management, reviewing the status, service level agreements, and effectiveness of information security and cloud services Clear ownership and accountability are defined and established for each cloud application and its related resources	
Security policies, processes, and procedures	The organization has a written and approved information security policy and plan including the use of cloud services. This policy is a living document, reviewed and updated regularly as per the latest development The organization has understood its legal, regulatory, civil, and privacy obligation requirements. These requirements are mapped to information security policy and considered in the cloud deployment program	Preventive and corrective

	Information security policy and plan adequately describe cloud security requirements and how these will be achieved There is a formalized process to follow changes in legal and regulatory requirements and update policy accordingly An owner has been nominated and documented for each policy and procedure that exists Management and all relevant stakeholders formally review the documents. At least annually Formal processes and procedures are defined and implemented for business-critical functions like change management, incident management, disaster recovery, and business continuity management Change management process and procedure adequately define – the process for documentation of change records, retention period per change records, priority classification rules for changes, approvals needed as per the priority of changes, test requirements, test plans, and rollback plans The incident management process covers – all phases of a security incident response management, escalation process, communication, and reporting procedure, contact	

	information, and procedures for key stakeholders Disaster recovery plan (DCP) and business continuity processes (BCP) cover – complete business impact analysis, control measures, and mitigation actions to reduce risk, recovery procedures including recovery time objective (RTO) and recovery point objective (RPO) have been identified for critical applications, databases, and assets. Disaster recovery and business continuity plans have been tested and lessons learned incorporated	
Global Regulations and cloud computing	The organization has identified and understood applicable government regulations, laws, and standards for its business in each location and country The organization a has clear understanding of what regulations and standards CSP offers and CSP is agreeing to audit by the CSU or a third party Determine separation of roles and responsibility between CSP and CSU on cross-border and legal jurisdictional issues and compliance responsibilities division Check the service level agreements between CSP and CSU and verify the implementation level of process for handling and	Preventive

	investigating the security breach, what roles and responsibilities CSP has in this Determine if CSP is transparent in providing the geographical location of data storage and binding with customer's compliance need to have data in a particular country only	
Risk Management	Enterprise risk management processes are defined, formally documented, repeatable, measurable, and agreed upon by relevant stakeholders. Approved ERM processes are implemented and maintained regularly Overall business risk tolerance is defined and agreed upon with higher management including cyber and cloud risk appetite Enterprise risk management strategy and appetite are aligned with its role in critical infrastructure Risk assessments are being conducted at planned time intervals considering the following -data governance requirements – understanding the location of sensitive data, servers, data in transit, databases, and network infrastructure The organization performs cloud vendor due diligence on regular planned intervals, identify relevant risks, rate them appropriately, reports them to management and	Preventive

	relevant stakeholders to adjust cloud operations accordingly	
Asset Management	The organization has done classification and prioritization of information assets as per CIA based risk analysis and identified the privacy and protection needs for each asset accordingly Before moving to the cloud, has the organization identified the controls which were available in an internally hosted system but are not provided by the CSP? What is the organization's plan to have those controls in place? Determine if the organization has evaluated and decided cloud service and deployment model based on its privacy and protection needs for each asset Obtain the process of deciding, and documenting. setting up and monitoring the configuration or security requirements of each information asset deployed to the cloud As per judgmental selection, Inquire and verify if information assets deployed in the cloud are configured as per documented configuration or security requirements Find out and inspect the evidence showing that organization regularly reviews and	Preventive and detective

	assess asset configuration and security requirements Obtain the organization change and configuration management process for assets deployed in the cloud. Inquire if changes are being prioritized and formal time has been allocated for scheduled changes Enquire if emergency changes in cloud assets follow the process of proper risk assessment, testing, and additional approvals Identify the volume of regular changes vs emergency changes Determine the method or tool the organization uses to assess vulnerability in cloud assets. Inspect the method of interpretation, prioritizing, and documenting output from a scanning tool Inspect and find out if the high and critical vulnerabilities have been remediated as per the agreed schedule Determine the evaluation method organization uses to identify assets deployed in the cloud which are being charged but not adding any business values Obtain and inspect the organization's process for defining, implementing, and following data retention and data-purging for assets deployed in the cloud. Find out the	

	evidence of data archiving and removing as per the defined process for a cloud asset Is the organization performing penetration testing as per the agreed schedule? Who are the personnel informing the statement of work, how do they maintain a non-disclosure agreement, and who are the people receiving the penetration testing report? Are identified vulnerabilities being remediated as per the defined timeline and priority?	
Identity and logical access control	Review the process of Organization has established user access policies and procedures to ensure identity and access management for all internal and customer users Access to cloud applications and network devices like firewalls, mobile, servers, databases, and workstations is authorized through unique credentials and complex passwords. Multifactor authentication is implemented where necessary Automatic time out if inactive for a certain period and automatic lockout after repeated failed access attempts Verify if password files are suppressed from all output, restricted, and encrypted? Procedure to disable cloud applications accounts that are inactive for a defined period	Preventive

	Access permissions are identified and managed based on segregation of roles and responsibilities and principles of least privilege Determine how users with high network privilege are restricted access to sensitive data Verify if users are given access based on their job profile Review the process of terminating access to cloud applications when the user leaves the company Review remote users' access policy and procedure are established and implemented. Remote connections are established only on a need basis Remote connections are encrypted, logged, and monitored Verify if the organization regularly reviews the cloud application and user access Determine and check if the organization has separated	
Business Continuity and Disaster Recovery	A disaster recovery plan and business continuity plan are reviewed and approved by relevant stakeholders and management. Extensive training has been provided to	Detective and corrective

	operation users and they have understood this very well DRP and BCP have defined roles and responsibilities, manual workaround, lines of communication and have an owner responsible for incorporating lessons learned, updates, and approvals Determine if CSP has DRP and BCP controls in place and the organization has assessed those controls. Does CSP provide evidence of its DRP and BCP plans testing? CSP has considered physical protection (protection against fire, flood, natural disaster, earthquake, tsunami, explosion, civil unrest, etc.) in their DRP and BCP and has mitigations plans in place against all these physical risks Determine if the organization has considered business continuity for its critical applications and databases in case of CSP has disruption? Critical cloud applications are having a backup at multiple data centers Disaster recovery and business continuity operational personnel and coordinators are crosses trained on their roles and responsibilities During the planning and testing of DRP and BCP organization has identified its critical applications and service and threats	

	associated with them understood all dependencies like CSP, processes, vendors, determine RTO and RPO for critical applications and services, and established maximum tolerable disruption period and resources required for recovery	
Network configuration and management	Ensure the organization has developed a network architecture diagram depicting high-risk environments and data flows, the defense-in-depth mechanism is used to protect against network-based cyber-attacks Identify the number of virtual private clouds per root account, total root accounts in use, what are the regions VPC are deployed, what are the peering connections between VPC Critical cloud assets and their data have been secured using network architecture based on organization security requirements and best practices Determine method and frequency of reviews to assess compliance of cloud assets network security architecture with the defined standard. Verify that non-compliance deficiency is being remediated promptly Enquire if the organization has implemented security information and event management (SIEM). Check if baselines and	Detective

	alerting capabilities are appropriately defined and function as intended Determine relevant cloud environments are existing to deploy different business environments (production, staging, R&D). Find out the process for maintaining logical isolation of all environments and detecting non-compliance Discover how the organization is controlling inbound and outbound cloud network traffic? Is it aligned with the organization's access control policy through the firewall? Identify firewall rules, routing tables for each subnet, network access control list, etc. Ensure the organization is using the least privilege principle to provide and maintain cloud access controls. Verify access control process for each administrative tool, cloud root accounts, command-line interface, management console, etc. Ensure processes and procedures are existing in the organization to incorporate on-premises systems and data with cloud applications. Inspect the methods organization uses to integrate or migrate data and make sure that security requirements and guidance were incorporated	

	Verify the connection between the organization and cloud services, make sure VPN connectivity is highly available	
Security Incident management	Determine the organization's security incident response process, plan, and documentation. Verify all these documents are reviewed and approved by relevant stakeholders and within the timeframe decided by the organization. Make sure that the document is a living document, which means changes are being updated and approved regularly Find out if the organization's relevant staff and management have a clear understanding and knowledge of security incident response plan, process, and documentation to act in the event of a security incident Make sure that crises communication plans and processes are in place and known to relevant stakeholders. Find out if operational staff and management are aware of the process of reporting legal, customer, and regulatory authorities about a security breach. Are they aware of their roles and responsibilities during a security breach? Do they know about the distribution list of individuals to be included in crisis communication? What are the requirements to inform the authorities and media?	Detective and corrective

	The organization is conducting a simulated exercise to prepare the team to respond against a security threat to improve its security response capabilities. Check if meeting minutes were recorded, reports were created, lessons learned were organized and incorporated after each exercise Verify if accountable operational and security staff are aware of security events within the time frame. SIEM-generated alerts are being delivered to relevant operational and security staff, they know and perform their tasks within time limits. They are aware of how to identify false positives and false negative alarms The organization is archiving and retaining for the determined time frame all the needed information related to security incident event Inspect if crises communication contact information is kept up to date. Contact information for internal and external partners is being updated regularly Determine whether cloud service provider support staff have appropriate access created to handle the event during a security incident. Cloud service providers know their roles and responsibilities very well. They know whom to communicate with and	

	collaborate with at the CSU side during the event Escalation process and channels are known to internal CSU and CSP operational and security staff	
Data Security and Encryption controls	Ensure Organization has performed and maintained data and information classification based on data sensitivity, type, value, and criticality to the organization. Identify if the Data owner had been nominated for each data type. Data owners are aware of their responsibilities and governing data under their purview Determine organization had established policies and procedures to support data security aligned with its risk strategy to maintain confidentiality, integrity, and availability across business functions, jurisdiction, and multiple system interfaces Verify Organization created specification of cloud data and information protection and privacy based on established data security policies and procedures Check agreement and verify that in case of customer data usage as part of the service, CSP will inform CSU about associated risk and compliance impact Inspect needed reviews and approvals are in place in case the customer's production	Preventive

	data is being used in a non-production environment. Sensitive information in production data is masked and aligned with all regulatory and legal requirements Ensure complete removal of data according to policy and standards from all storage media. Review sanitization techniques and measures implemented for secured removal of data and ensure data are not recoverable by any means. Spot-check trash cans and shred bins to ensure confidential data is destroyed according to policy Determine and ensure audit logs are maintained and reviewed regularly in a cloud environment. Inspect the adequacy of audit logs that it contains appropriate content. Logs are not deleted before review and archived according to policy. Audit logs are secured as per CIA rules. It is important that network perimeter and systems (Windows, Unix/Linux servers, switches) logs are monitored and reviewed constantly Determine protocols and levels of encryption defined, agreed upon, and used for each cloud application and data in use, data in transmission, and data at rest. Review third-party contracts to verify defined encryption and security protocols are used to secure data at rest, in use, and transition	

	Owners had been identified and nominated for encryption keys. Cryptographic key management policies have been defined. Does CSP inform the customer, in case of changes in the CSP cryptosystem and CSU needs to implement or update some of the controls? Encryption keys are not stored in the cloud Determine if the organization has a mechanism to generate alters or notifications, in the case of cloud application and data encryption failure or misconfiguration. Identify how these alerts are maintained when there is a change in the cloud application Find out if CSP provides, true multitenancy and manages granular privilege for all data information in this environment	
Security continuous monitoring	Ensure the organization has identified, formally documented, and establish minimum monitoring and logging requirements of each cloud application and asset. The organization is assessing and reviewing these requirements regularly Inspect that cloud applications are configured based on minimum requirements and generate monitored events required by the organization Obtain the evidence that individuals or groups are receiving alerts when there is	Preventive and Detective

	comptonization in cloud application logging functionality Ensure the organization is retaining and archiving cloud application-generated logs for a defined time. Appropriate access to the logs has been provided using least privilege and job responsibility criteria Ensure logs are reviewed by responsible personnel periodically at a defined period. Determine the method of logs investigation to find out suspicious events or activities, communication, and remediation approaches	
Cloud-based Audit and compliance assurance	Identify if any legal counsel evaluated CSP contracts, protection and confidentially, and intellectual controls? What if there is a change in control of the cloud provider? Ensure that organization had considered standard audit and compliance issues while identifying and deciding about cloud provider, service, and deployment model. Find out the auditor's independence, technical, and professional capabilities by checking provided audit report which states identified deficiencies and recommendations for remediation Identify cloud service providers' processes and procedures for identity and access management and authentications placed in	Preventive and detective

	the cloud. What is the way to audit or have an independent audit report on this? Obtain the cloud service provider process for patching and testing. How does it impact applications moved to the cloud? Ensure the organization had identify and implemented additional changes needed in its endpoint security measures to move to the cloud Investigate if the organization used standard frameworks like COBIT, CSA, or NIST to understand the system and infrastructure life cycle management for the cloud	
Configuration and change management	Obtain evidence and ensure the organization follows defined and agreed to change and configuration management process during the development and launch of new applications or data, infrastructure, and network components in the cloud environment Verify external third-party providers are also adhering to the agreed policy and procedures for change and configuration management for cloud applications Verify unauthorized software is not installed or allowed to install on organizationally owned devices, networks, and system components	Preventive

	Ensure change management policies are applicable in changes of operating systems, versions update, patching, and applications version of mobile devices	
Mobile Security	The organization has provided an approved list of applications to mobile device users to store or access data managed by CSP Organization communicated to mobile device users' policy prohibiting use of non-approved applications Detective and preventive controls should be in place to prohibit the alteration of mobile devices' built-in security Ensure technical controls are configured in mobile devices and BYOD to enable automatic lockout screen Technical controls are in place to enforce the organization's mobile device password policy and prohibit the password pin length and authentication requirement changes Ensure mobile device and BYOD users are aware of the data backup policy and the requirement of anti-malware software usage Ensure authorized mobile device users can remotely install the latest security-related patches	Preventive

Human resource and Awareness Training	Verifies if privileged users are trained and understand their roles and responsibilities Review and verify if vendors and contractors understand and comply with roles and responsibilities defined in contracts and agreements Ensure background checks had been performed to hire employees. Newly onboarded personnel need to sign agreements to adhere to security and governance policies before accessing organization assets and resources Determine and verify the evidence of disabling accounts and access promptly for individuals who are terminated or resigned from the organization. Ensure organizational owned assets are returned within the defined time when personnel resigned or got terminated The organization had identified and defined non-disclosure and confidentiality agreement that need to be signed by all personals Ensure roles and responsibilities are clearly defined and understood with third-party contractors. Verify if third party contractors and vendors are complying with cyber security policies and roles and responsibilities	Preventive and detective

	Ensure the organization's senior executives are well educated and trained on cybersecurity knowledge. They have adequate knowledge to perform their roles and responsibilities Obtain and review the organization's training material and calendar to ensure materials are updated and training has a schedule as per cages in the threat environment	
Data Center Security	Ensure organization data center physical security perimeters are established to secure information systems Obtain evidence of approval to relocate or transfer data, software, or hardware Make sure a secure and safe working environment and office facilities have been provided to organization staff	Preventive

5 Results and discussion

5.1 Answer to the research question and outcome of the thesis

The goal of this thesis was to find out the answer to the research question, 'what are the changes required in traditional audits and compliance management to address cloud-specific attributes and recommendations?'. The author performed the following tasks to understand the answer to the research question and provide the outcome of the thesis:

Literature review analysis and unstructured interviews

- lot of existing material, literature, and documents were reviewed and analyzed to gather comprehensive information on cloud system's constitution, its essential characteristics, service and delivery model, and various cloud terminology.
- based on service and delivery model, detailed knowledge was gained on cloud compliance responsibilities division between provider and customer.
- detailed understanding of challenges with securing cloud.
- evaluated all possible key risks areas in cloud computing.
- Unstructured interviews with colleagues and friends working in IT and cyber security areas were performed to gain detailed knowledge and legitimize the initial findings as per literature review

Semi-structured interview analysis

- Literature review analysis and unstructured interviews contributed to defining the attributes and detailed description to be added to the checklist tool. This checklist provides key domain areas to be audited on the responsibility of those areas (provider/customer)
- Semi-structured interviews provided feedback in assessing and validating solution implementation that is a checklist development and applicability. All the feedback and comments were incorporated to fine-tune the cloud audit checklist which can assist customers, auditors, and compliance analysts to perform value-added cloud audits

As an answer to the research question, it can be summarized that following changes in traditional audits and compliance management are needed to address cloud-specific attributes. Research concludes that auditor and compliance manager should:

- know the steps to perform cloud risk assessment,
- understand the scope of the cloud computing environment, dependencies on third parties, and new controls or enhanced reliance on core security services,
- aware of division of roles and responsibilities between the cloud service provider, third party, and cloud service user,
- familiar with cloud security auditing frameworks and standards,
- know the steps to follow during information security audit planning and execution,
- understand organization's legal, regulatory, civil, and privacy obligation requirement, and
- aware of the user access management process, security incident management process, change management process, business continuity and disaster recovery management process.

5.2 Literature review analysis and unstructured interviews

The researcher started research by reviewing and analyzing existing material, literature, and documents on the topic to gather general and comprehensive information. The researcher analyzed a lot of material available through ZAMK (e-books on Skillport, IEEE, and Theseus), and available online through government and standards organizations. Reviewing literature provided the researcher not only a general overview but also detailed information for enhancing the understanding of the research question.

To determine and understand the cloud system's constitution, the researcher investigated ISO/IEC and National Institute of Standards and Technology (NIST) definition of cloud computing, its essential characteristics, and various cloud terminology. The researcher further enhanced the knowledge of cloud computing by understanding its service and deployment models in detail. The researcher found 'Security Guidance for Critical Areas of Focus in Cloud Computing v4.0' provided by the Cloud security alliance, very useful as it describes in detail all the aspects of cloud architecture, risk management, governance, and security. This guide has 14 domains that can provide all necessary cloud computing information and terminology to auditors. Cloud service delivery and deployment models indicate how cloud services are made available and consumed. There are

different attributes and implications for the end-users. Usually, a cloud deployment model depends on the infrastructure in which the deployment resides and who (CSP or CSU) controls the infrastructure. This knowledge and familiarity make auditors pay attention to important security aspects and better understand cloud compliance responsibilities division between provider and customer.

When understanding changes required in traditional audits to address cloud-specific attributes, it is important to understand the changes in traditional IT systems and cloud computing systems. The researcher found that IEEE papers and some books found through JAMK's Skillport were good to understand the pros and cons of each. Audit and security methods applied in traditional IT systems cannot be fully applied due to the concept of shared responsibility, access to multiple users across a large domain, and in the cloud computing and traditional security operations tools, do not work as the perimeter.

To better understand all aspects of cloud security for auditing and analyzing cloud keys risks and security issues researcher reviewed several widely published resources. Security threats and key risks identified in NIST, 2018 and ENISA,2012 were found interesting and useful at this point. Key risk areas for auditing like cloud governance, data protection and encryption, identity and access management in the cloud, shared technology vulnerabilities, etc. were analyzed in detail. The researcher further enhanced the knowledge by reviewing available cloud security auditing frameworks, compliance, and audit management process in cloud computing. This part of the study laid the foundation that supported the analysis and design of this research.

During the literature review, the researcher conducted unstructured interviews to legitimize the initial findings and gain detailed practical knowledge to define key concepts and domain areas for the 'cloud audit checklist' as an outcome of the thesis. Unstructured interviews also helped to assess the knowledge of the IT-auditors, compliance, and risk management experts on cloud computing auditing and the changes they have made in moving from traditional IT auditing to cloud auditing.

The researcher compiled all the gathered knowledge based on a detailed understanding of the literature review and unstructured interview and drafted a detailed cloud audit checklist.

5.3 Semi-structured interview analysis

Semi-structured interviews were conducted in March 2022. Altogether, the researcher interviewed 10 persons. Out of 10, one interviewee was working as a chief information security officer, four interviewees as an auditor, one as a compliance manager, two were risk managers and two were program and project managers. Most of them knew about the research being conducted and accepted the invitation instantly. The researcher considered this as a good sign indicating that interviewees are eager to know about the 'audit checklist' I prepared. All the interviewees participated very actively and provided constructive feedback and several improvement points on the audit checklist. Three auditors accepted to test the checklist by using this as an input in their upcoming audit assignment. As the interviews progressed, all the feedback and comments were incorporated to fine-tune the cloud audit checklist.

During the interview, the researcher discovered that most of the time organizations' moving to the cloud is driven by the intention of cost-benefit achievement, not as an IT or business strategy. Organizations need to have a clear understanding and analysis of security and compliance risks from an auditor's perspective before moving to the cloud. Regarding cloud security auditing standardization, almost all interviewees had an opinion to add cloud-specific important control areas into the commonly used IT security auditing standards and remove the controls which are no longer relevant.

6 Conclusion

Cloud computing has become an essential component of today's society and significantly changed the way traditional IT system has been used. More and more organizations are adopting serverless and service-oriented architecture. Cloud service providers continuously adopting measures and new capabilities to provide economic reasons and data security to cloud service customers. However, security risks are increasing due to remote labor, changing legal and geo-political landscape, and cloud service providers introducing new vulnerabilities while adding new capabilities. Organizations must understand and address compliance and security risks through IT audits or assessments before procuring and moving to cloud services. As cloud services and systems are different than traditional IT system, there is a need for a change in traditional IT auditing to build trust and compliance in cloud environment and make cloud computing successful. Hence, the main question and objective was to research and analyze areas where traditional audits and compliance need to be changed to address cloud-specific attributes and recommendations.

A combination of qualitative and constructive research methodology was used. The research was first conducted using 'document analysis/literature review' and 'un-structured interview' methods of qualitative research methodology. Constructive research methodology together with semi-structured interview, was used to develop an 'audit checklist' as an outcome of the research. In this research work, interviews served dual goals, firstly un-structured interviews helped in gaining detailed knowledge, legitimize the initial findings as per literature review, and define key concepts. Secondly, semi-structured interviews provided feedback in assessing and validating solution implementation that is a checklist development.

Research conducted by reviewing and analyzing lot of literature, material, and documents available online through IEEE, Skillport, Theseus, government, and standard organizations like NIST, ENISA, CSA, ISO/SEC, etc. The researcher further enhanced the knowledge of cloud computing by understanding cloud system's constitution, its essential characteristics, service and delivery model, and various cloud terminology. The researcher found 'Security Guidance for Critical Areas of Focus in Cloud Computing v4.0' provided by the Cloud security alliance, very useful as it describes in detail all the aspects of cloud architecture, risk management, governance, and security. Challenges with securing cloud and evaluation of all possible key risks areas in cloud computing defined in NIST, 2018 and ENISA, 2012 were found interesting and useful.

The research demonstrates that organizations should always understand the security and compliance risks of overall business opportunities and appetite for risk before adopting the cloud. The risks of moving to cloud services should be compared to the risks of continuing with traditional solutions. Organizations should understand the importance of security audits and take feedback from internal auditors on the security status. The research objective was met by having and answer to the research question that there is a need for a paradigm shift in traditional IT auditing to embrace and leverage the advantage of modern era of cloud computing. Auditors and compliance managers should have the knowledge and good understanding of cloud computing systems, its delivery and service model, division of roles and responsibilities between CSP and CSU, cloud key risks and security issues, cloud-specific auditing frameworks, and auditing processes are important for auditors to transition from traditional IT auditing to cloud-specific auditing. The desired outcome of the thesis was achieved by developing a cloud audit checklist using the comprehensive study of literary material and having feedback from participants during interviews. Three auditors agreed to use and further evaluate the cloud audit checklist in their upcoming audit assignments.

Although there are several security frameworks available, specific to different industries to provide a holistic approach to protecting organizations, there is no single mandatory cyber security or cloud security framework applicable for all organization. For example, PCI-DSS is mandatory framework for processing credit card data, all US public companies must comply with SOX compliance, and so on. Most of organizations are giving priority to their mandatory applicable frameworks and gaining cyber security protection along with that. During interviews it was apparent that SOX compliance is ‘the priority’ for US public companies and GDPR compliance for companies operating or dealing with EU citizen’s personal data. Most of these companies perform the risk assessments from SOX or GDPR point of view and its possible that certain aspects of cyber security in cloud are overlooked. Due to this, there was some conflict in interviewees perspective and opinion on cloud services security. There is no mandatory cybersecurity framework applicable to organizations providing timely, consistent, and sufficient reporting. To address this, recently Security and Exchange Commission (SEC) has proposed a new rule which will require mandatory cybersecurity disclosures from companies about “cybersecurity incidents, governance, strategy and risk management.

Though the thesis project achieved its objective and produced the outcome successfully, some limitations and shortcomings were identified. There was no possibility to perform the real cloud audit in a real cloud environment and on some topics, interviewees also have limited exposure,

some areas researched in a superficial way. Also, during the literature review and interview process, it was apparent that cloud auditing and compliance cannot be only point-in-time activities as cloud service users and cloud service providers both expect and deliver new functionality, services, and innovation, respectively. Manual audit results become obsolete in very short time. With dynamic, high operational complexity of clouds and fast-paced technology evolutions, it is desirable from cloud service providers to have runtime security auditing processes and provide continuous assurance against security threats. It opens a potential topic and new area for future research to have continuous audit and compliance with cloud computing.

Hopefully, internal auditors, compliance analysts, and cyber resilience team members will use the 'audit assessment checklist' and information provided. This checklist can also be used as a tracking cloud security implementation status and assessing maturity level. This tool can be used as a basis (requirements specification) to decide and select cloud service providers. Researcher gained lot of knowledge in cloud service terminology, delivery and service models, shared responsibility model and more over on performing overall cyber and cloud audit. During research, author passed and achieved 'Certified Information System Auditor' certificate. The main benefit of the thesis for the author was to prepare for the IT auditor jobs, confidently demonstrate in-depth knowledge about cyber security, and receive internal IT auditor job offers in two Fortune 500 companies.

References

Ames, B., & Brown, F. (2011). *Auditing the cloud. Internal Auditor*, 68(4), 35-39. http://search.ebscohost.com.ezproxy.jamk.fi:2048/login.aspx?direct=true&db=bsh&AN=67123098&site=ehost-live

Bassett, G., Hylender, C.D., Langlois, P., Pinto, A., Widup, S., (2021). *DBIR Master's Guide*. Verizon Business. https://www.verizon.com/business/resources/reports/dbir/2021/masters-guide/

Becker, H., Berger, P., Luckmann, T., Burawoy, M., Gans, H., ... & Mills, C. (2002). *Observation and interviewing: options and choices in qualitative research*. In May, T. (Ed.), Qualitative research in action (pp. 200-224). SAGE Publications. https://www.doi.org/10.4135/9781849209656

Bejtlich, R. (2004). *The Tao of Network Security Monitoring Beyond Intrusion Detection*. Addison-Wesley Professional. https://isbnsearch.org/isbn/9780321246776.

Bengtsson, M. (2016). *How to plan and perform a qualitative study using content analysis*. NursingPlus Open, 2, 8-14. https://doi.org/10.1016/j.npls.2016.01.00

Bharadwaj, D. R., Bhattacharya, A., & Chakkaravarthy, M., "*Cloud Threat Defense – A Threat Protection and Security Compliance Solution,*" 2018 IEEE International Conference on Cloud Computing in Emerging Markets (CCEM), 2018, pp. 95-99, doi: 10.1109/CCEM.2018.00024.

Brumă. L. M., (2021). *Cloud security audit – issues and challenges*, 16th International Conference on Computer Science & Education (ICCSE), 2021, pp. 263-266, doi: 10.1109/ICCSE51940.2021.9569654.

Chen, L., Takabi, H. (eds), & Nhien-An L. (2019). *Security, privacy, and digital forensics in the cloud*. [Skillsoft version] Available from https://masterworkshop.skillport.com/skillportfe/main.action?assetid=146072

Cloud Security Alliance (CSA). (2017, July). *Security Guidance for Critical Areas of Focus in Cloud Computing v4.0. Cloud Security Alliance*. https://cloudsecurityalliance.org/artifacts/security-guidance-v4/

Columbus, L. (2018). *83% Of Enterprise Workloads Will Be In The Cloud By 2020*. Forbes. https://www.forbes.com/sites/louiscolumbus/2018/01/07/83-of-enterprise-workloads-will-be-in-the-cloud-by-2020/?sh=18dd101d6261

Costa, D., (2017, March 7). *CERT Definition of 'Insider Threat'* - Updated [Blog post]. Available from: http://insights.sei.cmu.edu/blog/cert-definition-of-insider-threat-updated/

Chou, D. (2009, January 13). *Cloud Computing and the Microsoft Platform*. Available from: https://dachou.github.io/2009/01/13/cloud-computing-and-microsoft-platform.html

European Network Information Security Agency (ENISA), Glossary [cited July 2014]. Available from: https://www.enisa.europa.eu/activities/risk-management/current-risk/risk-management-inventory/glossary.

European Network Information Security Agency (ENISA), 2012. *Cloud Computing: Benefits, risks, and recommendations for information security*. Available from https://resilience.enisa.europa.eu/cloud-security-and-resilience/publications/cloud-computing-benefits-risks-and-recommendations-for-information-security

Halpert, B., (2011). *Auditing cloud computing: a security and privacy guide*. [Skillsoft version] Available from: https://masterworkshop.skillport.com/skillportfe/main.action?assetid=44303

ISO/IEC. (2014, October). ISO/IEC 17788:2014 *Information technology — Cloud computing — Overview and vocabulary*. ISO. Available from: https://www.iso.org/standard/60544.html

ISO 10011-1:1990. ISO. (2022)., Available from https://www.iso.org/standard/17940.html.

JAMK University of Applied Sciences. (2018). *Pedagogical and ethical principles*. Available from: https://studyguide.jamk.fi/en/study-guide-masters-degrees/information-aboutjamk/pedagogical-and-ethical-principles/

Linthicum, D., (2013). *Power Outages are the Most Pervasive Reasons for Cloud Outages*. Available from: http://research.gigaom.com/2013/03/power-outages-are-the-most-pervasive-reasons-for-cloud-outages/.

Kananen, J. (2015). *Online research for preparing your thesis: A guide for conducting qualitative and quantitative research online*. JAMK University of Applied Sciences.

Kasanen, E., Lukka, K., & Siitonen, A. (1993). *The Constructive Approach in Management Accounting Research*. Journal of Management Accounting Research, 5, 243-264. http://search.ebscohost.com.ezproxy.jamk.fi:2048/login.aspx?direct=true&db=bsh&AN=9701211561&site=ehost-live

Leavy, P. (Ed.). (2014). *The oxford handbook of qualitative research*. ProQuest Ebook Central https://ebookcentral-proquest-com.ezproxy.jamk.fi:2443

Majumdar, S., Madi, T., Wang, Y., Tabiban, A., Oqaily, M., Alimohammadifar, A., Jarraya, Y., Pourzandi, M., Wang, L. & Debbab, M., (2019), *Cloud Security Auditing, Springer*

May, T. (Ed.) (2002). *Qualitative research in action*. SAGE Publications Ltd https://dx.doi.org/10.4135/9781849209656

Mell, P. & Grance, T. (2011, September). *The NIST definition of cloud computing. National Institute of Standards and Technology (NIST)*. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

Patrick, Z. P. G., & Satyanarayana, K. (2020). *optimization of service level agreements (SLAs) within SaaS cloud infrastructure*. Journal of Critical Reviews, 7(1), 414-420.

Panetta, K. (2019). *Is The Cloud Secure*. Gartner. https://www.gartner.com/smarterwithgartner/is-the-cloud-secure

Portney, L. 2019. *Foundations of Evidence-Based Practice*. 4th edition, F.A. Davis Company Clinical Research: Applications

Rountree, D., Castrillo. I., (2014), *Cloud Deployment Models* https://www.sciencedirect.com/topics/computer-science/cloud-deployment-model

Ryoo, J., Rizvi, S., Aiken, W., & Kissell, J. (2014). *Cloud Security Auditing: Challenges and Emerging Approaches*. IEEE Security & Privacy, 12(6), 68–74. https://doi.org/10.1109/msp.2013.132

Vahradsky, D. (2012). *Cloud risk: 10 principals and a framework for assessment*. ISACA, 5, 1-12.

Valcheva, S. (2018, March 19). *Qualitative Data Analysis Methods And Techniques*. Blog for Data-Driven Business. https://www.intellspot.com/qualitative-data-analysis-methods/

Wang, L., Ou, M., & Xun, H. (2019). *DeaPS: Deep Learning-Based User-Level Proactive Security Auditing for Clouds.* Paper presented at the - 2019 IEEE Global Communications Conference (GLOBECOM), 1-6. 10.1109 / GLOBECOM38437.2019.9014172

Yin, R. (2018). *Research Methodology: Case study research and applications*, 6th ed. SAGE Publications