MASTER

INFORMATION SYSTEMS MANAGEMENT

MASTER'S FINAL WORK

DISSERTATION

CLOUD SECURITY: AN AUDIT FRAMEWORK

JORGE ALEXANDRE DA COSTA BALULA

OCTOBER - 2022

Lisbon School of Economics & Management
Universidade de Lisboa

MASTER

INFORMATION SYSTEMS MANAGEMENT

MASTER'S FINAL WORK

DISSERTATION

CLOUD SECURITY: AN AUDIT FRAMEWORK

JORGE ALEXANDRE DA COSTA BALULA

SUPERVISION:

PROF. DR. ANTÓNIO MARIA PALMA DOS REIS

OCTOBER - 2022

Agradecimentos

É sem margem de dúvida que começo por agradecer à minha família, ao meu pai, Jorge, à minha mãe, Isabel, à minha irmã, Cátia e aos meus avós, Felisbela e Adelino.

Agradeço por todos os esforços, por toda a disponibilidade, e todo o amor, carinho, confiança e dedicação.

Agradeço ao Professor Doutor António Palma dos Reis por ter aceite orientar esta dissertação e por todo o apoio, boa disposição, sugestões e suporte que demonstrou ao longo do decorrer da execução da mesma.

Ao Professor Doutor Rui Manuel Trigo Pereira Guedes por toda a disponibilidade, simpatia e dedicação, bem como por todas as sugestões.

A todo o departamento de Audit & Assurance da Deloitte e clientes pelas entrevistas e por todos os esclarecimentos prestados.

E por fim, e nunca menos importante, aos meus amigos, Simão, Luís, Guilherme Lopes, Guilherme Paiva, José, L'uboš, Kanush, Bernardo, David e Indra, o meu muito obrigado pela vossa amizade, apoio e companheirismo.

Resumo

O objetivo desta dissertação é a construção de uma *framework* de segurança que englobe todos os ambientes *cloud* independentemente do modelo, provedor, tipo, serviço ou recursos implementados.

Desta forma, foram realizadas entrevistas com profissionais de auditoria de firmas *Big* 4 e especialistas em TI e *cloud* de departamentos de sistemas de informação do setor bancário acerca de temas como abordagem de auditoria, riscos na *cloud*, avaliação de controlos, procedimentos de auditoria, ambiente de *cloud* e abordagem de documentação.

Com os dados obtidos, foi possível construir uma *framework* que abrange áreas de TI e SI como controlo de acessos lógicos, gestão de operações, gestão de alterações, segurança do ambiente, integridade da rede e proteção da informação.

Abstract

The main objective of this dissertation is the development of a security framework that encompasses all cloud environments regardless of the model, type, provider, service, or resources that are implemented.

To achieve that, interviews were conducted with audit professionals from the Big 4 firms and from the banking sector IT and cloud experts, on topics like audit approach, risks in the cloud, control evaluation, audit procedures, cloud environment, and documentation approach.

With the data collected, it was possible to construct a framework that covers IT and IS areas such as logical access control, operations management, change management, environment security, network integrity, and information protection.

List of Abbreviations and Acronyms

CAR - Control Addressing Risk

COBIT - Control Objectives for Information and Related Technologies

CPA - Certified Public Accountancy

CSP - Cloud Service Provider

FIPS - Federal Information Processing Standard

GDPR - General Data Protection Regulation

IaaS - Infrastructure as a Service

ICD - Internal Control Deficiencies

ICFR - Internal Control over Financial Reporting

ICT - Information and Communication Technologies;

IPE - Information Produced by Entity

IS - Information Systems

ISACA - Information Systems Audit and Control Association

ISMS - Information Security Management System

IT - Information Technology

ITIL - Information Technology Infrastructure Library

ITL - Information Technology Laboratory.

PaaS - Platform as a Service

PII - Personally Identifiable Information

RAIT - Risk Arising from Information Technology

RMF - Risk Management Framework

SaaS - Software as a Service

SOC - Service Organization Controls

Table of Contents

1. Introduction

By taking a look at the current landscape of how organizations are managing their technological infrastructure, we find that, over the past few years, there has been a rapidly growing transition from on-premises data centers that host, support, and help manage a company's business operations to cloud computing.

Cloud computing services allow customers to rent a cloud provider's hardware and use all of its functionalities over the internet through a pay-per-use model (the client only pays the provider for the resources utilized). This means that companies are now capable of hosting their entire IT infrastructure without owning any on-premises servers.

This tremendous increase in the usage of cloud computing services is justified by the multiple advantages of cloud computing over traditional computing. These include the ability to access data anytime from anywhere, geographical mobility benefits, and the ability to scale resource usage depending on the organization's continuous and volatile needs.

This also means that the company will not be responsible for the maintenance of the depreciating assets that host the underlying IT infrastructure.

Because of the ever-growing advantages and ease of cloud adoption, these services are amassing tremendous popularity with incredible growth prospects for the future. In a study that included 45 technologically developed countries, it was found that from 2010 to 2016, cloud computing capital expenditure presented a 42.5% growth totaling 100 billion dollars (about $310 per person in the US) in 2016 (Jitendra, 2017). A Cisco projection indicated that in 2021 cloud computing marketing would reach the 400-billion-dollar threshold (Vu, Hartley & Kankanhalli, 2020). Recent statistics in a study presented by Facts and Factors, show us that the cloud computing market capitalization in 2021 was 429.5 billion dollars (about $1,300 per person in the US), remarkably close to what Cisco predicted.

This, combined with the high availability, elasticity, agility, geo-distribution, disaster recovery, and scalability, make it nearly impossible for companies to disregard the shift (Griffith, 2015).

The cloud provider is mostly responsible for maintaining and assuring cloud security. As an emerging technology, cloud computing services introduce several security threats and challenges, therefore, service providers need to establish confidence and trust with

their clients to operate their services. Since the resources are shared, privacy and confidentiality must be considered.

However, it is no secret that this technology also comes with its own set of risks to the customer. Despite the total or partial hosting of software in a cloud provider's server, the client remains responsible for the data, software maintenance, access management, internal segmentation, segregation, change management, and operations management (Mosher, 2011). These responsibilities vary depending on the client's contracted service, cloud model, and cloud type.

To attend to a client's necessity of assessing the security integrity of their systems, services, and underlying infrastructure held in the cloud, we must address the risks that can compromise the IS of the company with well-thought controls to mitigate and eliminate threats. There are many ways to accomplish this, one of them being IT audits based on frameworks such as ISO 27001 or others depending on the type of clients and other variables. To achieve this, I intend to develop a generalized cloud security audit model that addresses all the described needs to assess, evaluate, implement, and improve the overall state of IT and IS in the cloud.

The main objective of this dissertation is the proposition of a cloud security audit model framework through the assessment of cloud computing risks and security threats, the development of controls that address those risks as well as the configuration of testing procedures for each control. Each control will be designed to mitigate the risk it addresses. The model focuses on areas of ICT specific to the cloud such as service models, deployment models, contracted products and services understanding, shared responsibility model, outsourcers involvement, logical security, change management, and operations management. It is intended for this framework to apply to all cloud services (AWS, Azure, GCP, and others).

This dissertation is structured in the following way: 1 - Introduction; 2 - Literature Review regarding cloud concepts, IT security risks in the cloud, and IT audit frameworks; 3 – Methodology; 4 – Data collection and analysis; 5- Cloud Security Audit Framework; and 6 - Conclusion.

2. Literature Review

2.1. Cloud Computing

In 2003, Google issued a publication regarding a recent technology that had been around for some time but only as a theoretical concept, giving it relevancy by presenting it in the public eye. Then, in 2006, with the release of the Amazon EC2, cloud computing was a fully functioning service. Cloud computing is undoubtedly one of the most ambiguous technological definitions to ever exist, however, it can be defined as the delivery of computing resources and capabilities on-demand through the internet. Putting it simply, it is a type of computing where IT services and resources are made available by a large-scale hardware infrastructure simply with an IP network connection (Qian, Luo, Du & Guo, 2009).

In 2019, Rashid and Chaturvedi, trying to help institutions and individuals understand the way cloud computing can provide them with reliable, and low-cost services in diverse fields of application, produced a study that identifies the following main characteristics of cloud computing the following: 1) extensive capabilities of computing resources, elevated scalability and elasticity potential, a shared collection for virtualized and physical resources, diligent resource scheduling and generalized applications.

2.1.1 Public, Private, and Hybrid Cloud

Among the cloud computing types, each presents its characteristics, advantages, and disadvantages to the customer, each one of them needs a different approach when auditing for system security and compliance.

The most frequent type of cloud service used by companies in IT and IS environments around the world is the public cloud. In the public cloud, the third-party cloud services and resources provider is responsible for the ownership and maintenance of resources, hardware, and infrastructure. The IT and IS services and resources at matter are delivered to the client through the internet. In this type of cloud service contract, the hardware and software, from an auditor's perspective when considering all the relevant variables, controls, and criteria regarding system security, must only consider the components that

are responsibility of the audited entity while not addressing the service provider's owned IT/IS resources (Jansen & Grance, 2012).

When the usage of IT resources and services, as well as the deployment of the very same resources and services, are performed exclusively by an enterprise, we consider it the private cloud. The underlying infrastructure that supports the company's operation can be hosted on-premises or by a cloud provider, however, in the case of the latter, only that organization's member should have access to the cloud environment. To achieve this, services and resources must be made available through a dedicated network to only an organization and its members (Doelitzscher, Sulistio, Reich, Kuijs & Wolf, 2011).

The only option that offers a method of optimizing internal and external resources to the fullest is the hybrid cloud. It offers easier scalability and flexibility options and a wider array of deployment alternatives. Protection is also an improvement on the client's side since it shares responsibility with a certified cloud provider that specializes in system security, compliance is easier to achieve and with all this, it is overall a better deal without completely disregarding the hardware that the client has already purchased.

It has the capacity of altering its capacities depending on the client's computing needs and it allows the customer to adopt a mixture of internal and external hardware without any spillover of computing resources (Li, Wang, Li, Li, Wang & Du, 2013).

2.1.2 Cloud Computing Service Models

Infrastructure as a Service (IaaS) is an instance that offers services in the realm of computing capabilities, data storage, and other services and resources through the Internet. In this model, cloud providers manage IT infrastructures such as a data warehouse, a virtualized or physical server, and network resources making them obtainable to client organizations through virtual machines exposed on the Internet. This provides capabilities like the possibility of executing workloads quicker, with ease, more flexibility, and reduced costs. This model presents lower obstacles to entry, but it may be necessary to invest a substantial initial sum to build and support the cloud infrastructure (Gorelik, 2013).

In the publication “Cloud Computing Models”, Gorelik affirms that platform as a service (PaaS) is a model that provides clients with an alterable application outlet as well as tools that encompass an already established software pile utilizing the internet. Normally, tools such as these are necessary to develop applications (Gorelik, 2013). Providers of the PaaS model are required to host the software on owned hardware. This model allows developers to not have to install or update hardware and software that is built internally as their only means to properly operate an application.

A method of delivering applications as services through the internet is named Software as a Service (SaaS). Rather than installing and maintaining the software, the customer can access it via the Internet, passing on responsibility to the provider for complex software and hardware management and maintenance. These applications are often named internet-based software or hosted software. SaaS applications are operated on the service provider’s infrastructure. The provider is only accountable for managing security, access to the application, software availability, and application performance. With the only client's responsibility being the data (Cusumano, 2010).

2.1.3 Shared Responsibility Model

As mentioned before, the use of cloud services presents many possible benefits. However, these benefits come with responsibilities and require detailed knowledge of specific cloud services used.

A shared responsibility model is a security framework that imposes security responsibilities that the provider and its users fall under to define responsibility over assets, hardware, software, and other components or resources.

If the client operates and maintains its IT infrastructure internally, the enterprise and its staff are accountable for assuring the security of the on-premises assets, as well as the applications and data that are dependent on it.

When the client shifts to a public cloud model, it passes some of these IT security and compliance responsibilities to the cloud provider. Each party is liable for different areas, and, to guarantee full coverage of assets, the client and provider must work alongside (Bennet & Robertson, 2019).

2.2. Security Audit Framework

In an attempt to help organizations to conduct security audits for today's complex networks that transit across multiple domains, security estates, and enterprises, Onwubiko published "A Security Audit Framework for Security Management in the Enterprise" in 2009 where he defines a security audit as an approach utilized to determine the security of an organization's information and data without the usage of the cost and other associated damages of a security incident. This means that the audit must take an independent outlook on all the processes and steps of its workflow and lifecycle.

This type of audit is conducted and performed as a way to assess the effectiveness of an organization's capacity and ability to protect its valued or critical assets, by keeping them secure, private, and integral (Pereira & Santos, 2010).

2.2.1.Audit Components

2.2.1.1. Risks

In 2018, in the paper "The increasing role of IT auditors in the financial audit: risks and intelligent answers", Barta tries to understand the present situation of the IT audit role and involvement in financial reporting and auditing, by interpreting the risks involved parts encounter, and by providing executable and specific countermeasures when using competent applications.

In this paper, Barta describes and defines audit risks as the risks of financial statements being materially inaccurate or, in the case of IT audits, the IT software and hardware being untrustworthy and inaccurate, compromising the financial data integrity even the slightest bit. Risks must be identified and mitigated because in some cases, even the audit assertion declares that the financial reports are free of any material misstatements.

Taking a risk and lowering its impact level through adequate testing and evidence is, in fact, the primary objective of an audit. Many moving parts are involved and can be affected by a company's financial statements, therefore, risks, when not properly

addressed can carry a major legal liability for the certified public accountancy firm performing the work (Houston, Peters & Pratt, 1999).

2.2.1.2. Controls

As a mean to guarantee that the security and privacy procedures in a company's operations environment are effective in its purpose, a control can be adequate and proper archive and storage of records and data, access control on the company's physical and virtual environment, with critical infrastructure deserving a more attentive look, and properly logging and keeping the logs of the accesses, and alterations executed upon the enterprise's infrastructure and as a way of assessing how compliant and secure an organization's procedures are, audit controls are administered (Mazza & Azzali, 2015).

2.2.1.2.1. Control Design and Implementation

Once processes and controls are established and documented in the client organization operations environment, the auditor must assess the design and implementation of the controls in place. It is crucial to differentiate the design and implementation testing from the operating effectiveness testing. Assessing the design of a control implicates considering if that control is theoretically adequate and efficient to prevent, detect, and correct, material misstatements or IT risks triggered by IT elements in the application environment of the customer organization (Libby, Artman & Willingham,) effectively and properly.

When developing an internal control procedure and implementing it in an adequate environment, the auditor has evidence and guarantees that the client is truly operating the control. But this proves to be insufficient because it does not provide satisfactory proof and evidence that the fundamental operation of the control is effective and adequately mitigates the risk it addresses throughout the audited period. To assure total compliance with auditing standards, auditors first need to assess the design of the control, and only then, after realizing that the design is effective, can they test the implementation of that control, to do that, auditors simply verify if the organization is implementing what was proposed in the design and the control itself. It is nearly worthless to assess the

implementation of the control when is understood that the control being tested is inherently inefficient, inadequate, and incapable of design.

Appropriate procedures to test the design and implementation of controls can encompass the following: 1) inquiring regarding entity personnel; 2) observing the application and execution of specific controls; 3) confirming the existence of and reviewing documents and reports that the organization has produced; 4) delineation of a sample of transactions through the information system (Engvang & Jradi, 2021).

A prevalent way of approaching the testing the design and implementation of controls is to summarize an inventory of important controls and test them separately. This approach tends to work well for smaller customers where there are few controls to assess.

2.2.1.2.2. Control Operating Effectiveness

To test the effectiveness of a specific control auditing service providers must estimate whether the control was or was not operated adequately in a specific timeframe.

Testing the operating effectiveness of control is a safeguard for the auditor, assuring that the control that the client claims to be in place, has been implemented and established for some time. Utilizing a Type 2 report[1], SOC 1, or SOC 2 the testing of the operating effectiveness of controls is mandatory. As a mean to establish reliance on them, all controls that are found to be relevant in the client's environment must be assessed to guarantee that they have operated effectively throughout the audited period (Gramling, O'Donnel & Vandervelde, 2010).

This procedure is different from verifying that controls that have been implemented. Many auditors confuse these procedures, resulting in inadequate and insufficient evidence to explain the reliance placed on controls, the evaluation of risks, and the reduction of sample sizes, and consequently insufficient audit evidence to provide a basis as support for the audit opinion.

[1] Type 2 reports typically cover 12 months and include a design and operating effectiveness test.

Some auditing firms are determined to launch compliance testing at the same time as the audit fieldwork. This is justified because the audit planning is completed in the office and not at the customer's establishment.

When these test conclusions are negative, the audit approach will need to observe some changes, taking impact in the substantive testing. In the case of it having been started already, this may mean that staff has wasted time by having to extend substantive samples. In some extreme cases, the staff responsible for the audit may even run out of time to accomplish the work promptly.

2.2.1.3. Findings, Deficiencies, and Recommendations

Findings are the results and conclusions of control testing in an audit. Institutions are obliged by regulatory entities to carry out frequent audits to determine whether best practices, regulatory conditions, norms, policies, and standards are followed (Furqan, Wardhani, Martani & Setyaningrum, 2020). Audit findings, once the testing is concluded, must be presented to the client to convey what was uncovered through the conducted trials and received evidence.

Additionally, findings must be completely and fully supported by evidence about how the entity's operations measure up against the audit criteria as a mean to present the findings with enough basis to support the auditor's claims of a finding. These criteria are summarized in a document that auditors employ as a guide to conduct their assessment of the entity's processes, procedures, and workflow. It can include strategies, guidelines, policies, procedures, and the requirements an entity must meet (Libby & Frederick, 1990).

Finding conclusions display control conformity or nonconformity against the audit criteria. If the audit concludes that the entity operations are being conducted appropriately, the finding will indicate conformity when assessing against the audit criteria. Otherwise, in the case of the entity having processes and procedures that are not satisfactory when testing against the very same criteria, the assessment will show nonconformity against the audit criteria.

In the 2009 research article "Former Audit Partners on the Audit Committee and Internal Control Deficiencies", Naiker and Sharma attempted to explore and comprehend the affinity amongst ICD with the presence and existence of prior audit associates on the

committee of auditors who could demonstrate some sort of affiliation or no affiliation whatsoever with the organization's external auditor. As described by the authors in the article, deficiencies are ineffective design and execution of a control. This prevents the members of an organization from detecting and correcting potential significant occurrences that must be addressed promptly. Weakness or deficiency in a control or a mixture of deficiencies in inner control of an organization's processes and procedures that have a direct correlation in the impact of financial data and information while being considered not as severe and impactful as the worst kind of deficiency is considered significant, the material weakness. Yet, it carries sufficient relevancy, since it requires the engagement and time of accountable personnel who hold responsibility over the client enterprise's data. There is a direct impact in the ICFR the deficiency that caused that impact must be considered a material weakness without any other criteria being considered.

Auditors must consider two dimensions of a control deficiency when categorizing them. 1) The likelihood; 2) Magnitude and severity (material, significant or insignificant) (Dusenbury, Reimers & Wheeler, 2000).

Upon classification, the deficiency must be communicated, and the methods differ depending on their types. In case of a control deficiency, the audit team must report to the manager. Regarding significant deficiencies, auditors must report to the audit committee and upper management. And finally, in regard to material weaknesses, auditors are obliged to report externally, as well as to the audit committee and upper management (Bedard & Graham, 2011).

Final audit report recommendations emphasize, and present actions expected to enhance and improve the entity's process and procedural performances when implemented. The appropriate implementation of these suggestions agreed upon by management is a crucial step to take complete advantage of an audit. The responsibility for implementation of the agreed recommendations typically lies with senior managers of the business area that was audited. Prosperous implementation of these recommendations requires strong senior management supervision and planning to define clear responsibilities and timeframes to address the issues at cause.

In some cases, a committee consisting of auditors has a key role in monitoring the execution of recommendations. Audit committees aid the responsible management to

guarantee that the expected advantages of audit reports are realized. The internal audit function supports the audit committee in maintaining surveillance of execution by providing advice on management's advancements when implementing these recommendations (Alzeban & Sawan, 2015).

2.2.1.4. Audit Conclusions

Audit conclusions consist of the reporting of the audit process through an audit report that must be prepared extremely carefully and skillfully to present assertive conclusions with the proper basis to the client. Forming an opinion regarding a company's financial statements is, as we have determined before, the main objective of an audit. However, IT audits, have as their main goal, the assessment of a customer's IS environment, as a means to guarantee that the extracted financial information is trustworthy. Audits are executed as a method to obtain appropriate security and provide enough trust in the client's financial reporting, by identifying material misstatements (Russel, 2006).

The conclusions of an audit and the generated reports are a principle of managing the audit process with reporting representing the last step and procedure of the whole audit approach. Conclusions must be autonomous, independent of any client's intervention, and based on facts and evidence. Any conclusions drawn that have no basis other than assumptions, must be disregarded as it is considered unprofessional to take this approach. By drawing a set of conclusions, auditors are enabled to form opinions regarding the client's financial statements or IT environments, depending on the nature of the work (Tan & Yip-Ow, 2001).

2.3. The basis for IT Security Audit

When auditing an organization's IT/IS infrastructure, regardless of its nature, the firm responsible for conducting the audit must administer standards, frameworks, and norms on governance and compliance to support their work.

These norms, standards, and frameworks are produced by regulatory entities to ensure that organizations comply with regional, national, or international laws and regulations. Typically, these refer to areas such as privacy, security, access control, regulatory

compliance, and incident management, although it may vary from one to the other. Nevertheless, audits should apply one or several of the recommendation presented by these standards as a basis, to assess the client's overall IT and IS compliance.

These standards and norms are not completely linear since the audit must take into perspective many aspects and characteristics that may be internal or external to the audited client. Some of these characteristics are the organization's size, location, business model, and type.

2.3.1. ISO 27001

ISO frameworks are a variety of policies, processes, and procedures that organizations should follow and comply with. Specifically, the ISO 27001 is a framework that supports the protection of information and data systematically, with low costs to the enterprises, companies, and agencies adopting it. This adoption can be done by implementing an ISMS.

The issue of this framework supplies adopting organizations with the required expertise to protect valuable information and data by acquiring ISO 27001 certifications. This way, certified members can show and prove to their customers, business partners, and regulatory agencies that the data handled by the certified entity is effectively managed to create an image of confidence and security internally and externally.

The protection of information and data confidentiality and privacy is the main objective of this framework. It explicitly indicates that only authorized personnel should have the privilege and authority to access explicit and detailed information. Data integrity where particularly displays that information must be kept integral and whole. And finally, availability, where it states and defines that information should be made accessible for authorized personnel whenever it is required (Brenner, 2007).

2.3.2. ISO 27018

Another standard that belongs to the ISO family is the ISO 27018, a framework that addresses cloud computing-specific issues, threats, data, and information security and privacy.

In the matter of cloud computing services, this standard was the first in addressing its privacy and security issues, being issued in 2014 as support added to the ISO 27001, which was the first international standard of exercise for cloud privacy and security. It provides support to cloud service providers that are required to process, manage, and maintain personally identifiable information (PII), especially those who deal with large volumes of data influx, as a way of evaluating the risk these companies are exposed to and mitigating them by enforcing controls to protect this kind of data and information (Kemp, 2015).

Creating a common array of security controls that, by being enforced by a public cloud provider, allow for the adequate processing of PII is the main objective of this standard. It aims to aid these providers with compliance and governance matters, more specifically with appropriate responsibilities when dealing with and handling PII.

By following the proposed guidelines and complying with them, PII processors, maintainers, and handlers now have a guide to be more transparent is a critical issue providing cloud service customers with the ability and confidence to choose a secure and compliant PII processing service provider based on factual information. With this standard, customers are now able to enter and join a contractual agreement with the data processor with confidence and ease (de Hert, Papakonstantinou & Kamara, 2016).

2.3.3. COBIT

In an attempt to aid and provide support to firms in the design, organization, maintenance, and execution of information management procedures, ISACA issued an IT governance, management, and compliance standard named COBIT.

It can be easily broken down into a set or collection of IT control objectives and goals to support the financial auditing community, offering a tool that allows better navigation around the growth of IT services, resources, environments, and infrastructures.

There have been several updates and upgrades in the model in an attempt to broaden the scope, by adding updated information in regard to risk management, information governance, and data security (Mangalaraj, Singh, Taneja, 2014).

2.3.4. ITIL

ITIL is a framework designed to regularize a business's selection, planning, delivery, maintenance, and general lifecycle of IT services.

As a way to standardize the sampling, planning, delivery, maintenance, supervision, and general lifecycle of IT services and resources in the business environment, ITIL was created.

It has the main objective to enhance the efficiency and accomplishment of anticipated IT services and resources delivery.

It is a framework that enables and allows administrators to play the role of business service units, other than just offering support in the back end. Its department's exercises and workflows as well as costs of arising necessities from the industry must be targeted by the best practices and overall guidelines proposed by ITIL. These must be flexible to adapt as the business expands or diminishes (Martins, 2010).

2.3.5. GDPR

Without any doubt, the strongest and strictest regulation on data security and privacy is GDPR.

It was assembled by the European Union, beginning being enforced upon entities on May 25, 2018. Despite being created by a European entity, this regulation proposes and imposes obligations that companies that collect data that is bonded with individuals in the EU must strictly follow and comply with.

Whenever an entity breaks or presents non-compliance by violation of any privacy or data security criteria, the EU is eligible to fine the entity on matters that can reach the dozens of millions of euros. This is utilized as a demonstrative measure of the importance of GDPR.

With the issue of this regulation, Europe demonstrates how strongly data privacy and security matters must be taken by everyone that collects EU citizens' data. This is justified by the fact that we live in an era where individuals are feeding cloud service providers with extremely sensitive and critical data, combined with the growing number of data breaching occurrences.

It is undoubtedly an extensive, detailed, and highly specific regulation. These characteristics turned GDPR into one of the most difficult regulations to comply with, with this issue being more prevalent in smaller-sized companies and entities (Wachter, 2018).

2.3.6. NIST SP 800-53

The NIST SP 800-53 introduces several new controls regarding security and privacy that all U.S. national IS must comply with. There exist particularities that allow some organizations and their information systems to be non-compliant with the publication, depending on if it is a matter of national security.

SP 800 series encompasses several special publications, and the SP 800-53 is a component of the sequence. Its main objective is to report and inform on matters of analysis, procedures, processes, and measures in IS security on the ITL. It adds to the exercise of the previously mentioned areas for public and private enterprises, governmental organizations, and companies connected with the education industry.

It is a publication that presents, in particular, steps in the RMF as a means to regulate the security control sections for federal IS abiding with the security conditions that are imposed by the FIPS 200. This encompasses a decision regarding the baseline set of controls that are based on the previously published FIPS analysis of the impact of the worst-case scenario, allowing the modification of the controls appropriating it based on previous knowledge and present infrastructure requirements, and evolving security and privacy management with the assessment of organizational risks as the foundation, covering a total of 18 different areas regarding IS/IT environments (Tariq, Tayyaba, Ashraf, Khan, 2016).

NIST security regulations are expected to be implemented in all enterprises and governmental organizations and agencies (with some exceptions), that are obliged to

comply with the measurements, processes, and procedures regarding IS/IT security imposed by this regulation. IS currently in development is expected to comply with this special publication upon release in the production environment (Amiruddin, Afiansyah, Nugroho, 2021).

3. Methodology

Considering the objectives and the proposed research of this dissertation, the research design has a qualitative and descriptive approach.

As stated before, cloud services are a relatively recent technology and auditing security aspects of the cloud remain a gray area. Despite there being several security audit frameworks that can be applied in the cloud there is a lack of academic and professional work in the cloud auditing field. With this in mind, my proposal for this thesis is the development of a framework that assesses how secure a cloud environment, its data, and applications are.

The proposed framework aims to be a generalized audit model. With this, I want to say that the framework can be applied to any type, any model of cloud services or resources, regardless of the provider and environment that the client has in place.

To accomplish this, risk assessment interviews were conducted with IT audit professionals from major firms and financial organizations that have increased knowledge maturity in cloud environments, services, resources, and security.

The qualitative research methodology fits the objective of this thesis better than any other method since unstructured interviews and the analysis of interview conclusions can vary tremendously, making it extremely difficult to achieve the expected result through quantitative research.

The interviewed employees belonged to IT, risk and security departments, and, firstly, the objective of conducting unstructured interviews was to, in a dialog, identify the risks that these employees considered to be most relevant and common in their experience with cloud environments. From there, once the risk matrix was fully developed, the unstructured interviews were once again applied with internal control and audit

department employees to validate and assure that the identified risks made sense and were sufficiently capable of becoming the baseline upon which the framework was built upon.

Having the risk matrix validated, I conducted a set of unstructured interviews with Big 4 internal control and audit employees to start developing controls that were, from an auditor's perspective fully capable of mitigating, entirely, the proposed risks.

Once the full set of controls were built, a whole new round of interviews were carried out to ascertain that the controls were well designed and implemented in a cloud framework optic.

The research strategy chosen was design science focusing on development and performance of a designed theory with the precise intention of improving the functional performance of that theory.

4. Data Collection and Analysis

To gather relevant data, interviews with employees from the Big 4 firms were conducted. And, given that building a framework that is robust enough to ensure that the clients of auditing firms are conducting their operations accordingly is a priority throughout this work, these clients were also interviewed to obtain both parties' perspectives on the matter. It is relevant to mention that the majority of the audience that was interviewed belonged to the financial/banking sector with the client interviewees belonging to security, IT and risk departments.

The purpose of these interviews was to understand clients' needs regarding their production cloud environment from the perspective of an auditee and learn what risks organizations face in their cloud services to develop, and comprehend the approach adopted by auditors when evaluating control and adopting their methodology to the cloud.

The data that was gathered from the interviews, was analyzed through a reasoned and deductive approach. This study started with the research literature on the proposed themes of this dissertation and the research strategy was designed to build a tool that was proposed as a premise of this work. The analysis of the notes taken during the interviews focused on the evaluation of the propositions or hypotheses in relation to the already existing knowledge of the relevant material.

To support the data collected from the interviews, research of empirical data was conducted.

5. Cloud Security Audit Framework

5.1. Planning

Primarily, we must fully understand the client's cloud environment. To accomplish that, we need to understand what service model is being utilized in each cloud service that supports an application that are being considered in the audit; figure out what deployment model is being used in the in-scope applications; understand what cloud services are being used as support for the relevant applications; comprehend what the company is responsible for concerning the management of the cloud services and resources being used; understand how vendors and outsourcers are involved in the management of the underlying cloud services and resources in place; we must ask what regions and services are being utilized to sustain relevant applications; the question in regards the number of accounts that support the applications that are in scope; understand how the cloud environment is segregated, depositing special attention to the inbound and outbound traffic; comprehend how users authenticate in the cloud as well as critical components of the cloud; understand how users are granted their access permissions to the cloud environment's services and resources.

5.2. Shared Responsibility Model

As discussed before, when adopting a cloud environment, the responsibility over all the assets (this includes software, hardware, data, and all the underlying supporting infrastructure) is shared. As a method for standardization of the utilized shared responsibility model when considering which components should be audited and which should not.

Presented below, in figure 1, we can observe how the responsibility is shared among both parties, and in table 1, we can see how auditors may approach different components, depending on the model that the client has integrated into their relevant applications.

Figure 1: Shared Responsibility Model

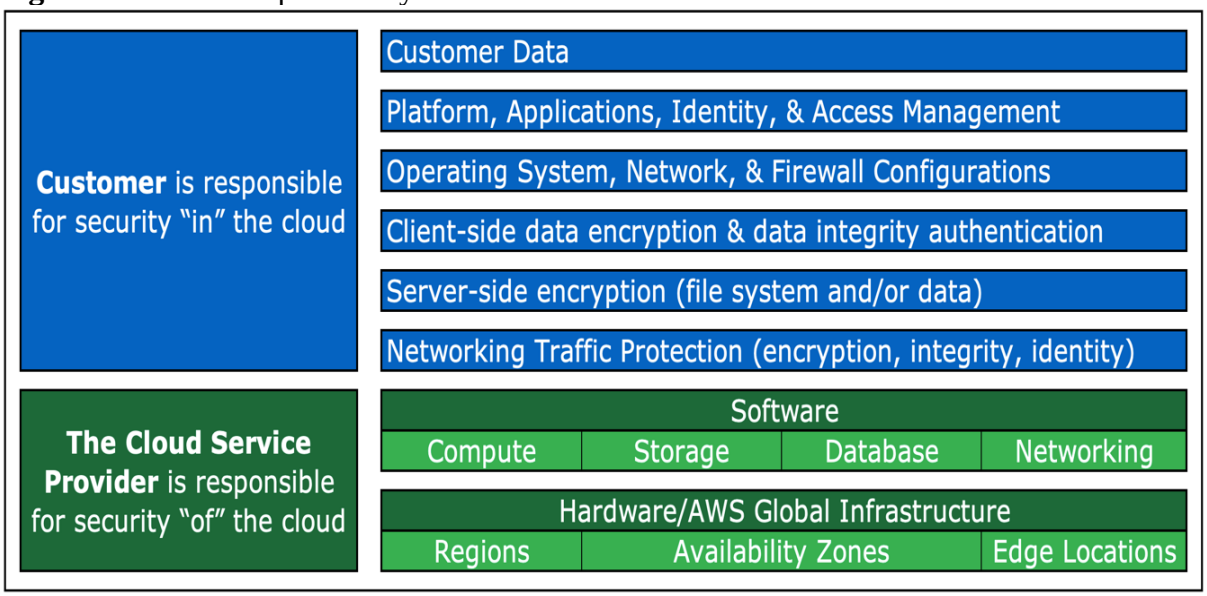


Table 1: Approach Guide for Auditing Cloud Components Based on CSP

Cloud Stack	IaaS In-House	IaaS CSP	PaaS	SaaS
Application	Audit Directly	Audit Directly	Audit Directly	Audit Directly
Middleware/Software stack	Audit Directly	Audit Directly	Audit Directly / Rely on third-party SOC 1 & 2	Rely on third-party SOC 1 & 2
Servers and operating systems	Audit Directly	Audit Directly	Rely on third-party SOC 1 & 2	Rely on third-party SOC 1 & 2
Management console	Audit Directly	Audit Directly / Rely on third-party SOC 1 & 2	Audit Directly / Rely on third-party SOC 1 & 2	Rely on third-party SOC 1 & 2
Hypervisor/Data storage/File storage	Audit Directly	Rely on third-party SOC 1 & 2	Rely on third-party SOC 1 & 2	Rely on third-party SOC 1 & 2
Physical	Audit Directly	Rely on third-party SOC 1 & 2	Rely on third-party SOC 1 & 2	Rely on third-party SOC 1 & 2

5.3. Framework

This section of the paper will present the audit framework. This constitutes the identified RAITs and one or a set of multiple controls developed to address the risks presented. To ease the presentation of this framework, RAITs will be described first and

following that, will be one or a set of tables referring to the control that addresses that RAIT.

RAIT.01: Users have access privileges and rights beyond the necessary to perform their assigned responsibilities. This can create improper segregation of duties.

Table 2: Control Addressing Risk 1

Control ID	CAR.01
Control Description	User access privileges for new users and modified user access are approved by the appropriate management. These include standard application/services/resources profiles, critical financial reporting transactions, and segregation of duties throughout the process.
Addressed RAIT	RAIT.01
Design Evaluation	Discuss with management to comprehend the process in which new access and changes to access are requested and approved. Specifically, ponder acquiring an interpretation of the following attributes: • Policies and practices related to granting user access; • Individuals or groups accountable for approving access; • Individuals or groups responsible for issuing access; • How user access requests are submitted, approved, and documented; • Whether a tool is used to provision new access and how that tool is controlled; • Determine whether there is a segregation of duties between the approver and the person granting the access in the system. Examine evidence to corroborate the design of the control.
Operating Effectiveness Procedures	Obtain a report of the credentials that includes user name, user creation date, password enabled flag, password last use date, password last changed, and MFA status. With user creation date as basis, identify the users created in the period of intended reliance. Draw a selection of new and modified users and test the following attributes: • The user's access request was approved by appropriate management; • Requested access is consistent with access granted in the system; • Access granted is commensurate with the user's assigned duties and enforces appropriate segregation of duties; • Segregation of duties is maintained between the approver and the person granting the access in the system.

Table 3: Control Addressing Risk 2

Control ID	CAR.02
Control Description	Access for removed and/or transferred users is withdrawn or altered promptly.
Addressed RAIT	RAIT.01
Design Evaluation	Discuss with management to comprehend the controls related to terminating access to the application for terminated or transferred users. Specifically, ponder acquiring an interpretation of the following attributes: • Policies or procedures related to user de-provisioning; • How IT management is notified of terminated and transferred users; • How access is removed upon termination or transfer. Is the same process used for employees and non-employees; • Whether the process for removing access is manual or automated; • Whether a tool is used to de-provision access; • The method for removing access to the application; • What are the expectations for timely removal of user access? Examine evidence to corroborate the design of the control.
Operating Effectiveness Procedures	Obtain a listing of cessations for employees and contractors for the period of intended reliance from Human Resources. Make a selection of users that were separated from the organization. For each user selected, test the following attributes: • Access privileges for the released user are no longer active in the system. Such access was terminated, deleted, or disabled in a timely manner. To accomplish this obtain the credential report, and compared the list of terminated employees and contractors with the report obtained. Identify if any of the users still have access. Any exceptions noted must be questioned and the root cause must be understood.

Table 4: Control Addressing Risk 3

Control ID	CAR.03
Control Description	User access is periodically reviewed.
Addressed RAIT	RAIT.01
Design Evaluation	Discuss with management to comprehend the process to review user access to the application. Specifically, ponder acquiring an understanding of the following attributes: • Policies, procedures, standards, and guidance for reviewing user access; • Procedures and responsible individuals to review user access; • Frequency of the access review; • Scope of review and what is considered to be an exception; • What level of detail the review is performed at; • How the review is documented; • Whether a tool is used in performing the access review and if so, how that tool is controlled; Examine evidence to corroborate the design of the control.
Operating Effectiveness Procedures	Challenge management responsible for performing the user access review control and obtain evidence that management adequately reviewed the information. This may include reperformance and examination of documentation to establish that: • User access review included a complete and accurate population of users who can gain access to the cloud service account, by considering all avenues through which access can be granted to users: • Review was properly documented and performed at the appropriate level of detail to ascertain whether access was consistent with each user's current job responsibilities; • Review was performed by appropriate management personnel with proper segregation of duties enforced; • System access was appropriately modified in a timely manner for users flagged as exceptions during the review.

Table 5: Control Addressing Risk 04

Control ID	CAR.04
Control Description	Access is authenticated through individual user IDs and passwords or other methods as a mechanism for validating that users are authorized to gain access to the system. Password parameters meet company and industry standards.
Addressed RAIT	RAIT.01
Design Evaluation	Discuss with management to comprehend the authentication controls (e.g., password minimum length, complexity, expiration, history, and account lockout) relevant to the application. Specifically, ponder acquiring an interpretation of the following attributes: • Policies, procedures, standards, and guidance regarding authentication controls and password requirements; • The specific settings that are enforced (length, complexity, password change, history, and account lockout) and the consistency of those settings with industry standards ; • Whether the cloud Root Account (in case there being one) has its password manually changed to meet the organization's policy, has Multi-Factor Authentication (MFA) Enabled, and if the MFA is enabled; • Whether accounts are disabled after a period of inactivity; Examine evidence to corroborate the design of the control.
Operating Effectiveness Procedures	Obtain a listing of password parameter configurations for users that have access to any sort of cloud environment, services or resources; Obtain a listing of identity providers that process trusted external users; Obtain listing of password parameter configurations for Root User Account and verify that the configurations comply with company policies; Obtain MFA configuration settings to verify that MFA is enabled for root account Validate if configured parameters comply with company policy or industry best practices.

Table 6: Control Addressing Risk 5

Control ID	CAR.05
Control Description	Privileged-level access is authorized and appropriately restricted.
Addressed RAIT	RAIT.01
Design Evaluation	Discuss with management to comprehend the controls related to privileged-level access. Specifically, ponder acquiring an interpretation of the following attributes: • Organizational Policies related to information security and protecting privileged-level access; • Organizational structure of the security administration function; • Description of users and roles assigned privileged-level access; • Individuals with the authority to use privileged-level access; • Individuals assigned privileged access do not have conflicting privileges that lead to a segregation of duties conflict; • External user profiles such as system vendors, consultants, or emergency user profiles with privileged-level access; • Management of root user account; • Use of permission boundaries and service control policies to restrict user privileges; • Management reviews the appropriateness of access provided to the cloud service access roles and associated permissions. Examine evidence to corroborate the design of the control.
Operating Effectiveness Procedures	Identify privileged-level access users and accounts as well as roles or groups that grant that privileged access. Challenge the appropriateness of the level of access of each identified user using Human Resources employee lists, and application user lists, and understanding whether the privileged user should have that type of access based on its responsibilities and duties in the entity. When a generic or service user is identified, inquire with management to question the appropriateness of that access if the evaluation of the nomenclature or description of the user doesn't allow for proper conclusions.

RAIT.02: Improper changes are made directly and/or instantly to financial data through means other than application transactions.

Table 7: Control Addressing Risk 6

Control ID	CAR.06
Control Description	Only authorized personnel with adequate job responsibilities and assigned role should have access to application data files and/or database objects, tables and data. This access properly approved by the appropriate management.
Addressed RAIT	RAIT.02
Design Evaluation	Discuss with management to understand how sensitive files/directories and/or objects/tables/data are secured. Specifically, ponder acquiring an interpretation of the following attributes: • Policies or procedure guides related to the protection of sensitive files/directories and/or objects/tables/data; • Individuals, or groups of individuals, that should be granted access to these items; • Whether management has specifically identified which files/directories and/or objects/tables/data are sensitive; • What type of information is contained in the sensitive files/directories and/or objects/tables/data and the reason they are sensitive. • What cloud products/services are used to store sensitive files and directories. Examine evidence to corroborate the design of the control.
Operating Effectiveness Procedures	Obtain the report with policies, groups, or other methods that the organization grants access to critical applications or database data files. For each policy considered to be privileged, view the attached entities (Users, Groups & Roles). For each Group or Role attached to the policy, determine the associated users. For each user identified with privileged-level access, test for the following attributes: • Access privileges are authorized and appropriate for the user's assigned duties based on inquiries with management (indicate the persons we inquired with); • Access privileges are authorized and appropriate for user's assigned duties based on inspection of their job function (include reference to the corroborating source, such as an organizational chart).

RAIT.03: Inappropriate changes are made to system software. This includes operating systems, networks, change management software, databases, and access control software.

Table 8: Control Addressing Risk 7

Control ID	CAR.07
Control Description	Privileged-level access to any software that is changeable is authorized and appropriately restricted.
Addressed RAIT	RAIT.03
Design Evaluation	Discuss with management to comprehend the controls related to privileged-level access. Specifically, ponder acquiring an interpretation of the following attributes: • Organizational Policies related to information security and protecting privileged-level access; • Organizational structure of the security administration function; • Description of users and roles assigned privileged-level access; • Individuals with the authority to use privileged-level access; • Individuals assigned privileged access do not have conflicting privileges that lead to a segregation of duties conflict; • External user profiles such as system vendors, consultants, or emergency user profiles with privileged-level access; • Management of root user account; • Use of permission boundaries and service control policies to restrict user privileges; • Management reviews the appropriateness of access provided to the cloud service access roles and associated permissions. Examine evidence to corroborate the design of the control.
Operating Effectiveness Procedures	Identify privileged-level access users and accounts as well as roles or groups that grant that privileged access. Challenge the appropriateness of the level of access of each identified user using Human Resources employee lists, and application user lists, and understanding whether the privileged user should have that type of access based on its responsibilities and duties in the entity. When a generic or service user is identified, inquire with management to question the appropriateness of that access if the evaluation of the nomenclature or description of the user doesn't allow for proper conclusions.

Table 9: Control Addressing Risk 8 (Design)

Control ID	CAR.08
Control Description	Environment changes are adequately and correctly tested and approved before being moved into the production environment.
Addressed RAIT	RAIT.03
Design Evaluation	We have to comprehend how the company handles changes to the cloud infrastructure, as well as application-related changes. Changes to applications, Operating Systems (OS), and databases can be documented here or within the other Discuss with management to comprehend the control related to change testing in a pre-production environment before production release and the appropriate approvals necessary before implementing a change into the production environment. Specifically, ponder acquiring an interpretation of the following attributes: • Products and tools used in the cloud environment to support both infrastructure and application layers. • The change management process for the various types of changes in the cloud, such as configuration changes, system deployments, policies, etc. We should understand who is responsible for each type of change and what process is followed for each type of change; • The change management methodology; • Criteria required for any pre-approved changes and how management monitors changes within this category • Steps in the system development methodology that relate to testing, or other established policies, procedures, standards, and guidance; • Structure of test/development and production environments; • User and tool automation involvement in testing; • Testing methods; • Retention of test results; • Criteria for test success (i.e., 100%=pass or 90%=pass); • Any test failures not resolved before migration to or implementation in production; • How often changes are typically made, and if any changes were implemented during the audit period; • Criteria for determining when testing needs to be performed; • Persons who have authority and responsibility for approving changes; • Tools used to document the approval and testing and changes and how the tools are controlled; • Tools used in the migration process and how the tools are controlled Examine evidence to corroborate the design of the control.

Table 10: Control Addressing Risk 8 (Operating Effectiveness)

Control ID	CAR.08
Control Description	Environment changes are adequately and correctly tested and approved before being moved into the production environment.
Addressed RAIT	RAIT.03
Operating Effectiveness Procedures	As changes to cloud policies can alter access to resources, there should be a control in place to ensure changes to policies are appropriate and approved by management. Obtain account authorization detail evidence and select a sample of policies using sampling guidelines that were created or modified during the period and test the following attributes: • The change was tested prior to implementation. • The change was approved by management before implementation. If change tickets are used for the sample selected, the team needs to perform all required IPE procedures to ensure the completeness and accuracy of the ticketing system, as indicated in the firm's guidance. Information Used as Audit Evidence Considerations Obtain the population of relevant events to cloud resources. The following areas should be covered as Operating System and Database controls testing, these changes are typically driven by application changes. Make a selection of changes pertaining to in-scope cloud Services. For each of the selected changes, test for the following attributes: • The change was tested and/or backout plans were created prior to implementation. • The change was approved by management before being installed on the server. • Emergency change followed the company's change management policy for any pre-approval process.

Table 11: Control Addressing Risk 9

Control ID	CAR.09
Control Description	Access to implement changes into the application production environment is appropriately restricted and segregated from the development environment.
Addressed RAIT	RAIT.03
Design Evaluation	Discuss with management to comprehend the control related to restricting access to implement changes. Specifically, ponder acquiring an interpretation of the following attributes: • Policies and procedures related to the development, modification, and testing of application systems in an environment separate from the production environment; • Whether the entity or vendor owns the source code of the application; • Procedures to segregate the production environment from the development, modification, and testing environment; • Where development and testing are performed and who has the responsibility to perform development and testing; • Who has responsibilities to implement changes to the production environment and the specific access required to implement changes to the production environment; • Whether a tool is used to migrate changes and how that tool is controlled; • How segregation of duties is enforced to ensure developers do not have access to production; • How access is managed for emergency development and testing approaches; Examine evidence to corroborate the design of the control.
Operating Effectiveness Procedures	Examine the listing of users with access to facilitate changes to production and test the following attributes: • Access privileges are authorized and appropriate for the user's assigned duties based on inquiries with management; • Access privileges are authorized and appropriate for user's assigned duties based on inspection of their job function; • Compare a list of users that have access to approve/move changes to production to a list of users that have access to development. Determine that users cannot perform both functions and that segregation of duties is maintained; • Generic accounts require access based on business needs and access to the accounts is appropriately restricted and controlled.

RAIT.04: Systems are not appropriately configured or updated to restrict system access to properly authorized and appropriate users.

Table 12: Control Addressing Risk 10

Control ID	CAR.10
Control Description	The key attributes of the security configuration are appropriately implemented.
Addressed RAIT	RAIT.04
Design Evaluation	Discuss with management to understand the key attributes of the security configuration for the application. Specifically, ponder acquiring an interpretation of the following attributes: • Policies, procedures, and standards related to the security configurations for the cloud environment; • Key attributes of the security configuration for the cloud environment, like managing the root account, access keys, MFA, etc.; • If secure communication with the cloud for accessing resources is implemented, and if access to resources from public sources is allowed; • How management validates the security configuration is following company standards; • How management logs and monitors changes to security configurations. • Interview responsible and/or accountable individuals to determine how the enterprise develops and deploys individual applications and related resources (assets) within the environment. Consider how the enterprise sets, monitors and ensures minimum security requirements for assets. Examine evidence to corroborate the design of the control.
Operating Effectiveness Procedures	Obtain a system-generated list of cloud resources for the in-scope accounts. For the resources identified, ensure no security groups allow ingress from inadequate ports. Review Inbound and Outbound rules for Security Groups identified as part of the Data Gathering Procedure and ensure that suspicious ports are not left open to connect from anywhere. Review all Network access control lists being used and look for suspicious ports and destination/source IP addresses (Inbound and Outbound) to verify that traffic is not allowed from/to all sources.

RAIT.05: Financial data cannot be recovered or accessed promptly when there is a loss of data.

Table 13: Control Addressing Risk 11

Control ID	CAR.11
Control Description	Financial data is backed up on a regular basis according to an established schedule and frequency. Backup media are stored in an appropriately secure location.
Addressed RAIT	RAIT.05
Design Evaluation	Discuss with management to comprehend the mechanisms utilized to backup financial data regularly. Specifically, ponder acquiring an interpretation of the following attributes: • The group or individuals responsible for scheduling backups and defining backup requirements; • What financial data and/or information is backed up; • The schedule and frequency in which the backups are performed; • The tools used to perform backups; • Where backup media is stored and how it is secured; • The corrective actions are taken when there is a backup failure, including what evidence is retained to demonstrate the resolution of the failure. Examine evidence to corroborate the design of the control.
Operating Effectiveness Procedures	Identify critical applications/databases and verify that data is being backed up frequently. Inspect the configuration to test that backups of financial data are scheduled to occur according to policy. Guarantee that MFA Delete is enabled on critical storage allocations. This will prevent the accidental deletion of critical data, for instance, financial data and log data. If cloud products/services are not used for the backup of data, acquire proof of the automated backup schedule for each relevant database or location containing relevant financial data. Examine the configuration to assess that backups of financial data are scheduled to occur according to policy.

5.4. Deficiency Reporting

Upon conclusion of testing the control design, implementation, and procedures, auditors must analyze all the problems, drawbacks and deficiencies identified and document them in a specific working paper.

This documentation must include the root cause of the deficiency, the system, or systems in which the problem was identified, the control linked to that problem, the date of the identification of the deficiency, the deficiency type the personnel responsible for the execution of that control and recommendations to mitigate the risk introduced by the problem at hand.

Once the document is completed, the client must be informed of the identified deficiencies through the analysis of the report and work around the problem to make the control effective.

5.5. Roll-Forward

After the client is notified of all the identified problems and the adequate time to fix them has gone by, the roll-forward procedures must take place.

To perform roll-forward, the audit team must extract all the information for all controls that proved ineffective to obtain up to date data.

Once the extraction is performed, the audit team must select a shorter sample than the one selected previously and follow through with the testing of the operating effectiveness procedures.

If the client applied the given recommendation and the evidence shows that the problem is now absent, the control roll-forward conclusion is effective, otherwise, the conclusion remains the same as the operating effectiveness.

In some cases, due to time constraints, the audit team cannot perform roll-forward procedures. In this case, the final control conclusion will rely solely on the operative effectiveness testing procedures and results.

5.6. Mitigating Procedures

Once roll-forward is concluded, the audit can finalize its work by mitigating all controls that proved to be ineffective throughout the entire audit process.

To achieve this, auditors must first understand the risk and its implications. Once that is achieved, the deficiency must be equally understood and comprehended.

Once auditors are informed of the cause and risk relationship, they can now inquire with management and start questioning any sort of aspects that could mitigate the risk attached to the deficiency. A good example of this is ineffective control of user terminations.

Let us assume that a user has left the company but remains active on a cloud service or resource user list. In this case, the auditor can ask management for a justification for the observed case, and to mitigate the risk of access, the last login date can be used to understand if there was any inadequate log-in in the system that may have represented danger or a security incident for the company. If the last log-in date shown is a date before the employee termination, the risk is now mitigated. If the login date is a date after the termination, auditors need to inform management to immediately deactivate the user and inspect activity logs to understand what the user performed in the system in their last interactions.

Once the mitigating procedures are finalized, auditors now have a green flag to emit results.

6. Conclusion

The objective of this research was the development of a robust framework that evaluates security aspects of cloud environments independently of what provider, model, type, resources, or services an organization is utilizing to conduct its operations.

It is apparent that a generalized framework that can be applied under any circumstance cannot obtain the level of detail and scrutiny that a model that was developed specifically for an environment (e.g., AWS, Azure, Google Cloud Platform, etc.) can achieve.

However, in some cases, small, medium-sized auditing companies, and independent entities do not have the resources available to develop an audit model for each flavor of the cloud, and since the study and development of generalist frameworks for cloud security are still in exceedingly initial stages, we decided that researching, investigating, and developing this model was an important addition to the literature.

Our study throughout the evolution of this thesis took two different routes, with one being around all the aspects of the cloud and how interactions in its environments take place, and the other on how an audit should be executed, its processes, components, the scope of the audit, and its deliverables. We considered both sides to be crucial for the development of this framework.

Regarding the complexity of the topic and all the components it encompasses, it was not an easy task to select the most relevant arguments for the development of this work, but the current selection seemed like the most appropriate for the objective of this paper.

It is relevant to mention that the topics of cloud services and cloud auditing are now more than ever growing in popularity among companies and individuals, and due to that, it is important for this framework to be updated in the upcoming years to address contemporary issues and matters that may surge with the passage of time.

In this dissertation, after researching the relevant topics, we presented a model that addresses several aspects and areas of an IT and IS environment in the cloud, however, there is room for expansion and improvement (e.g., networking access, maintenance, and management).

A limitation to this work was the lack of hands-on experience in an organizational cloud environment that could not only present a whole new and separate set of variables to analyze and research but a stronger in-depth understanding of how an environment works in an organizational context and environment.

Despite that, we believe that the proposed framework covers a wide range of IT and IS areas, issues, and risks that, and, when applied in practice it can obtain accurate and objective results for an auditing team to form a strong, independent opinion with enough basis to sustain it and argument in its favor.

References

[1] Alazie Dagnaw, G., & Ebabye Tsige, S. (2019). Challenges and Opportunities of Cloud Computing in Social Network; Survey. Internet of Things and Cloud Computing, 7(3). Retrieved from: https://doi.org/10.11648/j.iotcc.20190703.13

[2] Alzeban, A., & Sawan, N. (2015). The impact of audit committee characteristics on the implementation of internal audit recommendations. Journal of International Accounting, Auditing, and Taxation, 24. Retrieved from: https://doi.org/10.1016/j.intaccaudtax.2015.02.005

[3] Amiruddin, A., Afiansyah, H. G.,Nugroho, H. A. (2021). Cyber-Risk Management Planning Using NIST CSF v1.1, NIST SP 800-53 Rev. 5, and CIS Controls v8. Proceedings - 3rd International Conference on Informatics, Multimedia, Cyber, and Information System, ICIMCIS 2021. https://doi.org/10.1109/ICIMCIS53775.2021.9699337

[4] Barta, G. (2018). THE INCREASING ROLE OF IT AUDITORS IN FINANCIAL AUDIT: RISKS AND INTELLIGENT ANSWERS. Business, Management, and Education, 16(0). Retrieved from: https://doi.org/10.3846/bme.2018.2142

[5] Bedard, J. C., & Graham, L. (2011). Detection and severity classifications of Sarbanes-Oxley section 404 internal control deficiencies. Accounting Review, 86(3). Retrieved from: https://doi.org/10.2308/accr.00000036

[6] Bennett, K. W., & Robertson, J. (2019). Security in the Cloud: understanding your responsibility. Retrieved from: https://doi.org/10.1117/12.2521821

[7] Brenner, J. (2007). ISO 27001: Risk management and compliance.

[8] Cusumano, M. (2010). Cloud computing and SaaS as new computing platforms. Communications of the ACM, 53(4). Retrieved from: https://doi.org/10.1145/1721654.1721667

[9] de Hert, P., Papakonstantinou, V., Kamara, I. (2016). The cloud computing standard ISO/IEC 27018 through the lens of the EU legislation on data protection. Computer Law and Security Review, 32 (1). https://doi.org/10.1016/j.clsr.2015.12.005

[10] Doelitzscher, F., Sulistio, A., Reich, C., Kuijs, H., & Wolf, D. (2011). Private cloud for collaboration and e-Learning services: From IaaS to SaaS. Computing (Vienna/New York), 91(1). Retrieved from: https://doi.org/10.1007/s00607-010-0106-z

[11] Dusenbury, R. B., Reimers, J. L., & Wheeler, S. W. (2000). The audit risk model: An empirical test for conditional dependencies among assessed component risks. Auditing, 19(2). Retrieved from: https://doi.org/10.2308/aud.2000.19.2.105

[12] Engvang, J. A., & Jradi, M. (2021). Auditing and design evaluation of building automation and control systems based on EU.bac system audit – Danish case study. Energy and Built Environment, 2(1). Retrieved from: https://doi.org/10.1016/j.enbenv.2020.06.002

[13] Furqan, A. C., Wardhani, R., Martani, D., & Setyaningrum, D. (2020). The effect of audit findings and audit recommendation follow-up on the financial report and public service quality in Indonesia. International Journal of Public Sector Management, 33(5). Retrieved from: https://doi.org/10.1108/IJPSM-06-2019-0173

[14] Gorelik, E. (2013). Cloud Computing Models Retrieved from: https://dspace.mit.edu/handle/1721.1/79811

[15] Gramling, A. A., O'Donnell, E., & Vandervelde, S. D. (2010). Audit partner evaluation of compensating controls: A focus on design effectiveness and extent of auditor testing. Auditing, 29(2). Retrieved from: https://doi.org/10.2308/aud.2010.29.2.175

[16] Gërvalla, M., Preniqi, N., Kopacek, P. (2018). IT infrastructure library (ITIL) framework approach to IT governance. IFAC-PapersOnLine, 51(30). https://doi.org/10.1016/j.ifacol.2018.11.283

[17] Griffith, E. (2015). What Is Cloud Computing? Retrieved from: https://uk.pcmag.com/networking-communications-software/16824/what-is-cloud-computing

[18] Houston, R. W., Peters, M. F., & Pratt, J. H. (1999). The audit risk model, business risk, and audit planning decisions. Accounting Review, 74(3). Retrieved from: https://doi.org/10.2308/accr.1999.74.3.281

[19] Jansen, W., & Grance, T. (2012). Guidelines on security and privacy in public cloud computing? In Public Cloud Computing: Security and Privacy Guidelines. Retrieved from: https://doi.org/10.3233/gov-2011-0269

[20] Jitendra, S. (2017). Study on Challenges, Opportunities and Predictions in Cloud Computing", International Journal of Modern Education and Computer Science (IJMECS), Vol.9, No.3, pp.17-27, 2017.DOI: 10.5815/ijmecs.2017.03.03

[21] Kemp, R. (2015). ISO 27018 and personal information in the cloud: First year scorecard. Computer Law and Security Review. https://doi.org/10.1016/j.clsr.2015.05.013

[22] Li, Q., Wang, Z. yuan, Li, W. hua, Li, J., Wang, C., & Du, R. yang. (2013). Applications integration in a hybrid cloud computing environment: modeling and platform. Enterprise Information Systems, 7(3). Retrieved from: https://doi.org/10.1080/17517575.2012.677479

[23] Libby, R., Artman, J. T., & Willingham, J. J. (1985). Process Susceptibility, Control Risk, and Audit Planning. Accounting Review, 60.

[24] Libby, R., & Frederick, D. M. (1990). Experience and the Ability to Explain Audit Findings. Journal of Accounting Research, 28(2). Retrieved from: https://doi.org/10.2307/2491154

[25] Mangalaraj, G., Singh, Taneja, A. (2014). IT governance frameworks and COBIT - A literature review. 20th Americas Conference on Information Systems, AMCIS 2014.

[26] Martins, F. C. (2010). Implementing ITIL Change Management. Instituto Superior Tecnico.

[27] Mazza, T., & Azzali, S. (2015). Effects of Internal Audit Quality on the Severity and Persistence of Controls Deficiencies. International Journal of Auditing, 19(3). Retrieved from: https://doi.org/10.1111/ijau.12044

[28] Mosher, R. (2011). 34 ISSA PREEMINENT TRUSTED GLOBAL INFORMATION SECURITY COMMUNITY. ISSA Journal.

[29] Naiker, V., & Sharma, D. S. (2009). Former audit partners on the audit committee and internal control deficiencies. Accounting Review, 84(2). Retrieved from: https://doi.org/10.2308/accr.2009.84.2.559

[30] Neubauer, T., Ekelhart, A., Fenz, S. (2008). Interactive selection of ISO 27001 controls under multiple objectives. IFIP International Federation for Information Processing, 278. https://doi.org/10.1007/978-0-387-09699-5_31

[31] NIST. (2013). NIST SP 800-53: Security and privacy controls for federal information systems and organizations. NIST Special Publication, 5.

[32] Onwubiko, C. (2009). A security audit framework for security management in the enterprise. Communications in Computer and Information Science, 45. Retrieved from: https://doi.org/10.1007/978-3-642-04062-7_2

[33] Pereira, T. S. M., & Santos, H. (2010). A security framework for audit and management information system security. Proceedings - 2010 IEEE/WIC/ACM International Conference on Web Intelligence and Intelligent Agent Technology - Workshops, WI-IAT 2010. Retrieved from: https://doi.org/10.1109/WI-IAT.2010.244

[34] Qian, L., Luo, Z., Du, Y., Guo, L. (2009). Cloud Computing: An Overview. In: Jaatun, M.G., Zhao, G., Rong, C. (eds) Cloud Computing. CloudCom 2009. Lecture Notes in Computer Science, vol 5931. Springer, Berlin, Heidelberg. Retrieved from: https://doi.org/10.1007/978-3-642-10665-1_63

[35] Russell, J. P. (2006). Generating audit findings and conclusions. In Quality Progress (Vol. 39, Issue 12).

[36] Sahibudin, S., Sharifi, M, Ayat, M. (2008). Combining ITIL, COBIT and ISO/IEC 27002 in order to design a comprehensive IT framework in organizations. Proceedings - 2nd Asia International Conference on Modelling and Simulation, AMS 2008. https://doi.org/10.1109/AMS.2008.145

[37] Tan, H. T., & Yip-Ow, J. (2001). Are Reviewers' Judgements Influenced by Memo Structure and Conclusions Documented in Audit Workpapers? Contemporary Accounting Research, 18(4). Retrieved from: https://doi.org/10.1506/UG8M-8H3D-1GA2-7BYK

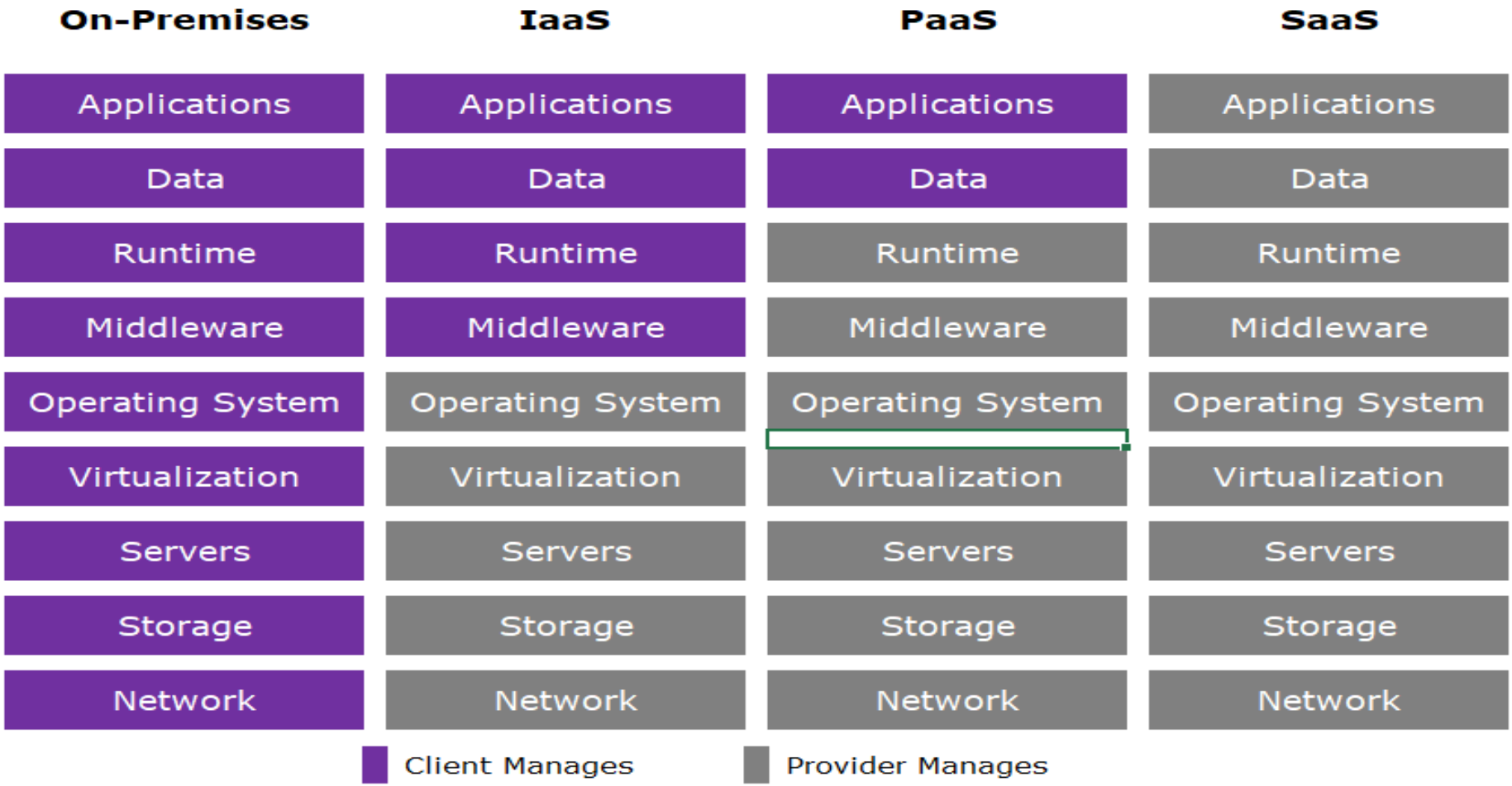
[38] Tariq, M. I., Tayyaba, S., Ashraf, M. W.,Khan, F. (2016). Analysis of NIST SP 800-53 Rev.3 Controls Effectiveness for Cloud Computing. 1st National Conference on Emerging Trends and Innovations in Computing; Technology, March.

[39] Vu, K., Hartley, K., & Kankanhalli, A. (2020). Predictors of cloud computing adoption: A cross-country study. Telematics and Informatics, 52. Retrieved from: https://doi.org/10.1016/j.tele.2020.101426

[40] Wachter, S. (2018). Normative challenges of identification in the Internet of Things: Privacy, profiling, discrimination, and the GDPR. Computer Law and Security Review, 34 (3). https://doi.org/10.1016/j.clsr.2018.02.002

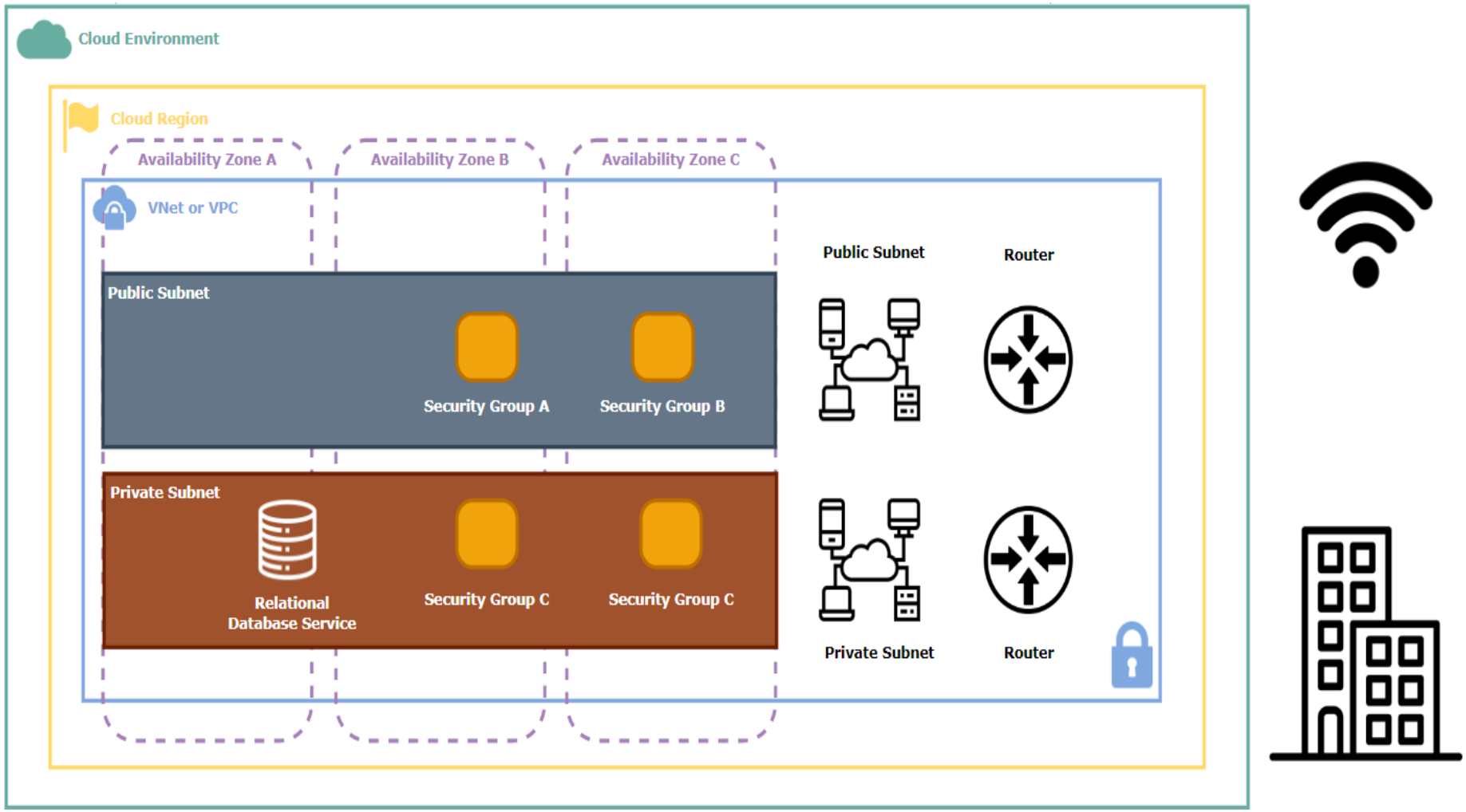
Appendix

Figure 1A: Component Responsibility Matrix



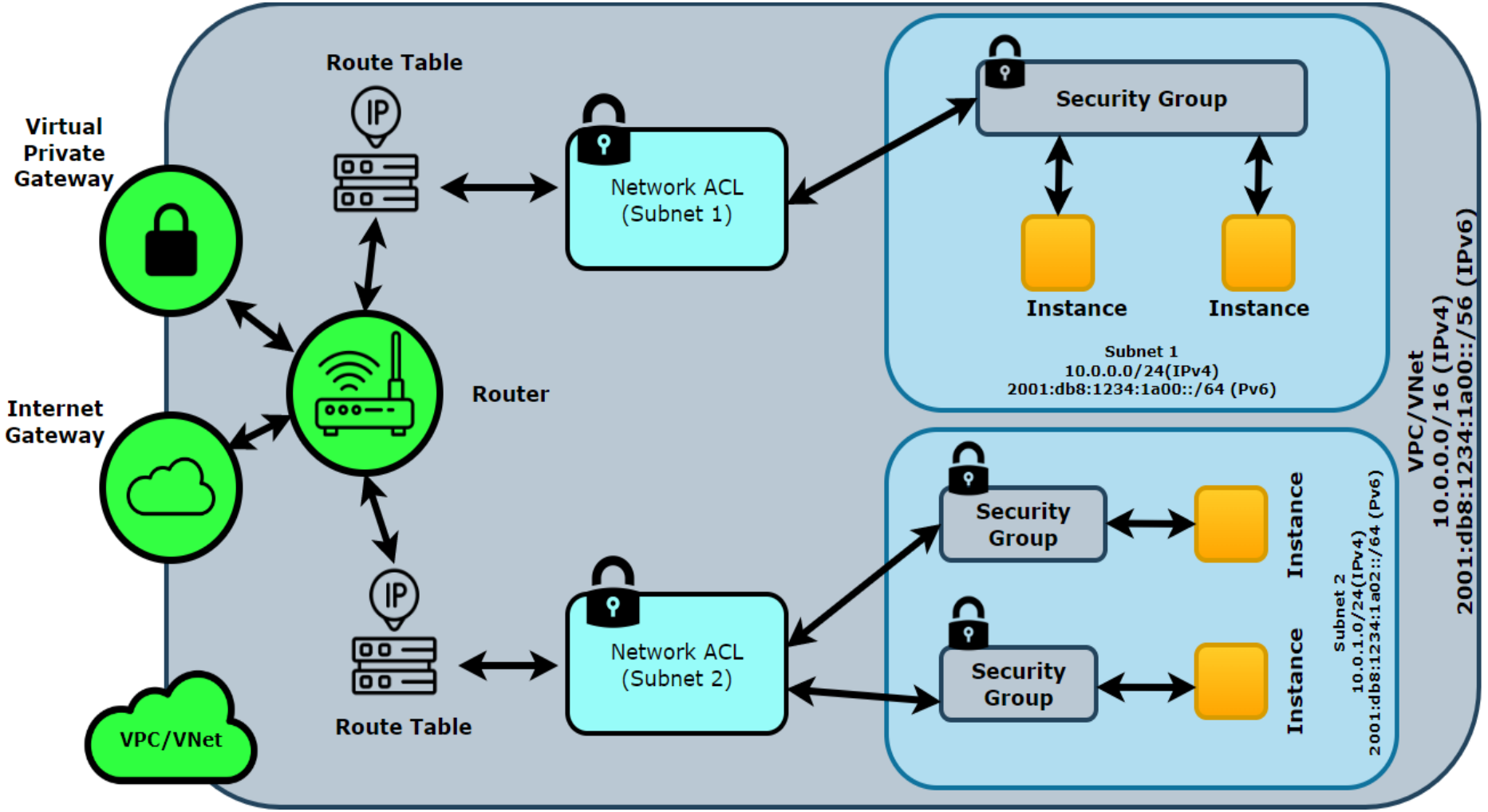
Source: Own Production

Figure 2A: Cloud Environment Architecture



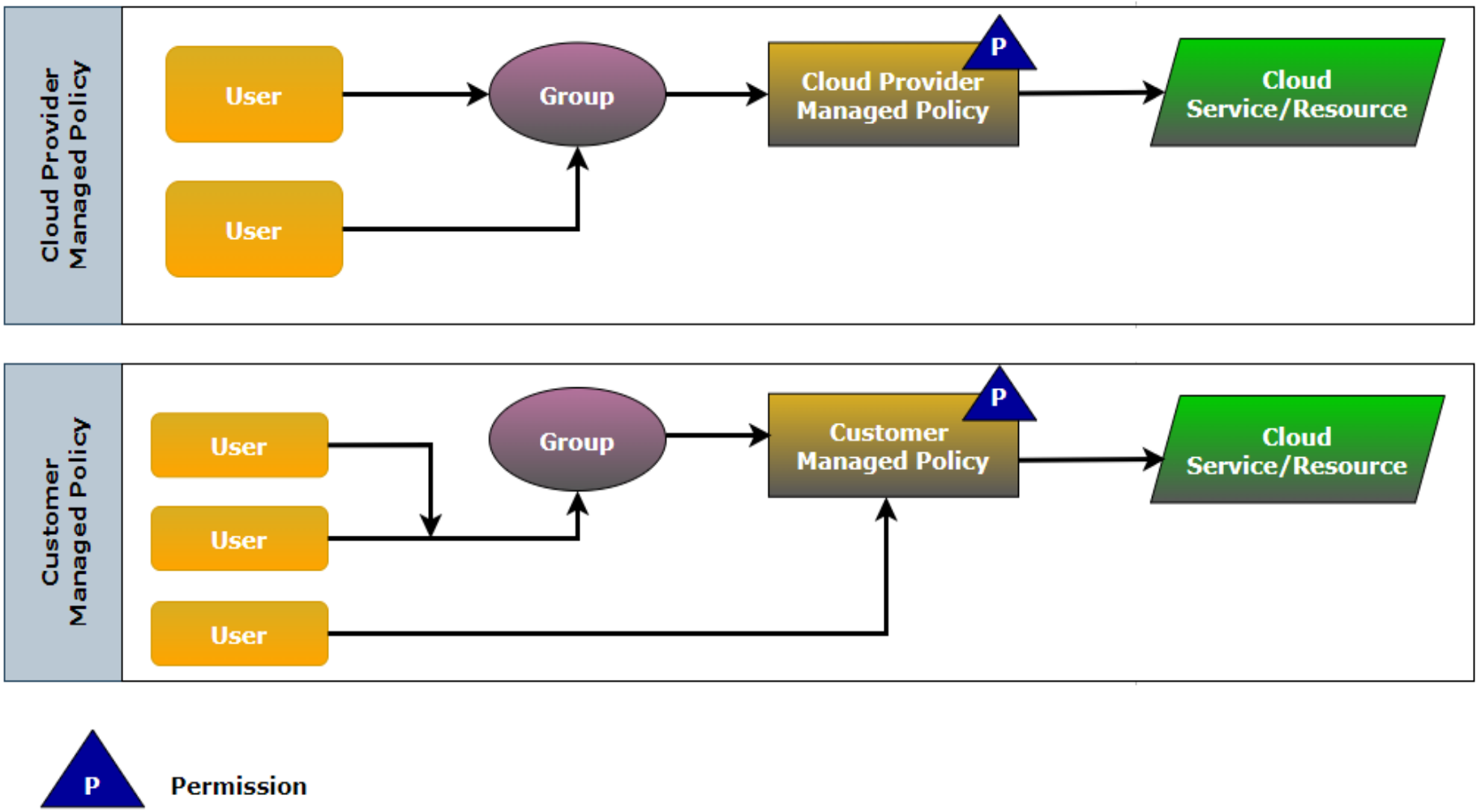
Source: Own Production

Figure 3A: Cloud Network Traffic Diagram



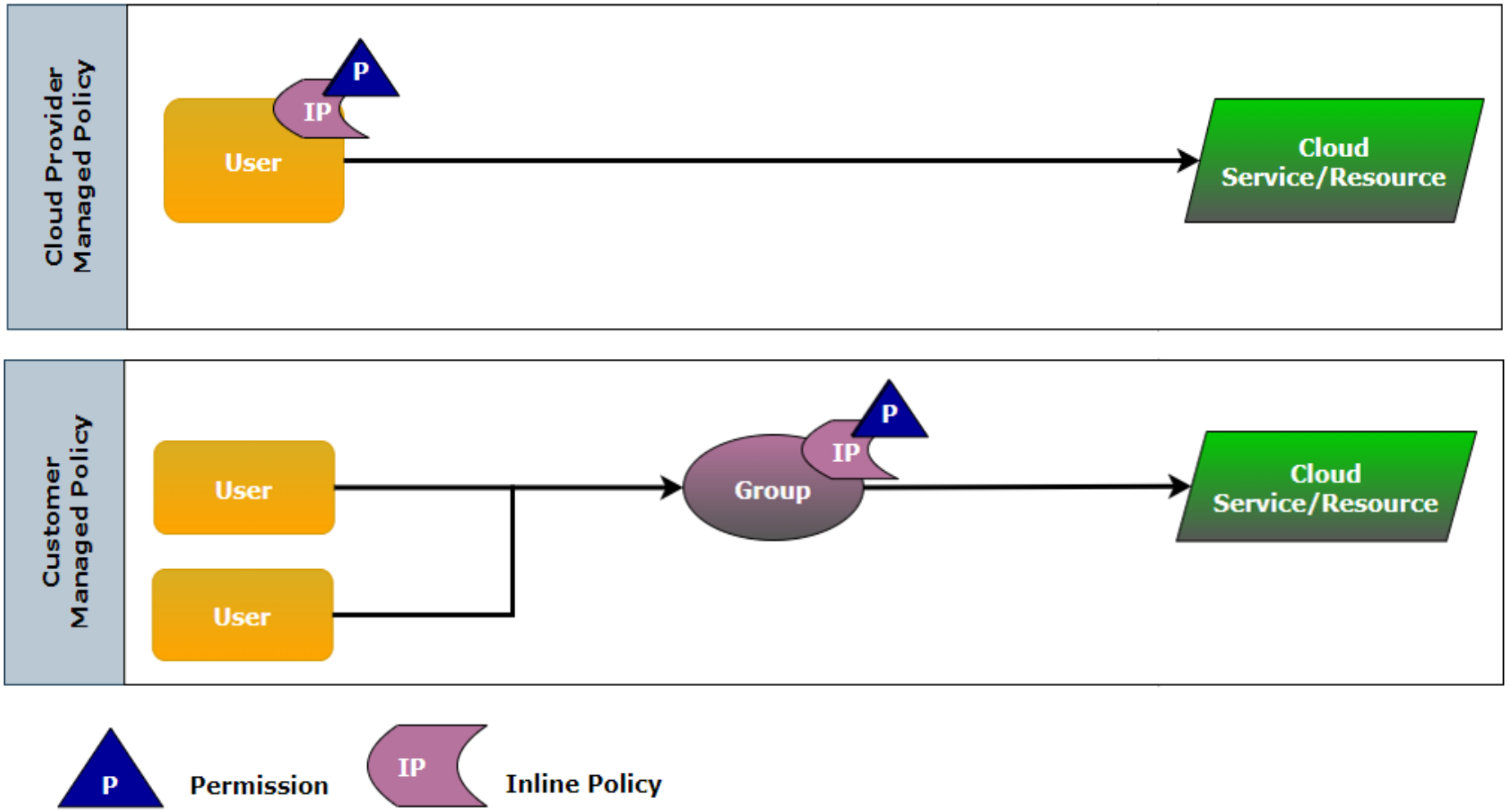
Source: Own Production

Figure 4A: Logical Access Policy Matrix



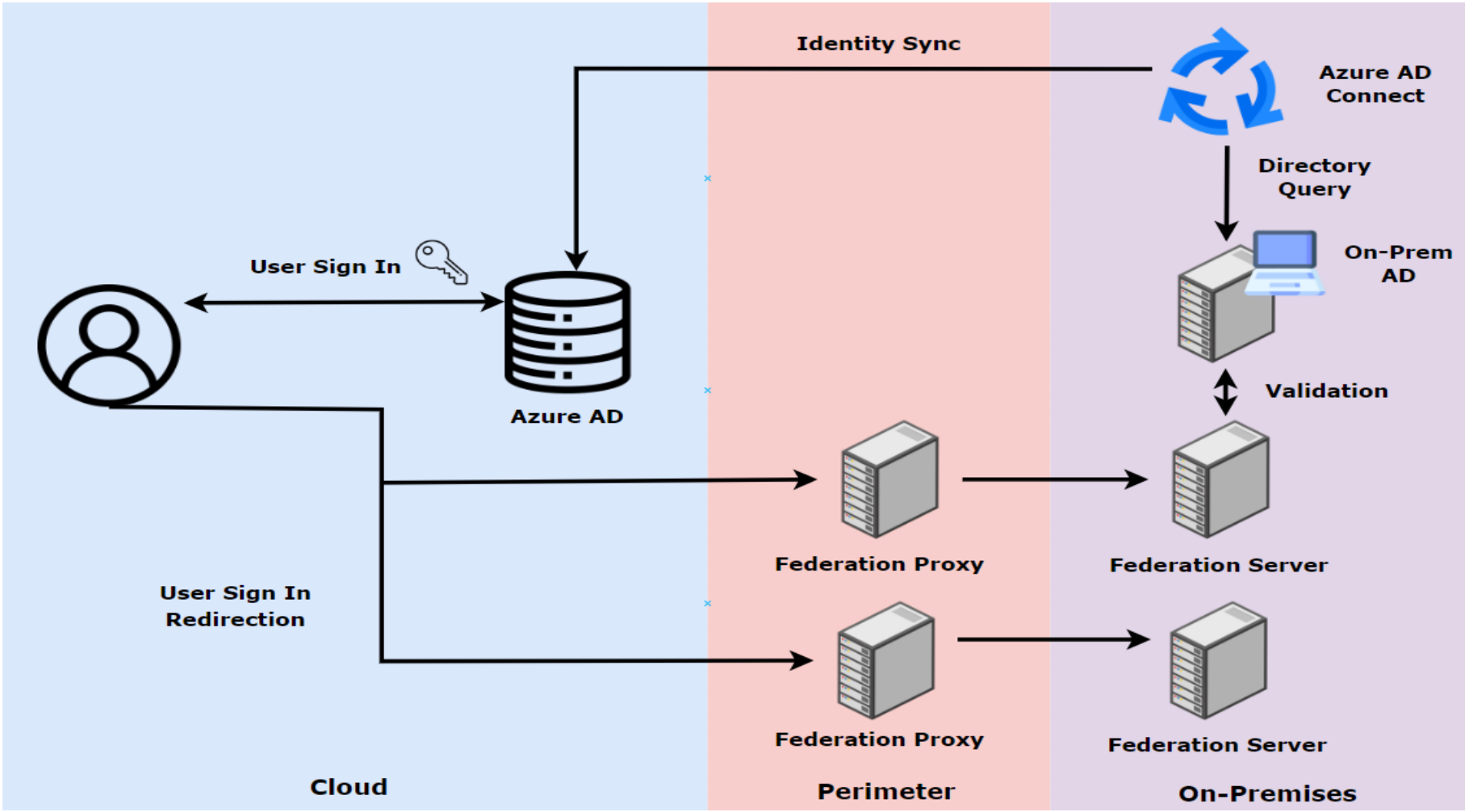
Source: Own Production

Figure 5A: Logical Access through In-Line Policy Matrix



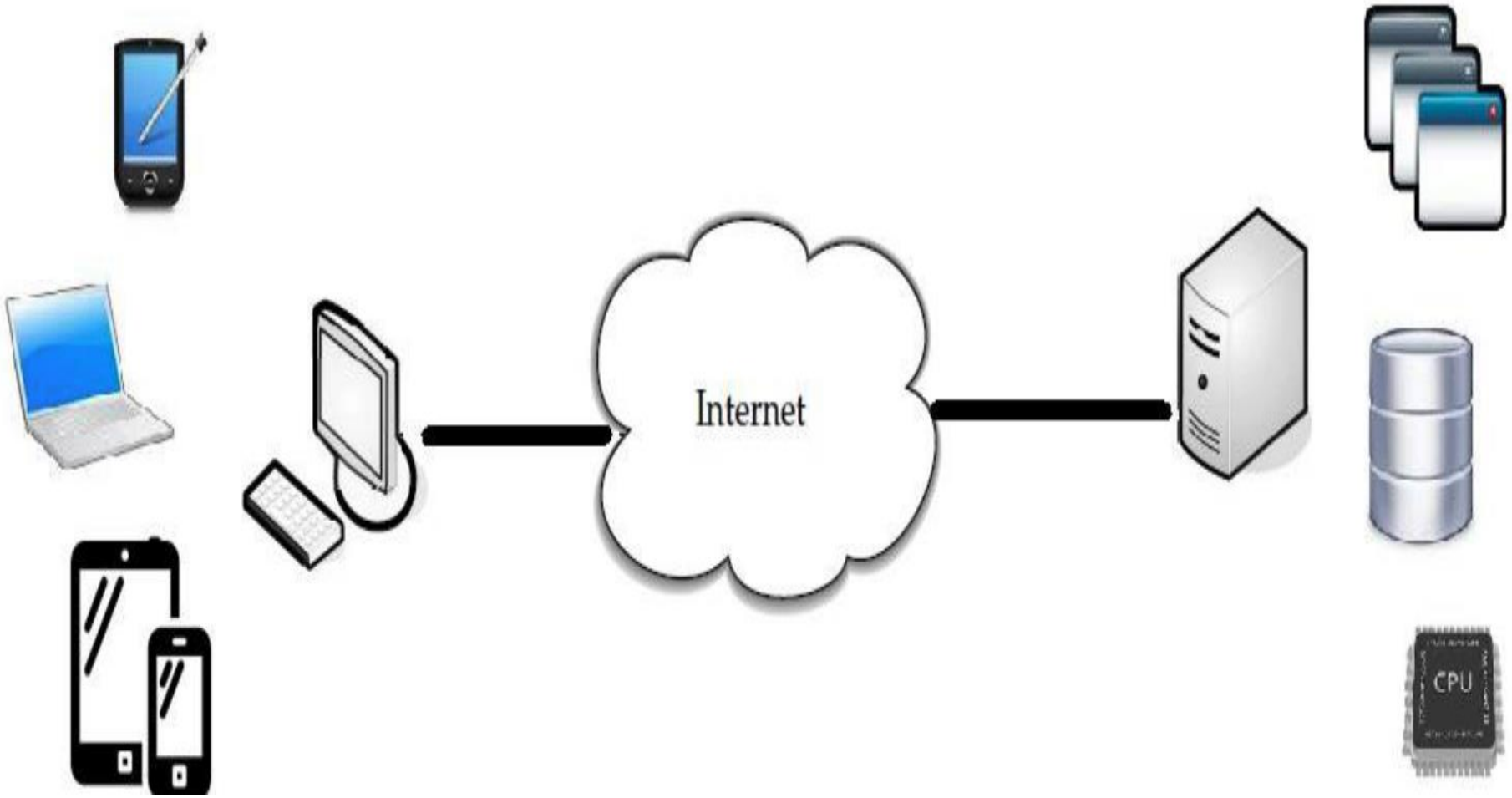
Source: Own Production

Figure 6A: Azure Logical Access of Hybrid Identities Matrix



Source: Own Production

Figure 7A: Basic Cloud Setup



Source: Alazie Dagnaw, G., & Ebabye Tsige, S. (2019). Challenges and Opportunities of Cloud Computing in Social Network; Survey. *Internet of Things and Cloud Computing*, *7*(3). Consulted on: https://doi.org/10.11648/j.iotcc.20190703.13

Figure 8A: Cloud Security Architecture

Layer	Security Issues
User Layer	Browser / Application: Authentication, SSL, HTTPs implementation, Public-Private Key Implementation
Service Provider Layer	Data Transmission: SLA monitor, Usage accounting and tracking Load Balancer Service (LBS) Policy Management User Identity Infrastructure refresh Audit and Regulatory Compliance etc.
Virtualization Layer	Virtual Machine –Virtual Machines creation, monitoring and operating system software on it. VM allocation to customers / consumers
Data Centre Layer	Physical security: network devices and servers Physical Infrastructure: Servers, CPU's, memory (RAM) and storage Identity and access management Legal and regularity compliance issues,

Source: Alazie Dagnaw, G., & Ebabye Tsige, S. (2019). Challenges and Opportunities of Cloud Computing in Social Network; Survey. *Internet of Things and Cloud Computing*, *7*(3). Consulted on: https://doi.org/10.11648/j.iotcc.20190703.13