

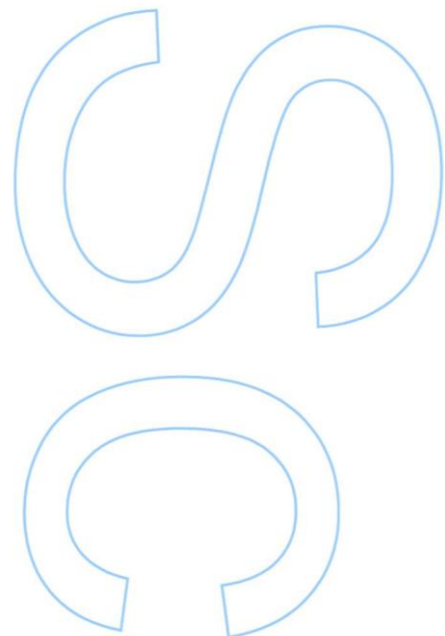
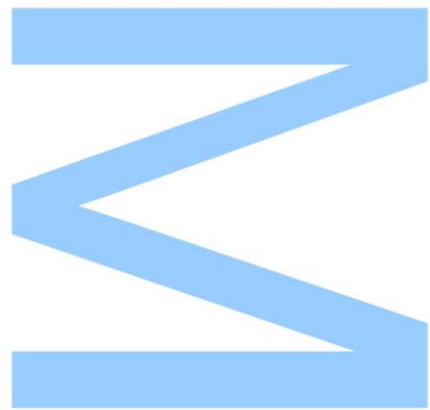
Healthcare Cloud Security Maturity Assessment Framework

Tiago Emanuel Gomes Novais

Mestrado em Segurança Informática
Departamento de Ciências de Computadores
2021

Orientador

Pedro Miguel Alves Brandão
Professor Doutor
Faculdade de Ciências da Universidade do Porto

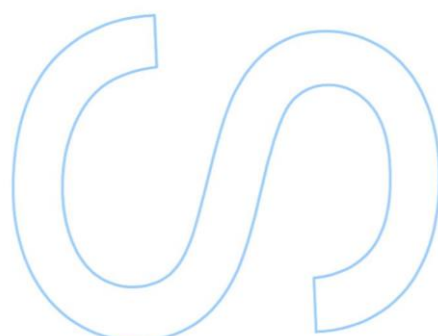
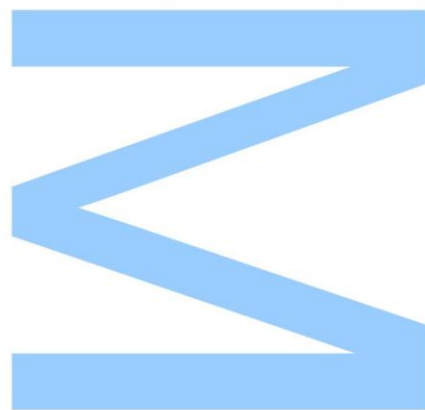




Todas as correções determinadas pelo júri, e só essas, foram efetuadas.

O Presidente do Júri,

Porto, ____/____/____



UNIVERSITY OF PORTO

MASTERS THESIS

Healthcare Cloud Security Maturity Assessment Framework

Author:

Tiago NOVAIS

Supervisor:

Pedro BRANDÃO

*A thesis submitted in fulfilment of the requirements
for the degree of Master's degree in Information Security*

at the

Faculty of Sciences of the University of Porto
Department of Computer Sciences

December 18, 2021

“ If the present world go astray, the cause is in you, in you it is to be sought. ”

Dante Alighieri

Acknowledgements

First and foremost, I would like to express my full gratitude and appreciation to Prof. Dr. Pedro Brandão. His constant cooperation, availability, and interest, always made me assure of what path should be pursued in the development of this thesis. Looking back, I know how fortunate I was to have you as my mentor. A sincere thank you to Prof. Dr. Ricardo Correia, and the CIOs that were kind enough to contribute to this work. To Dra. Maria João Campos, Dr. José Castanheira, Dr. César Quintas, and Dra. Maria Bastos Salazar, it was a pleasure meeting you.

Furthermore, I would like to thank everyone at Ernst & Young (EY) for providing me with all of the necessary conditions and aid to develop this work, especially to my tutor Pedro Monzelo, who proves to be an exemplar working role model for me every single day. In addition, a special thank you to Sérgio Martins and Sérgio Sá, for providing me with the opportunity of being a part of such a fantastic team.

Additionally, a special thank you to all the professors, and working personnel of FCUP. It might have been a rather quick passage, but I truly felt like I belonged. In this sense, I address all of my friends from the university when I say that I honestly will never forget you.

Moreover, my warmest thank you to my friends. Many of you I knew recently, and many others have watched me grow. Today I can say that neither of you can be replaced. Thank you all for being yourselves.

I dedicate this work to my parents, Alberto and Elisa, and my brother, Pedro, as well as the rest of my family. Since the moment I was born, you have given me everything to thrive. You are the reason why I have come this far, and to you, I promise to go even further.

Finally, to my amazing girlfriend and best friend, Francisca. I want to thank you with all my heart. It is hard to put into words how important you are to me. What I know for sure is that I could not be happier to complete yet another major step in my life with you by my side.

UNIVERSITY OF PORTO

Abstract

Faculty of Sciences of the University of Porto

Department of Computer Sciences

Master's degree in Information Security

Healthcare Cloud Security Maturity Assessment Framework

by [Tiago NOVAIS](#)

The present Master's thesis proposes a new maturity assessment framework for cloud security in healthcare. This work emerged from the necessity to establish cloud-specific controls directed to healthcare organizations (HCOs). As a result, this enables them to create a clear course of action for cloud security maturity, thus mitigating the likelihood of being exploited through cloud related-attack vectors. Therefore, the developed work aims at solving the challenges identified in the state of the art, and contributes to accurate evaluations of cloud security infrastructures in the health sector.

Cloud computing presents itself as a paradigm shift, from traditional computing systems. It is most relevant to understand what are the offered benefits of the cloud model, as opposed to on-premise infrastructures. In a similar fashion, healthcare security is addressed, presenting the investigation outputs. These consist of the security challenges that the sector has been facing throughout the recent years, as well as what solutions are offered from industry standards to combat the identified problems. As a result, the author details the synergy in combining cloud computing models and eHealth. Additionally, expounding on the existing standards and frameworks that establish and define security controls for both of the subjects.

Subsequently, the Healthcare Cloud Security Maturity Assessment Framework (HCS-MAF) tool is proposed as a solution for the identified gap between healthcare and cloud security. The framework consists of a holistic approach to assess the cloud security maturity of healthcare organizations, setting the ground for improvement roadmaps. Ultimately, leading HCOs to an optimizing maturity state, whereas a strong cloud foundation is achieved, and the organization focuses on continuously improving its security. The

framework's maturity model is based on the crossover of security standards. It is segregated between nine security domains, with associated maturity questions, for the user to respond. Based on the inputs submission, the tool renders a maturity result, quantifying the assessed cloud security's maturity as Initial (1), Managed (2), Quantitatively Managed (3), or Optimizing (4).

The tool was evaluated by stakeholders, complying with defined criteria to fit in the given scope. The results determined that the developed framework provides accurate results whilst performing an overarching maturity assessment. The proposed maturity model and security domains questions were provided with a solid classification, notwithstanding the great margin for future improvements.

Finally, it is concluded that the framework provides valuable insights to healthcare organizations with cloud computing infrastructures, or in the course of obtaining them. As a result, it grasps the security concepts between both subjects, thus positioning itself as a reliable maturity assessment tool for healthcare cloud security infrastructures.

Keywords: Framework, Cloud, Computing, Health, Security, Maturity, Assessment

UNIVERSITY OF PORTO

Resumo

Faculty of Sciences of the University of Porto

Department of Computer Sciences

Mestrado em Segurança Informática

Ferramenta de Avaliação da Maturidade de Segurança *Cloud* no Setor da Saúde

por [Tiago NOVAIS](#)

A presente tese de mestrado propõe uma nova ferramenta de avaliação de maturidade para a segurança em *cloud* na área da saúde. O trabalho desenvolvido emergiu da necessidade de estabelecer controlos específicos em *cloud* direcionados às organizações de saúde. Por conseguinte, é-lhes assim permitido desenvolver um plano de ação claro de maturidade de segurança em *cloud*, reduzindo, deste modo, a probabilidade de serem atingidos por vetores de ataque neste tipo de ambientes. Assim sendo, o trabalho desenvolvido visa solucionar os desafios identificados no estado da arte e contribuir para avaliações precisas de infraestruturas de segurança em *cloud* no setor da saúde.

A computação em *cloud* apresenta-se como uma mudança de paradigma, partindo dos sistemas de informática tradicionais. É de extrema relevância compreender assim quais são os benefícios que advêm deste modelo, em comparação com as infraestruturas locais. Do mesmo modo, a segurança na área da saúde é abordada nesta tese, apresentando os resultados decorrentes desta investigação. Estes consistem nos desafios de segurança que o setor tem enfrentado ao longo dos últimos anos, bem como as soluções que são oferecidas a partir das normas da indústria para enfrentar os problemas identificados. Consequentemente, o autor pormenoriza a sinergia em combinar modelos de computação em *cloud* e *eHealth*. Adicionalmente, expõe as normas e *frameworks* existentes que estabelecem e definem os controlos de segurança para ambos os temas.

Subsequentemente, a ferramenta *Healthcare Cloud Security Maturity Assessment Framework* (HCSMAF) é apresentada como uma solução para a lacuna identificada entre a área da saúde e a segurança em *cloud*. A *framework* consiste numa abordagem holística para avaliar a maturidade da segurança em *cloud* das organizações de saúde, permitindo uma melhoria futura dos planos de ação de segurança. Em última análise, conduz

a uma otimização do seu estado de maturidade, e desta forma atingir um nível sólido de segurança em *cloud*, garantindo que a instituição se concentra em melhorar continuamente neste sentido. O modelo de maturidade de *framework* é baseado no cruzamento de padrões de segurança. Assim sendo, é segregada entre nove domínios de segurança, com questões de maturidade associadas, para o utilizador responder. Com base na submissão dos *inputs*, a ferramenta calcula o resultado de maturidade, quantificando a maturidade da segurança em *cloud*. Como resultado, a maturidade pode ser classificada como Inicial (1), Gerida (2), Quantitativamente Gerida (3) ou Otimizando (4).

A ferramenta foi avaliada pelos *stakeholders*, e critérios foram definidos para os mesmos se adequarem ao âmbito do trabalho desenvolvido. Os resultados determinaram que a *framework* desenvolvida fornece resultados precisos, sendo que efetua uma avaliação abrangente de maturidade. O modelo de maturidade proposto, assim como as questões dos domínios de segurança, receberam uma classificação sólida, não obstante, existe grande margem para futuras melhorias.

Por fim, conclui-se que a ferramenta fornece informações valiosas para as organizações de saúde com infraestruturas de computação em *cloud*, ou as que se encontram no curso de as obter. Como resultado, a ferramenta agrega os conceitos de segurança entre os dois temas, posicionando-se como uma ferramenta confiável de avaliação de maturidade para infraestruturas de segurança em *cloud* no setor da saúde.

Palavras-chave: Ferramenta, *Cloud*, Computação, Saúde, Segurança, Maturidade, Avaliação

Contents

Acknowledgements	v
Abstract	vii
Resumo	ix
Contents	xi
List of Figures	xiii
List of Tables	xv
Glossary	xvii
1 Introduction	1
1.1 Document Structure	3
2 State of the Art	5
2.1 Cloud Computing	5
2.1.1 Cloud Computing Characteristics	6
2.1.2 Cloud Computing Models	7
2.1.2.1 Infrastructure as a Service - IaaS	7
2.1.2.2 Platform as a Service - PaaS	8
2.1.2.3 Software as a Service - SaaS	9
2.1.3 Cloud Computing Deployments	11
2.1.4 Cloud Computing Security	14
2.1.4.1 Cloud Security Challenges	14
2.1.4.2 Cloud Security Benefits	15
2.1.4.3 Cloud Security Frameworks and Standards	15
2.2 Security in Healthcare	16
2.2.1 Healthcare Challenges	17
2.2.2 Common Security Threats to Healthcare	19
2.2.3 Healthcare Cloud Systems	21
2.2.4 Healthcare Cloud Benefits	23
2.2.5 Healthcare Cloud Security Challenges	23
2.2.6 Healthcare Security Standards and Frameworks	25
2.3 Review of Cloud Security Maturity models for Healthcare	26

3	Development of the Healthcare Cloud Security Maturity Assessment Framework	29
3.1	Framework's Functional Requirements	29
3.2	Framework's Security Assessment	30
3.2.1	Identity and Access Management	31
3.2.2	Data Privacy and Management	33
3.2.3	Risk Management	35
3.2.4	Asset Management	35
3.2.5	Cryptography and Key Management	35
3.2.6	Infrastructure and Network Security	36
3.2.7	Compliance and Audit Management	37
3.2.8	Incident Response Management	37
3.2.9	Business Continuity Management	37
3.3	Capability Maturity Model and Metrics	39
3.4	HCSMAF Technical Implementation	41
3.5	Results Representation	44
4	HCSMAF Evaluation Results	47
4.1	HCSMAF Evaluation Planning	47
4.2	Evaluation Form	49
4.3	Evaluation Results	51
4.3.1	General Questions	51
4.3.2	Maturity Model Questions	52
4.3.3	Security Domains	52
4.3.4	TAMv2 Evaluation	54
4.3.5	Overall Results Discussion	56
5	Conclusion & Future Improvements	61
5.1	Future Improvements	62
A	HCSMAF Web Application	65
B	Evaluation Form	69
C	HCSMAF Standards Mapping Example	71
	Bibliography	73

List of Figures

2.1	Infrastructure as a Service (IaaS)[8]	7
2.2	Platform as a Service (IaaS) [8]	10
2.3	Public Cloud Diagram	11
2.4	Private Cloud	12
2.5	Community Cloud	13
2.6	Hybrid Cloud	13
2.7	Data Breaches of Healthcare in the US	19
2.8	Attacks on Healthcare in 2020	20
2.9	Verizon DBRI reports Healthcare breaches	21
3.1	Assessment Functional Requirements	30
3.2	Security standards domains mapping and crossover	31
3.3	HCSMAF Domains Structure	32
3.4	Framework's maturity model	40
3.5	Database's relational model	43
3.6	Client to Server Communications	44
3.7	Tool's Results page outputs	44
4.1	HCSMAF Interview Phases	49
4.2	General questions answers	51
4.3	Results for the Maturity Model	52
4.4	Results of the Security Domains	53
4.5	Results of the Maturity Questions	54
4.6	Results for the Perceived Usefulness (PU) - TAMv2	55
4.7	Results for the Perceived Ease of Use (PEOU) - TAMv2	55
4.8	Results for the User Acceptance to Information Technology (UAIT) - TAMv2	56
A.1	Appendix 1 - HCSMAF Webapp Assessment Page	66
A.2	Appendix 2 - HCSMAF Webapp Results Page	67
B.1	Appendix 3 - HCSMAF Evaluation Form	69
B.2	Appendix 4 - HCSMAF Evaluation Form Results	70
C.1	Appendix 5 - Framework's investigation and standards mapping exercise	71

List of Tables

2.1	Cloud Benefits	15
2.2	Cloud Security Standards and Frameworks	16
2.3	Healthcare solutions with potential use in cloud	22
2.4	Healthcare laws, regulations, and security standards	26
4.1	Evaluation form for stakeholders	50
4.2	Security Domain Results table	58
4.3	TAMv2 Sections Evaluation	58

Glossary

AWS	Amazon Web Services
ABAC	Attribute-Based Access Control
API	Application Programming Interfaces
BAA	Business Associate Agreements
BCMS	Business Continuity Management System
BCP	Business Continuity Plan
BIA	Business Impact Analysis
CASB	Cloud Access Security Broker
CSA	Cloud Security Alliance
CIA	Confidentiality, Integrity, and Availability
CIO	Chief Information Officer
CSC	Cloud Service Customer
CSP	Cloud Service Provider
CMMI	Capability Maturity Model Integration
CPU	Central Process Unit
DBRI	Data Breach Investigations Report
DLP	Data Loss Prevention
DoD	Department of Defense
DOS	Denial-of-Service
DPIA	Data Privacy Impact Assessment
DPO	Data Protection Officer

DRP	Disaster Recovery Plan
EHR	Electronic Health Records
ENISA	European Union Agency for Cybersecurity
EPIS	Electronic Prescription Information System
ERP	Enterprise Resource Management
FIPS	Federal Information Processing Standards
FTP	File Transfer Protocol
GCP	Google Cloud Platform
GDPR	General Data Protection Regulation
HCO	Healthcare Organizations
HCSMAF	Healthcare Cloud Security Maturity Assessment Framework
HIPAA	Health Insurance Portability and Accountability Act
HIS	Healthcare Information System
HSM	Hardware Security Model
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IaaS	Infrastructure as a Service
IDS	Intrusion Detection System
IPS	Intrusion Prevention Systems
IR	Incident Response
ISO	International Standards Organization
JAB	Joint Authorization Board
JSON	JavaScript Object Notation
LDAP	Lightweight Directory Access Protocol
LIS	Laboratory Information System
MTPD	Maximum Tolerable Period of Disruption
MDD	Medical Device Directive

MDR	Medical Device Regulation
NIST	National Institute of Standards and Technology
ORM	Object-relational mapping
OS	Operating System
OVF	Open Virtualization Format
PaaS	Platform as a Service
PACS	Picture Archiving and Communication system
PEOU	Perceived Ease of Use
PU	Perceived Usefulness
PHI	Personal Health Information
PII	Personal Identifiable Information
RBAC	Role-Based Access Control
REST	Representational state transfer
RIS	Radiology Information System
RPO	Recovery Point Objective
RTO	Recovery Time Objective
SaaS	Software as a Service
SFTP	Secure File Transfer Protocol
SIEM	Security Information and Event Management
SLA	Service Level Agreement
SAML	Security Assertion Markup Language
SPoF	Single Point of Failure
SoD	Separation of Duties
SRA	Security Risk Assessment
TAM	Technology Acceptance Model
UAIT	User Acceptance of Information Technology
VM	Virtual Machine

WAF	Web Application Firewall
WSGI	Web Server Gateway Interface
XSS	Cross-Site Scripting

Chapter 1

Introduction

In recent years, the evolution of information technology has enabled healthcare organizations to increase their effectiveness and efficiency, by providing the ability to electronically store and transfer medical data [1]. Medical data is considered to be one of the most sensitive types, as it includes Personal Health Information (PHI), and Electronic Health Records (EHR). As a result, hospitals have the responsibility to establish and implement security controls to protect patients' and employees' data. With the objective of controlling and auditing the security that these institutions implement, standards and regulations have emerged. In the United States of America (USA), the Health Insurance Portability and Accountability Act (HIPAA), created and signed in the year of 1996, introduced administrative, physical, and technical safeguards for PHI [2]. In the European Union, the General Data Protection Regulation (GDPR), introduced in 2016 and enforced in 2018, categorized health-related data as "sensitive" data [3]. The presented regulations had a positive effect on pressuring healthcare organizations to enforce best security practices, regarding confidentiality, integrity, and availability.

Nowadays, healthcare organizations face challenges of infrastructure maintenance, cybersecurity attacks, and data privacy compliance. As a consequence, these organizations have been struggling to deal with their vulnerabilities, leading to legal issues, service outages, and high maintenance costs [4]. These issues call for the necessity of adaptation, venturing on new technologies that can further enhance their infrastructure. Cloud computing technology presents itself as a solution to move from the traditional systems frailties and limitations to a modern and safer paradigm [5]. *Mell and Grance*, from the National Institute of Standards and Technology (NIST) [6], define this model as ubiquitous, convenient, on-demand network access to a shared pool of configurable

computing resources. The differentiating characteristics of the cloud computing model, such as its on-demand self-service, measured service, rapid elasticity, and flexibility [6], promote benefits for organizations to inherit. These include, but are not limited to, maintenance costs saving, higher security, increased system performance, and high resources scalability.

Despite the identified benefits, healthcare sector organizations are, in general, reluctant to adopt the cloud computing model. This skepticism is mainly due to the fact that the migration of patients' medical information to the cloud implies risks in terms of the security and privacy of sensitive health records [7]. These risks are associated with the involvement of third parties as data processors, the Cloud Service Providers (CSPs) [7]. Nevertheless, the author believes that, alongside the creation of credible security frameworks and standards, these organizations can adopt security measures and ultimately thrive with cloud computing technologies.

Cloud security has evolved throughout recent years. This is true considering the aptitude demonstrated by industry standards in creating new security controls directed to the technology. These are, but are not limited to, the Cloud Security Alliance (CSA) guidance [8] and cloud security controls matrix framework [9], the International Standards Organization's (ISO) ISO/IEC 27017:2015 [10], and ISO/IEC 27018:2019 [11]. Additionally, novel security frameworks have been developed with the purpose of assisting organizations to assess cloud security risks [12]. Nonetheless, an existing gap was identified between cloud security standards and healthcare security standards. The existing standards to assess cloud security controls show a heavy focus in organizations as a whole. Notwithstanding its positive effects, it lacks in focusing on solving cloud security challenges in the healthcare organizations. In a similar way, healthcare security standards still have not properly developed security controls addressing cloud computing challenges. As a result, it is a demanding task for these organizations to assess their cloud security maturity level and develop roadmaps for improvements.

This Master's thesis proposes a solution to solve the identified problem, by developing a maturity assessment framework that helps bridging the gap between cloud and healthcare security. The goal of the framework is to provide HCOs with a tool enabling them to evaluate their cloud computing infrastructure by performing a holistic maturity security assessment. As a result, identifying risks related to specific security areas, and mitigating them with the implementation of effective security controls.

1.1 Document Structure

The present document is structured as follows:

- **Chapter 2 - State of the Art:** This chapter details the theoretical support for the development of the Healthcare Cloud Security Maturity Assessment Framework, approaching several topics that are paramount to acknowledge in order to contextualize the framework.
- **Chapter 3 - Development of the Healthcare Cloud Security Maturity Assessment Framework:** This chapter details the development of the Healthcare Cloud Security Maturity Assessment Framework, implemented with the objective of providing an overarching evaluation over the defined cloud security domains. Its ultimate goal was to create a bridge between cloud and healthcare security, thus filling the existing gap, mentioned in the previous chapter, that healthcare organizations face when assessing the security of their cloud infrastructure.
- **Chapter 4 - HCSMAF Evaluation Results:** This chapter details the results from the evaluation phase of the HCSMAF. The objective of this phase was to validate the work and investigation performed to reach the final version of the tool. Thus understanding its applicability, usability, and how it can improve HCOs knowledge of their current state of maturity regarding cloud security.
- **Chapter 5 - Conclusion:** This chapter concludes the investigation's work, the framework's development, and respective results, highlighting its main outcomes and contributions.

Chapter 2

State of the Art

The following chapter details the theoretical support for the development of the Healthcare Cloud Security Maturity Assessment Framework, approaching several topics that are paramount to acknowledge in order to contextualize the framework. The first main section defines cloud computing and cloud security, identifying its main pillars, as well as benefits and challenges that come from it. It is followed by the deconstruction of the Healthcare sector in the scope of cybersecurity, the challenges that it faces, and why cloud computing presents itself as a key solution and opportunity to solve some of the main complications that the sector faces on a daily basis.

2.1 Cloud Computing

Cloud Computing is a rather recent and innovative technology that is already proving its potential by impacting the paradigm of computing. This technology makes it possible to access computing resources and facilities anywhere, thus guaranteeing increased flexibility for users to access data and hosted applications in the cloud. According to the National Institute of Standards and Technology (NIST), "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" [6]. The NIST definition takes note of five main characteristics that differentiate cloud computing from other existing traditional technologies. These characteristics are on-demand self-service, broad network access, resource pooling, rapid elasticity or expansion, and measured service [6]. Rather than owning their own computing infrastructure

or data centers, thus putting the responsibility on the organization's side, organizations can rent access to anything from storage, software, networks, and databases from a Cloud Service Provider (CSP). The cloud computing model trumps the on-premises model specially in terms of costs reduction, as it practically eliminates the need for the organization to invest in dedicated hardware, and reduces maintenance costs as it is performed by the CSP. According to Multisoft, "80 percent of companies saw operation improvements within the first few months of adopting the tech" [13], clearly showing an outweigh of benefits over disadvantages on adopting cloud computing. The trend for adopting this technology is exponential, as per Forbes statistics "By 2021, a staggering 83 percent of the company workload will be stored on the cloud." [13].

2.1.1 Cloud Computing Characteristics

Cloud computing, as defined by the National Institute of Standards and Technology (NIST), presents five main essential characteristics, detailed below [6].

- **On-demand self-service:** A Cloud Service Customer (CSC) can autonomously provision its own cloud infrastructure with more computing resources (e.g. storage, server time) without requiring assistance from the CSP;
- **Broad network access:** The access to the cloud is not limited to a certain network, for example, as it can be accessed through standard browsers and other clients, anywhere, anytime;
- **Resource pooling:** The cloud computing resources are pooled in a way that serves multiple cloud consumers/clients using a multi-tenancy model. This model guarantees a physical and virtual segregation between resources, which are dynamically assigned and reassigned according to consumer demand;
- **Rapid elasticity:** Resource capabilities can be elastically provisioned and released, in a rapidly scalable way according to consumer demand;
- **Measured service:** These systems automatically control the use of resources, by using a metering capability, measuring the parameters that are usually specified in the Service Level Agreement (SLA) between the CSC and the CSP. Resource usage can be monitored and controlled, and provides transparency of performance for both parties.

2.1.2 Cloud Computing Models

The NIST definition of cloud computing acknowledges three cloud "service models", Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Software as a Service (SaaS).

2.1.2.1 Infrastructure as a Service - IaaS

In a IaaS service type cloud, the majority of the responsibilities lies on the Cloud Service Customer (CSC) side, as the Cloud Service Provider (CSP) only manages Networking, Storage, Servers, and Virtualization. As the CSC does not have access to the underlying cloud infrastructure, it would then manage Applications, Data, Runtime Operations, Middleware, and Operation System (OS). These resources are pooled using abstraction and orchestration, based normally on Virtualization. This frees the resources from their respective physical limitations to enable pooling [14]. Typically, all these resources are tied together with the use of Application Programming Interfaces (API), which is the normal underlying communication method for these components. The majority of cloud APIs use REST (Representational State Transfer), which runs over the HTTP protocol, making it appropriate for Internet services [8]. This cloud service type is represented in the figure 2.1.

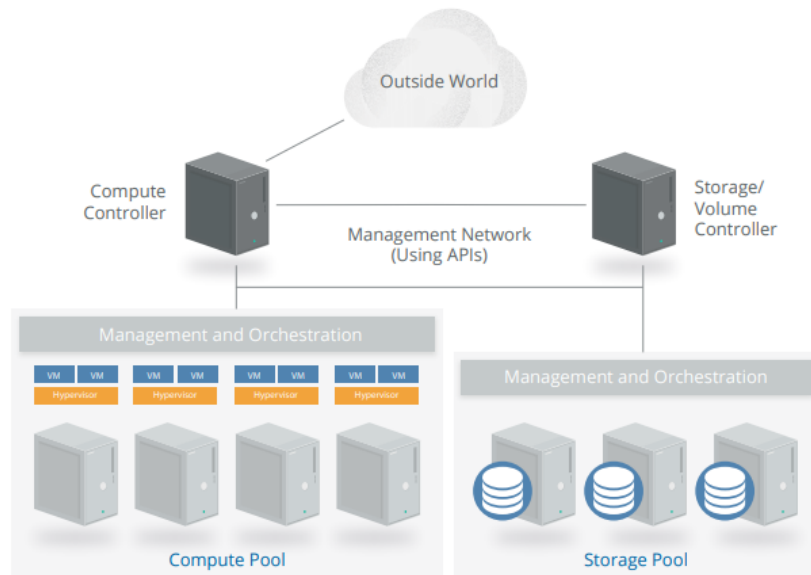


FIGURE 2.1: Infrastructure as a Service (IaaS)[8]

Within the various benefits offered by an IaaS service model, the most relevant are the following:

- Easy to automate deployment of storage, networking, servers, and processing power;
- The most flexible cloud computing service as the CSC has higher control of resources;
- Highly scalable;
- Resources can be purchased as they are needed, and costs are based on consumption.

Nevertheless, there are still some limitations and concerns that should not be overlooked, as such:

- Data security issues due to multitenant architecture;
- CSP outages make customers unable to access resources;
- Further training to IT team to make them familiar with the management of entire infrastructure.

Some major examples of IaaS cloud service platforms are DigitalOcean, Amazon Web Services (AWS), Microsoft Azure, Linode, among others.

2.1.2.2 Platform as a Service - PaaS

Platform as a Service Model (PaaS) adds an additional layer of integration with application development frameworks, middleware capabilities, and functions such as databases, messaging, and queuing [8]. This benefits developers, for example, as they are able to easily develop applications, and deploy them in a very cost-effective, and with further resource allocation flexibility [15]. The figure 2.2 is representative of the application layer support. Overall, the PaaS service model passes more responsibility over IT management from the CSC to the CSP. However, even though it is currently the less used cloud computing model, it is growing in fast rates. According to recent research, it showed that more than 25% of businesses use PaaS, and it is estimated that over 50% of existing organizations using cloud services have plans to set up a PaaS model in the future [16]. Adopting a PaaS service model brings benefits to the organizations, such as:

- Demands less skills for IT management and can catalyze the development of new applications;

- The CSP is responsible for server-side computing elements, meaning that the CSC does not need to take over installing, updating, upgrading, and maintaining computing components;
- A vast number of programming languages are usually supported by PaaS;
- Most suitable option for *Devops*, given the amount of support and high efficiency it presents to CSCs;
- The expenses involved in developing, testing and deploying apps are low when compared with other cloud-based models.

Besides the countless benefits it offers, it also presents some limitations and constraints, such as the following:

- Less flexibility when comparing to IaaS;
- The CSC has less control over managing data stored in third-party and vendor controlled servers. This can become a security problem as the CSC may not be able to apply specific security policies;
- As the CSC relies further on the CSP, this can mean that some services will be more dependent on the *modus operandis* of the CSP. This can become a problem of vendor lock-in as future migrations to other services may imply business consequences and challenging migrations.

Some examples of known PaaS services are AWS Elastic, Windows Azure, Amazon Web Services (AWS), Google App Engine, Heroku, among others [17].

2.1.2.3 Software as a Service - SaaS

Software as a Service (SaaS) is the most commonly wide used cloud service model on the market. According to Virayo, "80% of businesses use at least one SaaS application" [18]. The capability provided to the CSC by this service is the use of applications of the CSP, without managing any of the services, and the underlying cloud infrastructure. The CSP has the vast majority of responsibility and control. In contrast, the CSC has less autonomy and very limited responsibility over the cloud infrastructure. As the software applications in this case are present in the cloud and controlled by the CSP, they can be accessed via APIs and Web browsers by the end-users, which are the CSCs. The main advantages that the SaaS service model presents are the following:

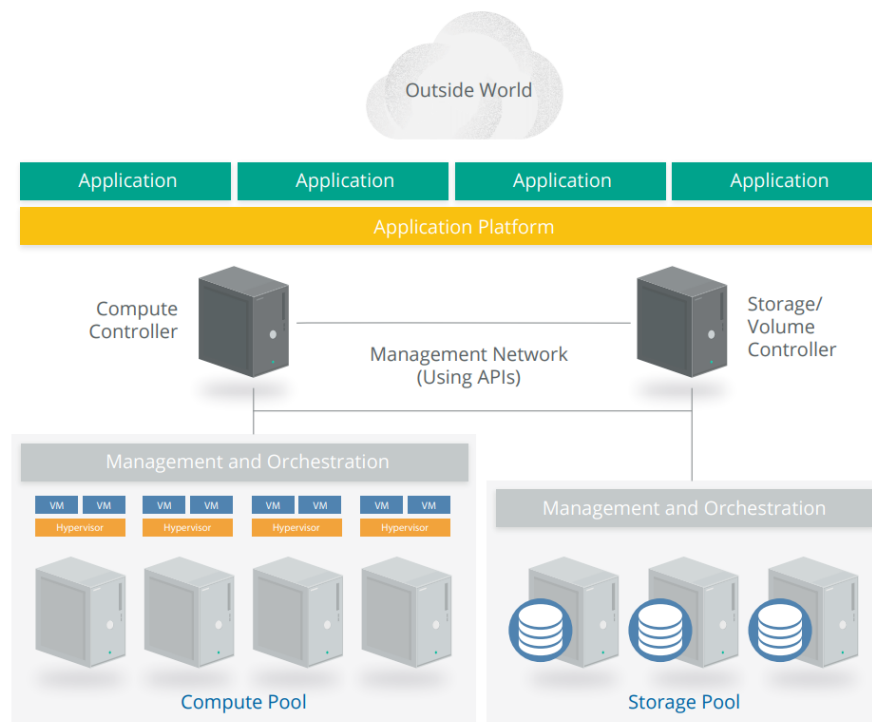


FIGURE 2.2: Platform as a Service (IaaS) [8]

- The fact that it does not involve hardware and setup costs for the CSC;
- The SaaS cloud service is easily available anywhere and anytime;
- Most scalable cloud service model;
- Usually it is pay-per-subscription model, meaning that the cost can be estimated and more resources can be added on-demand;
- More affordable when comparing to the rest of services and on-premises;
- The responsibility to guarantee service performance and availability is on the CSP, relieving the CSC from such burden.

Even though the SaaS model is the most adopted and beneficial for several organizations, it still brings disadvantages to some. The following are the most relevant:

- Users do not have any control over the hardware that manages and stores their data;
- The CSC has no access to the software that it is running on, only the CSP;
- Sometimes it is challenging to integrate existing SaaS applications with other considering the restrictive actions a CSC has;

- Higher chance of vendor lock-in has the dependence on the CSP rises.

Examples of existing, and known, SaaS cloud service models are Google Workspace, Salesforce, Dropbox, Cisco Webex, among others.

2.1.3 Cloud Computing Deployments

According to NISTs' and ISO/IECs' definition of Cloud Computing, there are currently four cloud deployment models [19][10]. Similarly to the different service model, one deployment model does not surpass the other. Instead, each model should be considered for a given scenario in which the necessary business requirements can be met. The deployment models are present below.

Public Cloud

The Public Cloud, as its name suggests, is a type of cloud deployment that supports all users and is publicly available to anyone who wants to make use of a computing resource, such as OS, Central Process Unit (CPU), storage, memory, or even software, like applications, databases, on a subscription-based payment [20]. This type of cloud deployment can be operated, managed and maintained by an organization that typically sells computer services to the public. The figure 2.3 demonstrates how this cloud deployment type interacts.

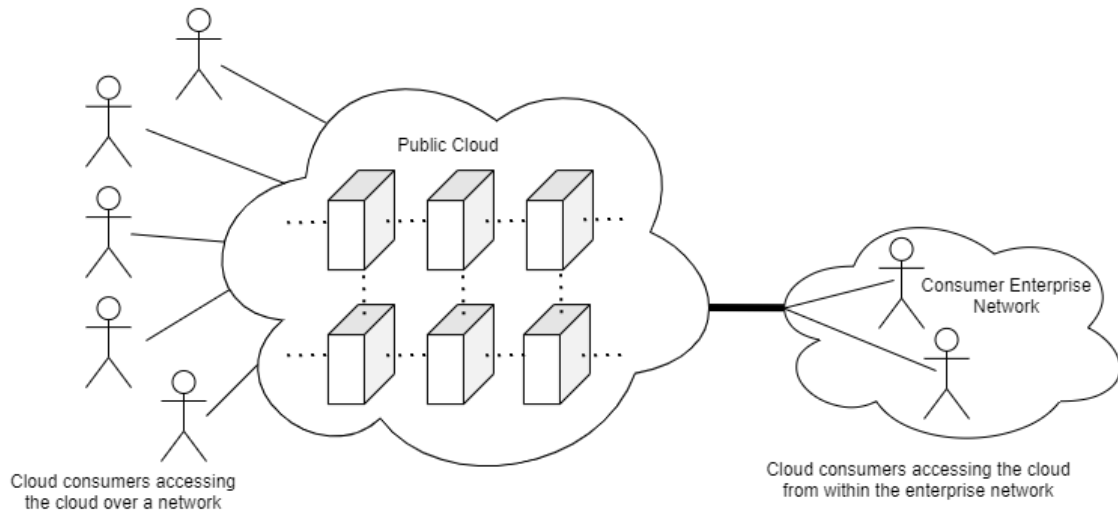


FIGURE 2.3: Public Cloud Diagram, based on [19]

Private Cloud

Unlike the previous cloud deployment model, the Private Cloud is solely managed by a

single organization. Such infrastructure can be managed internally or by an external organization, a service provider, that assures its maintenance either on-site or off-site [21]. Private clouds are expected to be more costly, as it is more expensive to acquire and maintain them. However, it provides further assurances of security and privacy to the organization. These deployment types are illustrated in the following figures 2.4a and 2.4b.

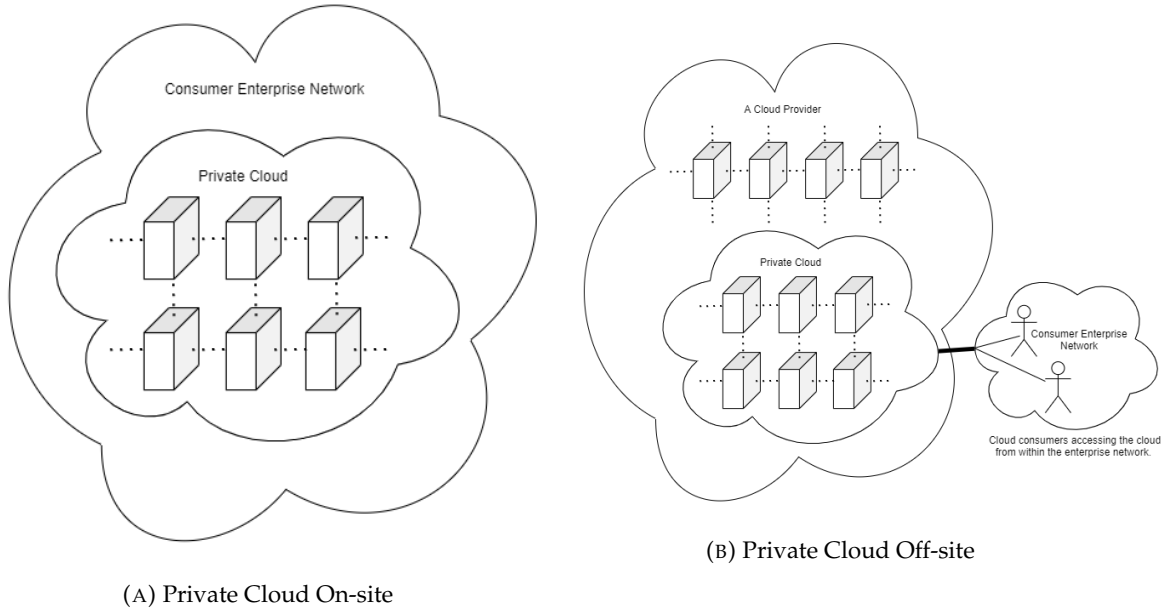


FIGURE 2.4: Private Cloud, on-site and off-site, based on [19]

Community Cloud

A Community Cloud deployment type serves a specific group of CSCs that have shared concerns, such as mission, objectives, security, privacy and compliance policy [6]. This cloud can still be managed either by an organization that implements it or a third-party, service provider, similarly to private clouds, and as such it can exist within the responsible organisation, or outside. An example where this can be applied is if two or more entities within a certain sector (government, health, utilities) need to share the computing infrastructure as they share the same goals, security and privacy requirements, and policies. This cloud deployment type is presented, for both on-site and off-site, in the following figures 2.5a and 2.5b.

Hybrid Cloud

A Hybrid Cloud can be seen as a combination of two or more clouds (public, private, community), abstracted from one another, but bound together by standardized or proprietary technology that enables data and application portability and interoperability [22].

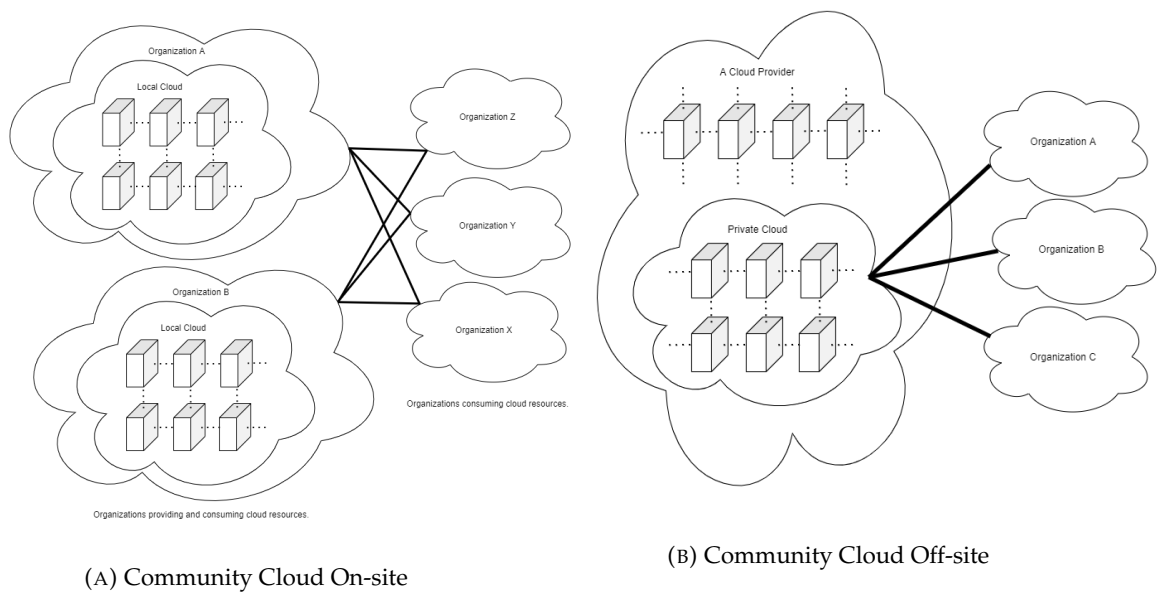


FIGURE 2.5: Community Cloud, for on-site and off-site, based on [19]

The figure 2.6 illustrates how this cloud deployment model operates.

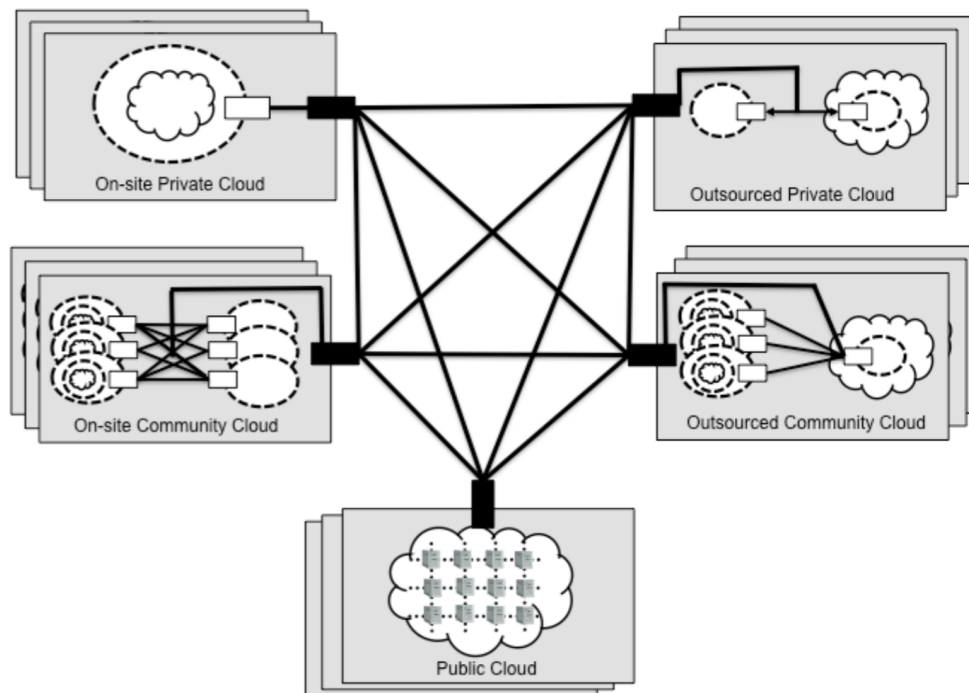


FIGURE 2.6: Hybrid Cloud Diagram [19]

2.1.4 Cloud Computing Security

This section details the landscape of cloud computing security, approaching its challenges, benefits, and the existing frameworks and standards that provide valuable insights for organizations to increase their cloud security readiness and capabilities.

2.1.4.1 Cloud Security Challenges

Cloud security is the entire bundle of technology and best practices that protect the cloud infrastructure, including underlying hardware, applications, data. As previously stated in the different Cloud Services, the security requirements and responsibilities vary from cloud service to another, as the responsibility shifts between the CSC and the CSP. Nevertheless, cloud computing has already proven to be effective against security threats that are very present and recurring in traditional computing models, such as on-premises. A recent survey from the Cloud Security Alliance (CSA) concluded that some traditional security concerns such as Denial-of-Service (DoS) attacks, shared technology vulnerabilities, and CSP data leakage, that once featured as previous threats to cloud computing security, were rated very low in regards of frequency. Thus, it means that these security incidents under the responsibility of the CSP seem to be less of a concern [23]. As SaaS cloud services are the most common nowadays, the majority of security incidents are situated higher up the technology stack, as a result of senior management decisions. The main threats to cloud security in the present, per Cloud Security Alliance (CSA), are the following:

1. Data Breaches;
2. Misconfiguration and Inadequate Change Control;
3. Lack of Cloud Security Architecture and Strategy;
4. Insufficient Identity, Credential, Access and Key Management;
5. Account Hijacking;
6. Insider Threat;
7. Insecure Interfaces and APIs;
8. Weak Control Plane;

9. Metastructure and *Applistructure* Failures;
10. Limited Cloud Usage Visibility;
11. Abuse and Nefarious Use of Cloud Services.

2.1.4.2 Cloud Security Benefits

Cloud computing presents itself as a solution to relieve the majority of the CSC from implementation and maintenance responsibilities, leading to free internal human resources for other tasks, reducing infrastructure costs, and provide further assurances of resilience and robustness. The main benefits around the security features provided by adopting cloud computing, as stated per European Union Agency for Cybersecurity (ENISA), can be found in the table 2.1 [12].

TABLE 2.1: Cloud Benefits

Benefit	Description
Benefits of Scale	In terms of financial expenses around implementing security controls, it gets cheaper to do so at a larger scale, for several security domains related to cloud security (patch management, identity and access management, hardening of virtual machines).
Resource centralization	Centralization may often bring disadvantages as it can be considered a single point of failure (SPoF), but the fact that resources are concentrated means that the defense perimeter can be reduced as well, leaving less probability of attack vectors by narrowing the attack surface. This also brings monetary benefits as it is easier to manage.
Rapid scalability of resources	The cloud computing model provides an opportunity for a CSP, or in some cases a CSC, to dynamically reallocate security resources for filtering, authentication, network traffic, encryption, amongst others. In this manner, it increases its robustness and resilience.
Patch Management	Usually, CSPs tend to be on top of any updates necessary for the resources involved in the cloud infrastructure, relaxing the CSCs in terms of responsibility of patch management and vulnerability monitoring
Market Differentiation	Nowadays organization need to provide assurances, especially for their clients, of security resilience, confidentiality, and integrity, and this is a strong driver for CSPs to improve and focus on security practices.

2.1.4.3 Cloud Security Frameworks and Standards

In resemblance with all computing infrastructures, cloud systems must be properly and proactively secured against the existing threats that are currently challenging organizations. All the potential benefits the cloud model offers can all be void if not implemented

and protected correctly, especially given the rate at which the technology is growing. As such, it is not surprising that cloud security frameworks and standards are gaining traction and being published to support organizations, both CSP and CSC, to secure their cloud infrastructure. These tools, presented in the table 2.2 can serve primarily to communicate the best security practises and countermeasures.

TABLE 2.2: Cloud Security Standards and Frameworks

Standard	Description
ISO/IEC 27017 [10]	This security standard developed for cloud service providers (CSPs) and users (CSCs) provides guidelines supporting the implementation of information security controls for cloud computing. Some of the presented guidelines are directed for cloud customers who implement the controls, and others for the cloud providers to support the implementation of those controls. The underlying framework of this standard is the ISO/IEC 27002, but the ISO/IEC 27017 adds cloud-specific security controls.
ISO/IEC 27018 [11]	This security standard is directed to cloud service providers (CSPs) who process Personally Identifiable Information (PII), as these entities are responsible for guaranteeing the necessary security controls to assure data integrity, confidentiality, and availability of this sensitive data type. It also has as an underlying framework, the ISO/IEC 27002, but the ISO/IEC 27018 includes additional requirements for CSPs.
CSA Cloud Controls Matrix (CCM) [9]	The CCM Guidelines from CSA offer cloud specific guidance towards the proper implementation of security requirements. This framework is split into 17 security domains, each with several controls.
ENISA Cloud Computing Risk Assessment [12]	This Risk Assessment documentation from ENISA specifies relevant cloud information, outlining some of the information security benefits and key security risks of cloud computing that every organization should be aware.
FedRAMP [24]	The Federal Risk and Authorization Management Program (FedRAMP) is a US government-wide program that provides a standardize approach to security assessment, authorization, and monitoring of cloud products and services, like Google Cloud Platform, Amazon Web Services, Microsoft Azure. It was created by the Joint Authorization Board (JAB) with representation from the Department of Defense (DoD) and the Department of Homeland Security (DHS).

2.2 Security in Healthcare

The Healthcare Industry is constantly evolving and, given how critical it is, there are emerging technologies to assist this area in every way possible. There is a growing necessity in efficient processes, service availability, effective coordination efforts, to further enhance the healthcare institutions' services. This industry can largely benefit from the

appearance of stable cloud technologies, as cloud can help eHealth to deliver a faster, more flexible, scalable, and cost-effective solution [25]. The cloud can support the storage, management, protection, and sharing of Electronic Health Records (EHRs), Personal Health Information (PHI), and any other relevant medical data that is paramount to be safely accessed. By achieving this level of maturity, healthcare organizations become more reliable, resilient, and efficient, as patients and healthcare personnel can access up-to-date health records and establish a trustful relationship between them.

2.2.1 Healthcare Challenges

The Healthcare sector has been dealing with an exponential rate of infrastructure and security challenges, as Healthcare Chief Information Officers (CIO) need to ensure that all critical infrastructure components and systems necessary for patient care and staff are properly functioning and performing at the optimum level [26]. Traditionally, these priorities might have seemed more manageable when the environment was hosted within the healthcare organization's own data centers, as an on-premises environment. In this way, the HCO's IT team can control network appliances, server speeds, and model of workstations as well as who uses and supports the equipment [26]. Nevertheless, this model forces responsibility of the CIOs and respective IT teams, as they need to ensure hardware refreshes, updates, upgrades, and the need to continuously hire and retain system administrators to administer the data centers, maintenance, and all kinds of system support. This can be a heavy and hinder task as all of the attack surface and service availability has to be managed internally, often focusing on managing the infrastructure alone instead of focusing on security and data privacy issues. The main concerns for a CIO and the respective IT Team when managing the security of a Healthcare Information System's infrastructure is securing the CIA triad, Confidentiality, Integrity, and Availability. Nowadays, it goes beyond just that, and organizations are forced to implement security controls related to Access Controls, Authenticity, Non-repudiation, Audit, and Data Ownership, in order to have a robust control over the attack surface.

Confidentiality

In healthcare, confidentiality plays a paramount role, as medical data is one of the most sensitive data and must be stored in a way that it remains undisclosed to unauthorized entities. Delegating data control to the Cloud may be a challenge as the number of parties that have control over the data increases, whereas having the systems on-premises

solves that problem. However, different challenges emerge, such as the difficulty of implementing access control mechanisms and strong encryption, that ultimately protect the data from being leaked or accessed by unauthorized individuals [5]. The doctor-patient relationship heavily depends of their information being protected, so achieving a high level of confidentiality is crucial. Another important factor to look out for is the existing regulatory frameworks, such as HIPAA (USA) [2] and GDPR (EU) [27], that may lead to heavy fines if healthcare organisations do not implement the necessary security and privacy controls to protect their sensitive data.

Integrity

Integrity ensures that the data present in the HIS is accurate and consistent, in a way that unauthorized parties cannot at any time modify/manipulate data. This can be hard to implement in traditional healthcare systems and requires experienced professionals to do it. Normally, cloud services provide good assurances of reliability for integrity and verification, typically resorting to cryptography in the means of hashing, and checksums, to verify if the data was modified or not. Audit trails to understand what user has modified what data. It is crucial to maintain data integrity and validity in an healthcare organization, as a simple modification on a patient's EHR records can lead to an erroneous treatment, and therefore medical consequences [28].

Availability

For a healthcare organization to operate with good conditions and guarantee the best service for its patients, it is key to assure service availability at all times, and whenever it is not possible to do so, to have a safeguard and backup plan for when it fails. It is rather frequent for traditional systems to have periods of EHR unavailability and downtime periods [29]. Usually, this happens due to human error, internet and power outages, hardware failure and cyber attacks, such as ransomwares and Denial-of-Service attacks [30]. An EHR downtime produces consequences on many levels, such as monetary costs, legal fines, and most importantly to the health of patients, as medical personnel are left blind when treating patients as their medical records are inaccessible. This is a major benefit of cloud computing, as cloud service providers manage the underlying infrastructure of the HIS, which usually are more stable than HCOs on-premises servers, possess improved physical controls to endure power outages and natural phenomena, and have well defined Disaster Recovery Plans in place to quickly recover from a downtime period [31].

2.2.2 Common Security Threats to Healthcare

The Healthcare sector is one of the most attacked sectors, and the trend has been growing. According to the HIPAA Journal between 2009 and 2020 alone, 3 705 healthcare data breaches of 500 or more records were reported to the US Department of Health and Human Service's (HHS) Office for Civil Rights, having resulted in the loss, theft, exposure, or impermissible disclosure of approximately 268 million healthcare records [32]. This trend, over recent years, is demonstrated in the following figure 2.7.

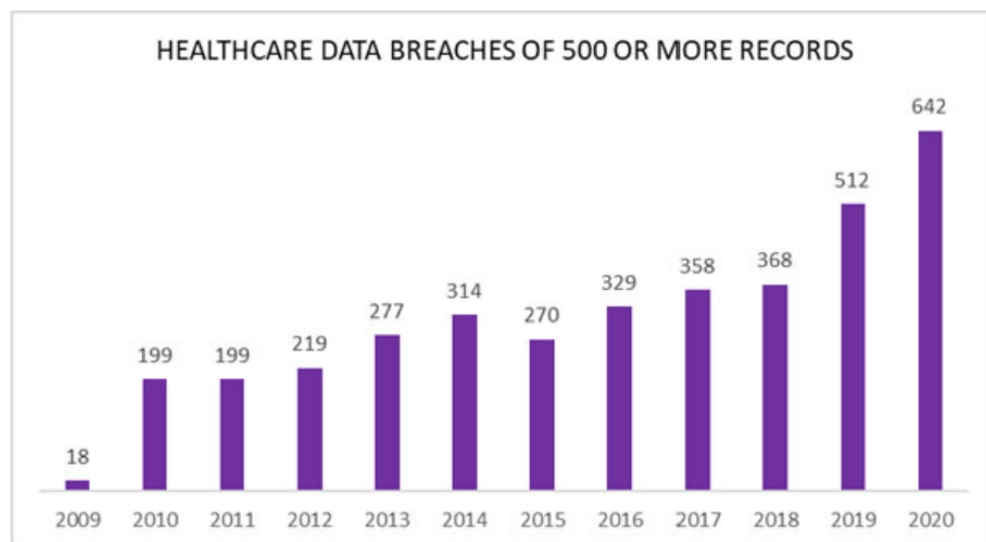


FIGURE 2.7: Data Breaches on Healthcare in the US [32]

This statistic is corroborated by others, as is the case of PurpleSec*, suggesting that 89% of healthcare organizations had patient data lost or stolen in the past two years alone [33]. This trend will continue rising, considering the value that EHR, PHI, and PII holds on the black market, and the pressure that malicious agents can make upon healthcare organizations to extort them. There are several attack vectors that can be exploited by malicious agents, the main ones being as follows in figure 2.8.

*PurpleSec is a Cyber Security company based in the United States of America.

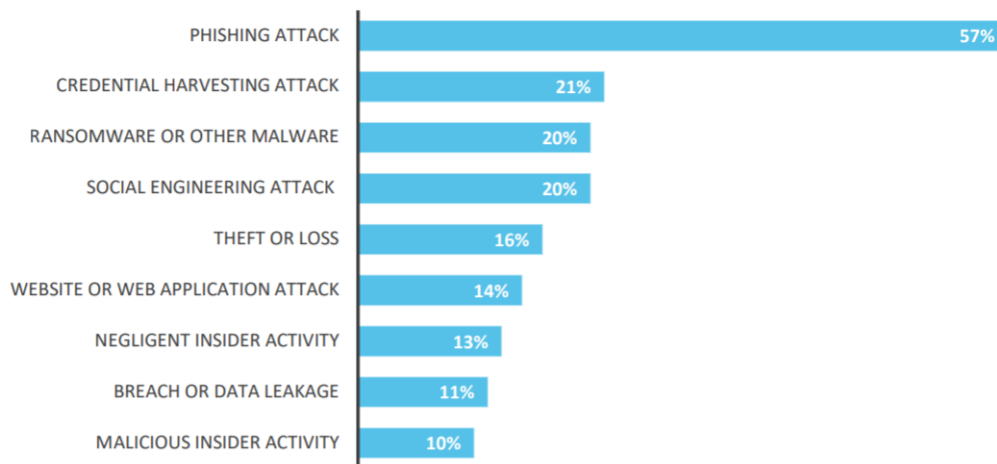


FIGURE 2.8: Attacks on Healthcare in 2020 HIMSS [34]

Besides the high volume of internal human error leading to security incidents, the actor's motives to attack this sector is primarily for financial purposes, ultimately accounting as the main attack motive for approximately 91% of the whole [35]. Up until 2019, the primary actors for security breaches were internal agents, meaning that the breaches were coming from the inside, whether for malicious intentions or basic human error, which turns out to be the most common. Nonetheless, since that year, external actors began to be the primary source of attacks to the industry. However, the sector still remains vulnerable to miscellaneous issues, derived from system errors, incompatibilities, and misshaped security controls, as the Healthcare Data Breaches Security Section from 2021's Verizon Data Breach Investigations Report (DBRI) evidences in the figure 2.9 [35].

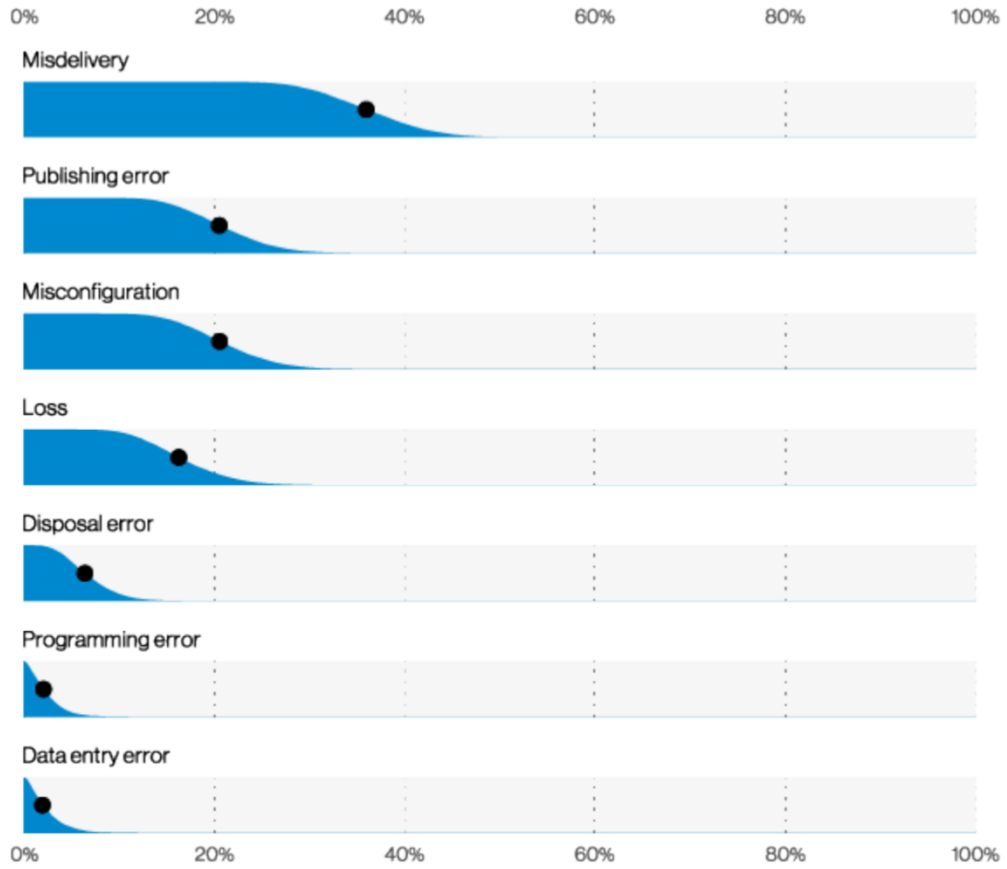


FIGURE 2.9: Verizon DBRI reports Healthcare breaches in 2021 [35]

These figures support the thesis's addressed problem of healthcare institutions showing serious struggles in adopting to new vulnerabilities and attack trends. Additionally, the numbers show that these institutions do not have the necessary security maturity to assertively tackle these issues, rendering their infrastructure vulnerable to the existing threats.

This is where the adoption of cloud computing models can contribute to a paradigm shift in HCOs. The following sections approach this subject, entering in further detail regarding potential benefits, challenges, and the existing security guidance.

2.2.3 Healthcare Cloud Systems

The Healthcare sector already has several existing cloud solutions, for each system type, at its disposal. These solutions may come as different cloud service models or cloud deployments, as it varies in terms of resources necessity [36]. The three most common deployment models for cloud Health Information Systems are Private Cloud, Public Cloud,

and Hybrid Cloud, respectively. [37]. Additionally, HCOs tend to support a Multi-cloud Infrastructure approach instead of a single cloud. This explains that the use of a single-cloud leads to further dependence of one cloud service provider. Ultimately, this can also be far more vulnerable due to service unavailability, and as such being considered a SPoF. [38]. This demonstrates that HCOs are concerned with their infrastructure security, even when deploying cloud based services. The table 2.3 offers a non-exhaustive overview of the main currently identified healthcare solutions, that can be migrated and used in a cloud environment.

TABLE 2.3: Healthcare solutions with potential use in cloud

Health Solutions	Description
Health Information System (HIS)	HIS solutions are mainly used to manage healthcare data, such as EHR and PHI, thus being one of the most critical systems in an healthcare organization. This data can be in the form of medical records, images, and even videos. Fundamentally, this system aggregates various other cloud services such as, Electronic Health Records (EHR), Picture Archiving and Communication System (PACS), Electronic Prescription Information System (EPIS), Radiology Information System (RIS), Laboratory Information System (LIS), Clinical Decision Support system (CDS), and Remote Patient Monitoring system (RPM).
Enterprise Resource Planning Systems (ERPs)	The ERP systems support the financial and inventory part of a Healthcare organization, e.g. Health Insurance Management, billing, human resource management, other non-clinical data management.
Patient Relationship Management (PRM)	A PRM system is similar to a Customer Relationship Management system (CRM), but with special focus on the healthcare sector. These systems support the management of patients, thus helping to improve patient communication, engagement, and access.
Cloud-based Network	This cloud type enables a healthcare organization to share infrastructure on an as-needed basis, allowing for increased flexibility in the case of more resources being required.
Health Data Analytics	Cloud technologies offer the ability to deploy machine learning and Artificial Intelligence (AI) services to support medical research, treatment recommendations, and patient engagement. Being a recently technology, it is still in early stages of development, but exponentially growing in terms of user confidence and usability.
Medical Devices Monitoring	These systems help medical professionals to actively and continuously monitor patient's health parameters, e.g. blood pressure, glucose measurement, electrocardiograms, in a remote way, whereas the patient can be at home and the medical professional receiving the necessary data via the system, accessible to authorized parties only.
Telemedicine Services	Telecommunication technology for remote patient assistance, enabling more efficient consultations with healthcare professionals.

2.2.4 Healthcare Cloud Benefits

As modern companies greatly benefit from this new era of transition to cloud computing infrastructures, the sector of healthcare does not remain indifferent. The main benefits for HCOs to adopt the cloud computing model [36] are presented below.

- **Data Availability:** The data would be available any time and any where to all relevant healthcare stakeholders, including physicians, clinics, hospitals, amongst others;
- **Energy and Maintenance savings:** No longer would the Healthcare organization need to support costs related to maintaining servers and data centers on-premises, resulting in less financial expenses;
- **Improved Service Quality:** By guaranteeing increased data access and portability, the interaction with patients can be greatly benefited;
- **Disaster Recovery:** The Healthcare institution has less responsibilities related to disaster recovery and business continuity, in most cases, as cloud service providers are the ones that manage the majority of the underlying infrastructure. Cloud providers usually offer redundancy in systems and services, making it less likely for service disruptions to occur;
- **Support for telemedicine:** With the COVID-19 pandemic the paradigm shifted in favor of remote sessions, and healthcare institutions readapted some of their consultations to online telemedicine sessions.

2.2.5 Healthcare Cloud Security Challenges

As much beneficial as cloud computing may present itself, it is only so when implemented properly, and with security in mind. The adoption of cloud computing in healthcare also has its limitations, such as the ones presented below [12]:

- **Lack of frameworks:** The lack of frameworks and standards for the proper implementation of generalized security, to all relevant domains, makes it hard for healthcare organizations to easily adopt this technology [36];
- **Legislation and Regulations:** Given that eHealth data (PHI, EHR) is considered as sensitive information, and subjected to various types of legal frameworks that vary

from one region to another, e.g. Health Insurance Portability and Accountability Act (HIPAA), General Data Protection Regulation (GDPR), push healthcare institutions to question whether the sharing of patient's data with third-parties could potentially pose a threat for them in terms of fines and legal consequences [36];

- **Proving Regulatory Compliance of the CSP:** It is difficult for CSCs to conduct the proper due diligence to CSP, to understand if the CSPs are compliant with their sets of policies and legal requirements. This task can be costly and most HCOs do not present the maturity to trigger such an action. As a result, this factor limits the options of CSPs collaboration. Nevertheless, there are CSPs that publicly detail that information online, or in other cases it is backed up from independent third-parties or certifications organizations [36];
- **Vendor Lock-in:** This challenge refers to the situation where the costs of switching from one CSP to another do not outweigh the benefits, and it is essentially dependant on the current CSP. This problem may derive from a number of factor, such as vendor's quality of services decline or never meets the desired threshold, the vendor changes their product offering in a way that it no longer meets the HCO's needs. This issue catalyzed the growing of the multi-cloud model, whereas a CSC collaborates with several CSP, distributing different services, thus diminishing the dependency on one [5];
- **Limited control:** Depending on the cloud service model, it may occur that the HCO has low control of the cloud infrastructure which can increase dependency on the CSP and lead to consequences related to control over data ownership [5];
- **Push for Interoperability:** The fact that the cloud leads up to a faster share of data and resources is considered as being beneficial, although it is challenging in the sense that there is a need to standardize and coordinate between different services in order to achieve that goal [36];
- **CSP Security:** The CSC needs to assess the existing security controls over data management, including data deletion and encryption, identity and access controls, privacy controls, amongst others. For this reason, it is paramount for HCOs to conduct the proper due diligence to the CSP in terms of security standards compliance, and implemented security policies and controls [36];

- **Improper Access Control:** One of the main pillars of cloud security is Identity and Access Management, as it is a shared environment. In the absence of adequate IAM security controls, the HCO may be subjected to data breaches, resulting in loss of confidentiality. It is fairly common in a hospital environment that data is shared across medical personnel and others, so it is a challenging task to implement and maintain these security requirements [7].

2.2.6 Healthcare Security Standards and Frameworks

As the Healthcare sector is such an important pillar of our societies, legislation plays a key role in defining cybersecurity requirements and data privacy protective measures. The legislation varies from region to region, having different regulatory frameworks when switching from the United States to the European Union, for example. Nevertheless, it is important to acknowledge and consult the existing legislation and frameworks, even though it may not be legally applicable, to understand what requirements should be met under certain circumstances. The following table 2.4 provides an overview of existing laws, regulations, and security standards for Healthcare.

TABLE 2.4: Healthcare laws, regulations, and security standards

Cloud Service Types	Description
Health Insurance Portability and Accountability Act Privacy Rule (HIPAA)	The HIPAA security law the USA's national standard to protect individuals' electronic personal health information that is created, received, used, or maintained by a covered entity [2].
HITRUST CSF	The HITRUST CSF, from Hitrust Alliance, is a framework that provides organizations with a comprehensive, flexible, and efficient approach to regulatory compliance and risk management [39].
General Data Protection Regulation (GDPR)	The GDPR is a European Union Regulation that imposes obligations onto organizations anywhere, so long as they target or collect data related to people in the EU. It is not directed to healthcare institutions, but it is in scope as the GDPR defines and establishes requirements for sensitive data, such as EHR, PHI, and PII [27].
HHS's Security Risk Assessment Tool	The HIPAA Security Rule requires all covered entities and its business associates to conduct a risk assessment of their healthcare organization. These HCO can do this by completing the SRA Tool, to highlights the areas where an organization's protected health information (PHI) could potentially be at risk [40].
Medical Device Directive (MDD)	MDD is a directive applicable to the European Union which objective is to harmonize the laws related to medical devices, in order for them to be placed on the market with credibility and providing security assurances to healthcare organizations [41].
Medical Device Regulation (MDR)	This regulation is bounded with the MDD, but far more detailed and extensive, thus providing more detailed information regarding the requirements for medical devices [42].

2.3 Review of Cloud Security Maturity models for Healthcare

The present section refers to the existing cloud security maturity models that can aid an healthcare organization with cloud infrastructure to evaluate its security and help fill the gaps in terms implementing directed security controls [43].

Cloud Security Capability Maturity Model

The CSCMM maturity framework consists of twelve security domains and four levels of maturity. Each security domain contains a set of cybersecurity practices, and the practices are achievement objectives specific for each cloud security domain [43]. This framework can be tailored for different cloud services (e.g. IPSaaS), as well as cloud deployments (e.g. public, private, hybrid). Additionally, it also provides the user with

valuable information as to implement and enhance an organization's cybersecurity capabilities on cloud systems [44].

NHS National Infrastructure Maturity Model

This framework was developed by the National Healthcare Service of England and has the objective of measuring how well are the secondary care providers, or healthcare organizations, in England making use of digital technology, with the ultimate goal of achieving a more efficient and paper-free system. The model measures maturity in terms of readiness, capabilities and infrastructure [45]. It is not targeted for security, even less to cloud security, but it provides valuable information for an HCO to improve itself [46].

Health Information Network Capability Maturity Model

The Health Information Network (HIN) Capability Maturity Model is a tool made by Canada Health InfoWay, that has the objective of assessing and formulate plans for the improvement of a Healthcare organization's operational capability. It comprises of 10 capability domains and 5 maturity levels for each. Nevertheless, this tool was made to increase the maturity of an healthcare organization's processes in order to become further autonomous, efficient, and develop a road-map for progression towards an increased maturity. Considering this, it does not approach cloud security and the necessary requirements to become more mature and increase its resilience [47].

Chapter 3

Development of the Healthcare Cloud Security Maturity Assessment Framework

The chapter that follows details the development of the Healthcare Cloud Security Maturity Assessment Framework (HCSMAF), implemented with the objective of providing an overarching evaluation over the defined cloud security domains. Its ultimate goal was to create the bridge between cloud security and healthcare infrastructure, thus filling the existing gap, mentioned in the previous chapter, which healthcare organizations face when assessing the security of their cloud infrastructure. The developed framework is the product of the extensive investigation of the state of the art. This tool was mainly developed for the top-management professionals, or any other similar roles, such as Chief-Information Officers, Information Security Managers, Chief Technology Officers with security knowledge over the cloud infrastructure. The final result shall then detail the performance of the submitted inputs, thus evaluating the overall security using a personalized Capability Maturity Model, explained in its respective section.

3.1 Framework's Functional Requirements

The Healthcare Cloud Security Maturity Assessment Framework makes use of questions, driven and sustained by security controls, with the objective of providing insights on the cloud security maturity level of the HCO. In this way, an opportunity is provided to acknowledge the security state of the cloud, and other relevant processes that accompany

it, in a fully autonomous way. To do this, it was necessary to establish and implement a set of functional requirements, to support its functional logic. These requirements are detailed below, in the figure 3.1.

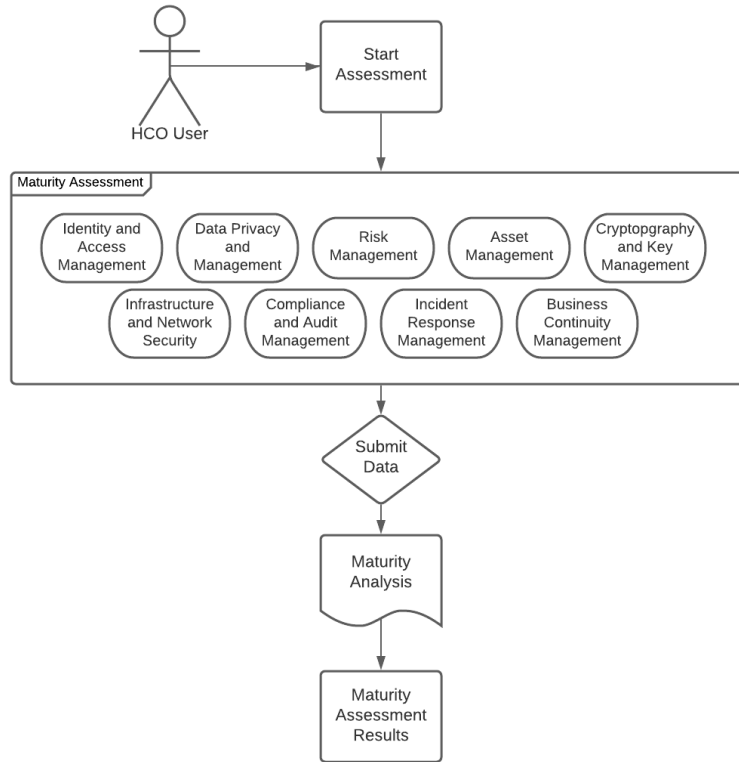


FIGURE 3.1: HCSMAF Flux Diagram

3.2 Framework's Security Assessment

The security domains addressed in the framework were established with the objective of serving two main purposes, provide real-world security controls tailored for healthcare organizations with cloud infrastructure, or prospecting to migrate to cloud, and to be user intuitive, thus being able to easily captivate the user and at the same time produce insightful results. A complete and unique standard for cloud security does not yet exist for the healthcare sector, as it is rather recent and constantly evolving [48]. Hence the need to perform a systematic review of the current standards with credibility in the security sector, and extract the security controls that could be merged in order to fill the mentioned gap between cloud security and healthcare. Henceforth, a deep analysis was performed, by

identifying the security domains and cloud-centric security controls that could be cross-referenced to find a balanced solution to the Healthcare sector. This extensive work was performed while utilizing several standards of security, that are contemplated in the resulting matrix, represented in the figure 3.2.

Domains	ISO/IEC 27017	ISO/IEC 27018	CSA CCM	ENISA	FedRAMP	NIST CSF	HITRUST CSF	GDPR	HIPAA/HITECH
Identity and Access Management	X	X	X	X	X	X	X		X
Data Privacy and Management (Portability & Interoperability)	X	X	X	X	X	X	X	X	X
Risk Management and DPIA	X	X	X	X	X	X	X	X	X
Asset Management	X	X	X	X		X	X		X
Cryptography and Key Management	X	X	X	X	X	X	X		X
Infrastructure and Network Security (Virtualization Security)	X	X	X	X	X	X	X		X
Compliance and Audit Management	X	X	X	X	X	X	X	X	X
Incident Response Management	X	X	X	X	X	X	X		X
Business Continuity Management	X	X	X	X	X	X	X		X

Legend: Cloud-compatible security controls General security controls w/ no cloud focus

FIGURE 3.2: HCSMAF Security Domains mapping with utilized security standards

The rationale behind the tool's domain selection was the fact that these domains are easily mappable between the standards, as seen in the figure 3.2. Nevertheless, only some of these standards have cloud-centric security controls that map, or can present themselves as compatible, to mitigate healthcare security challenges.

Each defined domain of the framework has sub-domains/sections, that specify the maturity questions for the overall assessment. These sections are specified in the following figure 3.3.

3.2.1 Identity and Access Management

The Identity and Access Management security domain aims to define the security controls that can be implemented to further enhance the security of cloud system in terms of identity management. This takes into consideration the identity lifecycle, starting from User/Account creation, account privileges management, readjustment, revocation, and deregistration. This domain also includes controls for securing a system with regards to

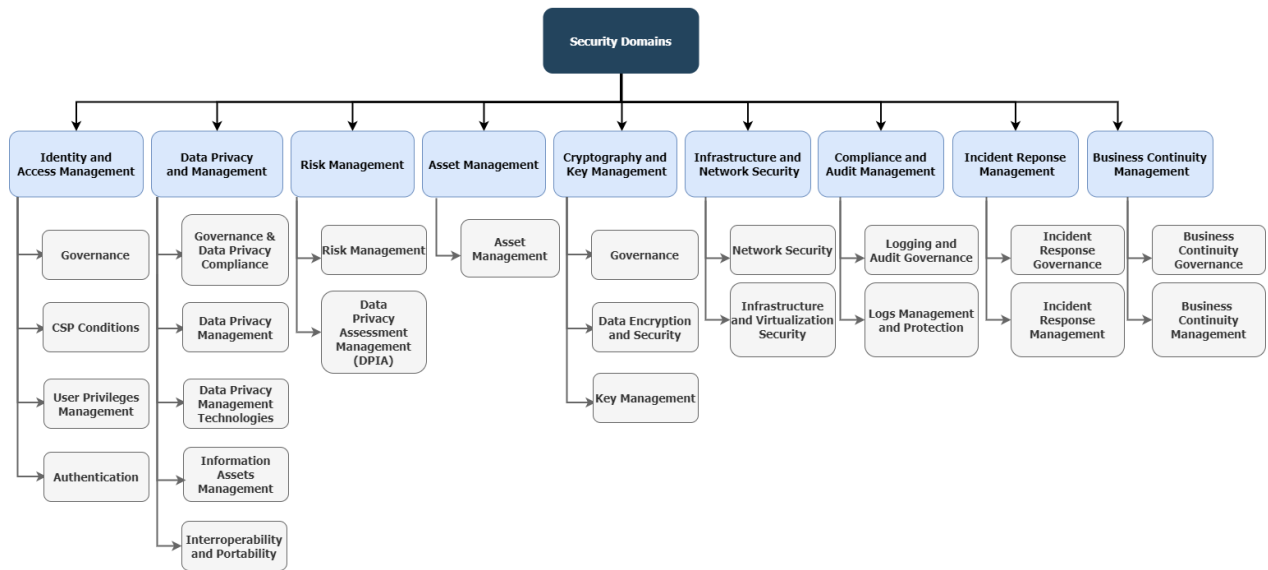


FIGURE 3.3: HCSMAF Security Domains and Sub-Domains/Sections

access control, increasing the reliability of a cloud system in terms of authentication, authorization, non-repudiation, and confidentiality. This is a crucial part of cloud security, and as such, the CSPs have to ensure that data and applications stored in the cloud are protected with strong authentication mechanisms [49]. Furthermore, users need to verify that their credentials for authentication are secure, and can usually follow existing guidelines from the HCO defining how passwords should be created to have a higher degree of security.

This domain provides maturity questions focusing on four (4) different sections in the IAM security domain, as presented below.

- **Governance:** This section provides queries around the establishment, and maintenance, of IAM policies, processes, and procedures, to understand if the HCO has this documents formalized, showing better organization and strategy, or if it has an ad-hoc approach to IAM management;
- **Cloud Service Provider Conditions:** This section highlights the CSPs minimum functions that has to provide to the HCO in order to effectively manage the IAM system in place. Aligned with the ISO/IEC 27017:2015 [10], the CSP must guarantee mechanisms for user registration, deregistration, and access privilege rights management, authentication, and authorization. Furthermore, the HCO must also perform the necessary due diligence to the CSP to understand if these requirements can be met, prior to signing with the CSP;

- **User Privileges Management:** This section approaches how the HCO manages user accounts with system access in regards to account privileges. The maturity questions were designed in a way to understand if good practices engineering principles are met, such as the Segregation of Duties (SoD), Least privilege (PoLP), Need-to-Know, and Event-by-Event [50] [51]. Moreover, it aims to understand what access control model is used in the cloud, such as the Role-Based Access Control [52], or Attribute-Based Access Control (ABAC) [53];
- **Authentication:** The final section on this domain is the authentication section, and it queries the user about what types of authentication mechanisms are used in the cloud systems, such as Security Assertion Markup Language (SAML), Lightweight Directory Access Protocol (LDAP), OAuth, and the use of multi-factor authentication, Identity Providers, to further enhance authentication and authorization security.

3.2.2 Data Privacy and Management

The correct management over data and data privacy is one of the most critical pillars of the security of an healthcare organization, mainly because of the sensitivity of the data that it stores, and processes every day. As per GDPR [27], healthcare data, such as PHI, EHR, are considered to be critical, and therefore, require increased protection. This domain is a challenge particularly for cloud security, as the data is stored and processed by third parties, like CSPs, which leads to several safeguards in regards to how that data is treated and protected [54]. The framework addresses these topics by defining questions that help understand the maturity of an HCO concerning five main areas. These areas are aligned with standards defining relevant healthcare data security controls, such as HITRUST CSF [39], HIPAA [2], GDPR [27]. Additionally, performing a crossover with a set of security controls directed at cloud computing systems, that would help meet the desired security level for a cloud infrastructure. The standards and frameworks that supported this were mainly the CSA CCM guidance [9], ISO/IEC 27018:2019 [11], specially designed for the protection of PII data in public clouds acting as PII processors, the ISO/IEC 27701:2019 [55], addressing privacy information management, and ENISA's cloud security for healthcare services [36].

The Data Privacy and Management security domain of the HCSMAF is segregated into five (5) different sections, presented below.

- **Governance and Data Privacy Compliance:** This section questions the user regarding the governance structure in place, with defined policies, processes, procedures, for data management and privacy. Thus, it defines security requirements for statutory compliance of data protection defined by the respective region regulations and laws [55];
- **Data Privacy Management:** This section queries the user to understand how the HCO manages third party relations with organizations that process and store medical data. When third parties are involved, HCOs should perform the proper due diligence and adhere to data privacy best practices. This is performed by establishing Business Associate Agreements (BAA) with data processors, identifying them, and promoting internal roles, such as Data Protection Officer (DPO), to handle data privacy both internally and externally [56];
- **Data Privacy Management Technologies:** This section aims to collect information regarding what technologies are being used by the HCO to provide further guarantees of security, such as, eDiscover mechanisms for electronic information, Data Loss Prevention (DLP) tools, and the use of Cloud Access Security Brokers (CASB) to enforce policies between the HCO and data processors [8];
- **Information Assets Management:** This section highlights how the HCO manages its information assets lifecycle, thus approaching important controls related to data creation, classification, retention periods, deletion, and CSP data management capabilities [57];
- **Interoperability and Portability:** These two concepts are paramount, specially in cloud computing environments, as they enable the HCO to have its data/applications standardized and completely portable from one CSP to another, or even when migrating to on-premises servers. It ensures consistency, hence reducing complexity issues when migrating applications or processing data. There are existing protocols that ensure these capabilities, such as the Open Virtualization Format (OVF), which is an open packaging and distribution format that details how virtual appliances should be deployed, managed and run on a virtual machines (VMs) [58].

3.2.3 Risk Management

This security domain is important for the HCO to gain overall knowledge and be conscious of what risks can affect the organization. Risk Assessments should be performed with the aim of understanding what risks can materialize, thus deciding whether to accept, mitigate, avoid, or transfer them, following ISO/IEC 27005 guidelines [59]. The entirety of the attack surface should be scrutinized, and a Risk Register should be kept, and maintained, to correctly manage risk. This domain also approaches the need of performing Data Protection Impact Assessments (DPIA), to help the HCO identify and minimise risks relating to personal data processing activities [60]. This is paramount to perform, given the reasons previously stated regarding the higher security necessity for PHI and EHR data protection.

3.2.4 Asset Management

The Asset Management domain addresses security controls that should be in place for management of assets belonging to the HCO. These assets can be both a part of the infrastructure, such as Virtual Machines (VMs), applications, used in cloud environments, as external assets that belong to the HCO, such as mobile assets (e.g. mobiles, laptops, medical devices) and infrastructure assets (e.g. routers, servers, switches). The better the asset management, the better is the HCO's knowledge around possible entry points for attacks and unauthorized accesses [57].

3.2.5 Cryptography and Key Management

The use of cryptography mechanisms is key to ensure strong protection to data at rest or in transit, to mitigate attacks like man-in-the-middle and data leakage [61]. This is one of the most challenging situations to manage, as it has a higher complexity of implementation bound to it. Cryptographic mechanisms aim to achieve confidentiality, non-repudiation, data integrity, and it must be implemented on both the HCO's and the CSP's side. One challenge that many CSCs face is that few CSPs share the encryption keys, leaving almost, or if not full, control to the CSP [36]. The encryption keys management is just as important as the encryption that it enables, as one cannot exist without the other. The domain approaches these questions in the following manner, presented below.

- **Governance:** Similarly to other domains, it questions the existing governance over management of cryptography and keys, such as formalized policies, procedures, processes, defining security requirements, including CSP due diligence over cryptographic capabilities [10];
- **Data Encryption and Security:** This section makes queries to understand if there are mechanisms in place to ensure data at rest and in transit encryption, both in the CSP side and client side. It is crucial to secure all endpoints, and for all communications to be encrypted, using Hypertext Transfer Protocol Secure (HTTPS), Secure File Transfer Protocol (SFTP), if FTP is used, among others;
- **Key Management:** The final section aims to determine if the HCO has security controls in place for the correct and secure management of cryptographic keys, whether for encryption/decryption, digital signatures, among others. Is it important to have a defined key management lifecycle with the objective of formalizing the security requirements to comply with. In each stage of the keys lifespan, from the creation to its destruction [62]. Further maturity can be obtained, when all these processes are in place and with periodical reviews, as well as using technologies such as Hardware Security Modules (HSM) [63]. An HSM can be both physical as well as cloud-based, and it ensures further security in this security domain, preferably when reaching for FIPS 140-3 compliant [64].

3.2.6 Infrastructure and Network Security

This security domain features questions around network security, querying on what network level security mechanisms are implemented and how are they managed. Additionally, a set of security controls for the cloud infrastructure are in place, addressing the security of the cloud-typical Virtualization Components. There needs to exist a coordinated effort between the HCO and the CSPs to understand the responsibilities of each party when it comes to managing the infrastructure and network.

The section separation is as follows.

- **Network Security:** This section addresses the overall governance around network security with the CSP, as well as what technologies are currently in place to act as defense mechanisms in this layer, e.g. Intrusion Detection/Prevention Systems (IDS/IPS), Cloud-Access Security Broker (CASB), Web Application Firewalls (WAF),

Security Information and Event Management systems (SIEM), Threat Intelligence tools [36];

- **Infrastructure and Virtualization Security:** This section lays out the parameters to understand the HCO's maturity in terms of cloud multi-tenancy, Virtual Machines (VM) isolation, and hypervisor security. This is a crucial pillar of cloud computing technology and should not be taken lightly, as the improper segregation and VM isolation between tenants can lead to serious security concerns [8].

3.2.7 Compliance and Audit Management

This domain aims to understand how the HCO, alongside the respective CSPs, performs in regards to logging management activities. A greater maturity is awarded when the HCO has controls in place to ensure well defined event logs, with defined responsibilities with the CSPs through the use of Service Level Agreements (SLA), such as log retention periods and deletion. It is important to implement audit trails mechanisms to control access to EHR records, PHI, and PII information present in the cloud [36]. The CSPs should provide log reports, at the HCO's request, specially with information on privilege operations logging activities.

3.2.8 Incident Response Management

This domain focuses on the governance and management of Incident Responses. It is important for HCOs to establish and maintain policies, procedures, processes, and plans for incident response, thus defining the security safeguards in each phase of the Incident Management Lifecycle. A possible example of Incident Response (IR) Lifecycle is Preparation, Detection, Analysis, Containment, Eradication, Recovery Post-Mortem/Post-Incident, and Lessons Learned [65]. The responsibilities of each party should be contractually defined in case of disruptive incidents, hence establishing proper coordination with the CSPs.

3.2.9 Business Continuity Management

The Business Continuity domain delivers important security controls, as it is the last barrier of defense to cause further disruption to a healthcare institution, in this context. The

maturity questions are laid out to acknowledge if the HCO has a defined Business Continuity Management System (BCMS), and how it is established. As per ISO/IEC 22301 [66], the five key phases of a BCMS lifecycle are defined as follows [67].

1. **Business Impact Analysis (BIA):** The BIA has the objective of reviewing existing business processes and identifying which of them are critical and non-critical. This decision takes into consideration specific criteria, previously defined, such as patients and employees' welfare, loss of revenue, legal fines, and HCO's reputation. As per ISO/TS 22317:2015, the ISO Guidelines for BIAs [68], the parameters like Recover Time Objective (RTO), Recovery Point Objective (RPO), and Maximum Tolerable Period of Disruption (MTPD) should be defined to properly understand what are the most critical processes;
2. **Risk Assessment:** As mentioned in the Risk Management domain, the HCO should identify the existing risks that can potentially cause service disruptions and harm the HCO at several levels;
3. **Solution Design:** In this context, the solution passes through the establishment and design of Disaster Recovery Plans (DRP), detailing the HCO's and CSP's strategies in certain disruptive incident scenarios. These DRPs involve arranging secondary sites, data/applications backups to restore critical business processes, and others;
4. **Implementation:** After the plans are made, the HCO must implement a Business Continuity Plan, providing an overall structure of the strategies that the HCO must take when certain disruptive disaster can potentially happen, or is currently happening. This Plan has the objective of identifying the roles and responsibilities of the organization, such as the structure of Crisis Management teams;
5. **Plans Testing:** The designed DRPs should be tested to understand if the HCO, alongside the CSP, is able to meet the RTO expectations and recover from a disruptive incident in time, thus mitigating the chances of severe disaster;
6. **Maintenance:** Both the BCP and the DRPs should be periodically reviewed, to guarantee that are constantly up-to-date with the critical processes of the HCO.

3.3 Capability Maturity Model and Metrics

A Capability Maturity Model was made with the objective of defining the different levels of cloud security maturity that a HCO can achieve. The maturity model is in line with the Capability Maturity Model Integration (CMMI) typically used for Maturity Assessments. It has the objective of assessing the quality of software and to help organizations improve the maturity of their software processes by evolving from ad hoc, chaotic processes to mature, disciplined software processes [69]. One needs to have a holistic top-down perspective to produce a security model that allows us to make an assessment of the overall security level of the entity requiring protection [69]. Nevertheless, the HCSMAF's maturity model was adapted for the scope of this tool, which are the healthcare organizations. As such, the maturity model presented for this framework is the following, presented in the figure 3.4.

The defined maturity levels from the utilized model, as presented in the figure 3.4 are the following:

- **Level 1 - Initial:** Mainly considers that the HCO has an Ad-Hoc approach to security, with little or no development regarding cloud infrastructure, and low-level of security awareness and communication;
- **Level 2 - Managed:** Describes an HCO that has some policies, procedures, or processes defined, with minimum critical security requirements implemented, with some of its services hosted in a cloud environment, but lacks performance when it comes to risk management, CSP due diligence, internal communication, and minimum Data Privacy controls for PHIs, PII, and EHRs;
- **Level 3 - Quantitatively Managed:** Considers that the HCO already has established policies, procedures, processes, that are periodically reviewed, and approach the main cloud security domains, with robust access controls and privilege management, solid data privacy security controls, such as strong encryption, information classification categories, data backups, data management and deletion;
- **Level 4 - Optimizing:** This is the maximum level of the maturity model, as it considers that the HCO has a major part of its infrastructure present in the cloud, it is continuously improving its cloud security. By achieving this mature level, it demonstrates exemplary governance, a solid control over data management, data

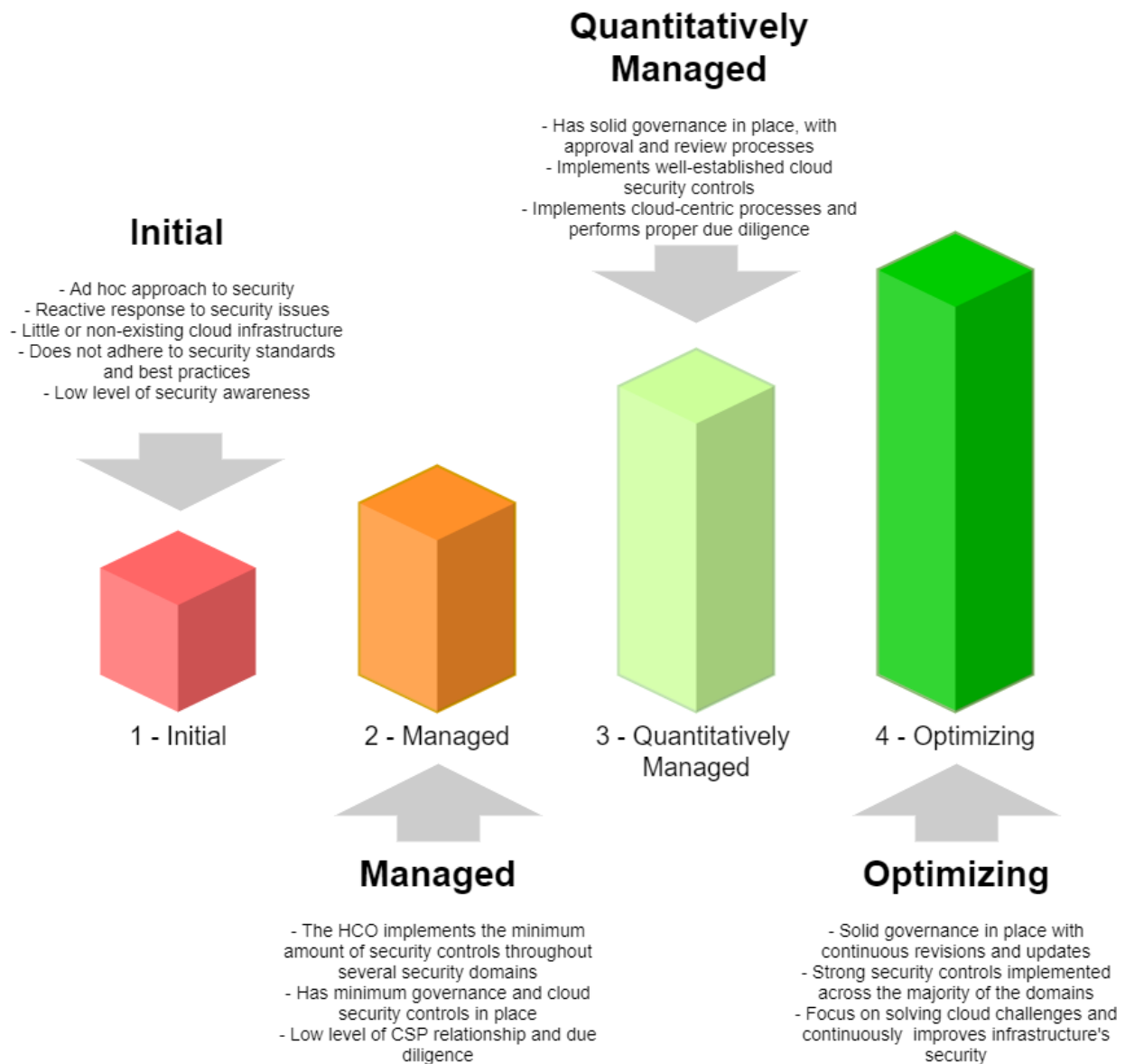


FIGURE 3.4: HCSMAF Maturity Model

privacy regulations, use of encryption, access control, business continuity, risk and CSP management.

Each of the defined security domains provides a maturity value to the overall equation of the final maturity output of the HCSMAF. Each of the respective questions, for each domain, have a linked maturity value, which is the "*weight*" parameter. This parameter can vary from one to four, aligned with the defined Capability Maturity values, being one the lowest, and four the highest. Typically, the questions that address security controls with higher complexity of implementation, offering higher security, and directed to cloud computing systems [9], are the ones that provide increased maturity to the final assessment's

result. The more the HCO adopts security measures to mitigate the main challenges of cloud security and healthcare, such as vendor lock-in, data privacy, access control, network and virtualization vulnerabilities, CSPs dependency, weak encryption mechanisms, service disruptions, the highest the overall maturity performance is. However, there are existing maturity questions that address common security controls, in which the implementation's complexity isn't high and still provides enhanced security, e.g. well defined information assets, identity and access management (IAM), and cryptographic lifecycles, as well as business agreements and well defined SLAs with CSPs.

After the assessment is performed, the maturity for each domain is calculated, to provide a clear and segregated view on the maturity performance. The formula for this calculation is presented below.

$$r = \frac{x_d}{X_d} \quad \forall d \in D$$

Where d represents a domain of the assessment, x_d defines the sum of the awarded maturity values in function of the submitted answers for the specific domain, and X_d represents the maximum maturity sum possible for the specific domain. In essence, the resulting value r is then normalized to a percentage value, in which the Level 1 corresponds to [0-25%[, Level 2 to [25-50%[, Level 3 to [50-75%[and Level 4 to [75-100%].

$$m = \frac{\sum_{d \in D} d}{|D|}$$

Finally, the overall result of the maturity assessment m corresponds to the sum of each security domain's maturity result divided by the total number of domains. This result follows the logic mentioned previously, and the result will be one of the four levels of maturity.

3.4 HCSMAF Technical Implementation

The HCSMAF tool was designed with the intent of aiding HCOs in a user-friendly approach, with simple usability, with cloud and healthcare centric security controls. To really cause a positive impact to HCOs organizations, the tool needed to be created and implemented as an application. The following section details the technical components of the tool, as well as the benefits that they offer.

Computing Model

The HCSMAF uses a centralized computing model, serving a client-server communication, sending data through an HTTP channel. The application is deployed in a cloud environment, Google Cloud Platform (GCP), on a Virtual Machine [70]. The reasons behind the choice of using GCP is the balance between affordable long-term pricing, security, and easy access control, as it enables to use Secure Shell (SSH) keys to quickly access Virtual Machines (VM) and deploy updated code, and backup redundancy [71].

Server-Side Implementation

The Server-Side of the web application was implemented with the use of *Python*, *Flask*, and *SQLAlchemy*. The choice of using *Python* programming language for the tool is supported by the fact that it is easy to deploy, very scalable, wide range of libraries, and enables the use of versatile Web Frameworks, like *Flask*. *Flask* is a Python-based web framework with little to no dependencies on external libraries [72]. It has two main components, which are key for the tool, which are *Jinja2* and *Werkzeug*. The first is a fast, expressive, extensible templating engine, and it ensures very few code replication, setting up base templates for the HTML files, without the necessary of duplicate code for separate web pages. The second, and most important purpose, is to render templates with data from the server, to the client. This means that the server creates operations to specific web pages, routed through the use of *Werkzeug*, enabling to process and manipulate data in the client side [73]. This communication is performed through the use of a *Web Server Gateway Interface* (WSGI), which has the role of serving as an interface to enable interactions between a Web server and a Web framework [74].

The technologies mentioned so far only serve the purpose of client to server communication, whereas the server-database communication is performed with the assistance of another component, the *SQLAlchemy*. *Flask* has this component built-in, and it uses an object-relational mapper (ORM), a programming technique for converting data between relational databases and object oriented programming [75]. This technology supports a wide range of database systems, e.g. SQLite3, MySQL, PostgreSQL, Oracle, Microsoft SQL Server [76], but the webApp uses SQLite, given its flexibility, simplicity, and reliability. The Database is composed with one main table, the primary key being a *questionnaireId* (Pk), that represents a unique identifier for an account's maturity assessment. The questionnaire table has only one attribute as a JSON object type, that contains all of the information of the questionnaire, including questions, answers and maturity weights. The decision around the use of a JSON object is the easiness in object manipulation, data

consistency, and smooth integration with *Jinja2*.

A representation of the database's relational model is demonstrated in the figure 3.5, along with attributes of the assessment's JSON object.

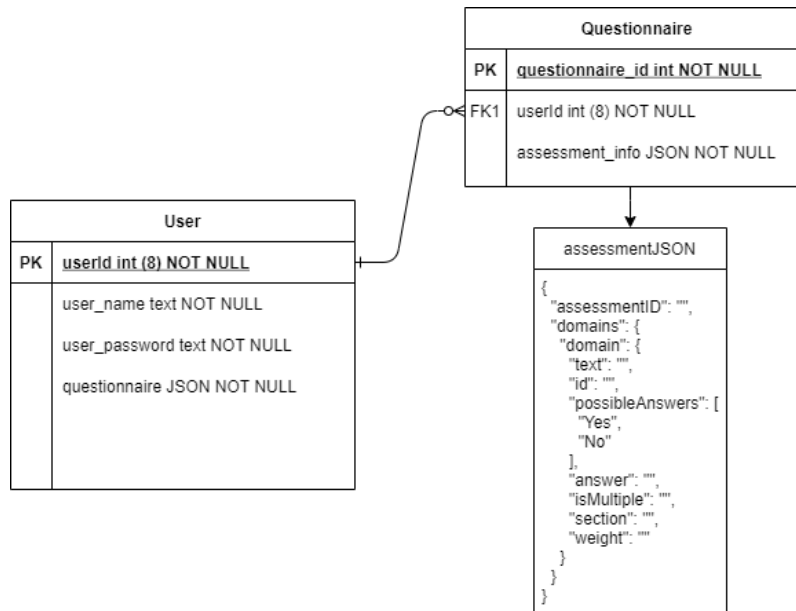


FIGURE 3.5: Database's relational model

Client-Side Implementation

The Client side of the web application was developed using *HTML* and *CSS*, as well as the use of *Jinja2*, as mentioned before. This technology plays a key role in the client-side as it renders the *HTML* templates whenever there is a routing action from the server-side, and enables effortless data manipulation, thus allowing for the *HTML* elements to be dynamically defined, promoting scalability. It also benefits with regards to security as it has a well defined automatic *HTML* escaping mechanism, that mitigates the likelihood of Cross-Site Scripting (XSS) vulnerabilities [77]. A representation of the developed client-server model, and the overall architecture of the HCSMAF tool, is demonstrated in the figure 3.6.

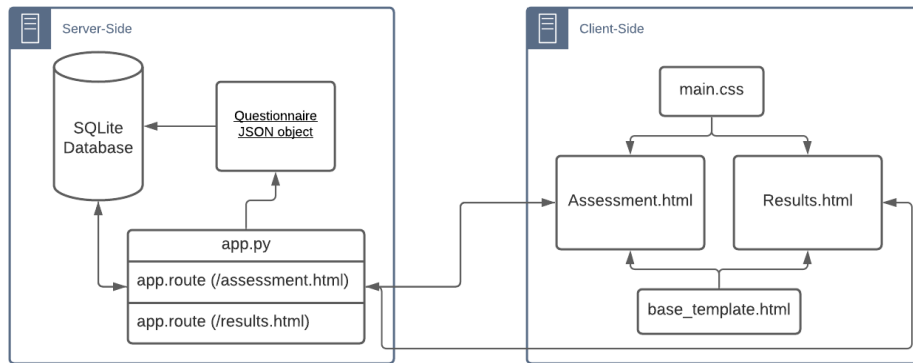


FIGURE 3.6: Client to Server Components Diagram

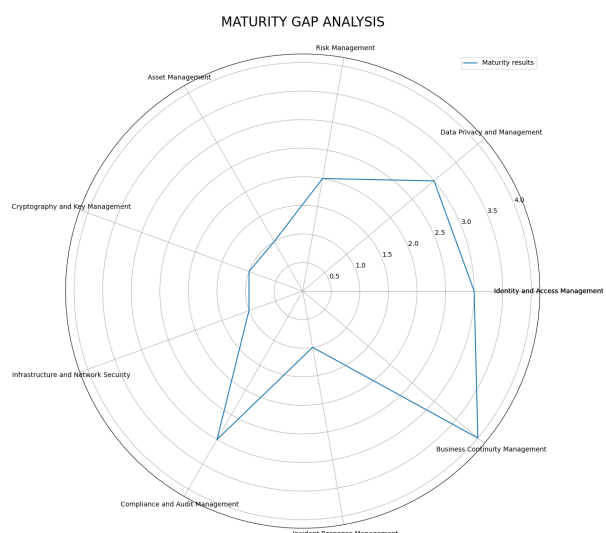
3.5 Results Representation

In the wake of undertaking the assessment, and submitting the inputs, the User may consult the final results, in the "Results" web page. The assessment results are displayed in two ways, in a table laying out the result for each security domain, as well as the overall result, and a GAP analysis graphic for easy reporting.

The figure 3.7a demonstrates the final results table display, segregating between security domains, as well as providing the overall maturity, and the figure 3.7b displays an example of a GAP Analysis radar graphic, with the maturity output for each domain.

Security Domain	Domain Maturity
Identity and Access Management	3
Data Privacy and Management	4
Risk Management	2
Asset Management	1
Cryptography and Key Management	1
Infrastructure and Network Security	1
Compliance and Audit Management	3
Incident Response Management	1
Business Continuity Management	4
Overall Result	2
HCO's Cloud Maturity	Managed

(A) Example of final maturity overview table



(B) Example of final maturity results GAP Analysis

FIGURE 3.7: Example of final maturity outputs in the Results web page

In this example, the maturity assessment resulted in the level 2 - Managed, with the domains of Data Privacy and Management and Business Continuity Management (BCMS) scoring the Level 4 - Optimizing maturity level.

The intent of the Results page was to provide a clean and simple overview of the assessment's results to the user. The HCO's Cloud Maturity result aligns with the Maturity Model in place, Initial, Managed, Quantitatively Managed, Optimizing.

Chapter 4

HCSMAF Evaluation Results

The following chapter details the results' output from the evaluation phase of the HCS-MAF. The objective of this phase was to validate the work and investigation performed to reach the final version of the tool, thus understanding its applicability, usability, and if it is recognized to be a maturity tool that narrows the existing gap between cloud security and healthcare.

4.1 HCSMAF Evaluation Planning

This section establishes the criteria and planning for the tool's evaluation. To establish reliable and credible results, stakeholders were identified, to be interviewed, with the objective of evaluating the tool. The developed tool has a scope limited to a certain type of stakeholder, mainly regarding the characteristics related to professional experience, academia, and organization roles. As a result, the following criteria was defined for the stakeholders selection and complied with. Thus, the stakeholders must:

- have an active role in the HCO's top management of the Information Technologies Department, as in Chief Information Officers (CIO), Chief Technology Officer (CTO), Lead Engineer, or any other similar role;
- have knowledge over the HCO's infrastructure management processes;
- have a professional experience of five years or more;
- have an academic background on Information Technologies, and reasonable knowledge on cybersecurity;

- be working in a healthcare organization, that has part of its computing infrastructure in cloud, or is prospecting to adopt a cloud computing model in the future.

Considering this, the stakeholders were identified, contacted, and the interviews were scheduled. The conducted interviews were a total of three, whereas two were performed on-site, and one was performed remotely via Zoom session. The profiles of the identified participants are identified below.

- **CIO of São João University Hospital Center:** This stakeholder has twenty-seven years of total professional experience in the Information Technology sector, applied to medical sciences, and has worked in the respective healthcare organization for the last six years.
- **CIO of Local Health Unit of Matosinhos (Pedro Hispano Hospital):** This stakeholder has a total of thirty-three years of professional experience, and has worked for the Central Services of the Portuguese Ministry of Health for eighteen years (1988-2006), and in the respective healthcare organization for the last fifteen years.
- **CIO of Porto University Hospital Center (Santo António Hospital):** This interview was conducted with two stakeholders. However, the results and feedback were provided as one. The interviewed have overall professional experiences in the industry of twenty-seven and twenty-three years. They have both been working at their current hospital for the last twenty years.

Finally, the interviews to the stakeholders were conducted respecting the phases presented in the figure 4.1.

1. **Start Interview:** Present the scope of the thesis, laying out its objectives, thus introducing the subject to the stakeholder;
2. **Gather Information:** Query the stakeholders on the current state of the HCO regarding its infrastructure, whether if part of it is on-premises or in cloud environment, main security challenges of the HCO, and in what fashion can cloud environments benefit the HCO;
3. **Present the HCSMAF:** Access the tool's domain and guide the stakeholder going through each security domain, sections, and maturity questions. Additionally, the maturity model and calculation was also explained for later evaluation by the stakeholder;

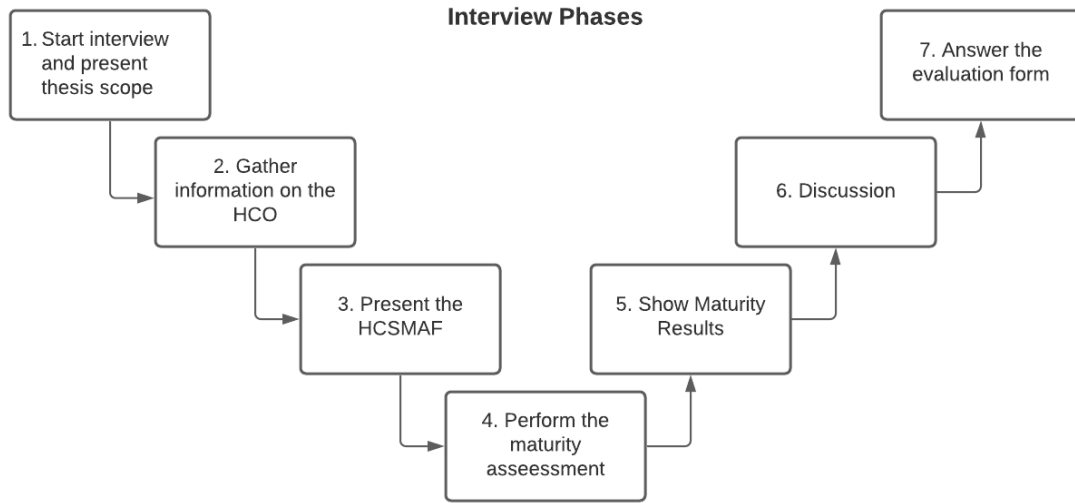


FIGURE 4.1: HCSMAF Interview Phases

4. **Perform Maturity Assessment:** The stakeholder performs the maturity assessment of the HCSMAF, and submits the answers;
5. **Assessment Results:** Show the assessment results page of the tool thus detailing the level of maturity for each of the domains, overall, and the GAP analysis;
6. **Discussion:** Discuss the overall tool with the stakeholder, identifying potential improvements, and highlighting its key points;
7. **Evaluation Form:** Send the tool's evaluation form to the stakeholder in order to get an objective feedback. The questions present in the Evaluation Form are presented in the next section of this chapter.

4.2 Evaluation Form

At the end of the interviews, the stakeholders were asked to answer a questionnaire which allowed the author to gather their insights on the HCSMAF tool. The form is divided between two main sections, the first is composed by standard questions that the author prepared and defined, related to the content of the framework, as in security domains, approached security controls, maturity model. The second section was based on the TAMv2 (Technology Acceptance Model version 2) questionnaire [78], assessing the framework's Perceived Usefulness (PU), Perceived Ease of Use (PEOU), and the User Acceptance of Information Technology (UAIT) [78]. These queries are defined in the table 4.1.

TABLE 4.1: Evaluation form for stakeholders

Sections	Questions	Answer Type
Standard Evaluation	Q1: What is the overall classification of the HCSMAF?	Numerical (1-5)
	Q2: What is the usefulness of the HCSMAF to assess the security of an organization's cloud infrastructure?	Numerical (1-5)
	Q3: How much do you rate the User Interface of the HCSMAF tool?	Numerical (1-5)
	Q4: Do you agree with the Maturity Model of the Framework?	Multiple choice (Yes; Yes but can be improved; No)
	Q5: How could the Maturity Model of the Framework be improved?	Text
	Q6: Do you agree with the security domains present in the Framework?	(Yes; Yes but can be improved; No)
	Q7: How could the framework's security domains be improved?	Text
	Q8: How much do you agree with each security domain and respective maturity questions of the framework?	Numerical per domain (1-5)
	Q9: Were the maturity questions in the security domain in line with what you believe it is crucial to assess in a cloud computing infrastructure?	(Yes; Yes but can be improved; No)
	Q10: How could the framework's maturity questions be improved?	Text
	Q11: Did you agree with the result output from your assessment?	Numerical (1-5)
	Q12: What are your final thoughts on the HCSMAF?	Text
TAMv2 Evaluation	Q13: Perceived Usefulness (PU) Using the system improves my performance in my job. Using the system in my job increases my productivity. Using the system enhances my effectiveness in my job. I find the system to be useful in my job. In my job, usage of the system is relevant.	Numerical (1-5)
	Q14: Perceived Ease of Use (PEOU) My interaction with the system is clear and understandable. Interacting with the system does not require a lot of my mental effort. I find the system to be easy to use. I find it easy to get the system to do what I want it to do.	Numerical (1-5)
	Q15: User Acceptance of Information Technology The results of using the system are apparent to me. I have no difficulty telling others about the results of using the system. The quality of the output I get from the system is high. I have no problem with the quality of the system's output.	Numerical (1-5)

The questions Q1, Q2, Q3 and Q11 define the stakeholders classification of the tool, regarding the overall performance, usefulness, user interface, and resulting output quality.

Regarding Q4 and Q5, the stakeholders classified the defined maturity model questions and whether if they agreed with them, and additionally, Q10 addresses possible improvements for the maturity questions. Another subset of questions relate to the security domains, these being Q8 and Q9, whereas the stakeholders classified each security domain and provided their opinion regarding possible improvements. Finally, Q12 queries the stakeholders on final thoughts considering all the previous answers and additional feedback.

4.3 Evaluation Results

This section aims to present the results from the interviews with the stakeholders, segregating between general questions, the maturity model, security domains, and the TAMv2 evaluation. For this purpose, the stakeholders are identified in the order of S1 (CIO of São João University Hospital Center), S2 (CIO of Local Health Unit of Matosinhos), and S3 (CIO of Porto University Hospital Center). The section closes with an overall discussion of the presented results.

4.3.1 General Questions

The general questions of the tool's functionalities, Q1, Q2, and Q3, respect to the stakeholders overall classification, usefulness, and user interface, respectively. The output result is represented by the figure 4.2.

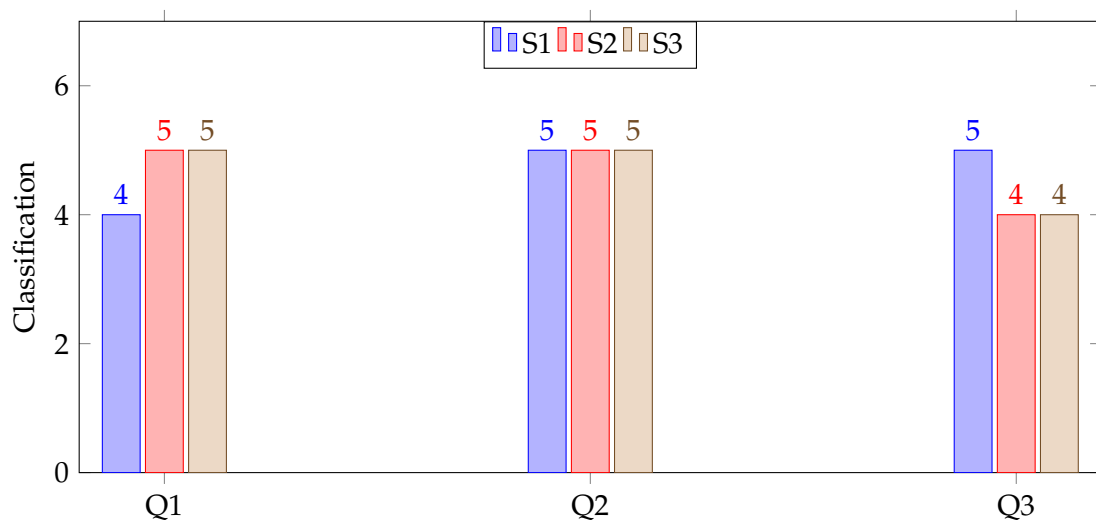


FIGURE 4.2: General questions answers

Analysing the outputs from the stakeholders evaluation of *Q1*, *Q2*, and *Q3*, we can infer that the tool had a very high classification, in a general perspective. In addition, it scored the maximum value in terms of usefulness, with all of the interviewed rating five points. Lastly, the stakeholders found the User Interface to be satisfactory, although showing room for improvement.

4.3.2 Maturity Model Questions

The questions addressing the maturity model utilized in the HCSMAF are the *Q4* and *Q5*. For the first, we can conclude that the stakeholders believe that the maturity model can improve but also agree with the one currently implemented, as shown in the figure 4.3.

Do you agree with the Maturity Model of the framework?

3 responses

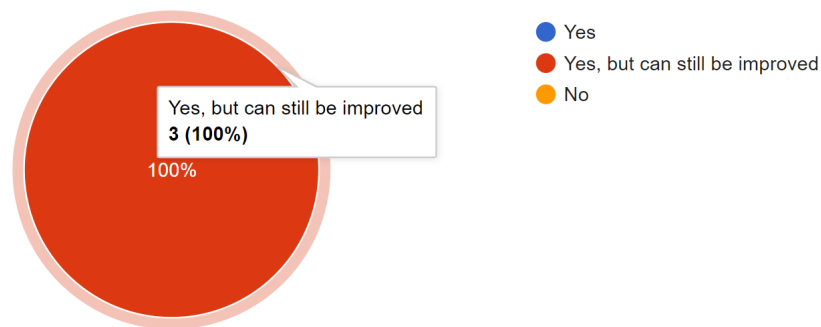


FIGURE 4.3: Maturity Model Response Chart

The *Q5* responses complement the previous one, with *S1* stating that the maturity model could potentially specify different maturity values when varying from public and private sector HCOs, as the private sector does not present the same budget constraints as the other.

4.3.3 Security Domains

The produced results regarding the security domains in the HCSMAF were overwhelmingly positive, with all stakeholders agreeing with the defined security domains, in respects to question *Q6*. Additionally, we conclude that no domain had a classification lower than four, in regards to *Q8*'s overall domains analysis. The results for each domain are presented in the figure 4.4.

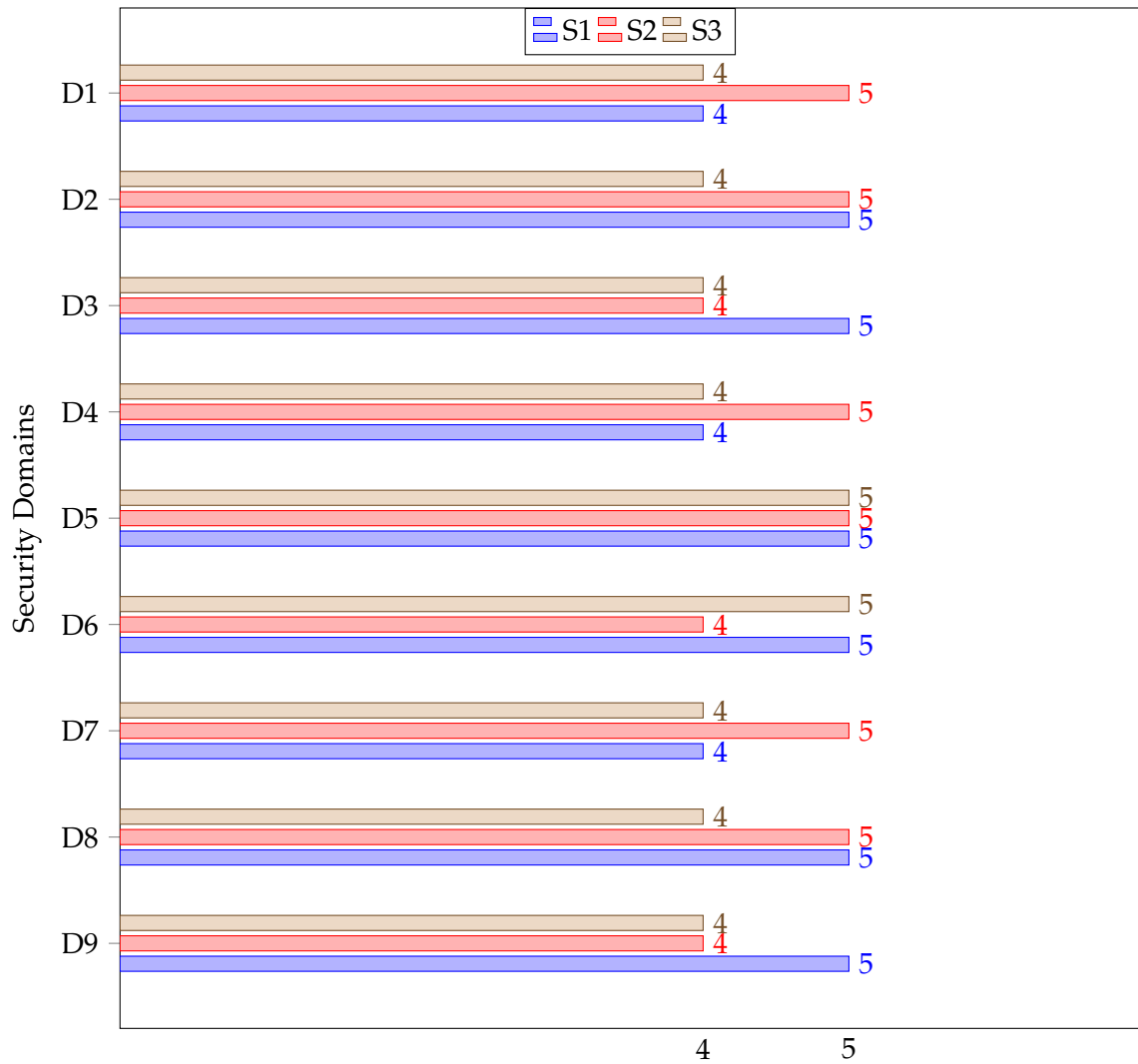


FIGURE 4.4: Q8 - Security Domains classification

Considering the multiple choice question Q6, we can infer that the stakeholders agree, with the unanimous answer being "yes". Additionally, for the question Q7, the stakeholders provided their insights regarding possible security domains in the future.

S1 mentions the necessity of addressing governance issues on the public health sector, as there are recognized bottlenecks in terms of budgets and instability, as the technology underlying the computing infrastructure can suffer changes on a yearly basis. S2 also identifies the necessity in addressing governance issues for the public health sector, and adds the need to direct maturity questions for obsolescence issues for core business

D1-Identity and Access Management; D2-Data Privacy and Management; D3-Risk Management; D4-Asset Management; D5-Cryptography and Key Management; D6-Network and Infrastructure; D7-Compliance and Audit Management; D8-Incident Response Management; D9-Business Continuity Management

software. S3, by the other hand, calls for the necessity of evaluating cloud storage components, with the goal of understanding if the allocated resources meet the hospital capacity demands. This is due to the fact that many medical doctors, and other healthcare professionals, require medical exams like TC scans, endoscopies, colonoscopies, to be available at any time. These exams are normally very heavy in terms of storage occupation, with values varying from fifty Gigabytes (50 GB) to half a Terabyte (1/2 TB), as per stakeholders comments. Additionally, S3 reiterates the need to have maturity controls directed at evaluating cloud incompatibility, promoting portability and interoperability.

Finally, the results of the question *Q9*, the maturity questions classification and applicability for an healthcare cloud security assessment, were in line with the feedback mentioned by the stakeholders. With these results, we can determine that the maturity questions can be improved to meet their expectations, as shown in the figure 4.5.

Were the maturity questions in the security domain in line with what you believe it is crucial to assess in a cloud computing infrastructure?

3 responses

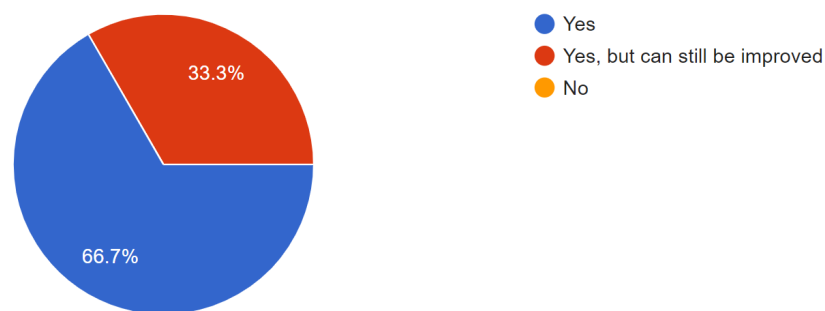


FIGURE 4.5: Maturity Questions Response Chart

4.3.4 TAMv2 Evaluation

The final section of the HCSMAF question's form had the goal of collecting objective data, application-driven, based on a reliable testing model, the Technology Acceptance Model (TAM) [78]. The model was adjusted to meet the application's needs, thus defining three different components for the TAMv2 evaluation. The components are the Perceived Use (PU), which refers to the degree to which a person believes that using a particular system would enhance his or her job performance, the Perceived Ease of Use (PEOU), which refers to the degree to which a person believes that using a particular system would be

free of effort [79], and the User Acceptance of Information Technology (UAI), referring to the degree which a person can perform what is expected from the system, including output results reliability and performance [80]. The classification interval is from one to five, one being the lowest score, and five being the highest. These components, and the respective question's results are presented in the figures 4.6, 4.7, 4.8.

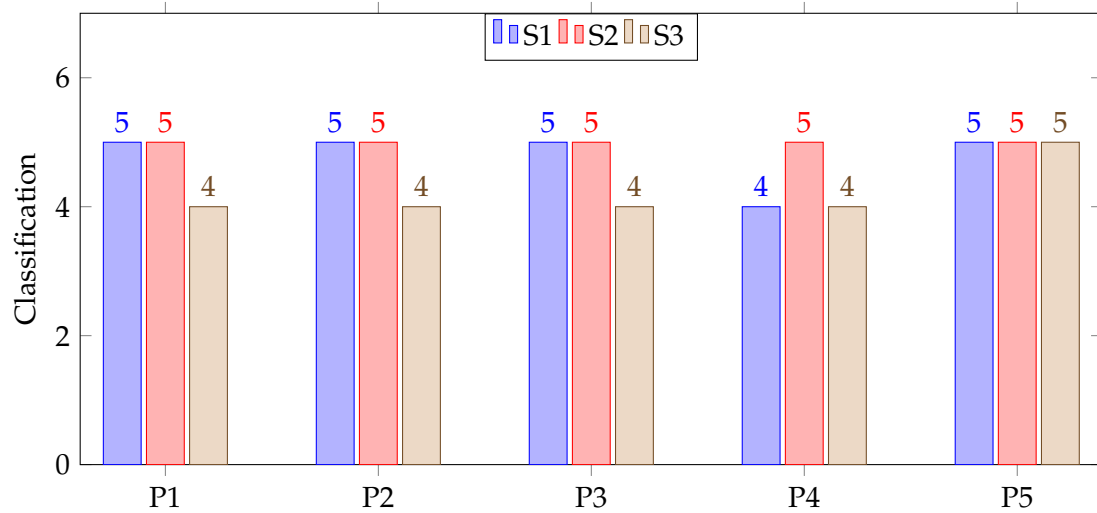


FIGURE 4.6: Q13 - Perceived Usefulness (PU) results

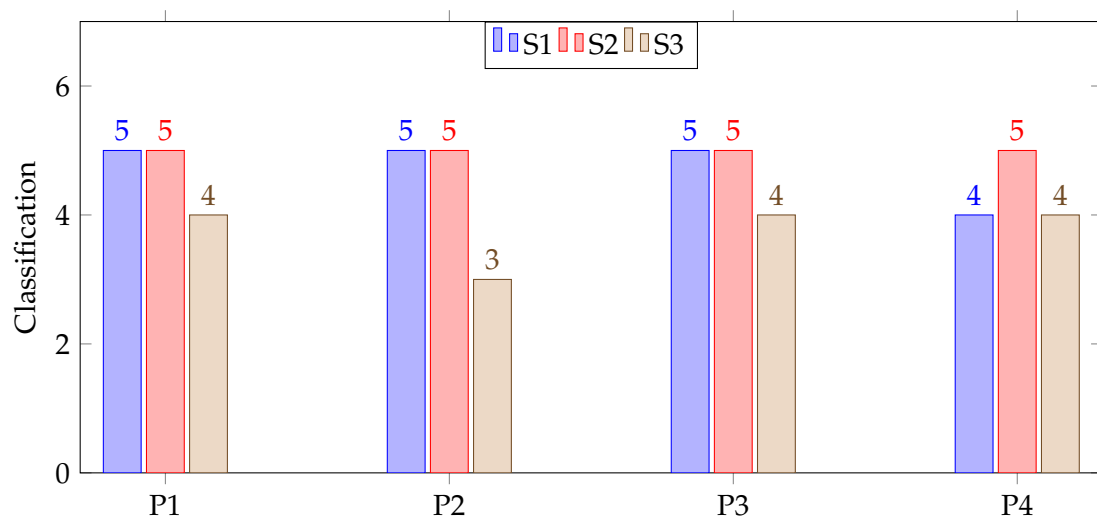


FIGURE 4.7: Q14 - Perceived Ease of Use (PEOU) results

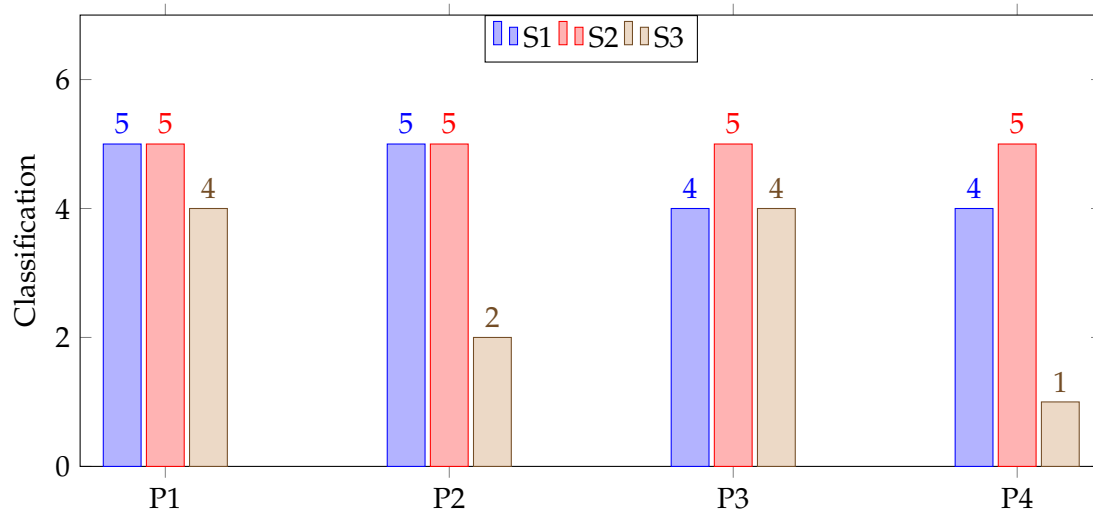


FIGURE 4.8: Q15 - User Acceptance to Information Technology (UAIT) results

The question *Q13*, Perceived Use (PU), obtained good results, with the responses averaging on a percentage of 93%. This means that the stakeholders found the tool to be useful and with potential to improve their job's effectiveness when assessing their cloud's security maturity.

In regards to the question *Q14*, Perceived Ease of Use (PEOU), it scored 90%, thus demonstrating that users find the tool to be easy to use and interact with. Although, one stakeholder identified that the tool requires some mental effort to complete the maturity form, scoring the lowest result (3) when comparing to its peers, shown in the figure 4.7.

Finally, the question *Q15*, the User Acceptance of Information Technology (UAIT), scored the lowest of the three TAMv2 components. Although it still demonstrated to have a high average score of 82%, it underperformed in terms of two parameters. One stakeholder identified that telling other people about the framework's results can be a hard task, attributing a score of two. Additionally, one stakeholder assigned a value of one to the quality of the system's outputs, thus being the lowest rated parameter.

4.3.5 Overall Results Discussion

The interviews to the stakeholders were performed with the objective of proving that the developed work, the HCSMAF tool, could serve as potential solution for the identified problems in the State of the Art of cloud security in healthcare. By considering the stakeholder's feedback, it is possible to acknowledge that cloud computing presents itself as a viable solution to solve the many challenges that healthcare institutions need to deal with on a regular basis, and tools like the one developed facilitate in resolving ever growing

concerns around the subject of security.

Furthermore, the stakeholders were questioned on what are the major security challenges they face currently, as well as how does cloud computing technology help, or would help them, mitigating those security challenges. Their responses are presented below.

Identified Security Challenges

- **Obsolete Technology/Legacy Systems:** This is one of the most common security issues identified by the stakeholders, as many HCOs use legacy systems, which are core to their infrastructure. Considering that these systems were developed without having *security-by-design* principles and implemented years ago, they present serious frailties and high susceptibility of vulnerabilities and attack vectors;
- **Lack of Resources Capacity:** The exponential volume of data, in transit and at rest, that hospital systems manage leads to instability, thus causing service outages. This compromises the systems availability, and puts the HCOs in serious distress;
- **Systems Maintenance:** The fact that the servers are managed on-premises lead to an increased effort related to patch management and system maintenance. This tasks can be heavy, requires experts, and the organization has to continuously monitor for new vulnerabilities on their systems that can exploited if not deal with.

Identified Cloud Benefits

- **Flexibility:** The HCOs systems capacities could improve rapidly with the flexibility and fast resource allocation that cloud computing provides, mitigating the likelihood of reaching system critical levels, disruptions, and systems outages;
- **CSP Maintenance:** A part of the infrastructure would be managed by cloud service providers (CSP), depending on the cloud model (SaaS, PaaS, IaaS), providing greater security to the HCO and releasing human resources for other tasks;
- **Modern Software:** Adopting cloud services could lead to migrating services, applications, and data from the legacy and insecure systems on-premises, to recently developed and continuously managed systems.
- **Backups and data storage:** Given the large volume of data that healthcare organizations deal with, especially from patient's medical exams, it is necessary to expand storage capacities and backups. Cloud computing is more flexible for storage capacity allocation, thus releasing institutions from this burden.

The stakeholders believe that the development of tools as the HCSMAF, and the upward trend of investigation of this subject, leads to a push in adopting the cloud computing model in healthcare institutions.

When assessing the interview's results, it is possible to conclude that the HCSMAF tool achieved a good performance in the stakeholders' perception. Even though the healthcare organizations, that the stakeholders belong to, still have a long path in adopting a cloud model, they recognized the advantages in the security domains selection, as well as the maturity model in place. The classification provided by the stakeholders for each security, as well as the averages, are presented in the table 4.2.

TABLE 4.2: Security Domain Results table

Domain	S1	S2	S3
Identity and Access Management	4	5	4
Data Privacy and Management	4	5	4
Risk Management	4	5	4
Asset Management	4	5	4
Cryptography and Key Management	4	5	5
Infrastructure and Network Security	4	5	5
Compliance and Audit Management	4	5	4
Incident Response Management	4	5	4
Business Continuity Management	4	5	4

Furthermore, by analyzing the TAMv2 results, we conclude that the HCSMAF tool has a very high percentage of usefulness. This is supported by the average score of the parameters Perceived Usefulness (PU) - 93,3%. In addition to PU, the Perceived Ease of Use (PEOU) performed similarly, thus demonstrating that the tool rendered as intuitive. In contrast, the component of the User Acceptance of Information Technology has a sub-standard performance when comparing to its peers, achieving an average score of 81,7%. These figures are demonstrated in the following table 4.3.

TABLE 4.3: TAMv2 Sections Evaluation

TAM Sections	S1	S2	S3	TAM Average (%)
Perceived Usefulness (PU) (%)	96	100	84	93,3
Perceived Ease of Use (PEOU) (%)	95	100	75	90
User Acceptance of Information Technology (UAIT) (%)	90	100	55	81,7

Despite the positive feedback from the stakeholders, opportunities for improvements of the framework were identified. Regarding the framework's content, the stakeholder's main concern relate to the necessity of differentiating public and private healthcare organizations. There are existing constraints that impact public HCO's cloud adoption, whereas in private HCOs they are not so common. Additionally, the stakeholders address the challenges of cloud incompatibility with core legacy systems and medical devices. For the tool's maturity model and maturity metrics, the stakeholders identified limitations in the "yes/No" answer method. They add the necessity of establishing an intermediate option for on-going implementations. Suggestions for the framework are later discussed in the Future Improvements section.

Ultimately, the interviewed stakeholders found the tool to be "useful", "interesting", and with "great potential", especially if it can meet the outlined improvements to increase the maturity result's accuracy.

Chapter 5

Conclusion & Future Improvements

This thesis presents itself, not only as a proposal to solve the identified challenges from the *State of the Art*, like the scarcity of cloud security guidance for the health sector but as an opportunity to assist in evaluating cloud computing models in one of the most vital sectors of society. This solution, in its essence, supports healthcare organizations to monitor their current cloud security landscape, evaluate it, and develop a roadmap to tackle their most vulnerable security domains. The author thoroughly believes that the proposed model helps healthcare organizations to meet their security demands. This is performed by first acknowledging their maturity levels, and achieving better governance over their cloud systems. This holistic approach aids these institutions to identify the risks that they are subjected to on a daily basis, and mitigate them by securing the systems that store, process, and transmit Electronic Health Records (EHR), Personal Health Information (PHI), and Personal Identifiable Information (PII).

This dissertation focused on the main problem, and secondly on the solution to solve it. First and foremost, on the arising necessity of bridging the gap of healthcare and cloud security, providing HCOs with the proper tools and information to autonomously assess their risks and security solutions. Secondly, on developing a tool that could present itself as a solution to the identified problem, with the potential of being utilized to achieve accurate results while being accessible, and user-friendly. To attain this, the author's approach concentrated on developing a lightweight web application, with an underlying security maturity assessment model. The presented work was segregated into different stages. These stages were performed as follows:

1. Identification of the common cloud and healthcare security challenges, as well as the investigation of the existing standards, frameworks, and regulations presenting

security controls and requirements.

2. Design of a framework for the evaluation of relevant security domains in cloud computing environments and infrastructures, in healthcare organizations, based on the conducted investigation. Moreover, integrating a capability maturity model with defined maturity metrics.
3. Design, implementation, testing, and deployment of a web application with the underlying content of the developed maturity framework. Furthermore, implementing outputs section with GAP analysis and overall maturity information.
4. Evaluation of the created web application, and respective maturity framework, with relevant stakeholders from renowned healthcare institutions.

The results obtained from the stakeholder's evaluation demonstrated that the tool was aligned with their expectations for a maturity assessment tool. It was shown to have an overall agreement in regards to the defined security domains, as well as the present maturity model. Nonetheless, the stakeholders recognized room for possible improvements. Mainly, they offered valuable inputs for increasing the results' accuracy for different types of healthcare institutions. In addition, they suggested security controls that address their identified security challenges.

In conclusion, the Healthcare Cloud Security Maturity Assessment Framework (HCS-MAF) tool has proven to be an effective starting point solution. Notwithstanding the fact that it can be improved, it demonstrated to have the potential to provide relevant insights to healthcare organization's security experts. As a result, this can lead to increasing their cyber resilience, reducing attack surface, improve regulatory compliance, and ultimately achieving an optimizing cloud security maturity.

5.1 Future Improvements

The proposed solution was developed under the defined scope for the thesis and was capable of meeting its objectives. However, throughout its development and results analysis, opportunities for improvement have emerged and were identified to be addressed in the future. The proposed future work is the following:

- Direct the maturity assessment to a specific audience. This would vary in terms of the type of healthcare organization, whether public or private, its dimension in

terms of employees and patient capacity. Additionally, the cloud deployment type could also be integrated into this flux, as the maturity model could differ between SaaS, PaaS, and IaaS. As a result, the assessment would produce more accurate results, as it would further adapt the maturity calculation to the reality of the HCOs.

- Create benchmarking indicators in the results section. This would benefit the user in gaining insights by comparison to its peers, understanding if the current maturity is below, in line, or above average.
- Upgrade the web application as a whole. Although it performed well in terms of user interface and output results, the tool can be improved in regards to security, by implementing *HTTPS (Hypertext Transfer Protocol Secure)*, login capabilities, and further graphics displays.

Finally, the framework's maturity model and security domains should be continuously reviewed. This would guarantee that the maturity questions are constantly up-to-date with emerging frameworks and standards, hence producing reliable and accurate results, as cloud security evolves and new trends emerge.

Appendix A

HCSMAF Web Application

Health Cloud Maturity Assessment

Incident Response Management | Data Privacy and Management | Risk Management | Asset Management | Cryptography and Key Management | Infrastructure and Network Security | Compliance and Audit Management

Network Security

Does your HCO have any defined policy, process, or procedure for Network Security?
Yes

Has your HCO implemented network-related security controls for both untrusted and trusted network connections and virtual instances?
Yes

Does your HCO fully rely on CSP for Network security?
Not Sure

Please select one of the following network security technologies that your HCO or CSP has implemented:

- ☒ Intrusion Detection System (IDS)
- ☒ Intrusion Prevention System (IPS)
- ☒ Cloud-Access Security Broker (CASB)
- ☒ Web Application Firewall (WAF)
- ☒ Threat Intelligence monitoring tools
- ☒ Advanced Threat Protection (ATP) tools
- ☒ Security Information and Event Management system (SIEM)
- ☒ Data Loss Prevention (DLP)

Does your HCO, alongside the CSP, take the proper measures to continuously maintain and test the network security technologies in use to support the existing security requirements?
Yes

Did your HCO verify if the CSP provides the necessary level of network security to align with the necessary security requirements in place?
Yes

Does your CSP provide guarantees of secure communications and system availability, such as IPsec, Secure Socket Layer (SSL) or any other Network level encryption and protection mechanisms?
Yes

Does your HCO establish, implement, maintains any policy, procedures, or process related to infrastructure and virtualization security?
No

Does your HCO enforce security controls related to hardening of virtualization components, such as host and guest OS, hypervisor, or infrastructure control plane?
Not Sure

Assessment Dashboards Knowledge User Settings

FIGURE A.1: HCSMAF Webapp Assessment Page

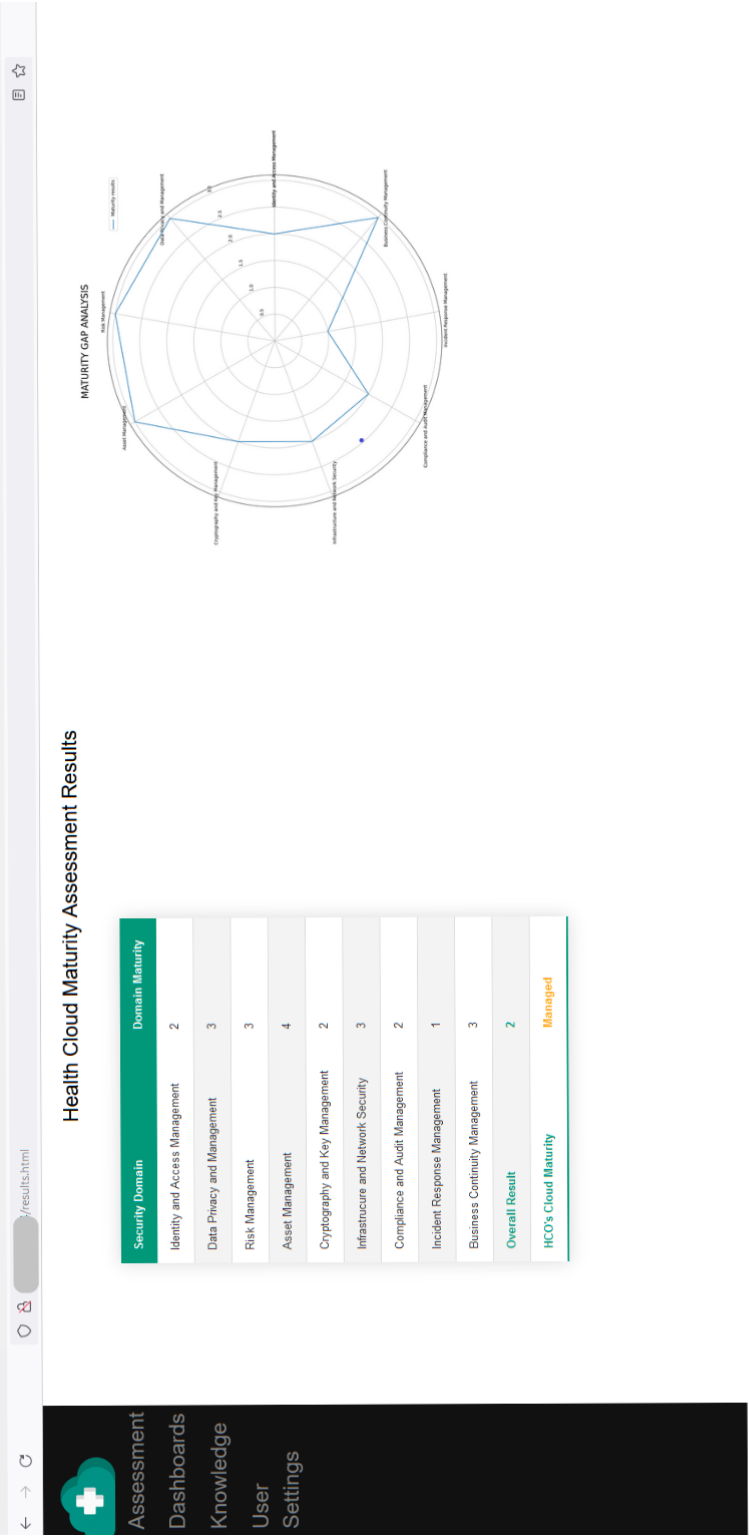
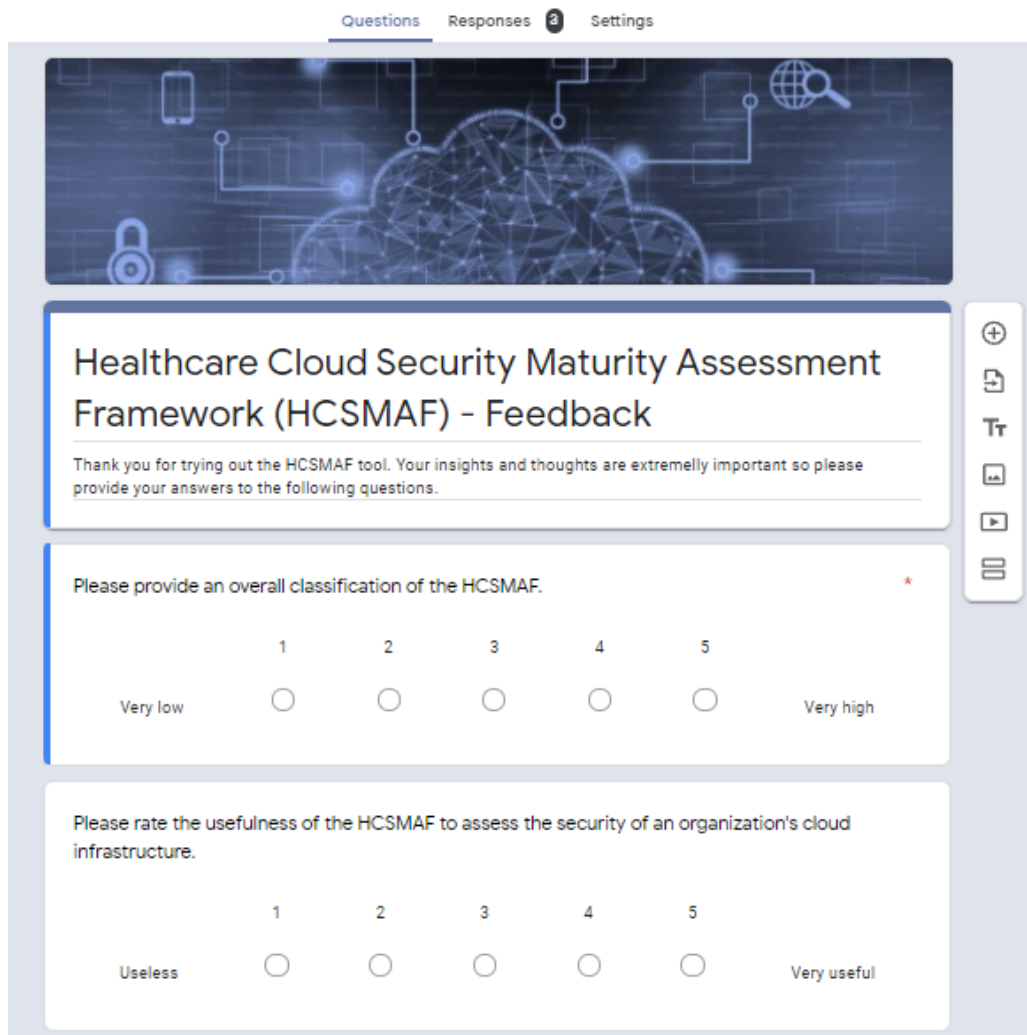


FIGURE A.2: HCSMAF Webapp Results Page

Appendix B

Evaluation Form



The screenshot displays the 'Questions' tab of the HCSMAF evaluation form. At the top, there are navigation links for 'Questions', 'Responses' (with a count of 2), and 'Settings'. Below these is a header banner with a blue background and white icons representing cloud security concepts like a smartphone, a padlock, a cloud network, and a globe with a magnifying glass. The main title of the form is 'Healthcare Cloud Security Maturity Assessment Framework (HCSMAF) - Feedback'. A thank-you message follows: 'Thank you for trying out the HCSMAF tool. Your insights and thoughts are extremely important so please provide your answers to the following questions.' The first question asks for an overall classification of the HCSMAF, with a 5-point scale from 'Very low' to 'Very high'. The second question asks for a rating of the usefulness of the HCSMAF to assess cloud infrastructure security, with a 5-point scale from 'Useless' to 'Very useful'. A vertical toolbar on the right side of the form contains icons for adding, deleting, translating, commenting, and navigating through the questions.

Questions Responses 2 Settings

Healthcare Cloud Security Maturity Assessment Framework (HCSMAF) - Feedback

Thank you for trying out the HCSMAF tool. Your insights and thoughts are extremely important so please provide your answers to the following questions.

Please provide an overall classification of the HCSMAF. *

Very low 1 2 3 4 5 Very high

Please rate the usefulness of the HCSMAF to assess the security of an organization's cloud infrastructure.

Useless 1 2 3 4 5 Very useful

FIGURE B.1: HCSMAF Evaluation Form



FIGURE B.2: HCSMAF Evaluation Form Results

Appendix C

HCSMAF Standards Mapping Example

Control Domain	Control Title	Control ID	Updated Control Specification			ISO 27017	ISO 27018
Audit & Assurance - A&A						Cloud Service Customer (CSC) Cloud Service Provider (CSP)	Cloud Service Customer (CSC) Cloud Service Provider (CSP)
Identity & Access Management - IAM							
Identity & Access Management	Identity and Access Management Policy and Procedures	IAM-01	Establish, document, approve, communicate, implement, apply, evaluate and maintain policies and procedures for identity and access management. Review and update the policies and procedures at least annually.			9.1.1; 9.1.2 - Specify user access to each separate cloud service that is used	N/A
Identity & Access Management	Strong Password Policy and Procedures	IAM-02	Establish, document, approve, communicate, implement, apply, evaluate and maintain strong password policies and procedures. Review and update the policies and procedures at least annually.			9.4.3 - 27002 - Maps	
Identity & Access Management	Identity Inventory	IAM-03	Manage, store, and review the information of system identities, and level of access			N/A	9.2.1 - Provide User registration and deregistration functions to the CSC As a security engineering on the cloud model used, the cloud provider should provide user management feature to the CSC such as User Inventory Mapping
Identity & Access Management	Separation of Duties	IAM-04	Employ the separation of duties principle when implementing information system access.				
Identity & Access Management	Least Privilege	IAM-05	Employ the least privilege principle when implementing information system access.			Nothing on 27007 and 27018 - But surely mention as security engineering principle	
Identity & Access Management	User Access Provisioning	IAM-06	Define and implement a user access provisioning process which authorizes, records, and communicates access changes to data and assets.			N/A	managing the access rights of the cloud customer, and specifications for usage of these functions
Identity & Access Management	User Access Changes and Revocation	IAM-07	De-provision or respectively modify access of movers / leavers or system identity changes in a timely manner in order to effectively adopt and communicate identity and access management policies.			Related to User Management -> 9.2	9.2.1 - Public Cloud PI Protection Implementation Guidance
Identity & Access Management	User Access Review	IAM-08	Review and revalidate user access for least privilege and separation of duties with a frequency that is commensurate with organizational risk tolerance.			9.2.5 e 9.2.6 -> 27002	N/A
Identity & Access Management	Segregation of Privileged Access Roles	IAM-09	Define, implement and evaluate processes, procedures and technical measures for the segregation of privileged access roles such that administrative access to data, encryption and key management capabilities and logging capabilities are distinct and			9.3.3 -> Use of multifactor authentication techniques. Aligned with existing risks	CSP should provide sufficient techniques for multi authentication
Identity & Access Management	Management of Privileged Access Roles	IAM-10	Define and implement an access process to ensure privileged access roles and rights are granted for a time limited period, and implement procedures to prevent the culmination of segregated privileged access.			9.3.3 -> Use of multi authentication techniques! Aligned with existing risks	CSP should provide sufficient techniques for multi authentication
Identity & Access Management	CSCs Approval for Agreed Privileged Access Roles	IAM-11	Define, implement and evaluate processes and procedures for customers to participate, where applicable, in the granting of access for agreed, high risk (as defined by the organizational risk assessment) privileged access roles.			9.3.3 -> Use of multi authentication techniques! Aligned with existing risks	CSP should provide sufficient techniques for multi authentication
Identity & Access Management	Safeguard Logs Integrity	IAM-12	Define, implement and evaluate processes, procedures and technical measures to ensure the logging infrastructure is ready-only for all write access, including privileged access roles, and that the ability to disable it is controlled through a procedure that				
Identity & Access Management	Uniquely Identifiable Users	IAM-13	Define, implement and evaluate processes, procedures and technical measures that ensure users are identifiable through unique IDs or which can associate individuals to the usage of user IDs.				
Identity & Access Management	Strong Authentication	IAM-14	Define, implement and evaluate processes, procedures and technical measures for authenticating access to systems, application and data assets, including multifactor authentication for at least privileged user and sensitive data access. Adopt digital			9.4.2; 9.4.3 -> Aligned with 27002	
Identity & Access Management	Passwords Management	IAM-15	Define, implement and evaluate processes, procedures and technical measures for the secure management of passwords.			9.4.3 -> Aligned with 27002	9.4.3 -> Aligned with 27002
Identity & Access Management	Authorization Mechanisms	IAM-16	Define, implement and evaluate processes, procedures and technical measures to verify access to data and system functions is authorized.				

FIGURE C.1: HCSMA Framework investigation and standards mapping exercise

Bibliography

- [1] R. Zhang and L. Liu, "Security models and requirements for healthcare application clouds," in *2010 IEEE 3rd International Conference on Cloud Computing*, 2010, pp. 268–275. [Cited on page 1.]
- [2] HHS, "The security rule," <https://www.hhs.gov/hipaa/for-professionals/security/index.html>, 2021, online; accessed 30 August 2021. [Cited on pages 1, 18, 26, and 33.]
- [3] European Commision, "What personal data is considered sensitive?" https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/sensitive-data/what-personal-data-considered-sensitive_en, 2021, online; accessed 24 September 2021. [Cited on page 1.]
- [4] E. AbuKhousa, N. Mohamed, and J. Al-Jaroodi, "e-health cloud: Opportunities and challenges," *Future Internet*, vol. 4, no. 3, pp. 621–645, 2012. [Online]. Available: <https://www.mdpi.com/1999-5903/4/3/621> [Cited on page 1.]
- [5] e. a. Al-Issa Y., Ottom M. A., "ehealth cloud security challenges: A survey," p. 1–15, 2019. [Online]. Available: <https://www.hindawi.com/journals/jhe/2019/7516035/> [Cited on pages 1, 18, and 24.]
- [6] N. I. of Standards and T. G. Technology, Peter Mell, "The nist definition of cloud computing," U.S. Department of Commerce, Washington, D.C., Tech. Rep. NIST SP 800-145, Change Notice September 2011, 2011. [Cited on pages 1, 2, 5, 6, and 12.]
- [7] J. JPC Rodrigues, I. de la Torre, G. Fernández, and M. López-Coronado, "Analysis of the security and privacy requirements of cloud-based electronic health records systems," *J Med Internet Res*, vol. 15, no. 8, p. e186, Aug 2013. [Online]. Available: <https://doi.org/10.2196/jmir.2494> [Cited on pages 2 and 25.]

- [8] Cloud Security Alliance (CSA), “Security Guidance for Critical Areas of Focus in Cloud Computing v4.0,” <https://cloudsecurityalliance.org/artifacts/security-guidance-v4/>, 2021, online; accessed 25 August 2021. [Cited on pages xiii, 2, 7, 8, 10, 34, and 37.]
- [9] Acherman, M., Arora, R., Banse, C., et al, “Cloud controls matrix (ccm),” <https://cloudsecurityalliance.org/research/cloud-controls-matrix/>, 2021, online; accessed 28 August 2021. [Cited on pages 2, 16, 33, and 40.]
- [10] “Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services,” International Organization for Standardization, Geneva, CH, Standard, December 2015. [Cited on pages 2, 11, 16, 32, and 36.]
- [11] “Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors,” International Organization for Standardization, Geneva, CH, Standard, January 2019. [Cited on pages 2, 16, and 33.]
- [12] ENISA, Catteddu, D., Hogben, G., Haeberlen, T., Dupre, L., “Top threats to cloud computing: Egregious eleven,” <https://resilience.enisa.europa.eu/cloud-security-and-resilience/publications/cloud-computing-benefits-risks-and-recommendations-for-information-security/view>, 2021, online; accessed 28 August 2021. [Cited on pages 2, 15, 16, and 23.]
- [13] Findstack, “The Ultimate List of Cloud Computing Statistics 2021,” <https://findstack.com/cloud-computing-statistics/>, 2021, online; accessed 25 August 2021. [Cited on page 6.]
- [14] IBM, “IaaS vs. PaaS vs. SaaS,” <https://www.ibm.com/cloud/learn/iaas-paas-saas>, 2021, online; accessed 25 August 2021. [Cited on page 7.]
- [15] S. Zhang, H. Yan, and X. Chen, “Research on key technologies of cloud computing,” *Physics Procedia*, vol. 33, pp. 1791–1797, 2012, 2012 International Conference on Medical Physics and Biomedical Engineering (ICMPBE2012). [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S1875389212015994> [Cited on page 8.]

- [16] Rswebsols, Souvik, "SaaS vs PaaS vs IaaS: Advantages, Disadvantages and Comparison," <https://www.rswebsols.com/tutorials/software-tutorials/saas-paas-iaas-advantages-disadvantages-comparison>, 2021, online; accessed 25 August 2021. [Cited on page 8.]
- [17] BMC, "saas-vs-paas-vs-iaas-whats-the-difference-and-how-to-choose," <https://www.bmc.com/blogs/saas-vs-paas-vs-iaas-whats-the-difference-and-how-to-choose/>, 2021, online; accessed 25 August 2021. [Cited on page 9.]
- [18] Virayo, "40+ SaaS Statistics to Guide Your Business in 2020," <https://virayo.com/saas/statistics/>, 2021, online; accessed 26 August 2021. [Cited on page 9.]
- [19] N. I. of Standards and E. S. Technology, "Evaluation of cloud computing services based on nist sp 800-145," U.S. Department of Commerce, Washington, D.C., Tech. Rep. NIST SP 500-322, Change Notice February 2018, 2018. [Cited on pages 11, 12, and 13.]
- [20] P. C. Chuvanik A., Schmidt K., "Chapter 21 - cloud logging," pp. 381–399, 2013. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/B978159749635300021X> [Cited on page 11.]
- [21] . N. P. Laszewski T., "Chapter 1 - migrating to the cloud: Client/server migrations to the oracle cloud," p. 1–19, 2012. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/B9781597496476000016> [Cited on page 12.]
- [22] C. I. Rountree D., "Chapter 3 - cloud deployment models," pp. 35–47, 2014. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/B9780124059320000037> [Cited on page 12.]
- [23] Cloud Security Alliance (CSA), "Top threats to cloud computing: Egregious eleven," <https://cloudsecurityalliance.org/artifacts/top-threats-to-cloud-computing-egregious-eleven/>, 2021, online; accessed 28 August 2021. [Cited on page 14.]
- [24] GSA, "Fedramp," <https://www.gsa.gov/technology/government-it-initiatives/fedramp>, 2021, online; accessed 28 August 2021. [Cited on page 16.]
- [25] L. Wang and C. Alexander, "Medical applications and healthcare based on cloud computing," *International Journal of Cloud Computing and Services Science (IJ-CLOSER)*, vol. 2, 10 2013. [Cited on page 17.]

- [26] Techtarget, "Healthcare-cloud-induces-benefits-in-storage-security," <https://searchhealthit.techtarget.com/feature/Healthcare-cloud-induces-benefits-in-storage-security>, 2021, online; accessed 28 August 2021. [Cited on page 17.]
- [27] GDPR, "What is gdpr, the eu's new data protection law?" <https://gdpr.eu/what-is-gdpr/>, 2021, online; accessed 30 August 2021. [Cited on pages 18, 26, and 33.]
- [28] HHS, "Hipa privacy rule," <https://www.govinfo.gov/content/pkg/FR-2013-01-25/pdf/2013-01073.pdf>, 2021, online; accessed 30 August 2021. [Cited on page 18.]
- [29] M. Bamiah, S. Brohi, S. Chuprat, and J.-L. Ab Manan, "A study on significance of adopting cloud computing paradigm in healthcare sector," 12 2012, pp. 65–68. [Cited on page 18.]
- [30] Opsworks, "Cost of downtime," <https://opsworks.co/cost-of-downtime>, 2021, online; accessed 30 August 2021. [Cited on page 18.]
- [31] M. Bamiah, S. Brohi, S. Chuprat, and J.-L. Ab Manan, "A study on significance of adopting cloud computing paradigm in healthcare sector," 12 2012, pp. 65–68. [Cited on page 18.]
- [32] HIPAA Journal, "Healthcare data breach statistics," <https://www.hipaajournal.com/healthcare-data-breach-statistics/>, 2021, online; accessed 30 August 2021. [Cited on page 19.]
- [33] Purple Sec, "Healthcare cyber security statistics," <https://purplesec.us/cyber-security-healthcare-statistics/>, 2021, online; accessed 30 August 2021. [Cited on page 19.]
- [34] "2020 himss cybersecurity survey," https://www.himss.org/sites/hde/files/media/file/2020/11/16/2020_himss_cybersecurity_survey_final.pdf, HIMSS, Report, 2020. [Cited on page 20.]
- [35] "Verizon 2021 dbir - data breach investigations report," <https://www.verizon.com/business/resources/reports/dbir/2021/data-breach-statistics-by-industry/healthcare-data-breaches-security/>, Verizon, Report, 2021. [Cited on pages 20 and 21.]

- [36] e. a. Liveri D., Drougkas A., "Cloud security for healthcare services," pp. 1–46, January 2021. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/B9781597496476000016> [Cited on pages 21, 23, 24, 33, 35, and 37.]
- [37] A. Fatima and R. Colomo-Palacios, "Security aspects in healthcare information systems: A systematic mapping," *Procedia Computer Science*, vol. 138, pp. 12–19, 2018. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S187705091831634X> [Cited on page 22.]
- [38] H. S. J. e. a. Abrar H., "Risk analysis of cloud sourcing in healthcare and public health industry," *IEEE Access*, vol. 6, pp. 19 140–19 150, 2018. [Cited on page 22.]
- [39] Hitrust Alliance, "The security rule," <https://hitrustalliance.net/product-tool/hitrust-csf/>, 2021, online; accessed 30 August 2021. [Cited on pages 26 and 33.]
- [40] ONC, OCR, "Security risk assessment tool," <https://www.healthit.gov/topic/privacy-security-and-hipaa/security-risk-assessment-tool>, 2021, online; accessed 30 August 2021. [Cited on page 26.]
- [41] EUC, "Council directive 93/42/eecl of 14 june 1993 concerning medical devices," <https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CONSLEG:1993L0042:20071011:en:PDF>, 2021, online; accessed 30 August 2021. [Cited on page 26.]
- [42] EU, "REGULATION (EU) 2017/745 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 5 April 2017 on medical devices," <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32017R0745>, 2021, online; accessed 30 August 2021. [Cited on page 26.]
- [43] O. O. Akinsanya, M. Papadaki, and L. Sun, "Current cybersecurity maturity models: How effective in healthcare cloud?" in *CERC*, 2019. [Cited on page 26.]
- [44] D. B. H. NGOC T. LE, "Capability maturity model and metrics framework for cyber cloud security," in *Scalable Computing: Practice and Experience*, vol. 18, 2017, pp. 277–290. [Cited on page 27.]
- [45] NHSUK, "Digital maturity self-assessment data model or structure," https://www.england.nhs.uk/wp-content/uploads/2017/08/digital-maturity-data-model_v2.pdf, 2021, online; accessed 31 August 2021. [Cited on page 27.]

- [46] NHS, "Digital maturity assessment," <https://www.england.nhs.uk/digitaltechnology/connecteddigitalsystems/maturity-index/>, 2021, online; accessed 01 September 2021. [Cited on page 27.]
- [47] J. Carvalho, A. Rocha, and A. Abreu, "Maturity models of healthcare information systems and technologies: a literature review," *Journal of Medical Systems*, vol. 40, p. 10, 04 2016. [Cited on page 27.]
- [48] H. Susanto, M. N. Almunawar, and C. Kang, "Toward cloud computing evolution: Efficiency vs trendy vs security," *Computer Science Journal*, vol. 2, pp. 2221–5905, 09 2012. [Cited on page 30.]
- [49] I. Indu, P. R. Anand, and V. Bhaskar, "Identity and access management in cloud environment: Mechanisms and challenges," *Engineering Science and Technology, an International Journal*, vol. 21, no. 4, pp. 574–588, 2018. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S2215098617316750> [Cited on page 32.]
- [50] M. Esna-Ashari, H. Rabiee, and S. Mirian-Hosseiniabadi, "Reliability of separation of duty in ansi standard role-based access control," *Scientia Iranica*, vol. 18, no. 6, pp. 1416–1424, 2011. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S1026309811001660> [Cited on page 33.]
- [51] J. Saltzer and M. Schroeder, "The protection of information in computer systems," *Proceedings of the IEEE*, vol. 63, no. 9, pp. 1278–1308, 1975. [Cited on page 33.]
- [52] NIST, "Role based access control," <https://csrc.nist.gov/projects/role-based-access-control>, 2021, online; accessed 15 September 2021. [Cited on page 33.]
- [53] T. R. Weil and E. Coyne, "Abac and rbac: Scalable, flexible, and auditable access management," *IT Professional*, vol. 15, no. 03, pp. 14–16, may 2013. [Cited on page 33.]
- [54] E. Abukhousa, N. Mohamed, and J. Al-Jaroodi, "e-health cloud: Opportunities and challenges," *Future Internet*, vol. 4, pp. 621–645, 07 2012. [Cited on page 33.]
- [55] "Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines," International Organization for Standardization, Geneva, CH, Standard, Aug. 2019. [Cited on pages 33 and 34.]

- [56] Netskope, "The bcm lifecycle: an overview," <https://www.mdsny.com/wp-content/uploads/2017/08/Netskope-Cloud-Compliance-Checklist-for-EU-GDPR.pdf>, online; accessed 17 September 2021. [Cited on page 34.]
- [57] "Information technology — Security techniques — Information security management systems — Requirements," International Organization for Standardization, Geneva, CH, Standard, Oct. 2013. [Cited on pages 34 and 35.]
- [58] DMTF, "Open virtualization format," <https://www.dmtf.org/standards/ovf>, 2021, online; accessed 16 September 2021. [Cited on page 34.]
- [59] "Information technology — Security techniques — Information security risk management," International Organization for Standardization, Geneva, CH, Standard, July 2018. [Cited on page 35.]
- [60] ITGovernance, "Data protection impact assessments and the gdpr," <https://www.itgovernance.co.uk/privacy-impact-assessment-pia>, 2021, online; accessed 15 September 2021. [Cited on page 35.]
- [61] F. Khan, J. H. Kim, L. Mathiassen, and R. Moore, "Data breach management: An integrated risk model," *Information and Management*, vol. 58, no. 1, p. 103392, 2021. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S037872062030330X> [Cited on page 35.]
- [62] N. I. of Standards and Technology, "Guideline for using cryptographic standards in the federal government: Cryptographic mechanisms," U.S. Department of Commerce, Washington, D.C., Tech. Rep. NIST SP 800-175B, 2020. [Cited on page 36.]
- [63] J. Attridge, "An Overview of Hardware Security Modules," SANS, Tech. Rep., 01 2002. [Cited on page 36.]
- [64] N. I. of Standards and Technology, "Security requirements for cryptographic modules," U.S. Department of Commerce, Washington, D.C., Tech. Rep. NIST FIPS 140-3, 2019. [Cited on page 36.]
- [65] J. Andress, "Chapter 1 - what is information security?" in *The Basics of Information Security (Second Edition)*, second edition ed., J. Andress, Ed. Boston: Syngress, 2014, pp. 1–22. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/B9780128007440000014> [Cited on page 37.]

- [66] "Security and resilience — Business continuity management systems — Requirements," International Organization for Standardization, Geneva, CH, Standard, Oct. 2019. [Cited on page 38.]
- [67] ITGovernance, "The bcm lifecycle: an overview," <https://www.itgovernance.co.uk/blog/the-bcm-lifecycle-an-overview>, 2017, online; accessed 17 September 2021. [Cited on page 38.]
- [68] "Societal security — Business continuity management systems — Guidelines for business impact analysis (BIA)," International Organization for Standardization, Geneva, CH, Standard, Sep. 2015. [Cited on page 38.]
- [69] L. Ngoc and D. Hoang, "Capability maturity model and metrics framework for cyber cloud security," *Scalable Computing: Practice and Experience*, vol. 18, 11 2017. [Cited on page 39.]
- [70] Google, "Google cloud overview," <https://cloud.google.com/docs/overview>, 2021, online; accessed 19 September 2021. [Cited on page 42.]
- [71] Thoughtwave, "What is google cloud platform? its services and advantages," <https://www.thoughtwavesoft.com/what-is-google-cloud-platform-its-services-and-advantages/>, 2021, online; accessed 19 September 2021. [Cited on page 42.]
- [72] i2tutorials, "Explain what flask is and its benefits?" <https://www.i2tutorials.com/explain-what-flask-is-and-its-benefits/>, 2021, online; accessed 19 September 2021. [Cited on page 42.]
- [73] palletsprojects, "Jinja," <https://jinja.palletsprojects.com/en/3.0.x/>, 2021, online; accessed 19 September 2021. [Cited on page 42.]
- [74] Brown, T., "An introduction to the python web server gateway interface (wsgi)," <http://ivory.idyll.org/articles/wsgi-intro/what-is-wsgi.html>, 2021, online; accessed 19 September 2021. [Cited on page 42.]
- [75] SQLAlchemy, "The python sql toolkit and object relational mapper," <https://www.sqlalchemy.org/>, 2021, online; accessed 19 September 2021. [Cited on page 42.]
- [76] Ahsan, M., "How to use python sqlite3 using sqlalchemy," <https://thinkdiff.net/how-to-use-python-sqlite3-using-sqlalchemy-158f9c54eb32>, 2021, online; accessed 19 September 2021. [Cited on page 42.]

- [77] CodeBurst, "Jinja2 explained," <https://codeburst.io/jinja-2-explained-in-5-minutes-88548486834e>, 2021, online; accessed 19 September 2021. [Cited on page 43.]
- [78] F. D. Davis, "Perceived usefulness, perceived ease of use, and user acceptance of information technology," *MIS Quarterly*, vol. 13, no. 3, pp. 319–340, 1989. [Cited on pages 49 and 54.]
- [79] Y. He, Q. Chen, and S. Kitkuakul, "Regulatory focus and technology acceptance: Perceived ease of use and usefulness as efficacy," *Cogent Business & Management*, vol. 5, no. 1, p. 1459006, 2018. [Cited on page 55.]
- [80] V. Venkatesh, M. Morris, G. Davis, and F. Davis, "User acceptance of information technology: A unified model," *Management Information Systems Quarterly - MISQ*, 01 2003. [Cited on page 55.]