Management of Cloud Risk Governance: Analyzing Top Risk Topics and a Maturity Model

Mats Vijverberg (6209815)
Master Thesis Business Informatics
Department of Information and Computing Sciences
09-07-2024

Supervisor:	Nico Brand
2nd Supervisor:	Nishant Saurabh
Daily Supervisor:	Stefanie van Zijtveld

Utrecht University

EY
Building a better working world

Table of Contents

Acknowledgements **5**

Abstract **6**

List of Abbreviations **7**

List of Figures **8**

List of Tables **8**

1 Introduction **9**
1.1 Background 9
1.2 Problem Statement 11
1.3 Research Question 12
1.4 Scope 13
1.5 Objectives 14
1.5.1 Contributions and Relevance 14
1.6 Structure 15

2 Literature Study **15**
2.1 Cloud Computing 15
2.1.1 Cloud Computing Characteristics 15
2.1.2 Cloud Computing Architecture 17
2.1.3 Shared Responsibility Model 20
2.2 Cloud Computing Governance and Risk 21
2.2.1 Cloud Computing Governance 21
2.2.2 Cloud Computing Risk 22
2.3 Cloud Computing Control Frameworks 28
2.4 Capability Maturity Model 29

3 Research Method **30**
3.1 Research Design 30
3.1.1 Conceptual Framework 31
3.1.2 Research Methodology 33
3.1.3 Epistemological Stance 34
3.2 Data Collection 34
3.2.1 Literature Review Design 34
3.2.2 Interview Design 36
3.2.3 Expert Opinion Validation 40
3.3 Analysis Techniques 42
3.3.1 Interview Coding 42
3.3.2 Maturity Model Creation 43
3.4 Methodological Limitations 43
3.4.1 Research Validity 44

4 Managing Cloud Risk Governance 44

4.1 Assessing Cloud Risk Governance 45

4.2 Improving Cloud Risk Governance 47

4.2.1 8 Top Risk Topics 48

4.3 A Maturity Approach on Cloud Risk Governance 54

4.3.1 Characteristics of Each Maturity Level 56

4.3.2 Goal of the Cloud Risk Governance Maturity Model 59

4.3.3 Using the Cloud Risk Governance Maturity Model 60

4.4 Towards Effectively Managing Cloud Risk Governance 61

5 Discussion 63

5.1 Summary 63

5.2 Interpretation 65

5.3 Implication 67

5.4 Research validity 67

6 Conclusion 68

7 Limitations 70

7.1 Future work 70

8 References 72

Appendix A – Code book 82

Acknowledgements

I would like to express my gratitude to those around me who have helped me complete this thesis over the past period. Everyone's critical eye and interest in this work have shaped it into what it is now. Without all the discussions and contributions, I would not have come this far on my own.

I would like to thank Nico in particular for his extensive willingness to think along and ability to work towards the end goal. It is always a pleasure to work and brainstorm together. It took a while to find the right topic at the beginning, but in the end, I think we succeeded. Throughout the entire process, you have guided and helped me where necessary with the greatest flexibility. I hope that we can work together again in the future. I would also like to thank Nishant for his help and guidance. As a second assessor, there is always more distance to the process, but nevertheless, it was always possible to meet up and brain storm together. I could always come to you with my questions, and the collaboration was good. I have found this to be a very pleasant experience.

I would also like to thank Stefanie for her guidance within EY. I always requires some adjustment and learning when writing a thesis at an organization, especially one like EY. You have helped me very well with this and always pointed me in the right direction. In addition, I could also come to you with anything that didn't directly relate to my thesis, which is certainly not a given. I am very much looking forward to our future collaboration! Besides Stefanie, I want to thank the rest of the DR&R team for the warm welcome and the pleasant and especially enjoyable working conditions. This kept me motivated to keep writing and allowed me to finish quickly. I look forward to our collaboration next year.

Once again, thank you to everyone who has supported me during this period!

Mats Vijverberg

Abstract

This research explores the challenges and strategies for effective cloud risk management within organizations. It addresses the complexities introduced by cloud computing, including varying responsibilities with cloud service providers (CSPs), rapidly changing technologies, and the need for alignment among multiple stakeholders. The study also investigates why organizations often struggle with cloud risk governance and how they can gain better control, providing practical, actionable steps. The focus is on the use of public cloud services within large organizations across various sectors, aiming to identify critical challenges and develop effective solutions for cloud risk governance.

A design science approach is used for this research. It begins with a comprehensive literature review to establish a theoretical foundation and identify gaps in current knowledge. This is followed by two phases of structured interviews with subject matter experts to gain insights into practical challenges and effective strategies in cloud risk governance. A third validation phase with experts follows. The collected data is coded to identify key cloud-specific risks and to construct the Cloud Risk Governance Maturity Model.

The research identifies "8 Top Risk Topics" as critical areas for organizations to prioritize. Additionally, it introduces the Cloud Risk Governance Maturity Model, which delineates five levels of maturity characterized by specific criteria across three dimensions.

The study concludes that effective cloud risk governance is achievable through a focused approach on the 8 Top Risk Topics and the application of the Cloud Risk Governance Maturity Model. Organizations can systematically assess their current governance state, identify areas for improvement, and progress towards an optimized level of maturity. The maturity model promotes a security-by-design approach, ensuring all stakeholders are well-aligned and integrating cloud risk governance into the organization's strategy and operational processes. This research contributes to the field by providing a structured framework for organizations to navigate the complexities of cloud risk governance. By implementing insights from the research, organizations can develop a cohesive and effective approach to cloud risk governance.

List of Abbreviations

API	Application Programing Interface
CMM	Capability Maturity Model
COBIT	Control Objectives for Information Related Technologies
CRM	Customer Relationship Management
CSP	Cloud Service Provider
DDOS	Distributed Denial of Service
FaaS	Functions as a Service
GRC	Governance, Risk, and Compliance
HRM	Human Resource Management
IaaS	Infrastructure as a Service
IAM	Identity Access Management
IoT	Internet of Things
ISACA	Information Systems Audit and Control Association
ISO	International Organization for Standardization
IT	Information Technology
ITIL	IT Infrastructure Library
NIST	National Institute of Standards and Technology
PaaS	Platform as a Service
SaaS	Software as a Service
SLA	Service Level Agreements
ToS	Terms of Service

List of Figures

Figure 1: Cloud Reference Architecture 18
Figure 2: Shared Responsibility Model 21
Figure 3: Design Cycle 31
Figure 4: Concept Diagram 33
Figure 5: Heatmap of Risk Topics 49

List of Tables

Table 1: Risk overview 23
Table 2: Section Criteria 36
Table 3: Keywords 36
Table 4: Interview overview 38
Table 5: Interview phase 1 protocol 39
Table 6: Interview phase 2 protocol 40
Table 7: Expert opinion validation protocol phase 3 41
Table 8: Overview of Research Validity 44
Table 9: Cloud Risk Governance Maturity Model 56
Table 10: Cloud Risk Governance Maturity Model recap vertical 65

1 Introduction

1.1 Background

In the past decade, cloud computing has drastically changed how organizations use and view IT due to its continuous rise in usage and popularity. It changes the traditional computing model by offering computing power on a pay-as-you-go basis delivered as a service. The cloud enables a flexible, scalable, and cost-effective way of offering IT to business's needs. The rise of cloud services has reshaped business IT management, including the area of IT risk management. Organizations and governments should understand that accountability and security are shared responsibilities. The Clingendael Institute highlights to European governments the concept of shared responsibility in accountability and security as an area that remains ill-defined, as articulated in a report commissioned by the AIVD (Gomes & Okano-Heijmans, 2024). An absence of specific regulations and controls, sufficient oversight, and knowledge play a significant role in governance issues. A dilemma that continues to escalate with the proliferation of increasingly complex cloud strategies.

Cloud computing governance addresses the multifaceted concept within the broad concept of IT governance. Weill and Ross (2004) define IT governance as *''specifying the decision rights and accountability framework to encourage desirable behavior in the use of IT.''* Within this domain, cloud computing governance focusses on policies, procedures, controls, and technologies that enable organizations to securely leverage cloud services. It addresses critical aspects such as risk management, compliance with regulatory frameworks, data security, and resource optimalization (Al-Ruithe et al., 2019; Amah et al., 2023; Brandis et al., 2019; De Haes et al., 2013; Fortis & Munteanu, 2014; Thuraisingham, 2020). Effective governance includes not only the establishment of policies and guidelines, but also ensures the alignment of cloud initiatives with the overall business strategy (De Haes & Van Grembergen, 2004). The importance is much discussed after the pioneering works of Henderson and Venkatraman (1999) on strategic IT alignment and those of Luftman (2004) with his work on the Strategic Alignment Maturity Model. Both works were inspired by Porter's work on competitive advantage and strategy (Porter, 1985). Organizations have the need to be as competitive and as efficient as possible, which influences their organizational practices, often trading their operational flexibility and efficiency for better governance (Porter, 1985). Without effective governance mechanisms to ensure that cloud deployments support organizational goals, there is a risk of misalignment. Governance can hinder to a point where cloud investments fail to deliver the expected value or support strategic priorities (De Haes et al., 2013). Even more so with cloud computing than with traditional IT, organizations must balance their need for compliancy and agility. Due to the stringent nature of cloud compliance, organizations can be constrained by legal, regulatory, and standards-driven directives (Taft, 2017). Conversely, maintaining flexibility is essential for fostering innovation and optimizing processes. The dichotomy between operational rigidity and operational efficiency highlights the tensions that organizations face in cloud computing. They need to be agile and innovative while remaining compliant with regulations. Effective governance of cloud computing is essential to achieving organizational goals and objectives while mitigating potential risks. As organizations grow, and they become more reliant on cloud computing, the importance of good governance is becoming more apparent. Despite its importance, the ambiguity surrounding cloud governance is increasing (Al-Ruithe et al., 2019).

As a result of the lack of governance, one of the most immediate concerns of inadequate cloud governance is the increased risk to data security and privacy. As with traditional computing, security is considered as one of the highest ranked risks in cloud computing (Aleem & Sprott, 2013; Dutta et al., 2013; Janet Julia Ang'udi, 2023; M'rhaoaurh et al., 2018; Youssef, 2019). This becomes increasingly complex when CSPs are used for different applications. Effective risk governance and compliance with various frameworks is crucial for organizations to maintain control while embracing cloud computing (Chauhan & Shiaeles, 2023). Without clear governance policies and controls, organizations may face vulnerabilities such as unauthorized access, data breaches, and loss of sensitive information. Poor governance can also lead to inefficient use of cloud resources, resulting in increased costs and reduced operational efficiency. To combat this, proper IT governance and compliance measures should be put in place. IT compliance involves ensuring that IT systems aligns with predefined policies, procedures, standards, guidelines, specifications or legal requirements (Brandis et al., 2019). These compliance requirements stem from both internal and external regulations (Hon et al., 2012; Latif et al., 2014). Internal regulations include operating procedures, while external regulations include laws, official regulations, or civil contracts.

Moreover, the cloud's intrinsic attributes already present several compliance challenges, as CSPs often host customer data and computing infrastructure in multiple jurisdictions, each with its own set of rules to comply with leading to regulatory complexities (Papanikolaou et al., 2014). Given its decentralized nature, cloud computing accountability extends beyond organizational boundaries across to service providers, transitioning from what used to be in internal control to a shared responsibility model (Apeh et al., 2023). A CSPs data handling method is typically outlined in a written contract, such as a Terms of Service (ToS) and Service Level Agreements (SLA). These documents define the shared responsibility between the CSP and the customer. However, standards regarding the format, content or expected security and privacy practices for these cloud ToS and SLAs are not universally agreed upon. Depending on the context there can be differences in each contract. This presents difficulties on how cloud can be governed. Organizations must both look from an internal and external governance perspective, where each perspective is concerned about different risk categories (Latif et al., 2014). This is later discussed in Section 2.1.3. Adding to this complexity are the sheer number of industry-specific requirements required in industries such as health care, public sector, insurance and banking, each with its unique set of compliance demands (Jayanthiladevi et al., 2023; Papanikolaou et al., 2014; Taft, 2017).

In addition, organizations frequently adopt a cloud strategy where they are utilizing various Cloud Service Providers (CSPs) to host their IT resources (Varghese & Buyya, 2018). These resources can be hosted on both a multi-cloud or one cloud. A multi-cloud is defined as an approach whereby the user or organization utilize different cloud services for different applications, a multi-cloud strategy may involve the use of several CSPs or a combination of CSPs and private clouds (Hong et al., 2019; Houidi et al., 2011; Petcu, 2013). Organizations may choose a multi-cloud strategy for various reasons, including avoiding vendor lock-in, optimizing for cost and performance, or to satisfy other requirements. Despite the benefits, diversifying CSPs poses more governance challenges due to added complexity. Organizations must manage varying security models, access controls, and compliance frameworks. This scenario increases the potential for security gaps and compliance issues.

These potential risks associated with improper cloud governance underscore the necessity for organizations to develop and implement comprehensive governance frameworks. Such frameworks should holistically address security, compliance, operational efficiency, and strategic alignment. Through recognizing and mitigating these risks, organizations can more effectively harness cloud technologies to realize their business goals while simultaneously protecting against potential threats.

1.2 Problem Statement

Cloud computing is recognized as a pivotal technology in modern organizations, yet a substantial gap in understanding the nuances of cloud risk governance persists. From a practical standpoint, there remains to be ambiguity on how responsibilities may rest both internally within organizations, as well as between the organizations and CSPs. The interplay between internal and external control is difficult due to a low level of standardization and common practices. In addition, there are many different cloud risk and compliance frameworks. The abundance of frameworks make it difficult for organizations to make choices, therefore, the use of the (correct) framework is sometimes overlooked. As cloud technology is generally already a difficult to implement within an organization, the focus is often on the implementation itself rather than on the potential risk of that implementation. Organizations struggle with shifting IT from existing business processes to a cloud environment, because IT products are often linked together. As a result, organizations often have not implemented cloud risk governance. If they use a framework, they also elect to construct and utilize their own custom-build frameworks, potentially intensifying the risk of non-compliance. All the aforementioned factors are magnified, when organizations use a multi-cloud strategy, further complicating the governance process. Regulations might differ between CSPs, and different frameworks may need to be used depening on the application. This hinders organizations in effectively leveraging cloud computing without added risks. Compliance issues can also manifest in increased costs and wasted resources. The added complexity of navigating internal and external compliance might hinder innovation due to the fear of non-compliance. Or, even worse, it puts organizations at risk while being unaware of potentials issues of cloud deployment. Organizations in various sectors are struggling with the challenges of adopting cloud in a way that aligns with their regulatory requirements, most acutely in sectors which are dealing with sensitive personal information such as healthcare and finance (Taft, 2017). The absence of good guidance and tooling presents a barrier for adoption of cloud computing and impacts innovation and competitiveness. Particularly small and medium-sized organizations may have difficulty in digital transformation due to the lack of resources (Johannsen et al., 2020). In addition, it is difficult for organizations to assess how well they are doing. Because of the enormous complexity of existing frameworks, it would be desirable to have a way to measure how current risk governance is performing. A model that indicates risk governance maturity would be of great value in this regard.

While existing literature does address a variety of cloud risk issues, it still falls short within the combined context of holistically addressing cloud governance and mitigation, with a focus on improvement (Bhushan & Gupta, 2017; Djemame et al., 2016; Mohanan et al., 2022; Tabrizchi & Kuchaki Rafsanjani, 2020). Various control frameworks exist but they are often very complex and extensive (De Haes et al., 2013; Di Giulio et al., 2017; Mohanan et al., 2022; Saripalli & Walters, 2010; Xie et al., 2012; Youssef, 2019). In practice, there is a need for an integrated and effective approach that offers a theoretical foundation for understanding the complexities of cloud risk governance while simultaneously enabling organizations to improve their current cloud governance. At this point in time, academic literature insufficiently explore the area of cloud risk management with a focus on improvement. While current existing risk governance models lack empirical validation across diverse organizational contexts (Apeh et al., 2023).

Organizations are not in control of cloud risks, and face challenges in effectively implementing cloud risk governance due to ambiguous responsibility distribution, a lack of standardization, and the complexity of multiple frameworks, which hinders compliance, innovation, and digital transformation. There is a need for an effective way to get a grip on cloud risks and measure and improve cloud risk governance maturity. This research purpose is twofold, it intends to bridge this gap by providing a cross-disciplinary perspective that integrates both the theoretical and practical perspective of risk management and IT governance principles, and offer a solution focused on improvement rather than purely on identifying risks adds to the current academic body. While the study also responds to the practical needs of organizations, as currently existing models are often not easily translatable into actionable steps.

1.3 Research Question

The problem statement highlights a gap in understanding and standardizing cloud risk governance, which arises from complexities organizations face when transitioning to cloud solutions. These complexities can lead to potential business problems, such as business continuity issues due to misconfigured cloud resources. In order to bridge this gap, the aim is to develop a best practice model that addresses minimum requirements and also incorporates a maturity dimension to assess and improve governance. This leads to the central research question:

How can organizations effectively manage their cloud-specific risk governance?

To systematically address this research question, it is helpful to break it down into targeted sub-questions that reflect specific objectives. These sub-questions, derived from the main research question, break down the concept of ‘effectively managing cloud-specific risk governance’ into its components: assessment, improvement, and maturity. Each component targets an aspect of cloud risk governance that helps to address and achieve overall effective management. This approach is inspired by Luftman’s (2004) fundamental work on IT governance. He uses a similar approach in which he poses these three questions to ultimately evaluate IT. The main research question is essentially an evaluation question which is why this approach is borrowed. In addition, each sub-question is accompanied by more questions which help in formulating the research objectives. Each objective relates to the sub-questions and provides a part of the answer. The result of each question is specific enough to be summarized into an interview question or a result in this document.

Sub-question 1

Assessment is a crucial step in managing cloud risk governance. It involves evaluating the current state of an organization’s procedures. To effectively assess an organization, a set of criteria must be selected along which measurements can be made. This results in the following sub-question:

How can organizations assess their cloud risk governance?

The goal of this question is to identify the risk factors which facilitate risk assessments. To answer this sub-question the following objectives should be identified. The objectives are formulated in questions below.

a) What common vulnerabilities are identified during assessments of cloud risk governance?
b) What criteria do organizations use to assess cloud risk governance?
c) What type of cloud is most vulnerable for governance risks?
d) What tools or methods do organizations employ to effectively assess their cloud risk governance?
e) What metrics or indicators are most tracked in cloud risk governance assessments?
f) Who are the stakeholders in cloud risk governance?

Sub-question 2

After completing the assessment phase, organizations must consider how to improve their governance strategies. This involves identifying the key aspects to focus on for effective improvement. The following sub-question describes the best practices that should address the minimum requirements.

How can organizations improve their cloud risk governance?

The best practices outline the approaches organizations should take in form of risk mitigation and control implementation to help the organization improve the cloud risk governance.

a) What is recommended by industry experts for enhancing cloud risk governance?
b) What measures have organizations implemented that led to recognized improvements in cloud risk governance?

Sub-question 3

By incorporating a maturity dimension, it allows organizations to develop an integrated and optimized approach to cloud risk governance. It reflects on the extent to which organizations' cloud risk governance practices are aligned within their organization. The subsequent sub-question provides a maturity aspect to the best practice model. Seeking to not just manage cloud risk governance, but to do so in a systematic way which is aligned with the organizations cloud landscape.

How can organizations achieve mature cloud risk governance?

The maturity aspect enhances the overall usability of the framework by defining the pathway organizations can follow to achieve it, while ensuring that their governance evolves to become a strategic asset.

a) What stages of maturity exist on cloud risk governance?
b) How can a stage of cloud risk governance maturity be achieved?

Together, the three sub-questions provide a structured approach to understanding how organizations can effectively manage their cloud-specific risks. By addressing each sub-question individually and by then integrating them, a robust best practice framework for effective risk governance is created. In Section 3.1.1 a rigorous approach to answering each sub-question is discussed.

1.4 Scope

The scope of this thesis is defined with a focus on specific aspects of cloud computing and risk management. First, the research is limited to examination of public cloud environments. While other types, such as hybrid clouds, might be of similar interest, they are outside the scope of this study. However, it is important to note that results might still be applicable. Second, the thesis investigates all service levels of cloud computing, because the impact of the various service levels on cloud risk governance is not yet understood. Additionally, this study targets organizations that utilize public cloud services and employ at least multiple services across different service levels from CSPs. These organizations must have existing risk management practices. The focus is on relatively large organizations, ensuring that the findings and recommendations of this thesis are applicable and beneficial to organizations that have the capacity to implement the cloud risk governance model. A as rule of thumb, relatively large organizations are defined as those where EY can effectively assist with enhancing there cloud risk management practices. Furthermore, all industries and sectors are considered. This is a consequential decision in the research since it determines the level of abstraction at which the artifacts are developed. It is clear that a much higher level of specificity can be achieved if there is a focus on certain sectors. Specific sectors, such as banking, are subject to stricter regulations and therefore have implicitly different risks.

Moreover, it is important to note that results of this study must always be viewed from a cloud perspective. This is discussed later more detail. What this entails is that a lot of risk topics and the maturity model can be applied to a more broader IT risk perspective. This study will focus on precisely those things that matter the most to cloud, and offer the best solution.

Finally, during this research, the perspective of the consumer is always considered. A customer is the entity that acquires services from a cloud service provider. They are the ones who may face certain risks and could implement certain controls for this. Therefore, all the risks discussed are considered from that perspective. However, the extent of certain risks, which becomes clearer later in the study, is often determined by the CSP. In this case, the customer could, for example, make contractual agreements for this.

1.5 Objectives

The research will examine the effects of the lack of standardization and common practices in cloud governance and risk management in organizations. It will consider the variances of risk management strategies and governance practices. The goal is to identify critical challenges organizations face, as indicated by existing control frameworks and literature. Subsequently, these findings will be ranked by industry experts and integrated into a model with a maturity aspect. This will be done through in-depth interviews with experts. Identified risks include governance risks, such as misalignment with business goals and inadequate accountability; compliance risks, focusing on regulatory and legal issues; and operational risks, including service availability, cost management, and performance. The goal of this study is to develop a comprehensive best practice model which focuses on minimum requirements for effective cloud governance. In addition, the model will incorporate a maturity dimension enabling organizations to effectively manage cloud risk governance.

The research will be conducted in collaboration with EY Consulting, and additionally aims to inform their market positioning regarding cloud risk, governance, and compliance management services. The research will consist of several stages to investigate the research problem, first investigating the current problems, then designing theory to treat the problems, followed by validation of the model. The design science approach, as described by Wieringa (2014), is a fitting approach for the problem, this is discussed in Section 3.1.

1.5.1 Contributions and Relevance

Academic contributions and relevance

This research seeks to fill the gap in understanding how organizations can effectively improve and assess their cloud risk governance. By exploring different cloud risks, a clearer picture can be created of the most complex issues organizations face when business depends on cloud computing. Qualitative insights from industry experts will be valuable for further research. In addition, this study encourages the research in collaboration between IT and business management studies. Also, this study provides more academic foundations for the use of a maturity matrices in cloud computing management. Moreover, this research contributes to a better understanding of the complexities and challenges in the rapidly evolving cloud ecosystem.

Societal contributions and relevance

On the societal level, the research contributes by enhancing the ability of organizations to assess and improve their current cloud-specific governance. The artifacts will serve as a guideline on how to deploy a risk management strategy. It also stimulates awareness on the importance of cloud security, possible leading to more informed decisions and less business disruptions. Currently, many organizations are not in control of their cloud risk. This research can help them gain control, potentially reducing costs and mistakes, and improving efficiency. Given the significance of cloud computing in today's digital age, this research holds substantial societal relevance.

1.6 Structure

The structure of this thesis is as follows: first, Section 2 covers the relevant literature, discussing relevant works on cloud computing, risk cloud governance and risk and compliance frameworks. Section 3 discusses the research method which includes the research design, data collection method, analysis techniques, and methodological limitations. In Section 4, the analysis of the findings is articulated. Results are presented in order of the sub-questions. Section 5, the discussion, starts by summarizing the work, then the interpretation and implication of the study is discussed, and finally there is a reflection on validity. Section 6 presents the conclusion of the thesis. In the final section, Section 7, the limitations and future work is discussed. Supplementary to the main body, the document includes a list of references and appendices.

2 Literature Study

The following section is structured as follows. Section 2.1 discusses related works on cloud computing characteristics, architecture, and responsibility models. This section helps to scope the research. Section 2.2 discusses cloud computing governance and associated risks. Providing an overview of all possible risks as described in current literature. The following Section 2.3 discusses cloud computing risks, and various cloud risk management frameworks. These frameworks are used as a benchmark for implementing a governance structure. Finally, this chapter is concluded by Section 2.4, which discusses the capability maturity model.

2.1 Cloud Computing

2.1.1 Cloud Computing Characteristics

Cloud computing, fundamentally, enables the storage, management, and processing of data over the internet, rather than through local computer systems (Qian et al., 2009). More broadly, it represents a significant shift from conventional on-premises techniques to scalable, virtualized resources available online. It entails delivering IT services through extensive, cost-effective computing units interconnected by IP networks. According to the National Institute of Standards and Technology (NIST), cloud computing is a "computing model that provides ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, serves, storage, applications, and services) that can be rapidly provisioned and released with minimal management efforts or service providers interaction" (Mell & Grance, 2011). This definition has gained wide acceptance. There are five essential characteristics of cloud computing (Gong et al., 2010; Mell & Grance, 2011; Rashid & Chaturvedi, 2019).

The first characteristic is *on-demand self-service*, which means that the consumer can individually provision computing resources without requiring human interaction. The second characteristic is *broad network access*. This means that computing capabilities are available over the network and accessible through standard mechanisms, promoting heterogeneity across various client platforms. The third characteristic is resource pooling. This means that the CSPs computing resources are pooled together to service multiple customers using a multi-tenant model. Now different physical and virtual resources are dynamically assigned to customers according to their current demand. Customers generally do not have control or knowledge over the provided resource. They can however often specify the location of their data. The fourth characteristic is *rapid elasticity*. It means that capabilities can be elastically provisioned and released to rapidly scale inward and outward with demand. This often happens automatically. The fifth characteristic is *measured service*. It means that cloud systems automatically control, optimize, and measure usage of resources. Resource usage can be monitored, controlled, and reported which provides transparency for both the CSP and the customer.

Beyond the five principal characteristics identified by NIST, cloud computing exhibits several supplemental attributes of significant interest (Rashid & Chaturvedi, 2019). Notably, cloud computing benefits from substantial economies of scale, enabling CSPs to offer services at a lower cost relative to on-premises solutions. Another advantage is its enhanced reliability, achieved by utilizing multiple redundant sites, which contributes to the cloud's suitability for business-critical functions. Furthermore, cloud computing is often highly customizable while simultaneously being an one-size fits all solution; it is adaptable to specific business needs while offering standardized solutions that broadly cater to various industry requirements being an all-encompassing solution. CSPs provide an array of services, positioning themselves as comprehensive solutions for a wide range of business operations. Additionally, the flexibility of cloud services allows customers to access these capabilities from any location and through diverse devices, ranging from powerful workstations to handheld devices, effectively democratizing access to substantial computational resources.

Cloud computing offers several advantages over traditional on-premise solutions, yielding mutual benefits for both consumers and providers (Abdalla & Varol, 2019; Dillon et al., 2010; Qian et al., 2009; Sajid & Raza, 2013). For instance, CSPs can meet fluctuating business demands by dynamically allocating more resources when the customer requires it. CSPs achieve lower cost and energy savings by sharing costs among many users. Upfront investment cost, total cost of ownership, and total operational cost is reduced, thereby minimizing associated business risk. Additional benefits include enhanced business resilience due to the improved capability of disaster recovery. In terms of maintenance, responsibilities such as storage and data backup management are shifted to the service provider, offloading these tasks from the consumer.

Of course, cloud computing is not without its drawbacks and challenges. Privacy and data security are often major concerns. Data is often stored in multiple locations across multiple jurisdictions, complicating regulatory compliance. (Papanikolaou et al., 2014). Organizations often do not want sensitive data, such as trade secrets, stored at external partners. Additionally, reliance on third-party service providers for mission-critical IT infrastructure can complicate compliance management (Menasce & Ngo, 2009). Business processes which are critical for operation are often highly regulated, including the IT supporting those business process. Although CSPs are contractually bound by SLAs and are subject to penalties if they do not comply, organizations remain concerned about the implications of outsourcing essential business services.

At present, cloud computing has been widely adapted by businesses ranging from startups to multinational corporations. Cloud computing underpins contemporary business models, and especially those that require agile and rapid adaption to market changes. Gartner projects that by 2028, cloud computing will be an essential component of business operations (Gartner, 2023b). The technology is instrumental in facilitating remote work and virtual collaboration, which have become integral to the functioning of the global economy. There are scarcely any sectors left untouched by cloud computing. Additionally, ongoing advancements in technologies such as artificial intelligence (AI), advanced machine learning, edge, and quantum computing are poised to further unlock automation capabilities (Gartner, 2023a).

2.1.2 Cloud Computing Architecture

The architecture of cloud computing serves as the foundational framework that guides the delivery of services in both individual consumer and enterprise environments. It is a blueprint for the standard technologies, service models, deployment strategies, and operational practices central to the cloud. The conceptual reference model as described by NIST identifies 5 major actors, with each specific activities and functions (Liu et al., 2011). The first actor, the cloud consumer, is an individual or organization that engages in a business relationship with a cloud provider to utilize cloud services. Consumers use SLAs to specify requirements of technical performance. The second actor is the cloud provider, an entity responsible for making cloud services accessible to consumers. Always referred to as a CSP. The next role, the cloud auditor, is an independent entity that conducts comprehensive assessments of cloud services, encompassing evaluations of the cloud service operations, as well as performance and security audits. The cloud broker, the fourth actor in the model, acts as an intermediary that facilitates the delivery of cloud services by mediating between cloud providers and consumers. Lastly, the cloud carrier provides the essential connective infrastructure that enables the transportation of cloud services between providers and consumers.

The framework establishes a widely recognized architecture that defines several roles for the CSPs as a central entity upon which consumers can deploy applications, store data, and use computational power. The CSPs operates in a layered model where each layer corresponds to a specific part of the service delivery. These layers consist of service deployment and service orchestration, both of which are detailed in subsequent sections, as well as cloud service management, and protocols for ensuring security and privacy. The reference architecture is shown in Figure 1, and is adopted from Liu et al. (2011). The reference architecture is useful for understanding the complexities of cloud computing and is foundational knowledge for this thesis.

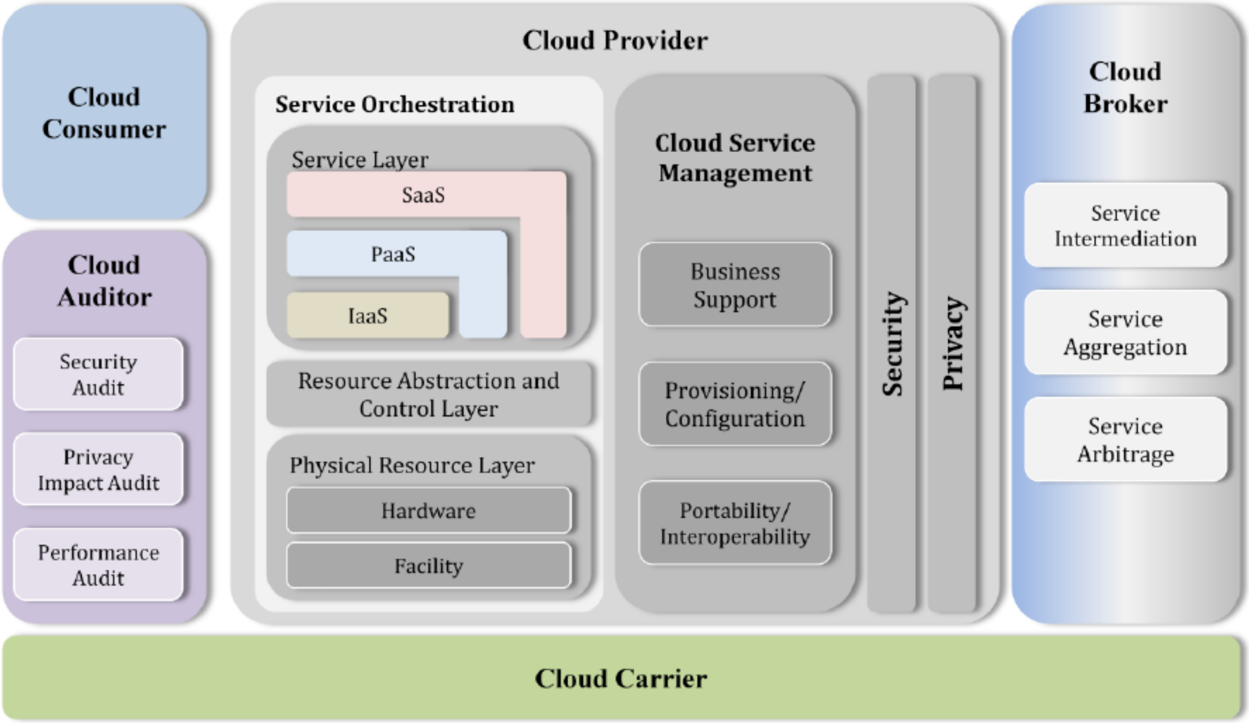


Figure 1: Cloud Reference Architecture

2.1.2.1 Deployment Models

Cloud infrastructure can operate in four different deployment models: public cloud, private cloud, community cloud, and hybrid cloud (Dillon et al., 2010; Gong et al., 2010; Liu et al., 2011; Rashid & Chaturvedi, 2019). These deployment models refer to the specific configuration and environments made accessible to the consumer. The main differences are in the exclusivity of the resources. They define who has access to the infrastructure, the specific controls in place, and the physical location where the services and data are stored. Note that during this research project the scope is limited to public cloud. However, to present a broad and complete picture the other deployment models are discussed as well.

Public Cloud

The public cloud deployment model features resources that are available to the general public over the internet, typically following a pay-per-use pricing structure. These resources are owned and managed by the CSP and are provisioned to multiple users concurrently. The CSP sets the cost structure, which may vary according to the services offered. Public clouds are recognized for their high availability and scalability, making them an attractive option for a wide range of applications.

Private cloud

A private cloud is a deployment model dedicated to a single organization or entity, offering a more controlled environment for cloud services. Whether hosted on-premises or managed by an external service provider, the infrastructure and services of a private cloud are exclusively utilized by the organization it serves. Organizations may favor a private cloud for various reasons, with primary considerations typically focused on enhanced data security and compliance with regulatory requirements. Additionally, the limitation of data transfer to a local context within a private cloud may be a significant concern for some entities.

Community cloud

A community cloud is shared between a group of consumers which usually have a shared concern and objective such as security requirements or policy considerations. This collaborative platform can be hosted by a third-party or internally across participating organizations.

Hybrid cloud

Hybrid cloud deployment is a combination of several other deployment models. Depending on the deployment parts of the application can be in public or private cloud. Usually, the entities remain unique and operate alongside each other. Organizations may opt for a hybrid approach to leverage the expansive resources of the public cloud for certain components of their operations while maintaining sensitive aspects within the secure confines of a private cloud. However, hybrid clouds can present challenges with interoperability, as seamless integration between the diverse platforms is requisite for optimal functionality.

2.1.2.2 Orchestration and Service Models

Cloud orchestration refers to the coordination, arrangement, management and provisioning of cloud system components in order to provide automated cloud resources to customers (Liu et al., 2011). It is often conceptualized in a three-layered model. The bottom layer is the *physical resource layer*, which includes all physical resources such as servers, storage, networking, and all other computing infrastructure, but also facility resources such as electricity, heating, ventilation, and air conditioning. The middle layer is the *resource abstraction and control layer*, which acts as mediator between the physical and service layers. This layer provides and manages access to the physical computing resources through virtualization. Technologies such as hypervisors, virtual machines, virtual networks, and virtual data storage are used to manage flexibility. These technologies are the underlying heart of cloud computing. This software layer ties the numerous different physical layers together and enables resource pooling and dynamic allocation. The top layer is the *service layer*, which is the interface for cloud consumers and provides them with the services. It comprises of three services, Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS), which are all detailed in subsequent sections.

Infrastructure as a Service (IaaS)

Infrastructure as a Service (IaaS) represents the most foundational service model offered by CSP. In this service model, CSPs only offer computing and networking resources over the internet. The CSP is accountable for managing crucial hardware like the CPU, memory, and storage, made available through a virtualized layer. Besides hardware, the CSP is also responsible for providing networking capabilities. Applications and the operating system are excluded from this layer. The primary advantage of IaaS is the flexibility to pay for hardware usage, rather than requiring a large upfront investment. Moreover, the utilization of on-demand resources ensures cost-effective resource usage. Additionally, the cloud provider assumes responsibility for hardware maintenance, which absolves the users of this responsibility. When hosting a private cloud and encountering a middle of the night, critical component failure, an employee would traditionally have to troubleshoot the issue. Additionally, the cloud provider assumes responsibility for hardware maintenance, which absolves the users of this responsibility. However, with a cloud provider, this cumbersome responsibility is taken care of. Examples if IaaS services are Amazons Elastic Cloud Compute or EC2, Microsoft Azure or Google Compute Engine.

Platform as a Service (PaaS)

The Platform as a Service (PaaS) model extends beyond the foundational offerings of IaaS. PaaS encompasses the capabilities of IaaS, including the delivery of computing and networking resources, while additionally facilitating the deployment and management of operating systems and application-specific resources such as databases. Under the PaaS model, the CSP assumes the task of hosting applications, although the development and provision of the applications themselves remain the users' responsibility. Additional services available under the PaaS model include web services, security, and database integration. The users are offered less flexibility in exchange for less responsibility. While PaaS affords users a more streamlined operational role by offloading certain responsibilities to the provider, it also translates to reduced flexibility in configuring the underlying platforms compared to IaaS. This trade-off allows users to focus more on the development and deployment of applications without the complexities of managing the supporting infrastructure. Examples include services like Google App Engine, SAP Cloud Platform, Salesforce Lightning, and AWS Lambda.

Software as a Service (SaaS)

The final layer in the service model is Software as a Service (SaaS). In this service model, the CSP is accountable for both the operation and maintenance of the application. The user has limited control over configuration. However, the user benefits from not having to worry about managing hardware, software, networking, security, databases, or other resources. SaaS is widely used for business applications in many domains including email and communication tools, customer relationship management (CRM), financial management, human resource management (HRM), and more. Prominent examples of SaaS include Wix, Salesforce, Microsoft Office 365, and Google Workspace. On the consumer side some examples are Spotify, Netflix, Zoom, and Adobe Creative Cloud.

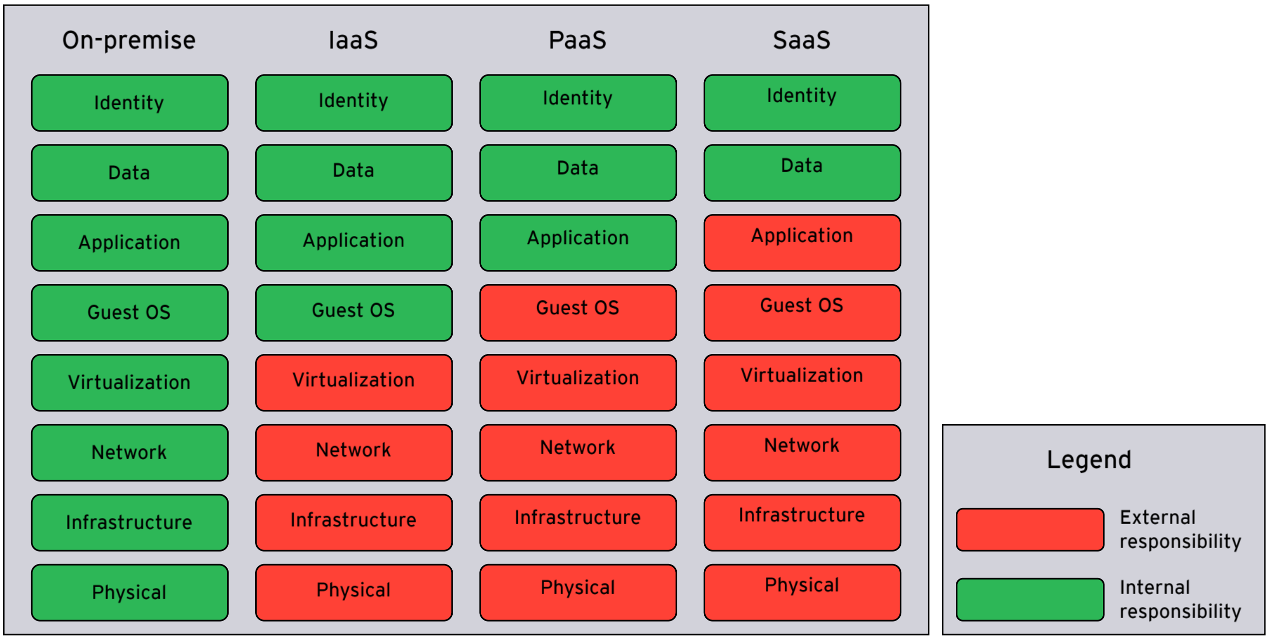
During this study all three service models are discussed and researched. Currently, it is not fully understood if different service models are more likely to have certain cloud risks. Often organizations use SaaS and IaaS or PaaS products simultaneously which makes it difficult to assess them separately in terms of risk. However, different service levels may be more susceptible to certain risks, so understanding the differences is a prerequisite.

2.1.3 Shared Responsibility Model

As adoption of cloud computing increases, control of resources of cloud systems is becoming increasingly complex. Liu et al. (2011) argue that both the cloud provider and the cloud consumer share the control of resources in cloud systems. The shared responsibility model dictates that the cloud provider is responsible for the security ‘of’ the cloud and the consumer is responsible ‘in’ the cloud (AWS, 2024). The cloud providers responsibilities are tied to the infrastructure and regulations that are in place. They are expected to ensure that their platforms are secure and robust against intrusions, and that they offer security and encryption capabilities. Customer’s responsibilities vary depending on the chosen service model (SaaS, PaaS, IaaS). Below the shared responsibility model is depicted in Figure 2. It shows by color whether the CSP or the customer is responsible for managing a particular part of the service. A green color indicates that the customer is responsible, while red indicates that the CSP should take responsibility for managing and maintaining a service. Figure 2 also describes the on-premises situation, describing what needs to be managed compared to a cloud environment. It is interesting to note that cloud providers demand so-called "shared" responsibility. However, it is clear that the responsibility is not shared but divided between a customer and a CSP. For the sake of consistency, the division of responsibilities will be referred to as 'shared' throughout the thesis.

In general, the responsibility for managing and controlling parts of the technology stack is detailed in contracts between the CSP and the customer. However, as shown in Figure 2, there are eight more general levels that can be distinguished (Bennett & Robertson, 2019). With a SaaS service model, customers are expected to manage user access and protect their data within the application. In a PaaS service model, customers are responsible for deploying applications and managing configuration settings. In the IaaS service model, the customer is responsible for managing the operating system, runtime, applications, and data. Regardless of the type of deployment, the customer is always responsible for handling data, endpoints, accounts, and access management (Microsoft, 2023).

Understanding the concept of the shared responsibility model is vital for understanding the impact of certain risks. Some risks are, depending on the service model, always at dependent on the CSP, while others are nearly always at the customer level. Datacenter security, for example, is a risk that the customer can only address through contractual agreements.



On-premise	IaaS	PaaS	SaaS
🟩 Identity	🟩 Identity	🟩 Identity	🟩 Identity
🟩 Data	🟩 Data	🟩 Data	🟩 Data
🟩 Application	🟩 Application	🟩 Application	🟥 Application
🟩 Guest OS	🟩 Guest OS	🟥 Guest OS	🟥 Guest OS
🟩 Virtualization	🟥 Virtualization	🟥 Virtualization	🟥 Virtualization
🟩 Network	🟥 Network	🟥 Network	🟥 Network
🟩 Infrastructure	🟥 Infrastructure	🟥 Infrastructure	🟥 Infrastructure
🟩 Physical	🟥 Physical	🟥 Physical	🟥 Physical

Legend

🟥 External responsibility

🟩 Internal responsibility

Figure 2: Shared Responsibility Model

2.2 Cloud Computing Governance and Risk

2.2.1 Cloud Computing Governance

The imperative need for good governance in business operations has been highlighted by historic events that demonstrated the consequences of poor financial oversight. The accounting scandal of the scandal of the 2000s, which led to major corporate collapses, prompted a new regulatory action such as the Sarbanes-Oxley Act (Coates, 2007). This act not only led to struct reforms to enhance financial disclosures but underscored the wider imperative of sound governance practices across all domains to mitigate various risks. While the focus was on financial institutions, these events precipitated a broader organizational shift. Good governance became much more important, including the domain of IT governance. The importance of good IT governance cannot be overstated, as it has direct impact on the overall performance and strategy of the organization. Weill and Ross (2004), in their research, demonstrate that good It governance allows organizations to make informed decisions on IT investments, enables them to manage risks effectively, and ensures that business operates as efficiently as possible.

Cloud computing governance is another subset of IT governance. It inherits most principles and applies them to cloud computing. It refers to the policies, procedures, and frameworks that organizations implement to manage and mitigate cloud security risks effectively (Amah et al., 2023; Apeh et al., 2023; De Haes et al., 2013; Khalil et al., 2016; Mikkola, 2021; Thuraisingham, 2020). The extra focus on cloud computing governance stems from the unique set of challenges cloud computing poses. These include the dynamic nature of resources, the shared responsibility framework, and data privacy concerns. In comparison with traditional IT governance, within cloud governance, responsibility is shared between the organization and the CSPs. When organizations employ cloud services from multiple CSPs, governance becomes even more challenging. Research shows that most problems related to cloud are related to governance (Al-Ruithe et al., 2019). The most important problem in cloud computing is the lack of expertise and resources (Khalil et al., 2016). Good governance frameworks can provide guidance but they often fall short in user-friendliness and practical effectiveness (Amah et al., 2023).

2.2.2 Cloud Computing Risk

With cloud computing, a risk refers to the potential for loss or damage that may arise when using a cloud service due to the wide range of threats. These threats can affect data, applications, and infrastructure. Cloud risk can stem from various problems such as malicious attacks, legal issues, compliance violations, technical failures, or inefficient management practices (Alouffi et al., 2021; Dutta et al., 2013; Farrell, 2010). Cloud risk is formally defined as an unexpected impact on the confidentiality, integrity, and availability of the cloud service (Albakri et al., 2014). An example of cloud risk materializing is when organizations experience data exposure due to a security breach at a cloud service provider.

To attain a comprehensive understanding of cloud risk, it is essential to understand the general definition and concepts. A risk is commonly defined as a possibility of an adverse event occurring that causes harm or loss (Youssef, 2019). Risk analysis can be done manually, although there are some researches who specify the need for an automated approach (Albakri et al., 2014; Saripalli & Walters, 2010; Sendi & Cheriet, 2014). In a structured approach as defined by ISO/IEC 27005 (2022), such as with risk assessment frameworks, several key elements are defined:

1. Threat: Threats and sources should be identified. They can be natural or human-caused, accidental, or deliberate. Threats can result in damage to the system or harm the organization.
2. Vulnerability: A vulnerability is a weak point that can be exploited by a threat, potentially imposing harm upon the asset or organization. Unless there is no risk, a vulnerability has a corresponding threat, or it is exploited.
3. Asset: Defined as anything that has a value to the organization. Both information and business processes are considered as primary assets. Hardware, software, network, personnel, site, and organizational structure are considered supporting assets.
4. Likelihood: The likelihood, or the probability is the estimate of how often a threat might exploit a vulnerability which affects an asset. The estimation can be based on historic data, statistical analysis, expert judgement, or a combination of these elements.
5. Impact: Impact is the measure of harm that would be caused if the threat successfully exploits the vulnerability. The impact can be quantified in terms of financial loss, reputational damage, or operational disruption among others.

6. Risk Level: A combination of the likelihood and the impact. Risks with a high-risk rating are often given a higher priority.
7. Control measure: These are strategies, procedures or mechanisms put in place to minimize or eliminate the risk. Effective control measures reduce either the likelihood, the impact, or both.
8. Residual risk: After implementing controls there is often some level of risk remaining, this is the residual risk. This risk is often accepted by an organization on continuously monitored.

According to Dutta et al. (2013) cloud risk can be categorized into four different concepts.

1. Technical or Security Risk: This category contains the risks associated with data quality or integrity, data maintenance, system performance, system integrity or data security. The manifestation of such risks can result in service disruptions or unauthorized access. Distributed Denial of Service (DDOS) attacks can lead to a lack of service availability, or poorly functioning applications can lead to escalated costs.
2. Compliance or Organizational Risk: These risks have considerable implications on various organizational facets, including IT governance, compliance adherence, and vendor lock-in. Additionally, there are challenges in business continuity and resilience due to discontinuing services of CSPs, risk planning and risk management, and supply chain failure.
3. Operational Risk: Risks in this domain involve issues related to SLAs, financial complications, or resistance from users. Operational risks may also stem from a deficiency in knowledge or training, poor service availability due to insufficient resource allocation, and other functional bottlenecks.
4. Legal Risk: Legal risks encompass concerns such as violations of data privacy due to failing architecture that should protect user data, different data protection laws in various jurisdictions, legal disputes between enterprises and CSPs, or inadequate contractual agreements that fail to encapsulate the full scope of SLAs.

Within each category there are many specific risks which can lead to business problems. Various authors write about risks, but they do not all overlap (Chao & Baptista, 2009; Sharma et al., 2021; Singh & Pandey, 2014). However, we opted to follow the approach as described by Dutta et al. (2013) The Table 1 below summarized risks both from frameworks and common academic literature. The Table 1 is a list of risk topics accompanied by a description. Each risk topic is put into a category as defined by Dutta et al. (2013) and the source is also cited. The various risk topics are gathered from a variety of sources which are found using the search protocol described in Section 3.2.1.1.

Table 1: Risk overview

Risk category	Risk topic	Description	Source
Technical Risk	Endpoint security risks	Compromised endpoints refer to devices that have been infiltrated by attackers. This can serve as a gateway to a cloud environment for further attacks, data theft, and spreading of malware.	(Cayirci et al., 2016; Cloud Security Alliance, 2024; Hendre & Joshi, 2015; International Organization for Standardization, 2015)
	Account security risks	Account security refers to the threat of hijacking a tenant. Unauthorized access can lead to data loss and configuration loss. Account security is also concerned with bad	(Cayirci et al., 2016; Hendre & Joshi, 2015; Irfan et al., 2015; Subramanian & Jeyaraj, 2018)

		password policies.	
	Data interception risks	Data interception refers to unauthorized access to data during transmission. This can result in confidential information being exposed or tampered with, compromising privacy. As such this risk is similar to privacy issues.	(Cayirci et al., 2016; Dutta et al., 2013; Irfan et al., 2015; Subramanian & Jeyaraj, 2018)
	Data deletion risks	Improper data deletion occurs when data is not completely removed from systems or storage devices. An issue which is more present in cloud environments due to the easy spread and multiplication of data. This issue is also related to privacy.	(Cayirci et al., 2016; Dutta et al., 2013; Irfan et al., 2015)
	Data leakage risks	Data leakage involves the unauthorized transmission of data from within an organization to an external destination. Often a result of improper encryption, or identity access management.	(Cayirci et al., 2016; Dutta et al., 2013; Hendre & Joshi, 2015; Irfan et al., 2015; Subramanian & Jeyaraj, 2018)
	Sprawling risks	Sprawling risk arises from the uncontrolled expansion of IT resources, making it difficult to manage and secure the infrastructure effectively. This can lead to inefficiencies, increased costs, and security vulnerabilities.	(Jayanthiladevi et al., 2023; Tracy, 2016)
	Infrastructure failure risks	Infrastructure failure occurs when the physical or virtual components of a system fail, causing service outages. Leading to service disruptions. This issue is not caused by the customer but by the CSP.	(Cayirci et al., 2016; Cloud Security Alliance, 2024; Dutta et al., 2013, 2013; International Organization for Standardization, 2015; Irfan et al., 2015; Subramanian & Jeyaraj, 2018)
	Service availability risks	Service availability risks arise from attacks on the platform or CSP outages. An example would be a denial of service attack which leads to temporary service outage.	(Cayirci et al., 2016; Cloud Security Alliance, 2024; Dutta et al., 2013; Hendre & Joshi, 2015; Irfan et al., 2015)
	Encryption risks	Refers to any issues with encryption of data. Often it is not enabled at some services.	(Cayirci et al., 2016; Cloud Security Alliance, 2024; International Organization for Standardization, 2015)
	API security risks	Insecure APIs can be exploited to gain unauthorized access to systems and data connected to the cloud environment. Often due to human error or update issues. APIs often link multiple cloud environments together, now one weak link can cause trouble across the entire environment.	(Cloud Security Alliance, 2024, 2024; Hendre & Joshi, 2015; International Organization for Standardization, 2015; Irfan et al., 2015; Subramanian & Jeyaraj, 2018)
	Data loss risks	Data loss refers to the unintended destruction,	(Cloud Security Alliance,

		corruption, or deletion of data. For example by not managing archiving correctly, which is easily done in cloud environment.	2024; International Organization for Standardization, 2015; Irfan et al., 2015; Subramanian & Jeyaraj, 2018)
Organizational Risk	Vendor lock-in or lock-out risks	Dependency on cloud provider due to need for specific products or services. Can limit flexibility and increase costs.	(Cayirci et al., 2016; Dutta et al., 2013)
	Cloud-specific governance risks	Lack of specific cloud governance means inadequate policies and procedures for managing cloud resources. This can lead to various governance related issues.	(Cayirci et al., 2016; Cloud Security Alliance, 2024; Dutta et al., 2013; International Organization for Standardization, 2015)
	Third-party management risks	Involves issues of contractual agreements. Relating to issues between the cloud provider and customer. Often caused by issues between intermediaries and the customer.	(Cayirci et al., 2016; Cloud Security Alliance, 2024; Dutta et al., 2013; International Organization for Standardization, 2015; Irfan et al., 2015)
	CSP termination or acquisition risks	CSP termination or acquisition can disrupt services, leading to migration challenges, and increased costs.	(Cayirci et al., 2016; Dutta et al., 2013)
	High value concentration risks	High value concentration occurs when critical data or functions are concentrated in a single location or provider, increasing the impact of any failure or breach. This can lead to significant operational and financial risks. Especially true for the three large CSP's.	(Irfan et al., 2015; Subramanian & Jeyaraj, 2018)
	Business continuity risks	Business continuity involves the disruptions caused by cloud dependency.	(Cayirci et al., 2016; Cloud Security Alliance, 2024; International Organization for Standardization, 2015)
	Cost risks	Cost issues refer to the financial challenges associated with cloud adoption, including unexpected costs, budget overruns, and poor cost management.	(Cloud Security Alliance, 2024; International Organization for Standardization, 2015)
	Lack of cloud specific knowledge	Lack of cloud-specific knowledge involves insufficient expertise in managing and securing cloud environments. This can lead to misconfigurations, security risks, and operational inefficiencies.	(Dutta et al., 2013)
	Threat management risks	Threat management involves identifying, assessing, and mitigating cloud specific threats. Improper management can lead to various issues.	(Cayirci et al., 2016; Cloud Security Alliance, 2024; International Organization for Standardization, 2015)

Operational Risk	Natural disaster risks	Natural disasters such as earthquakes, floods, and hurricanes can physically damage data centers, leading to service outages and data loss.	(Cayirci et al., 2016; Dutta et al., 2013)
	Human resource risks	Human issues include errors, negligence, or malicious actions by employees on cloud specific problems.	(Cayirci et al., 2016; Cloud Security Alliance, 2024; Dutta et al., 2013; International Organization for Standardization, 2015; Irfan et al., 2015)
	Datacenter security risks	Datacenter security involves protecting physical and virtual components of data centers from unauthorized access and threats.	(Cayirci et al., 2016; Cloud Security Alliance, 2024; Dutta et al., 2013; International Organization for Standardization, 2015)
	Logging risks	Improper logging can result in incomplete or inaccurate records of cloud systems. This can hinder compliance efforts or security. Proper logging is not always enabled by default at CSP's.	(Cayirci et al., 2016; Cloud Security Alliance, 2024; International Organization for Standardization, 2015)
	Malicious insiders	Similar to account security risks, but from inside actors. Will continue to be considered as a single topic.	(Cayirci et al., 2016; Hendre & Joshi, 2015; Irfan et al., 2015; Subramanian & Jeyaraj, 2018)
	Change management risks	Poor change management on cloud specific systems can lead to system downtime, security vulnerabilities, and operational issues.	(Cloud Security Alliance, 2024; International Organization for Standardization, 2015)
	Identity access management risks	Identity access issues involve challenges in managing user identities and access permissions. Inadequate controls can lead to unauthorized access, data breaches, and compliance violations. Often problematic due to the number of access controls.	(Cayirci et al., 2016; Cloud Security Alliance, 2024; Dutta et al., 2013; International Organization for Standardization, 2015; Irfan et al., 2015)
	Privacy risks	Combination of several technical risks but also no knowledge about what is seen as critical information. Privacy issues arise from the mishandling of personal or sensitive information.	(Cayirci et al., 2016; Cloud Security Alliance, 2024; Dutta et al., 2013; International Organization for Standardization, 2015)
Legal Risk	Laws and regulations risks	Non-compliance can result in legal actions and fines. Breaking the law by mismanagement is highly problematic.	(Cayirci et al., 2016; Dutta et al., 2013)
	Changing jurisdiction risks	Changing jurisdiction involves dealing with different legal and regulatory requirements when data crosses national borders. This can	(Cayirci et al., 2016)

		complicate compliance efforts and expose the organization to legal risks. Often an issue in cloud environment due to the ease of data replication and processing in varying jurisdictions.	
	Licensing risks	Licensing rules pertain to the legal use of software and technologies. Violations can lead to legal penalties, financial losses, and operational disruptions.	(Cayirci et al., 2016; Dutta et al., 2013)
	Intellectual property risks	Intellectual property risks involve the theft or unauthorized use of proprietary information. Can lead to issues since data is stored at other organizations.	(Dutta et al., 2013)
	Due diligence risks	Insufficient due diligence involves inadequate assessment of cloud specific issues. Similar to compliance risks.	(Cloud Security Alliance, 2024; Dutta et al., 2013; Hendre & Joshi, 2015; Subramanian & Jeyaraj, 2018)
	Compliance risks	Compliance issues arise when an organization fails to adhere to cloud specific regulatory requirements and industry standards. Also inadequate internal control.	(Cayirci et al., 2016; Cloud Security Alliance, 2024; Dutta et al., 2013; International Organization for Standardization, 2015; Subramanian & Jeyaraj, 2018)

In view of the cloud shared responsibility model, cloud risks can be segmented into internal and external risks. Internal risks originate from within the organization and often result from inadequate policies. With effective governance there is a possibility to mitigate those risks. Contrastingly, external risks are risks that originate from outside the organization, such as disruption in service availability. These risks can be even more devastating to operation than internal risks.

There are various surveys which underscore the high potential risks with cloud computing, with particular concern for data security and the necessity of robust encryption measures (Aleem & Sprott, 2013; Dutta et al., 2013; Janet Julia Ang'udi, 2023; M'rhaoaurh et al., 2018; Youssef, 2019). These surveys also articulate the importance of maintaining data integrity, ensuring that data is kept reliable and unchanged over the course of its existence. Vendor lock-in is identified as a significant risk, typically occurring when organizations gradually build more applications on a platform and do not know which services are tied together. They become heavily reliant on a single platform's service, leading to difficulties when transitioning to different CSPs. The dynamic nature of cloud computing introduces complexities in identity access management (IAM), necessitating fine-grained access controls and strict policy enforcement to thwart unauthorized access. Moreover, the operational availability of cloud services can be jeopardized by Distributed Denial of Service (DDoS) attacks, which are intentionally orchestrated by malicious entities.

Good governance is integral to managing risks effectively. It incorporates strategic planning, policy development, and continuous monitoring from all multiple stakeholders to create a robust risk environment. Proper governance ensures that risks assessments are carried out and that policies are enforced. Cloud strategies should be aligned with business objectives while compliance with legal and regulations are maintained.

As part of the study the risks, as presented earlier in the list above, are all discussed. During the later stages of this study, the risks are used and ranked. The table above shows what exactly the risks entail, and where they originate from.

2.3 Cloud Computing Control Frameworks

Regulatory compliance is built upon an array of legal frameworks, security practices, and data protection regulations. To help organizations achieve and maintain compliance, structured guidelines, best practices, and security controls need to be put in place. Collectively these are called cloud security frameworks. Cloud security frameworks are created to assist organizations in their understanding of vulnerabilities and consists of a collection of rules, standards, and best practices (Chauhan & Shiaeles, 2023). Many different regulatory frameworks exist, each with its own focus and purpose. Frameworks such as ISO/IEC 27017, COBIT, NIST, and CSA CCM, although differing in scope, share a common goal. Depending on the application and environment of an organization different frameworks might be useful. The scope and complexity of frameworks determines their applicability at varying organizations. Most commonly, they offer security measures that align with regulatory requirements, provide methodologies to identify, assess, and mitigate cloud-specific risks, and provide guidance for governance. Di Giulio (2017) compares several frameworks and finds that some frameworks include more controls than others but overall they provide similar guidance. This highlights the importance of a good selection approach when needing to implement a cloud security framework. There are several other frameworks such as FedRAMP or Cis Controls but only the aforementioned frameworks are discussed in this section.

ISO/IEC 27017

The ISO/IEC 27017 is an international standard that provides guidelines on information security specific to cloud computing (International Organization for Standardization, 2015). It builds on the ISO/IEC 27002 standard by extending the controls to address some cloud-specific issues. The standard adds some specific controls to cover areas such as data encryption, access control, and operation security. In contrast to other non-cloud-specific frameworks, this standard recognizes responsibility of both the CSP and the customer, who share responsibility.

COBIT 5

COBIT 5 is a framework that is developed by the ISACA (Information Systems Audit and Control Association) and provides guidelines, practices, and an analytical tool to help organizations ensure IT is aligned with business and compliant with regulation (ISACA, 2012). COBIT 5 is generally more IT governance focused with a broad stakeholder focus and risk focus. It helps organizations align with business goals and improve risk management.

NIST SP 800-144

This framework provided by the National Institute of Standards and Technology (NIST) provides a comprehensive overview of privacy and risk considerations specific to public cloud computing (Jansen & Grance, 2011). Compared to all other frameworks, NIST is much more focused on privacy and security aspects instead of governance compared to other standards such as COBIT 5 and ISO/IEC 27017. The standard delves in the specific challenges of data privacy at a public cloud, covering specific threats and vulnerabilities. The guidelines emphasize a risk-based approach to security and privacy which includes considerations for lifecycle management, IAM, and incident management.

CSA-CCM

The CSA-CCM framework is a control framework for cloud computing which is designed to provide the fundamental security principles to guide cloud customers (Cloud Security Alliance, 2024). It is aimed at helping both CSP and customers understand the security and risks of cloud coverings. It features an extensive list of controls for various relevant cloud computing domains. It aligns well with the ISO/IEC 27017 standard and NIST SP800-144 framework. The framework provides a structured approach for identifying risks and implementing controls within an organization. Moreover, the framework includes a questionnaire which maps certain questions to risk values. It is used by various researchers for other models (Cayirci et al., 2016). It is one of the most popular control frameworks for cloud.

2.4 Capability Maturity Model

The Capability Maturity Model (CMM) serves as a tool for assessing and improving the process maturity of an organization (M. C. Paulk et al., 1993). It can be used in varying contexts such as software development, but also IT governance and integration, or project management (Aguiar et al., 2019; Carcary, 2013; Le & Hoang, 2017; M. Paulk, 2002). The CMM framework is designed to help organizations enhance their processes in a systematic way. It works by defining a series of detailed levels, each representing a different degree of maturity. IT responsibility often lies with management, who benefit the most from maturity models for effective improvement (Becker et al., 2009). The framework describes a path from ad hoc processes to mature and continuously improving processes. The goal of the framework is to help organizations increase their efficiency and effectiveness in certain operations. The CMM outlines the following 5 levels of maturity:

1. Initial (Level 1): At this level, processes, IT governance, and risk management are often in an undocumented state. Success and proper management are often by virtue of individual efforts and successes. This level often leads to inconsistency and poor quality. At this level risk management is often overlooked (Carcary, 2013).
2. Managed (Level 2): Organizations begin to establish basic principles and management practices, including the documentation of processes and risks. The introduction of the first lead to improved and more repeatable outcomes.
3. Defined (Level 3): At this level a shift occurs from process or technology specific control to an organization wide control. Planning, documentation, and standardization are becoming commonplace. Processes are starting to get integrated into a coherent system, or control set.
4. Quantitatively Managed (Level 4): From this point, organizations are starting to leverage data to assess performance. Controls are in place and governance is properly managed. An alternative name for this level is controlled. Since this name is more fitting for this study, that will be used.
5. Optimizing (Level 5): The final maturity level is characterized by a continuous process of improvement. Organizations are able to leverage data to drive improvement. They continuously adapt to changes, challenges, and opportunities.

Implementing a CMM framework involves assessment of the current process against the criteria set by the model. In general, organizations progress through the maturity levels by developing a sophisticated process management and governance structure. The longer organizations work with certain technologies the higher the level might be. It is however not easy for organizations to progress though the levels due to a lack of knowledge, resistance to cultural change, and the potential for high resource and time allocation (M. Paulk, 2002).

In this research, the CMM framework will be adopted to integrate a maturity aspect for the assessment of effective cloud risk governance. A control based perspective is used, where the level of awareness, and control process are considered as levels for maturity. The construction of the maturity model is discussed in Section 3.3.

There are three different approaches to making a maturity model (Pöppelbuß & Röglinger, 2011). The first is descriptive, which will be used for this study, and focuses on an as–is assessment of the entity under study. The second serves a prescriptive purpose, used to identify a desirable maturity level and with guidelines. The third, a comparative maturity model, allows for benchmarking. During this study the descriptive maturity model is developed, with the ability to extend the model to a prescriptive model. The model will provide a detailed description of current practices, and maturity level within the organization, but not specific guidelines for reaching a higher level. However, many recommendations can be derived from the current state and other maturity levels.

The descriptive maturity model is used since it only requires criteria and no improvement measures. This is outside the scope of the study. The descriptive maturity model has a definition of the maturity dimensions, a definition of the application domain, offers basic explanation. Moreover, it has verifiable criteria for each maturity level (Röglinger et al., 2012). This is satisfactory for the current goal of this study. Various other works serve as examples for this study (Akinsanya et al., 2020; Cano M., 2023; Katz, 2023; Le & Hoang, 2017; Röglinger et al., 2012).

3 Research Method

3.1 Research Design

This section outlines the research methodology employed to examine cloud risk governance. The chosen method and framework help to explore the challenges organizations face when managing cloud services. Wieringa's Design Science Cycle offers a structured methodological approach for conducting research that bridges the gap between theoretical and practical problems (Wieringa, 2014). The cycle is useful for designing, creating, and evaluating treatments and artifacts to solve real-world problems. Within the realm of IS research, an artifact is something that is created such as models, frameworks, or systems. A treatment is the interaction between the artifact and the problem context. The complete design science cycle which consists of five steps, is called the engineering cycle. It is a rational problem-solving process which consist of the following steps: problem investigation, treatment design, treatment validation, implementation, and evaluation. Design science in IS research is often restricted to the first three tasks when designing for real-world problems. From the perspective of external stakeholders, the design cycle does not produce an implementation. An implementation would be an actual prototype and result, while only an artifact will be developed. Thus, this research will only focus on the first three phases of the engineering cycle which are called the design cycle.

The initial phase, problem investigation, involves defining the specific issue and gap in the current knowledge base. The environment in which the problem exists is analyzed together with the stakeholders. The goal of the problem investigation phase is to prepare for designing of an artifact. The second phase, treatment design, focusses on development of the artifact, which usually is a model, method, framework, or system in the context of IS research. It consists of two steps, the first is conceptualization where a good theoretical understanding and foundation is built, and the second, design development, where the artifact is created. The third, and for this research final phase, treatment validation, is concerned with reviewing the created artifact. It is compared against existing knowledge and reviewed by subject matter experts. The effects of the artifact are compared against the problem context to see if it contributes to the stakeholders' goals. This cycle is repeated until the results are satisfactory. The design cycle is displayed in Figure 3.

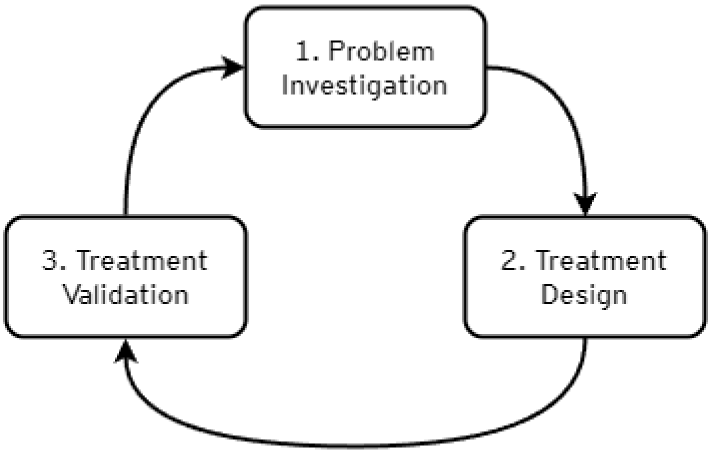


Figure 3: Design Cycle

In the subsequent sections the research design, including the research method, data collection strategies, and analysis techniques will be discussed.

3.1.1 Conceptual Framework

Each phase within the design science cycle comprises a series of methodical steps and expected deliverables, as proposed in the conceptual framework. This framework provides an overview of artifacts and research methods, and the connection between the two. It consists of three phases which are discussed in the subsequent sections below. The reporting phase is also depicted in the model. This conceptual model follows the guidelines as proposed by Verschuren and Doorewaard (2010).

Problem investigation phase

During the first phase, problem investigation, three primary parts are composed: the conceptual model, which articulates the context and outline of the thesis with logistical and practical aspects, and the research objectives, which contains the problem context, background information on the topic, and research questions, and the research strategy which contains the choice of research methods and justification in terms of the research objectives and questions. These parts are merged and part of this thesis.

At the start of the research, it is important to set up a conceptual plan that outlies how the rest of the research will proceed. Good research always starts with strong research questions. To clearly understand the current issues within organizations in terms of cloud risk governance, various professionals at EY are interviewed. Several relevant problems emerge from the interviews, which, combined with the initial literature study, leads to the current research questions.

The preliminary literature study begins with an investigation into the most relevant and influential works in the current academic context. As outlined in Section 3.2.1, through using the snowballing method, other related literature was found. In the process an overview of all literature was created incorporating the title of the research, the authors, and key information regarding the discussed topics of each academic work. The key information consisted of a short recap and labels based on the expected contribution to the complete literature overview. The semi-systematic search protocol is detailed in subsequent sections. The goal of this literature review is twofold: first, all current issues are compared to all identified issues in literature, thereby creating an overview of all potential difficulties of cloud risk governance within organizations. Not all problems documented historically maintain their significance over time, nor are all organizations necessarily cognizant of potential emerging risks. Creating a comprehensive overview is therefore critical. Second, the review explores existing literature for possible solutions determining their effectiveness. Or if solutions are non-existent, the gaps where solutions have yet to be proposed are identified. Then, it can be determined what the important aspects of good cloud risk governance are. Comparing different regulatory frameworks offers the opportunity to assess which problems are more or less important in certain contexts, offering valuable insights for the subsequent steps. The results of this study are in Section 2.

The problem statement and research questions are derived from this literature review and the initial interviews. During the next phase the first solution to the research problems are formulated by expanding the literature review and doing more interviews. The problem statement is discussed in the Section 1.5.

Treatment design phase

The second phase, treatment design, consists of several steps leading to the first draft of the cloud risk governance assessment model. The first step, which is still part of the literature review, is to answer sub-questions SQ1-A and SQ1-B. These results provide the relevant information necessary to conduct the next interview. Sub-questions SQ1-A and SQ1-B provide a list of cloud risks or cloud risk capabilities. During the interviews, the process of which is described in Section 3.2.2, various questions are asked to gather evidence for sub-questions SQ1-C through SQ1-F. Information from the interviews is extracted through content analysis, which is described in Section 3.3.1. The actual artifact is then designed using the data from the interviews. In the next round of interviews, the maturity aspects are discussed through questions about how organizations can improve their cloud risk governance. As the sub-question SQ2 is answered, more desk research is done to construct a maturity aspect on the cloud risk governance assessment model. Then, another round of interviews is conducted to discuss and verify the maturity aspect on each risk capability. The interviews are coded again, and the first concept of the cloud risk governance maturity model is constructed.

Treatment validation phase

Upon creation of the model the third and final phase, treatment validation, begins. The validation process consists of two steps: initially, findings are verified with subject matter experts on cloud risk outside EY. These expert interviews delve into their perspectives on the most critical cloud risk issues that require organizational attention. Moreover, the experts contribute to refining the proposed maturity levels and the characteristics of associated with each one. Subsequently, the model undergoes further review and evaluation through a case study. This case study is performed at an external organization to primarily test the maturity aspect of the model, but also verify the assessment model. This data is essential for analyzing the effect of the different levels. It is important to note that the design cycle includes a recursive element, represented by the green arrow in Figure 4, whereby artifact design and validation phases are repeated until they no longer necessitate any modifications. At that point the definitive models are constructed.

Reporting

The final step in the process is the reporting of the findings. All results will be processed and described in the thesis. The thesis is constructed in a scientific manner and therefore does not necessarily contain the results in the order as defined by the conceptual framework.

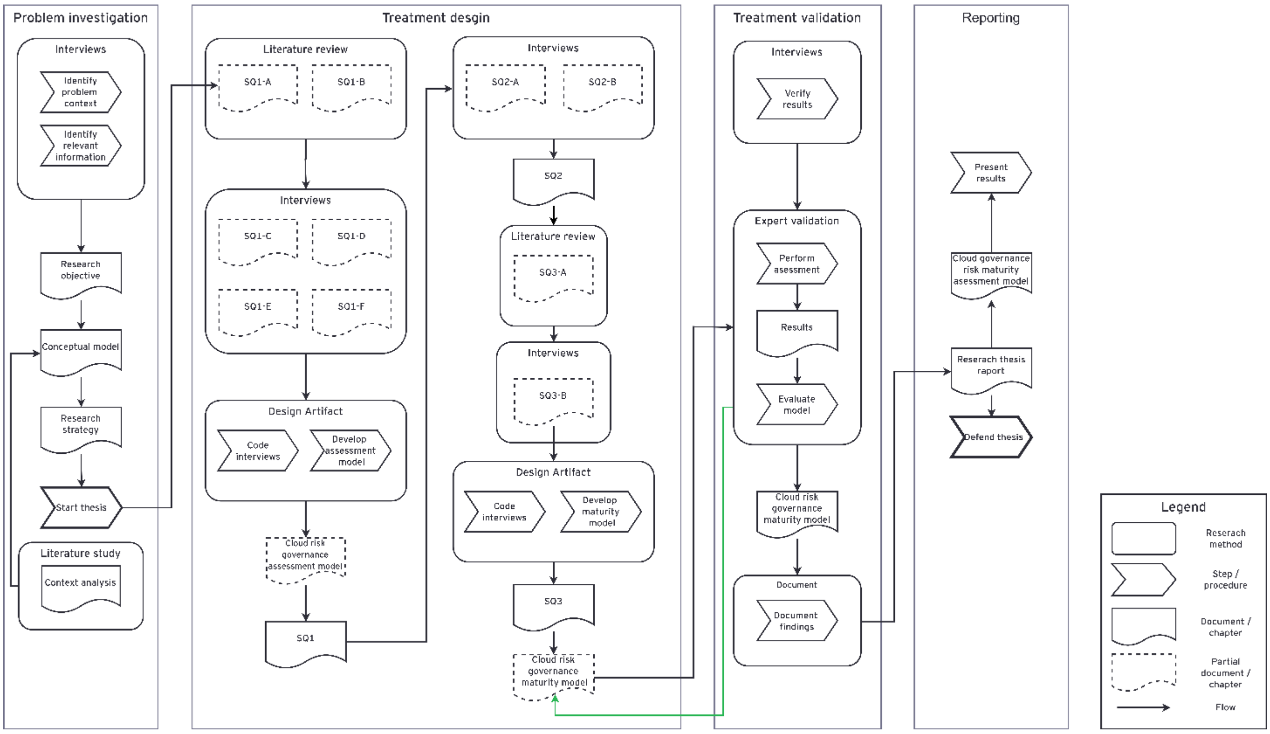


Figure 4: Concept Diagram

3.1.2 Research Methodology

As previously discussed, the primary research technique employed is design science. In this section, the usage of this methodology is justified. During the design and validation phases, other qualitative techniques were also utilized. To create the artifact, a literature review was conducted together with interviews. Interviews offer the ability to capture more unstructured data, which is imported in early exploratory phases of the research. When designing the artifact theoretical knowledge is often not available but practical knowledge is. Interviews help in discovering new areas of knowledge creation due to their free format and allow for easy deep diving into experiences. The interviews are coded and analyzed in a mostly deductive manner. The interview questions focused on gathering specific data about the current cloud risk governance landscape, and interviewees were asked to rank existing risk categories on online whiteboards. After coding the interviews, a thematic analysis is performed on the data. This involved identifying patterns and themes that emerge from the coded interviews and whiteboards. The thematic analysis helps in constructing the artifact by providing the practical insights not available from literature.

3.1.3 Epistemological Stance

This research adopts a pragmatic epistemological stance, which supports the application of design science research (Iivari, 2005). Pragmatism emphasizes the practical outcomes and the value of solutions in addressing real-world outcomes. This epistemological stance aligns well with the objectives of this study for assessing and improving cloud risk governance in a broad organizational context. This stance can be applied for all research questions. By bridging the gap between theory and practice, this research aims to develop knowledge with an emphasis on creating knowledge that is tangible for all stakeholders in this research. Additionally, an interpretivist perspective is adopted to gain a deeper understanding of the subjective experiences and meanings that individuals associate with their interactions with cloud risk governance processes. Design science fits well with this approach (Becker & Jörg, 2006). There is also a focus on the generalizability of the results, ensuring that the findings are applicable beyond the current context this research. The current context is defined by not only the scope of the research but also the environment. For examples, think of the country, research institute and host organization. A clear understanding of the impact of the research methods used is crucial, as it influences the reliability, validity, and impact of the study's conclusions. In information system research, design science is not value-free, meaning it always has some interpretive and even critical orientation (Iivari, 2007). This should be accounted for when evaluating the implications of the work. By evaluating these approaches and doing detailed reporting, the research aims to provide nuanced understanding of cloud risk governance, contributing valuable insights to the field.

3.2 Data Collection

Two primary data collection techniques were used, and this section outlines how they were performed. The first technique is data collection form a literature study, the second is from interviews. The literature study is found in Section 2, and explained in the section below. The interviews were done in three stages, the first being subject matter expert interviews, and the second expert validation interviews.

3.2.1 Literature Review Design

In scholarly research, literature studies are central to developing a comprehensive understanding of a given topic, aiming to establish a robust foundation and identify existing academic gaps. They serve a dual purpose: offering a theoretical baseline for the proposed study and aggregating the collective knowledge on the subject. Literature reviews can be conducted through two primary methodologies. The first is a more flexible, 'ad-hoc' method, which entails the identification and synthesis of relevant literature crucial for constructing the theoretical groundwork of the research question. The second, a systematic literature review, entails a thorough synthesis of the research field at large, providing a comprehensive overview (Paré & Kitsiou, 2017). Although the ad-hoc approach might yield a less comprehensive perspective than the systematic method – which is known for delivering replicable and verifiable outcomes – its utilization in this research is deemed appropriate. To facilitate the ad-hoc approach, some elements described by Kitchenman (2009) are used. The search strategy follows snowballing by Wohlin et al. (2012). This research justifies the use of this approach due to its provision of a systematic method for assembling all necessary literature, thus laying down a sufficient background. The following section describes the search strategy, the boundaries that are defined to select relevant literature, search keywords are defined. Together these sections describe the literature research protocol of this study.

3.2.1.1 Search Strategy

In this study, the preliminary tool for the literature study search included Google Scholar and the Utrecht University Library. The initial phase of the research involved a systematic approach where the focus was on finding relevant literature in the area of study. For this the keywords together with the selection criteria as outlined below where used. The research was not limited to the titles of the articles but also included a review of the abstracts. State-of-the-art articles were identified using the targeted search terms and the snowballing technique, which, along with existing systematic reviews, helped to pinpoint fundamental theories, methodologies, frameworks, and literature gaps, thereby delineating this study's scope (Wohlin et al., 2012). Additionally, reverse snowballing was employed to uncover the latest studies not included in previous reviews. Although this approach requires substantial effort, it ensures the inclusion of a wide range of perspectives in the dynamic domain of cloud computing. To validate my findings I used the following papers as starting point for snowballing and reverse snowballing. All studies that were found using the snowballing procedure were analyzed, provided they fit within the criteria. This process ensures the essential studies are captured.

- Alouffi et al. (2021)
- Al-Ruithe et al. (2019)
- Di Giulio et al. (2017)
- Janet Julia Ang'udi (2023)
- M'rhaoaurh et al. (2018)

In addition to Google Scholar, other search engines are used to prevent missing relevant literature. The other search engines are as follows:

- ACM Digital Library
- IEEE Xplore
- DBLP
- Science Direct
- Springer Link
- Scopus
- Research Gate
- Taylor & Francis
- Wiley Online Library

3.2.1.2 Selection Criteria

During the search procedure the following selection criteria are used. Publications predating 2010 are generally excluded due to their diminished relevance over time. Nonetheless, seminal theories and frameworks are retained irrespective of their publication date. Systematic literature reviews served as an additional source to extract pertinent insights from earlier works.

Table 2: Section Criteria

Included	Excluded
Studies published after 2010	Studies published before 2010
Studies published in English	Studies in other languages than English
Studies that relate to cloud computing	Non-peer reviewed studies
Studies that relate to regulatory frameworks	
Fundamental studies (Luftman, Porter, Henderson & Venkatraman)	
Systematic literature reviews from before 2010	
Peer reviewed studies	
Studies from research institutes	

Keywords

The following keywords were used during search for literature.

Table 3: Keywords

Topic	Keywords
Cloud computing	Cloud computing, Cloud service models, cloud architecture
Risk management	Risk management, IT risk management
Cloud risk governance	Cloud risk, Cloud risk governance, Cloud risk frameworks, Cloud risk management, Cloud risk governance maturity,
Risk control frameworks	COBIT, CSA CCM, ISO, NIST, Cloud control frameworks
IT governance	Luftman, Porter, COBIT, IT governance, cloud governance
Shared Responsibility model	Shared responsibility model, cloud shared responsibility model
CMMI	CMMI, maturity, cloud risk maturity, cloud maturity, IT risk maturity

3.2.2 Interview Design

3.2.2.1 Data Collection

Data collection for this research is carried out using three primary methods. The initial method involves data collection during the literature review phase, which is detailed in earlier sections. Subsequently, data is collected during the research by doing interviews. The interview protocol is described in the subsequent section. The third method incorporates case studies, of which the protocol is also discussed in subsequent sections.

3.2.2.2 Sampling Strategy

The sampling of interviewees is a central aspect of good research. They are selected based on their prior experience and knowledge in the field. Given the scope limitations of this study, a comprehensive approach is taken to recruit all experts who are available and willing to participate in interviews or case studies. In this case a non-probabilistic purposive sampling technique was used. Although it has some limitations, and may lead to biases, it is justified since only subject matter experts are able to provide the required information. This method allows for obtaining high-quality, and relevant data. The selected interviewees are detailed in the table below, however individual identities are all anonymized. Together with the interviewee ID other relevant information is noted, such as the current organization, work role, work area, experience, and perspective.

Selection criteria

There are several criteria that must be met in order to qualify as a subject matter expert for the interviews. The following criteria must be met to qualify as a subject matter expert. Interviewees must have at least 3-5 years of experience working with the cloud. An important note about experience is that cloud is a rapidly evolving field. Therefore, it is not unreasonable to qualify as an expert without many years of experience. It is required that individuals have been involved in several cloud-related projects or audits. Individuals with professional certifications are highly desirable. Participants must have a deep understanding of cloud-related risks, including security, compliance, operational, and strategic risks. Experience in assessing and mitigating these risks is essential. Candidates from different departments will be considered to provide a broader perspective and more generalizability. Recommendations from managers, supervisors, or other experts within the organization will be considered. These recommendations help verify the candidate's expertise and relevance to the study. Finally, it is highly desirable that participants are currently involved in cloud-related projects to ensure that their knowledge is up-to-date.

Table 4 provides an overview of all the interviews done during the research. For each interview, the following details are included: an ID which is a unique identifier of each interview together with the protocol that was used during the interview, the professional role and position held by the interviewee, the industry or branch the interviewee operates in, and the level of experience and years of experience in cloud security. All interviews were recorded with specific allowance of the interviewee, with the exception of interviews E9, and E13. The interviewees all agreed with the UU provided consent form before recording started.

To improve the anonymity of the participants, their cloud computing experience is grouped into buckets instead of exact years. The buckets are as follows:

- 0-3 years of experience = B1
- 3-5 years of experience = B2
- 5-8 years of experience = B3
- 8-10 years of experience = B4
- 10-13 years of experience = B5
- 13 years or more = B6

Table 4: Interview overview

#	Role	Industry	Experience
E1 – P1	Manager	Risk assurance	B4
E2 – P1	Manager	Risk assurance	B3
E3 – P1	Senior manager	Technology risk	B4
E4 – P1	Consultant	Digital risk	B2
E5 – P1	Executive director	Risk assurance	B5
E6 – P1	Senior manager	Risk assurance	B3
E7 – P2	Manager	Risk assurance	B4
E8 – P2	Senior manager	Technology consulting	B4
E9 – P2	Executive director	Cloud security advisory practice	B6
E10 – P2	Senior manager	Risk assurance	B3
E11 – P2	Consultant	Digital risk	B2
E12 – P2	Executive director	Risk assurance	B5
E13 – P2	Manager	Risk assurance	B3
E14 – P3	Senior cloud engineer	Insurance	B5
E15 – P3	Engineer and cloud researcher	Cloud development	B2
E16 – P3	Researcher at Open University	Cloud resilience	B3
E17 – P3	Senior cloud engineer	Cloud security	B3

A total of 12 individuals were interviewed in three phases of the research. In the first phase, six interviews were conducted using the interview protocol 1. In the second phase, another six interviews were conducted using the interview protocol 2. Finally, three interviews were conducted in the third phase, the expert validation phase, using the same protocols. To ensure anonymity, it is not deducible from the table above who the 12 different people were.

3.2.2.3 Interviews

Interviews are carried out using a primarily structured approach, adhering to a specific protocol. A protocol provides structure during the interviews, but notably towards the end of the conversation, there is room for open-ended discussions. With the interviewee's explicit consent, all interviews are documented through recording, and then transcribing. Most importantly, anonymity is always ensured. Table 5 below describes the process flow of the first phase of interviews. Each question has a minimum outcome that the respondent must at least answer. If this is not the case, a follow-up question is asked. This information can later be coded. The minimum outcome is found in the column 'Code'. The interviewees that participated in the this interview are denoted in Table 4 in column # with P1.

Interviews phase 1 question attribution

To be able to extract the right information from the interviews a structured approach was taken. Each interview question relates either to a research sub-question or to necessary information to be able to execute the research. Within the first phase interview protocol, question 6 investigates if a certain cloud deployment is more or less susceptible to risk, and also why, then others. If for example, SaaS products would be way less susceptible to risk, then the scope would shift. Deployment models are discussed in Section 2.1.2.1. Question 7 – 10 investigate existing cloud risk frameworks such as CSA-CCM, to see if and how they are used in practice. The questions also try to unveil what organizations actually employ. Then the final questions are about risk topics. We want to ask subject matter experts to identify the most important risk topics. These questions will help answering this. The risk topics that are presented are taken from Section 2.2.2. The phrasing of the questions was not specifically derived from any literature but phrased in a way we thought as most useful.

Table 5: Interview phase 1 protocol

Step	Type	Question	Code
1.	Opening	-	Explain goals of thesis and explain use of data. Inform on ethics.
2.	Informed Consent	To gather the most results from this interview I would like to record and later transcribe it. Everything will be anonymized. Do you agree with this?	Yes or No
3.	Work area	Where do you work and in which department?	Name of organization, type of organization, and department
4.		Can you describe your work for me?	Work area
5.		Did you have any previous experience with cloud risk?	Years of experience
6.	Cloud deployment	What types of cloud are susceptible to most risk?	Investigate effects of cloud
7.	Frameworks	Can you describe which frameworks are often used within organizations?	Most common frameworks
8.		What solutions do organizations often apply?	Current practices in cloud governance
9.		Can you explain why?	Reasoning on efficiency cloud governance
10.		What is the impact of control frameworks on governance?	Effect of control frameworks on governance
11.	Stakeholders	Who are the most important stakeholders in cloud?	Establish stakeholders
12.		What is the relation between DevOps teams and management?	Establish governance in cloud development
13.	Best practices	What do you think are the most important cloud specific risks?	Discover important risks
14.		Which risks controls should first be implemented?	Discover relation risks and controls
15.		Can you rank the following list of risks on importance. Risk factors are from Section 2.2.2	Establish best practices
16.		Why did you make these distinctions?	Reasoning

Table 6 below describes the interview flow of the second interview. Depending on the if the interviewee participated twice, more information was given about the research. The structure of the protocol is similar to the first protocol. The interviewees that participated in the this interview are denoted in Table 4 in column # with P2.

Interviews phase 2 question attribution

Similar to the interview questions of the first phase, the second phase interview questions are all phrased in such a way that the information is easily extracted. The questions 6 – 8 are part of the first validation step of the first phase. We ask participants to verify that the 8 risk topics we identified are actually the most important ones. Validation follows the principles as described by Wieringa (2014). Then question 9 – 13 try to uncover what maturity on cloud risk governance means within an organization. Participants are asked what they think maturity means and what the steps are. Then we present an example of the model as presented in Section 4.3, we participants are asked to judge the model. Iterative improvements are each time shown.

Table 6: Interview phase 2 protocol

Step	Type	Question	Code
1.	Opening	-	Explain goals of thesis and explain use of data. Inform on ethics.
2.	Informed Consent	To gather the most results from this interview I would like to record and later transcribe it. Everything will be anonymized. Do you agree with this?	Yes or No
3.	Work area	Where do you work and in which department?	Name of organization, type of organization, and department
4.		Can you describe your work for me?	Work area
5.		Did you have any previous experience with cloud risk?	Years of experience
6.	Previous results	-	Explain the results of previous study
7.		Do you agree with the 8 factors?	Validation previous results
8.		Do you agree with the categorization	Validation previous results
9.	Maturity	When do you think an organization is mature in cloud risk governance?	What is maturity
10.		How would you reach maturity?	Maturity steps
11.		What would you measure for maturity?	Maturity steps
12.		What would be the differentiating factors?	Maturity steps
13.		How would you check that?	Validation maturity

3.2.3 Expert Opinion Validation

The goal of the triple expert opinion validation is to validate the findings of the previous two phases of interviews. The expert validations consisted of a longer interview with two cloud engineers at an external organization, and a cloud engineer and researcher at Open University researching cloud resilience together. They provide valuable insight in the usefulness of our findings, the applicability of the findings, and the correctness. If experts agree on the usability of the model it validates the findings. The ensure anonymity of the two organizations that participated in the validation we will not provide great detail.

The triple expert validation are carried out using a primarily structured approach, adhering to a specific protocol to provide structure during the process, as with the interviews. Notably towards the end of the conversation, there is room for open-ended discussions. With the interviewee's explicit consent, all interviews are documented through recording, and then transcribing. Most importantly anonymity is always ensured. The interviewees that participated in the this interview are denoted in Table 4 in column # with P3.

Interviews expert opinion validation question attribution

Interview questions again follow the validation process as described by Wieringa (2014). Overall, the questions are designed to test whether the artifacts are useful for organizations to implement. We formulated them from four different below. These perspectives are derived from Wieringa (2014).

1. Relevance questions: Assessing if the artifact solves a real problem.
2. Design quality questions: Evaluating the quality of the design.
3. Performance questions: Focusing on how well the artifact performs in the current environment.
4. Utility questions: Assessing the practical utility or usability of the artifact within the current context.

First, in step 6 the results are shown and explained, then 7 – 12 focus on the risk topics. We ask the participants what they think of each topic, and if they agree with the selection. Then we discuss how they would apply this within their own organization and how they would benefit. Question 13 – 19 focus on the maturity model.

Table 7: Expert opinion validation protocol phase 3

Step	Type	Question	Code
1.	Opening	-	Explain goals of thesis and explain use of data. Inform on ethics.
2.	Informed Consent	To gather the most results from this interview I would like to record and later transcribe it. Everything will be anonymized. Do you agree with this?	Yes or No
3.	Work area	Where do you work and in which department?	Name of organization, type of organization, and department
4.		Can you describe your work for me?	Work area
5.		Did you have any previous experience with cloud risk?	Years of experience
6.	Validation results eight factors	-	Explain the results of study
7.		Do you agree with the 8 topics?	Validation previous results
8.		Do you agree with the categorization?	
9.		Do you think they are all useful?	
10.		Would this be useful in your organization?	

11.		How would you apply it in your organization?	
12.		Who would most benefit from it in your organization?	
13.	Validation results maturity	-	Explain the results of study
14.		What do you think of the model?	Validation of previous results
15.		Would this be useful in your organization?	
16.		How would you apply it in your organization?	
17.		Who would most benefit from it in your organization?	
18.		In what level would you place yourself?	
19.		How would you improve?	

3.3 Analysis Techniques

3.3.1 Interview Coding

For the first phase, the interview coding was done using a thematic coding, combined with a ranking exercise to quantify various risk factors. All interviews are transcribed and coded in NVIVO. Coding of the interviews was done in a mostly deductive manner since themes were developed from the interview questions. Examples of such codes can be found in the column 'Code' in Table 5 and Table 6. Quotes are extracted from the interviews as a way of providing evidence for the findings. Quotes are translated and sometimes rephrased to make them available for the research rapport. The codebook is found in Appendix A.

During the interviews digital whiteboards (Microsoft Whiteboard) are used to rank the risk topics. Subject matter experts are asked to drag and sort the topics, which includes the name of the topic and a short description, according to their importance. On the digital whiteboard no set amount of columns was displayed to avoid creating any bias. The experts had to create columns themselves if they wanted to. However, it was explained during the interviews that they should use columns. Thereafter, the digital whiteboards are recorded in a spreadsheet, with each cluster representing a different column. Each column represents a score of importance. Then the scores are normalized, since not every participant will be using the same amount of columns. As they are free in their distinction level to not influence the results. The normalized scores are then color-coded to allow for simple visual analysis. The coloring is automatically done by Microsoft Excel with a variability range of 1 – 8, and automatic red / green coloring. Thereafter, the risk topics are all sorted on their highest mathematical average and median. Risk topics which are mostly dark green represent the most pressing and important topics, while orange or reddish represent less important topics. This visual representation forms part of the proof together with the expert opinion of the interviewees. The visual representation mostly helps in identifying the important topics and making distinctions between which topics are essential. Topics that have too much red color are not considered for expert evaluation during coding. Doubtful cases can be analyzed thoroughly during the coding, whether they should be included in the framework or not.

3.3.2 Maturity Model Creation

The maturity model is constructed in the second phase of the project. The artifact is constructed by gathering data during the interviews. The coding of the interviews entails a discussion on the five defined maturity levels, being initial, managed, defined, controlled, and optimizing. These levels are browed from CCM, explained in Section 2.4. Coding is done in a similar deductive fashion for each maturity level following the codes in Table 6. However, since there is also some open debate on what maturity entails, we also do some inductive coding. Focusing mostly on what organization should be able to do if they are mature. The various levels of maturity are determined by the awareness of an organization in the possible cloud risks, and by their current control process. Participants are asked during the interviews how they would define each level. In addition they are asked what defining characteristics between levels are. Each maturity level requires an organization to meet all the characteristics of that specific level. This makes all the levels disjunct. So if an organization wants to achieve a higher maturity, they at least have to satisfy the requirements of each categories. During the interviews what those categories are researched by asking certain questions. From existing literature, discussed in Section 2.4, certain categories have already emerged and are also discussed during the interviews in order to give the participants ideas.

3.4 Methodological Limitations

Sampling

Most sampling was done in the form of convenience sampling from within EY. Participants with known cloud expertise and work history were asked to participate in the study. To keep a diverse pool of participants people from various work areas with varying backgrounds were selected. Auditors and consultants have different work, and also different perspectives on risk management. The sampling pool could have been expanded by including risk professionals from other organizations, unfortunately this was not during this research. In addition, to doing interviews at EY, two case studies were conducted at external organizations. These organizations were also samples as form of convenience sampling, but are both relevant.

Temporal constraints

Research as it is currently conducted has most of its relevance in the present, as organizations continue to evolve and risk practices continue to get better. However, this research directly contributes to the improvement of risk practices. In a perfect world, organizations would be so advanced that they would have implemented all of this study's recommendations.

Ethical considerations

This research has been conducted to the highest ethical standards. This is evident as the following ethical considerations were all addressed. An Utrecht University ethics scan was conducted before the research. First and foremost, informed consent was always obtained from all participants, who understood the purpose of the research and how their data would be used. The Utrecht University supplied consent forms was used for this. Second, all confidential participant data did not leave the provided and secured EY equipment. Finally, the utmost care was taken to ensure the anonymity of participants to protect their personal information.

Researcher biases

Great care was taken to ensure that no additional biases were introduced beyond the potential selection bias discussed above. Interview questions were carefully worded so as not to frame participants' responses. In addition, observer bias was mitigated by repeatedly seeking external validation from supervisors.

3.4.1 Research Validity

In the Table 8 an overview of the different aspects of research validity is provided. The first column covers the threat category, the second the potential risk, and the third the proposed mitigation.

Table 8: Overview of Research Validity

Threat	Risk	Mitigation
Construct validity	Inadequate definition of constructs	1. Using multiple sources of evidence. (literature, case studies and interviews) 2. Supervisors review the process. 3. Asking questions to experts about the idea of the construct itself.
	Disjunction of maturity model	1. Ask questions during interviews which explicitly mention disjunction.
Internal validity	Relation between variables	Using a detailed research framework, and asking about relationships during interviews.
	Confounding bias (other variables of influence)	Identified confounding variables in advance.
	Interviewee bias	Interviews are done in a standardized format to reduce variability.
External validity	Context specific findings	1. Selected interviewees with diverse backgrounds. 2. Asked interviewees for generalizable answers. 3. Provided detailed description of the scope of the study to enhance repeatability. 4. Gathered context specific variables and checked them against model.
	Small sample size	Included a diverse range of participants to enhance generalizability.
Reliability	Instrument instability (changing interview questions)	1. Thoroughly documented research process and interview questions. 2. Standardized interview questions.

4 Managing Cloud Risk Governance

In this section, all the results are discussed from the design phase of the research. The interviews and triple expert validations provide answers to certain sub-questions. We also discuss the constructed model and the results found during validation. This section is structured as follows: first we discuss the sub-question one on assessing cloud risks, then we discuss the 8 top risk topics, and thereafter we discuss the maturity model for cloud governance. Finally we conclude the section by answering the main research question.

4.1 Assessing Cloud Risk Governance

For organizations to assess their cloud risk governance they must first be equipped with the knowledge and tools to do so. It became apparent that organizations often do not possess the knowledge and thus usually do not do so. To assess any given organization, common cloud risks should be identified first. This section presents the findings on cloud-specific risks, the impacts of the different cloud service models, the different stakeholders in cloud risk and their roles and responsibilities, how organizations currently manage cloud governance by using frameworks, and what organizations should now do.

Cloud-specific risks

A first step in effectively managing cloud-specific risks is being able to identify the risks or most common vulnerabilities. When discussing risk in the cloud, it is important to delineate exactly what this means. Cloud-specific risks are risks that are extra relevant due to the intrinsic nature of the cloud, or specifically occur only in the cloud environments. Whenever we discuss cloud risks, we always talk about cloud-specific risks.

As part of the first phase of the study, all the different cloud risks were gathered. These can be found in Table 1 in Section 2.2.2. The collection of cloud risks are from different sources. With this inventory of possible risk topics, it is possible for an organization to perform a risk analysis. Each risk topic contains a variety of risks. These risks are however, organization specific. It depends on the application of the cloud, the configuration of the cloud environment, and possible regulatory requirements what risks actually exist. Within that set of risks, there are always risks that are of less importance or less relevant than others. Risk analysis can be performed in various ways, but generally speaking by first assessing threats and vulnerabilities. Then the potential risk is assessed by looking at the likelihood and impact. The results in a risk level on either a specific risk or risk topic. Depending on if there are already controls or other measures in place there is a residual risk. This method is derived from Section 2.2.

To illustrate, let's explore a common cloud-specific risk topic. Insecure APIs: Cloud services often use APIs to interact with other services and applications. Insecure APIs can be exploited by attackers to gain unauthorized access to data or services, and can thus result in a number of vulnerabilities and therefore risks. Organizations must for this reason ensure that their APIs are secure, regularly updated, and monitored for unusual activity. But depending on their usage of APIs and the cloud services they deploy, the risk differs. Obviously the risk increases as the use of APIs across critical systems increases. Which does not have to be the case within any given organization. Organizations should first assess how many APIs they use or have. Then they must consider the potential threat they pose to the organization. Next, they must assess the likelihood an API is not secured properly, and the chances if it being compromised. Then, the impact of a vulnerable API must be considered by for example investigating to which systems the APIs are connected. Then organizations must consider how they want to avoid such risks.

Assessment of risk governance in different cloud service models

In the investigation into how organizations assess their cloud risk governance, we identify which types of cloud deployments are most susceptible to poor risk management practices. The study considered the three primary service models: IaaS, PaaS and SaaS. The findings indicate that there was no real difference between the three service models. While IaaS and PaaS typically require more configuration compared to SaaS, which could lead to more vulnerabilities, the increased configurability does not correlate to a higher risk in terms of governance. SaaS services often require way less configuration but that does not mean there are less risks. Organizations tend to have way more SaaS services than IaaS or PaaS services resulting in more dependability. The less services of the deployment you manage yourself, i.e. networking, infrastructure, etc., the more you rely on the service provider (thus third-party risk). This reliance introduces other risks as organizations often lack a clear understanding of the division of responsibilities between themselves and the service provider. This confusion can lead to governance gaps, where essential risk may be overlooked or improperly mitigated. This study emphasizes the need of effective risk management independent of the deployment model.

Stakeholders in risk

We found that we can distinguish between three different stakeholders who each have their specific role in risk governance. The three different roles in this process are the Engineer (Cloud and Application Designer and Cloud Administrator), the (IT) Risk Team, and Management (Policy Enforcers and Creators). The engineer is responsible for the design and development of cloud infrastructure and applications. Engineers implement technical controls such as encryption, firewalls, and access management systems, but they also develop applications for an organization. They are the ones who create the software, deploy and manage it. The engineers can follow any software development method such as agile or waterfall. While the fundamental tasks are similar, the agile method introduces more difficulties since developers have more responsibilities. They must balance development and security. The IT risk team, or just risk team, focuses on identifying, assessing, and managing risks. This can be IT specific but does not have to be. For the sake of this research, the IT risk team is also concerned with cloud-specific risks. The IT risk team is responsible for developing and maintaining risk management frameworks, and policies that guide the use of cloud systems. They implement existing frameworks, or create their own, a topic which is discussed in a subsequent section. This team provides guidance to both the engineers and management. Management is responsible for overseeing the overall organization and in extension the cloud strategy. They are responsible for aligning business objectives and developing and deploying governance. This. among other things, involves creating policies related to cloud. Management overall responsibility for allocating resources, budget, and personal to support cloud initiatives, be it both development, deployment, and security.

The three roles described and defined above will be used throughout the rest of the study. They are three roles that play a role in the maturity model. Policies are defined by management, risk frameworks are defined by e.g. IT risk, and implementation is often done by engineers. The three different stakeholders play an important role in describing cloud risk maturity.

Cloud risk management frameworks

It might seem intuitive that one of the most straightforward approaches to risk management is to adopt an existing control framework. However, in practice, this is rarely the case. Existing control frameworks are typically extensive and ambiguous by design. As experts put it: “They are often huge and contain over 400 questions… ” To ensure broad applicability across diverse organizations, the institutions that develop these frameworks often want to make them as general as possible. This generality, while beneficial for wide application, means that these frameworks are not tailored to specific business processes, which is often a necessity for effective risk management.

Organizations therefore often choose to build and implement their own tailored framework. This approach, is complex and time-consuming. Developing a tailored risk management framework requires aligning all stakeholders on the objectives and scope of the framework. Before these frameworks can be enforced, they must receive approval from management, and the IT risk department must have a clear understanding of the specific requirements and risks involved.

To create good frameworks, it is essential to base them on existing, industry-tested methods. Ensuring that essential components are not missed. When organizations create their own frameworks they can either think of cloud risk topics themselves or borrow from existing frameworks. Organizations often make a mapping to existing frameworks to determine they are doing this properly. This is very time consuming and not very future-proof since the mapping it is based on may change.

Assess cloud risk governance

After having identified what a cloud-specific risk is, at what service level these risk often occur, who the various stakeholders are, and how organizations now do risk management, it is possible to investigate how to assess cloud risk governance. First as an organization you should assess which cloud-specific risks are most relevant to your organization. In the next section, we will explore effective ways of improving the cloud risk governance by discussing the most important topics. Any given organization should first analyze the context, and understand in what kind of environment it operates. It should understand the cloud usage, configuration and regulatory environment. As soon as this is all known a detailed risk assessment must be performed. Potential risks should be evaluated based upon their potential impact and likelihood, and then be prioritized. Then, organizations should evaluate the current governance framework, if one exists. Is it adapted to the current cloud environment or does it need to be updated? Next, they should identify who the three stakeholders are and what their current responsibilities are. Based on this, a gap can be identified in the current cloud risk governance.

4.2 Improving Cloud Risk Governance

When organizations have established how to assess an cloud risk governance, and who are responsible, the possibility of improvement comes into existence. The difficulty of improving on cloud risk governance lies in the fact that cloud technology is complex and often changing. Cloud computing is complex due the many different services, and the way you set them up, but also due to varying regulations that surround cloud, the focus on business development rather than control, disconnect between the stakeholders, and the vague responsibility model. There are things that organizations can do such as implement complex control frameworks and mitigate vulnerabilities. However, if organizations mitigate risks sporadically they remain to be not in control. This study shows that implementing complete existing control frameworks is often too difficult for organizations. As a result, organizations often do not do anything. In this research we sought to find the risk topics which are the most influential risk topics. The goal is to provide the organization with effective ways of improving on their cloud risk governance. These topics can then be implemented into existing or newly made risk management frameworks and increase cloud risk awareness. This section presents 8 Top Risk Topics organizations can build into risk frameworks or discuss with management.

Risk topic selection

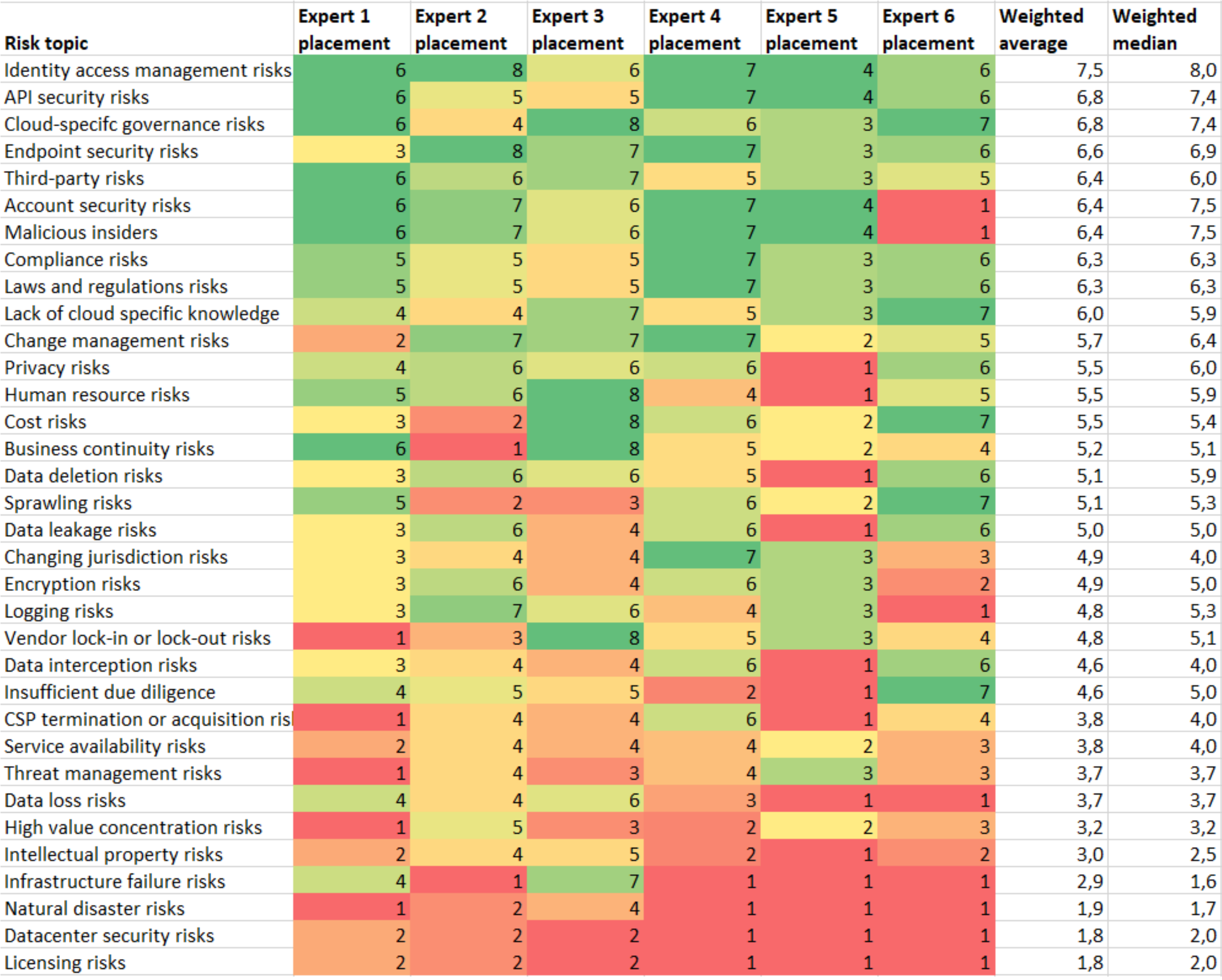
Selecting the most important risk factors helps organizations in effectively managing and mitigating cloud risks. By selecting the most important risk topics, organizations can concentrate their efforts in the areas that pose the greatest risk to their cloud environment and organization. Focused management efforts help align resources to the most significant threats. The goal is to move from a sometimes chaotic selection of what to focus on to an efficient prioritization. It ensures that resources are not spread thin across numerous less significant issues. Budget, personal and technological investments all follow the improved risk management strategy. Engineers should now not only focus on developing but also on security. Through the method detailed in Section 3 we derived the eight high-priority important risk factors. These will be discussed in subsequent sections.

4.2.1 8 Top Risk Topics

After analysis the following 8 Top Risk Topics were found. The 8 Top Risk Topics are presented in no particular order. In short, we found that identity access risks, API security risks, cloud-specific governance risks, and endpoint security risks were all ranked exceptionally high. We found that within each organization, these cloud-specific risks always require control. These are also often areas where organizations lack control, which results in increased risk. Then there were four other topics which were also ranked high. These topics were third-party risks, account security risks, laws and regulation risks, and compliance risks. Although some experts looked at these topics from other perspectives and then linked them to other topics. For example, account security is tied to IAM, and if the latter is done correctly, the former is less likely to go wrong and therefore ranks lower. It is partially true that if an organization does IAM right, account security risks are likely to be lower, but it is not necessarily so. Accounts can still be hijacked due to phishing attacks and poor password management, while account privilege is managed correctly.

When it comes to cloud risk governance, these 8 Top Risk Topics are the key topics on which organizations should focus. These results should be seen as a selection of the previously discussed cloud risks. The top risk topics have been extracted from the interviews. The heatmap is created of the individual risk topics to do qualitative visual analysis. It allows for easy visual analysis of the top topics by color. As already described, we normalized the scores of each individual expert interview since they did not all chose the same amount of columns. This was done to get the averages of each individual topic. We found that there was no significant difference between the average and the median. In Figure 5 the heatmap sorted for the weighted average is visible. The heatmap coloring was not normalized and automatically done based on the lowest and highest value of the column. Now when expert 2 and 5 rate a topic the highest it is colored the same.

The heatmap reveals several noteworthy insights. We found that first, account security and malicious insiders, which we now view as a one topic, are ranked relatively high by all experts, with the exception of Expert 6. Those who ranked this idea low suggested that if IAM is implemented effectively, the potential risks are reduced. Another noteworthy observation is that some experts have assigned relatively high rankings to business continuity, while others have placed it relatively low. This is due to the fact that some believe that IT systems supporting business operations should be available at all times, while others argue that public cloud infrastructure is often more resilient to outages than locally run IT systems. The risk associated with change management is often perceived to be high, yet some experts argue that the nature of change management in the context of public cloud is not significantly different from that of other circumstances. It is therefore not considered a top risk. Endpoints are frequently connected to the cloud, and while they can sometimes be managed from the cloud, they collectively represent a considerable risk. Human risks are sometimes scored high and sometimes low. Some argue that human risk is substantial due to unawareness and mistakes, while others argue that organizations should not blame users.



Risk topic	Expert 1 placement	Expert 2 placement	Expert 3 placement	Expert 4 placement	Expert 5 placement	Expert 6 placement	Weighted average	Weighted median
Identity access management risks	6	8	6	7	4	6	7,5	8,0
API security risks	6	5	5	7	4	6	6,8	7,4
Cloud-specifc governance risks	6	4	8	6	3	7	6,8	7,4
Endpoint security risks	3	8	7	7	3	6	6,6	6,9
Third-party risks	6	6	7	5	3	5	6,4	6,0
Account security risks	6	7	6	7	4	1	6,4	7,5
Malicious insiders	6	7	6	7	4	1	6,4	7,5
Compliance risks	5	5	5	7	3	6	6,3	6,3
Laws and regulations risks	5	5	5	7	3	6	6,3	6,3
Lack of cloud specific knowledge	4	4	7	5	3	7	6,0	5,9
Change management risks	2	7	7	7	2	5	5,7	6,4
Privacy risks	4	6	6	6	1	6	5,5	6,0
Human resource risks	5	6	8	4	1	5	5,5	5,9
Cost risks	3	2	8	6	2	7	5,5	5,4
Business continuity risks	6	1	8	5	2	4	5,2	5,1
Data deletion risks	3	6	6	5	1	6	5,1	5,9
Sprawling risks	5	2	3	6	2	7	5,1	5,3
Data leakage risks	3	6	4	6	1	6	5,0	5,0
Changing jurisdiction risks	3	4	4	7	3	3	4,9	4,0
Encryption risks	3	6	4	6	3	2	4,9	5,0
Logging risks	3	7	6	4	3	1	4,8	5,3
Vendor lock-in or lock-out risks	1	3	8	5	3	4	4,8	5,1
Data interception risks	3	4	4	6	1	6	4,6	4,0
Insufficient due diligence	4	5	5	2	1	7	4,6	5,0
CSP termination or acquisition risl	1	4	4	6	1	4	3,8	4,0
Service availability risks	2	4	4	4	2	3	3,8	4,0
Threat management risks	1	4	3	4	3	3	3,7	3,7
Data loss risks	4	4	6	3	1	1	3,7	3,7
High value concentration risks	1	5	3	2	2	3	3,2	3,2
Intellectual property risks	2	4	5	2	1	2	3,0	2,5
Infrastructure failure risks	4	1	7	1	1	1	2,9	1,6
Natural disaster risks	1	2	4	1	1	1	1,9	1,7
Datacenter security risks	2	2	2	1	1	1	1,8	2,0
Licensing risks	2	2	2	1	1	1	1,8	2,0

Figure 5: Heatmap of Risk Topics

From the insights of the heatmap and interviews we found the following: the 8 Top Risk Topics consisting of IAM Risks, API security risks, Cloud-specific governance risks, Endpoint security risks, Third-party risks, Account security risks, Compliance risks, and Laws and regulations risks. We also found that malicious insiders and account security are similar and can be seen as one. Moreover, that the low placement of account security by expert six is due it being seen as secure when IAM is secure. Change management is difficult but this is not attributed to cloud. Privacy risk is also an important topic but not a top topic. The rest of the cloud-specific risk topics are obviously interesting but should only be focused on if there is a specific need or if the organization is already in control of the 8 Top Risk Topics. The 8 Top Risk Topics will help an organization the most in improving their cloud risk governance.

If we look at the taxonomy as discussed in Section 2.2.2, we see that the 8 selected risk fall in pairs of two within each of the four described categories. We have therefore opted to include the taxonomy as part of the results. Technical risk contains account security risks and API security risks, operational risks include endpoint risks and identity access management risks, organizational risks include cloud-specific governance risks and third-party risks, and legal risks include laws and regulations risks and compliance risks. We will discuss each individual risk topic in the subsequent sections under the provided taxonomy. Generally speaking the taxonomy follows the following structure. Technical risk topics are more affected by the external environment, while operational risks are more focused internal perspective. Organizations must also address phishing prevention, password management, and user education to comprehensively manage account security.

Finally, before we discuss the individual risk topics, it is important to mention that topic names can be interpreted in multiple ways. A topic name such as account security, or third-party risk can be used not only in the context of public cloud, but also outside of it. Likewise a risk topic like compliance risk can be interpreted in many different contexts. However, in the context of this study, these only refer to risks that are cloud-specific. When we talk about third-party risk for example, we are referring to risks at service providers or their supply chain. The definition of each risk topic including the potential risks was extracted from literature or existing risk frameworks.

4.2.1.1 Technical risks

Technical risks include potential threats and vulnerabilities associated with the technical aspects of cloud computing. These risks typically revolve around issues such as system failures, security breaches, data integrity, and the reliability of cloud infrastructure and services. Technical risks are often managed by engineers rather than managers or risk departments.

Account security risks

This topic covers risks related to unauthorized access and potential breaches of cloud user accounts, including both internal and external threats. A comprised cloud user account or tenant can lead to data breaches, configuration loss or other issues. Control of the cloud environment can also cause disruptions in service or unauthorized use of resources. Each of the possible risks below is part of the topic account security.

One noteworthy finding by expert E2 from the interviews is that default passwords on accounts without direct administrator access can be exploited to gain unauthorized privileged access. This can result in unauthorized access to the cloud management console and a breach of tenant data.

The following possible risks can be part of this topic:

- Insider threats leading to data breaches
- Account hijacking by external attackers
- Weak or reused passwords
- Phishing attacks targeting account credentials
- Insufficient multi-factor authentication
- Poor password management practices
- Privilege escalation due to improper access controls

API security risks

Focuses on the vulnerabilities and threats associated with Application Programming Interfaces (APIs), which are integral to modern applications and services. They establish communication between various services and systems. Insecure APIs can lead to data exposure or unauthorized access to systems, or also service disruptions. APIs should be secured and encrypted, protected from invalid inputs, and continuously logged. The following risks are related to this topic.

As expert E1 noted, with public cloud most services are accessible from the internet and outside world. As became apparent from the interviews, given that APIs are basically externally available, you only have to misconfigure one API somewhere without realizing it and you are at risk. API security is also something engineering and maybe IT risk has insight into so it has to managed properly if to avoid risk.

The following possible risks can be part of this topic:

- Insecure authentication and authorization mechanisms
- Data exposure through unencrypted communication
- Lack of rate limiting leading to Denial of Service (DoS) attacks
- Insufficient logging and monitoring of API activity
- Injection attacks (e.g., SQL injection, command injection)
- Improper API input validation
- Use of deprecated or vulnerable APIs

4.2.1.2 Operational risks

Operational risks in cloud computing refer to challenges that arise from the day-to-day management and operational activities associated with cloud services. These risks include issues related to service availability, identity management, and the effective integration of cloud services with existing IT infrastructure. Often, employees need appropriate training and skills development to avoid problems.

Endpoint security risks

Endpoints are devices such as laptops, desktops, smartphones, but also Internet of Things connected devices, that are access points to the network and cloud environment. These devices can be target to cyberattacks due to their widespread use and sensitive data they handle. They are often not directly controlled by the IT department, which makes updating them more difficult. Or they are required to run constantly as downtime would cause a production outage. Unpatched software can thus be seen as a major security risk.

As with API security, experts E3 and E6 have indicated that the high number of connections with endpoints is a very cloud specific aspect. Therefore, it is crucial to understand that a single compromised endpoint can pose a significant threat to the organization. Endpoints are often highly interconnected with the cloud, making them potential access points. To mitigate this risk, it is essential to ensure that endpoints are adequately protected from the network and management portals.

The following possible risks can be part of this topic:

- Malware infections (e.g., viruses, ransomware)
- Physical theft or loss of devices
- Unpatched software vulnerabilities
- Unauthorized access to endpoint data
- Man-in-the-Middle (MitM) attacks on network connections
- Insecure remote access (e.g., VPN, RDP)
- Insufficient endpoint encryption

Identity access management risks

IAM topic deals with risks associated with the management of user identities and their access privileges to systems and data. The goal of IAM is that users have access to the right resources in the cloud environment. IAM risks often emerge if too much access is granted. It often happens that users are granted administrator access and are able to change everything in the cloud environment without actually needing it, which causes a major security concern. Something that can easily be avoided if organizations implement role-based access control, and the least privilege principle.

Many experts consider IAM to be the most critical risk topic in a public cloud environment. This is where a lot of potential issues can arise, where change is frequent, and where organizations often lag behind. To quote some interviewees E5 and E4: "IAM is a most critical part of my experience and where I have personally seen where people lacked the most." and "IAM is really important; if you don't do this right, things can really go wrong."

The following possible risks can be part of this topic:

- Weak or inconsistent access control policies
- Ineffective user provisioning and deprovisioning
- Unauthorized access due to role-based access control (RBAC) failures
- Overprivileged accounts
- Lack of identity verification mechanisms
- Credential stuffing attacks
- Poorly managed service accounts

4.2.1.3 Organizational risks

Organizational risks arise from internal factors within an organization that can affect the adoption, management, and governance of cloud services. They also include vendor management concerns, including contract negotiations, relationship management, and establishing clear policies and procedures for the adoption and use of cloud services. Organizational issues highlight the importance of effective communication, stakeholder engagement, and leadership commitment.

Third-party risks

Third-party risks arise when organizations rely on external vendors to perform services and provide products. This is an absolute given when using cloud computing services, regardless of the deployment model, from an external service provider (i.e. public cloud). It is more than obvious that they bring benefits, but they introduce a new set of challenges. Understanding these challenges is essential when managing them. This has to be mitigated by doing thorough due diligence and implementing good contracts and SLAs.

According to experts, the perceived complexity of the shared responsibility model plays a significant role. It is often seen as complex when it is just a matter of properly figuring out what needs to be done. However, CSPs indicate in many ways what needs to be addressed. As expert E1 said, "You just have to spend a lot of time, and therefore money, on this to understand what processes have underlying external processes, and how that is configured."

The following possible risks can be part of this topic:

- Third-party data breaches affecting your organization
- Lack of security controls at vendor sites
- Inadequate third-party risk assessments
- Dependency on third-party software with vulnerabilities
- Data leakage through third-party integrations
- Poor contract management and enforcement
- Compliance failures due to third-party actions

Cloud-specific governance risks

Focuses on the risks due to the lack of, or inadequacy of governance policies tailored for cloud environments, which can lead to security and compliance issues. A lack of cloud-specific governance means that there are no formal policies or practices which are specifically designed to manage cloud resources. The absence can lead to inconsistent practices, lack of accountability, inefficiencies in risk management, and security vulnerabilities. Clear policies should be established, which are specific to the cloud environment.

Cloud-specific governance is an interesting topic, as expert E4 said: "It depends a lot on the governance structure that an organization currently has in place. If an organization already has a solid governance structure in place that everyone is familiar with, then it is easy to add cloud risk. There are some changes that require awareness of engineers and managers, but you just need knowledge and expertise. However, if this is not the case, then cloud risk is more difficult to properly govern due to its inherent characteristics."

The following possible risks can be part of this topic:

- Misconfiguration of cloud resources
- Lack of visibility into cloud operations
- Inconsistent practices in cloud resource management
- Poor incident response planning for cloud environments
- Inadequate compliance with cloud-specific regulations

4.2.1.4 Legal risks

Legal risks relate to potential legal and regulatory challenges associated with the use of cloud services. These risks include compliance with data protection and privacy laws, jurisdictional issues related to data sovereignty, contractual obligations with cloud service providers, intellectual property rights, and liability considerations in the event of data breaches or security incidents.

Laws and regulation risks

Adherence to laws and regulations is critical for organizations operating in cloud environments. Failure to adhere to legal and regulatory requirements can result in significant consequences, such as penalties. The difficulty of complying to laws and regulations in cloud environments is due to the constantly changing regulations in different countries, and the fact that you operate across borders. This makes it harder to stay in control since the environment is more susceptible to change. To mitigate these risks it is important to develop a comprehensive risk management framework, to stay informed about regulatory changes, and conducting regular auditing.

As some interviewees said: "You just have to adhere to it regardless of the complexity." and "You easily put your data somewhere else which can be a big risk to laws and regulations."

The following possible risks can be part of this topic:

- Non-compliance with data protection laws (e.g., GDPR, CCPA)
- Violations of industry-specific regulations (e.g., HIPAA, PCI-DSS)
- Non-compliance due to varying jurisdictions
- Legal actions due to privacy breaches
- Non-adherence to international trade regulations
- Regulatory changes impacting business operations
- Lack of regulatory reporting mechanisms

Compliance risks

Compliance risks refer to the potential for an organization to be not compliant with cloud specific standards. There is the risk internal policies are not correctly aligned and contractual conditions are not correctly specified.

According to interviewees, specifically E4 said "We often see that the third line of defense (i.e., an accountant) is knowledgeable enough, but from a policy perspective, little consideration is given to proper cloud policy. As a result, the translation to true cloud-specific controls is lacking. So then nothing happens" and "If you don't test, don't check what you have set up or whether that is what you intend to set up. Then you just run a high risk on everything."

The following possible risks can be part of this topic:

- Failure to adhere to cloud specific industry standards (e.g., ISO 27017)
- Inconsistent implementation of internal policies
- Poor audit readiness and response
- Inadequate training and awareness programs
- Non-compliance with contractual obligations
- Insufficient compliance monitoring and enforcement

4.3 A Maturity Approach on Cloud Risk Governance

Once organizations know which risk topics to focus on, they should improve in their overall risk governance. Using a maturity model focused on risk governance provides a structured framework that organizations can use to assess their current capabilities, identify gaps, and implement improvements systematically. The maturity model that is proposed follows the CMM example, by defining five levels. Each level represents a different stage in which an organization can operate in. By changing the governance policies, and way of working organizations can advance in the different maturity levels. The findings on a Cloud Risk Governance Maturity Model are detailed below.

The advantage of using a maturity approach lies in the fact that it creates a structured way of improving. Moreover, it creates more risk awareness within the organization. Awareness not only at the IT risk department, but also at the management level and the engineering level. It is precisely this awareness that facilitates a good risk management practice. Cooperation between all three parties is required, especially with cloud, which is later elaborated upon.

During the study, it has become apparent that there are two different schools of thought when it comes to maturity. One school argues that the foundation lies in the implementation of controls. The better an organization has implemented these, the better its risk management. Here, the outcome is important, and quality is ensured, but not always the action. The second school believes that management processes are at the heart of good maturity. If the processes are well-designed, then good management and action will follow. In this case, action is well ensured, but quality and verifiability less so. This concept of maturity is therefore at the foundation of the model. Both schools of thought are incorporated and processed within it. Additionally, it was mentioned that when discussing maturity in the context of cloud risk, it is not easy to establish a specific measurement point because the technology regularly changes. Therefore, the ability to adapt must also be taken into account. An organization is considered mature when it is fully in control of the risks. You are in control if you know where these risks are located, if you know how to deal with them, and if you implement this well. However, there is naturally a gradient here, organizations can know what they need to do but still struggle to implement it. It is along this gradient that they must progress. If they also do not know what they are doing, they are at serious risk.

Taking all this into account, we come to the following findings. First, it is necessary for organizations to identify current risks. A thorough risk analysis is therefore essential for level 1. We find that stakeholders interests are not aligned in level 1 and policies are still being developed. There is no control over cloud risk yet. It is important to note that this does not mean that an organization is at high risk. It is possible that engineers have already implemented good security measures and that certain precautions have been taken. In fact, organizations at level 1 may have inherently less risk than those at level 3, due to good work of the engineers. However, there is no control, no governance, and no structure. It is not measurable and verifiable by anyone, and the risk governance process is not developed. This is certainly not desirable. What happens next is that at some point policies and governance are introduced by management. Policies are rules that processes and engineers must follow, and they describe the implementation of risk frameworks. A risk department or IT risk department is introduced and they come up with controls that are implemented from the top down. This is not monitored and improved. Without oversight, the policy cannot be consistently enforced. At a higher maturity level, there is monitoring and auditing, but because of the lack of alignment between the three stakeholders, policy enforcement remains inconsistent. This is the rapid pace of change in cloud technology which is a cloud-specific problem. Only when engineers are aware of the risks and the corresponding measures can they apply them consistently across the changing cloud landscape. This is what the following maturity levels should include. The discussion of top-down versus bottom-up risk management is central to this. This is explained in a later section on the intended usage of the maturity model. First, the findings are put into a maturity model and discussed.

In Table 9 the complete Cloud Riks Governance Maturity Model is shown. It features 6 columns with five maturity levels discussed in Section 2.4. The first column contains the relevant criteria areas described in 3 different characteristics. A characteristic, or sometimes a dimension, describes a specific area in which certain requirements must be met. The first characteristic, describes the development and enforcement of policies and governance frameworks at each maturity level. It highlights how organizations formalize their risk management strategies and ensure compliance with internal and external requirements. The second details the internal process of the organization in developing the cloud and applications. It focuses on the alignment and communication between various stakeholders, as well as the approach to implementing policies and controls. The third row, describes how controls and risk management activities are executed and monitored at each maturity level. Only when an organization meets these requirements, as well as the requirements in the other two dimensions, does it reside at a particular maturity level. The other five columns contain the five maturity levels: initial, managed, defined, controlled, and optimized. Each time the text within a maturity level is in *italics* and *grayed out* it means that characteristics are similar to the previous level. Not all characteristics of a certain maturity change when a higher level is achieved. If for example, policies and governance are defined and enforced, nothing more can change on that perspective.

Table 9: Cloud Risk Governance Maturity Model

Maturity level / area	Initial	Managed	Defined	Controlled	Optimizing
Policy and governance	No formal cloud policies or governance, a risk analysis is performed.	Cloud policies and governance frameworks are defined but not consistently enforced.	*Cloud policies and governance frameworks are defined but not consistently enforced.*	Cloud policies and governance frameworks are defined and consistently enforced.	*Cloud policies and governance frameworks are defined and consistently enforced.*
Process	Communication about cloud risk between management, IT risk and engineering not aligned and sporadic.	Cloud policies and controls are implemented in a top-down manner, lacking consistent communication and coordination.	*Cloud policies and controls are implemented in a top-down manner, lacking consistent communication and coordination.*	Top-down implementation of cloud policies with substantial input from engineering, strong alignment between IT risk and management.	Security by design with bottom-up implementation of cloud security controls, IT risk and engineering department fully aligned ensuring automated comprehensive risk management.
Implementation	Ad-hoc responses to threats, with no specified cloud controls or monitoring mechanisms.	Cloud controls are implemented and documented, no monitoring and auditing.	Cloud controls are implemented and documented, and regular monitoring and auditing.	Cloud controls are implemented and documented, and measured for improvement, regular monitoring and auditing.	Development is done with security by design, Cloud controls implementation and control is part of development cycle ensuring ongoing and automated improvement.

In the sections below we provide more detail to each maturity level of what is to be and not to be expected of an organization, and its characteristics. Then we discuss some intentions of the model and finally how to use the model.

4.3.1 Characteristics of Each Maturity Level

4.3.1.1 Initial level

At the first level, the initial level, organization lack many policies and ways of working to do effective risk management. There is an absence of structured governance, which leads to mostly ad-hoc responses to threats. An important aspect of this layer is that the communication between the three stakeholders, IT risk department, the engineers, and management, is sporadic an uncoordinated. It results in a lack of specified controls and monitoring mechanisms. In this approach organizations have no control over their cloud risk governance. A key component of the first level is conducting a thorough risk analysis. As was also highlighted in the interviews by E7: "A thorough risk analysis is the foundation for level 1. This analysis must be realistic and supported throughout the entire organization. So, it's not just an analysis that is drawn up by IT risk, but one that is jointly prepared by IT risk and the engineers, and then must be endorsed by management." However, conducting the analysis is just the beginning. What follows is the implementation. Risk analysis also have to be continuously performed, so update the understanding of risk for the organization.

To recap, import characteristics of the initial level are:

- **Policy and governance:** No formal cloud policies or governance, a risk analysis is performed.
- **Process:** Communication about cloud between management, IT risk and engineering not aligned and sporadic.
- **Implementation:** Ad-hoc responses to threats, with no specified cloud controls or monitoring mechanisms.

4.3.1.2 Managed level

In the next level, the managed level, organizations made their first step in cloud governance by defining risk governance policies and possibly frameworks. However, these policies are not consistently enforced across the entire organization. Leading to variability between various departments and/or applications. The implementation of the policies and risk frameworks happen in a top-down manner. IT risk departments come up with policies and management enforces the use of them. There is a lack of alignment between the three stakeholders which hampers effectiveness. In this stadium the policies are not yet consistently enforced across the entire organization, and not monitored or audited. Audits can either be internal audits or external audits done by other organizations. Controls and documentation exists, but are not comprehensive enough. Especially organizational and operational risks are still difficult to manage. This level is described by E7 as: "At the point where you also have formal policies and procedures regarding the mitigation of risks, for example in the form of controls, you enter level two. At this level, they may not be fully implemented and controls are not yet fully testable."

An overview of the characteristics of the managed level:

- **Policy and governance:** Cloud policies and governance frameworks are defined but not consistently enforced.
- **Process:** Cloud policies and controls are implemented in a top-down manner, lacking consistent communication and coordination.
- **Implementation:** Cloud controls are implemented and documented, no monitoring and auditing.

4.3.1.3 Defined level

With yet another jump in maturity, the next level is the defined level. At this level organizations have defined policies and frameworks as with the previous level but in that aspect not much changed. The process in which cloud technology and cloud applications are developed also did not change much. There is still a lack of consistent communication and a mostly top-down approach from management. What however did change compared to the managed level, is that the implemented controls are now monitored and regularly audited. This is a large step towards getting in control, since organizations are now able to measure their performance. Regular monitoring and auditing helps to ensure compliance and avoid problems with laws and regulations. This level is described by E9 as: "Technically sound, there is a governance baseline and everything is being implemented. What is missing is upward communication that leads to constant improvement." This is necessary to be consistent through the rapidly changing landscape of cloud technology.

The characteristics of the defined level are:

- **Policy and governance:** Cloud policies and governance frameworks are defined but not consistently enforced; similar to managed level.
- **Process:** Cloud policies and controls are implemented in a top-down manner, lacking consistent communication and coordination; similar to managed level.
- **Implementation:** Cloud controls are implemented and documented, and regular monitoring and auditing.

4.3.1.4 Controlled level

The next level, the controlled level, represents a significant advancement in risk governance maturity. Policies and governance frameworks are not consistently enforced. Cloud risk management practice is now an important organizational aspect. There is still a mostly top-down implementation of policies, however, now with a substantial input from engineering. Alignment between the three different stakeholders is strong and communication is effective. Cloud risk management practices are established, and enforced, while engineering is security aware. Monitoring is done in a similar manner as in the defined level. But the increased alignment between the stakeholders does lead to more efficient improvement. When an organization reaches this level, it can already consider itself as really mature. It is compliant and effective in mitigating risks. There is however still a slight disconnect between how policies are created, enforced and executed. The policies can have various different forms such as controls, or automated measures. There is still a strong emphasis on how cloud risk management practices and no full integration from the bottom-up. It is important to note that this is not at all bad. On the contrary even, it is necessary for organizations to achieve the highest maturity levels. Good cloud risk management practices have to be in place. Otherwise it is difficult to show that you are compliant and follow all necessary regulations. Interviewees also described that an important element of level 4 is self-assessment and improvement. This is partly made possible by the alignment of the three stakeholders.

A recap of the characteristics of the controlled level:

- **Policy and governance:** Cloud policies and governance frameworks are defined and consistently enforced.
- **Process:** Top-down implementation of cloud policies with substantial input from engineering, strong alignment between IT risk and management.
- **Implementation:** Cloud controls are implemented and documented, and measured for improvement, regular monitoring and auditing.

4.3.1.5 Optimizing level

At the final and most mature level, the optimizing level, organizations achieve the highest cloud risk governance maturity. Policies and governance frameworks are enforced across the entire organization. In addition, policies and frameworks are continuously improved from best emerging best practices. This is due to security being integrated into the design face. During the interviews E9 describes it as a full bottom-up approach to the implementation of security controls and measures is taken. The full alignment and collaboration between the three stakeholders, IT risk, engineering and management departments ensures cloud risk management is an integral part of the development lifecycle. This enables continuous improvement or security practices across the entire organization. These thoughts are reiterated by expert E8, E10, and E11. Automated risk management and control implementation can be part of this cycle.

- **Policy and governance:** Cloud policies and governance defined and consistently enforced; similar to controlled level.
- **Process:** Security by design with bottom-up implementation of cloud security controls, IT risk and engineering department fully aligned ensuring automated comprehensive risk management.
- **Implementation:** Development is done with security by design, cloud controls implementation and control is part of development cycle ensuring ongoing and automated improvement.

This maturity model for cloud risk governance offers a structured approach for organizations to assess and enhance their risk management capabilities. By systematically progressing through the levels of maturity organizations can achieve a more sophisticated and effective cloud risk governance. This model fosters a culture of continuous improvement and integration of the various stakeholders of cloud risk governance.

4.3.2 Goal of the Cloud Risk Governance Maturity Model

The idea of the maturity model is to help organizations develop in the area of cloud risk governance. As indicated in Section 2.4, it is a descriptive maturity model. This means it describes the maturity level an organization currently may be at, depending on a number of factors. With this knowledge, organizations can create their own plans to improve on all points, and thus achieve a higher level of maturity. The specific conditions an organization must meet to reach this level will be discussed in the next section.

This model's structure results from several findings made during interviews about cloud risk. We consciously chose to deviate from maturity models such as those of NIST and ISO. During the interviews, it emerged that one of the biggest problems with cloud risk governance is the disconnect between the three stakeholders, especially between IT risk and management and the engineers. As noted in an interview: "Those who need to determine which boxes to check are often at a different layer in the organization, but they are the ones who know what they are talking about in terms of cloud." The technology is so complex and changes so quickly that good risk governance must be supported by the entire organization. True maturity indicates that risk management is fully supported by the engineers, who understand what is happening and must indicate what is needed. From the bottom up, risk frameworks should be established and supported by IT risk departments and management. These frameworks will then align with the IT that the organization actually uses.

However, this is a challenge. People who understand both the technology and the value of good risk management are often few. As highlighted in the interviews: "Most engineers don't have the overview. They just do their job and try to develop or implement as quickly and well as possible. They don't want to think about risk management because that's traditionally what the IT risk department is concerned with. Yet they often have the knowledge to create good controls because they understand the technology."

The goal of this maturity model is to bring these perspectives closer together and to show organizations how they can grow in terms of policy and governance, implementation of controls and monitoring, and the work process. What makes this model unique is the integration of the three dimensions and the stipulation that an organization can only progress to the next level if there is growth in all three dimensions. We describe this as a security-by-design approach, emphasizing awareness and a good strategy. A quote from the research reflects this well: "[...] the highest maturity actually comes down to a good alignment between different control lines and management, having a good discussion and escalation structure where constant consideration is given to these kinds of topics. Especially in large organizations where many different bodies need to look in the same direction. Ultimately, an organization runs on people who perform certain actions." This connection between engineers and other parts of the organization is essential for good cloud risk governance due to the clouds intrinsic characteristics. Engineers have to manage constant change and complexity of the technology. We discovered that with cloud technology, you simply cannot do without the involvement and alignment of the engineers. In itself, this is not a particularly exciting discovery, but incorporating it into a maturity model is the innovative part. By choosing to deviate from existing models, we created a unique model that can help organizations achieve maturity on multiple dimensions. Looking at cloud risk governance from a holistic management perspective as well as from a workforce perspective.

4.3.3 Using the Cloud Risk Governance Maturity Model

As mentioned earlier, the maturity model is a descriptive maturity model. This means that it describes only the types of maturity that exist and where an organization falls within them, not what organizations need to do to improve. To use the model, an organization would need to develop a questionnaire that would allow it to place itself in one of the different levels, or at least conduct some form of internal research. This could include questions about the various controls implemented, the policies and control frameworks in place, and the awareness and collaboration of engineers.

The maturity model can be used within a company to raise awareness among all three stakeholders and to familiarize everyone with the complexity of cloud risk management. For management, it can be used to demonstrated that policies from the top-down are not the only requirement for a mature risk management practice. At the IT risk department, the model can be used to create awareness among both engineers and management about the importance of risk management at different levels. Meanwhile, with engineers, the model can be used to raise awareness about risks and the importance of their involvement. A core component of the maturity model is that an organization can only move up a level if it has reached the next level across all three axes, or characteristics. Therefore, an organization must not only have policies in place, but they must be monitored and there must be the right level of awareness among all three stakeholders. This is particularly true for the engineers who need to understand what they must do and why they must do it, and who must genuinely support and execute these actions. Organizations need to address this as they implement the Cloud Risk Maturity Model. Combined with the Top 8 Risk Topics, cloud risk governance can be effectively managed.

At the first level, organizations need to establish cloud policies and governance. They also need to consider that there is currently no alignment between the three stakeholders, so communication channels should be opened. There is currently only an ad hoc response to threats, so some cloud controls should be established. If organizations can do this, they can move on to level 2. At level two, organizations should start monitoring and auditing the controls that are in place. They should be within a defined control framework and be auditable. To achieve level three, this should be done on a regular basis. Auditing can be either internal or external. At level three, organizations have a fairly solid risk management practice. However, they lack alignment among stakeholders, which prevents policies from being consistently enforced across the organization and controls from being regularly updated and maintained. This, in turn, is problematic due to the rapidly changing environment of the cloud. Only when this is resolved will organizations be able to grow to the highest level of maturity.

4.4 Towards Effectively Managing Cloud Risk Governance

The relationship between the findings of assessing cloud risk governance, improving, and the maturity model is essential for effectively managing cloud risk governance. This section first reiterates the research questions and structures the results, then the relationship is discussed. To systematically address the central research question, it was broken down into three sub-questions. Each sub-question targeted an aspect of cloud risk governance to help address and achieve overall effective management. The approach was inspired by the instrumental work of Luftman (2004) on IT governance. Since cloud is just an IT tool and way of computing, this theory was readily applicable. The sub-questions were supported with more questions which will also be answered in this section.

Sub-question 1 results

The first sub-question studied how organizations can assess their cloud risk governance. The goal of the research question was to identify risk factors which facilitates assessments, and discover how organizations currently address cloud risk governance. The research question was as follows:

How can organizations assess their cloud risk governance?

We found that organizations have to identify cloud-specific risks, and consequently the most vulnerable cloud risks. We discovered that the type of cloud deployment does not impact the impact risk management practices heavily. Although the more you rely on a service provider the more risks shifts. This was also emphasized in the final validation interview. However, with newer cloud technologies this might change. We identified three different stakeholders, the Management (policy enforcers and creators), the IT Risk team (risk management), and the Engineers (cloud administrators and application developers or designers). It became apparent form the interviews that organizations often do not use existing cloud governance frameworks due to their complexity and relative ambiguity.

Below the objectives are formulated in questions below with a short summary of the results:

a) What common vulnerabilities are identified during assessments of cloud risk governance?
We identified a list of cloud-specific risk topics found in Section 2.2.2.

b) What criteria do organizations use to assess cloud risk governance?
Organizations use generic risk assessment methods. First risks are identified, then their likelihood and impact are determined. Then their risk level is determined, and if controls are already implemented a residual risk remains. No special risk assessment method is required for cloud risk. Although there are some researches who specify the need for an automated approach.

c) What type of cloud is most vulnerable for governance risks?
No specific cloud deployment is always more vulnerable for governance risk. However, due to increased configuration complexity IaaS and PaaS environments allow for more vulnerabilities to exist, it is not necessarily the case that they exist.

d) What tools or methods do organizations employ to effectively assess their cloud risk governance?
Organizations cloud use cloud risk management frameworks or other methods. There is no specific answer to this question. An interesting observation from the interviews however, was that organizations can unconventional measures like service outage time to measure risk in development and deployment for example.

e) What metrics or indicators are most tracked in cloud risk governance assessments?
This objective did not yield any relevant answers.

f) Who are the stakeholders in cloud risk governance?
In cloud risk management there are three stakeholders which have to work together. They are the Management (policy enforcers and creators), the IT Risk team (risk management), and the Engineers (cloud administrators and application developers or designers).

Relation to other sub-questions

The results of the first sub-question feed into second question. The results showed that organization should look at cloud-specific risk topics. However, they also showed that organizations are not waiting for yet another large and ambiguous cloud risk framework. Therefore we decided to focus on specific topics instead of on all of them to concentrate resources and budget. Implementing a small subset of essential risk topics would allow for this.

Sub-question 2 results

The second sub-question discussed how organizations can improve their cloud risk governance. The sub-question was as follows:

How can organizations improve their cloud risk governance?

We found that we should focus on a subset of risk topics. So we asked industry experts to rank the risk topics that were earlier identified. This resulted in 8 Top Risk Topics discussed in Section 4.2.1.

Below the objectives are formulated in questions below with a short summary of the results:

a) What is recommended by industry experts for enhancing cloud risk governance?
The 8 Top Risk Topics.

b) What measures have organizations implemented that led to recognized improvements in cloud risk governance?
Organizations often implement controls, but there are also other measures that can help. There was no specific answer to this question. The aim was to identify if organizations implement certain frameworks or other measures but they often did not. However, if organizations had to be compliant with stringent regulations, such as banks, they often implemented extensive self-made control frameworks. They were sometimes based on existing ones, and sometimes even mapped. Experts did point out that mappings are often very inefficient since control frameworks can change and mappings need to be redone.

Relation to other sub-questions

The 8 Top Risk Topics are created using the results of the previous sub-question. The risk topic can now be implemented into new or existing control frameworks at organizations. However, this directly make an organization efficient in managing cloud risk governance. For this, an mature cloud risk governance environment is also required. This is due to the rapid changes in cloud technology.

Sub-question 3

The third and final sub-question researched incorporating a maturity dimension into cloud risk governance. Looking at the extent to which organizations cloud risk governance practices are aligned within their organizations. The research question was as follows:

How can organizations achieve mature cloud risk governance?

We designed and created a maturity model called the Cloud Risk Governance Maturity Model. It was based on the CMM and featured similar levels. Then it incorporated 3 dimensions or categories which defined the maturity level of an organization. The dimensions are policy and governance, process, and implementation, which are defined in Section 4.3.

Below the objectives are formulated in questions below with a short summary of the results:

a) What stages of maturity exist on cloud risk governance?
There exist five stages of maturity with three dimensions. Each dimension describes an area in which the organization can be mature. See Section 4.3 for details.

b) How can a stage of cloud risk governance maturity be achieved?
A next stage in maturity can be achieved by fulfilling the requirements for that stage. Specific requirements are future work.

Interplay between results

The relationship between the assessment, improvement, and maturity models is crucial for effective cloud risk governance. The assessment phase lays the foundation by identifying risks and vulnerabilities, informing the improvement strategies. These strategies now feed into the maturity model, providing a structured approach to enhance governance practices systematically. This iterative process ensures continuous improvement and adaptation to emerging risks and technological advancements. Combined the results facilitate effective cloud risk governance and management. In the following section the results will be discussed. The discussion is followed by the conclusion of the report.

5 Discussion

5.1 Summary

The central research problem addressed in this study is the difficulty organizations face in controlling cloud risks and effectively implementing cloud risk governance. This challenge is compounded by unclear responsibility allocation, the absence of standardization, difficulty of understanding cloud intrinsic risks, and the difficulties of navigating large governance frameworks. These obstacles require a robust mechanism to grasp and manage cloud risks, as well as to evaluate and enhance their cloud risk governance maturity. To address these issues, the research aims to develop a best practice model that not only outlines the minimum requirements for effective governance but also integrates a maturity dimension to assess and incrementally improve governance practices.

In researching cloud risk governance we concluded the following. We found that cloud-specific risks are risks that are extra relevant due to the intrinsic nature of the cloud, or specifically occur only in the cloud. Besides, we found that due to reliance on service providers organizations are often confused in where their responsibilities lie. Moreover, we found that organizations do not often use existing cloud risk frameworks due to the difficulty of implementing them. They are often very ambiguous to be broadly applicable. This is not per se bad, but due to their enormous size difficult to implement. As some experts put it “they are a beast of a framework”. This study opted to focus of a selection of 8 topics to make improvement for organizations more effective. Also keeping the models non-specific so they would be broadly applicable in various contexts.

This is resulted in a selection of 8 Top Risk Topics organizations should focus to improve their cloud risk governance. These topics have been distilled through various interviews and are as follows:

- Identity access management risks
- API security risks
- Cloud-specific governance risks
- Endpoint Security risks
- Third-party risks
- Account security risks
- Laws and regulation risks
- Compliance risks

Focused management of these risk issues is recommended as a means of effectively aligning organizational resources to mitigate the most pressing threats to the cloud environment. This strategic prioritization not only streamlines efforts, but also ensures that investments in people, budget, and technology are focused on improving the overall cloud security landscape.

This was followed by the introduction of the Cloud Risk Governance Maturity Model. This model is structured to guide organization through 5 stages of maturity. The goal of this maturity model is to bring the various perspectives of the 3 uncovered stakeholders – management, IT risk, and engineers – closer together, and to show organizations how they can grow in terms of policy and governance, execution, and work processes. We discussed the security-by-design approach, emphasizing awareness and a good risk strategy is essential within organizations. Recognizing the connection between engineers and other parts of the organization is the only way to achieve the highest maturity. In the table below the Cloud Risk Governance Model is presented in a compact (vertical) manner.

Table 10: Cloud Risk Governance Maturity Model recap vertical

Level	Characteristics
Initial	▸ **Policy and governance:** No formal cloud policies or governance, a risk analysis is performed. ▸ **Process:** Communication about cloud between management, IT risk and engineering not aligned and sporadic. ▸ **Implementation:** Ad-hoc responses to threats, with no specified cloud controls or monitoring mechanisms.
Managed	▸ **Policy and governance:** Cloud policies and governance frameworks are defined but not consistently enforced. ▸ **Process:** Policies and controls are implemented in a top-down manner, lacking consistent communication and coordination. ▸ **Implementation:** Controls are implemented and documented, no monitoring and auditing.
Defined	▸ **Policy and governance:** Cloud po*licies and governance frameworks are defined but not consistently enforced;* similar to managed level. ▸ **Process:** *Cloud policies and controls are implemented in a top-down manner, lacking consistent communication and coordination;* similar to managed level. ▸ **Implementation:** Cloud controls are implemented and documented, and regular monitoring and auditing.
Controlled	▸ **Policy and governance:** Cloud policies and governance frameworks are defined and consistently enforced. ▸ **Process:** Top-down implementation of cloud policies with substantial input from engineering, strong alignment between IT risk and management. ▸ **Implementation:** Cloud controls are implemented and documented, and measured for improvement, regular monitoring and auditing.
Optimizing	▸ **Policy and governance:** Cloud po*licies and governance defined and consistently enforced;* similar to controlled level. ▸ **Process:** Security by design with bottom-up implementation of cloud security controls, IT risk and engineering department fully aligned ensuring automated comprehensive risk management. ▸ **Implementation:** Development is done with security by design, cloud controls implementation and control is part of development cycle ensuring ongoing and automated improvement.

The relationship between the assessment, improvement, and maturity models is crucial for effective cloud risk governance. After an organization has identified the stakeholders and they have performed a risk analysis they are able to improve on their cloud risk governance. The improvement is rooted in the implementation of the 8 Top Risk Topics. They help an organization focus their resources more effectively. This feeds into the maturity model, providing a structured approach to effectively improving cloud risk governance.

5.2 Interpretation

The results, and in particular the artifacts as described in Section 4, can be used in a multitude of ways within organizations. The objective was to ensure their broad applicability, with the understanding that they must be tailored to the specific organization. The artifacts, the 8 Top Risk Topics, and the Cloud Risk Governance Maturity Model, when utilized collectively, can be effectively used in a broad range of organizations, provided that they make use of public cloud services. In various sectors, the 8 Top Risk Topics are often relevant, and it is always advisable to pay particular attention to them. Due to numerous cloud-specific characteristics, organizations will always have to address these issues. An interesting and recent example has emerged where Dell, a technology company, was hit by a major attack on an API that was not secured (Abrams, 2024). As a result, 49 million customer records were stolen. The article also emphasizes an increase in the number of attacks due to unsecured APIs, highlighting the importance of this research. Additionally, the Cloud Risk Governance Maturity Model is highly useful in any organization. Creating awareness around cloud risk is beneficial in almost all contexts.

Benefits to organizations

Organizations should greatly benefit from implementing the research findings. By adopting the 8 Top Risk Factors organization are able to mitigate the most important risks. Awareness about cloud risk is raised and many improvements can be made. The research is also useful for organizations facing challenges in aligning their risk management practices with their overall cloud strategy. By integrating insights from the assessment, improvement, and maturity dimensions, organizations can develop a cohesive and effective approach to cloud risk governance, and possibly also cloud deployment. A few key advantages can be thought of:

1. Organizations can identify and mitigate cloud-specific risks more effectively, reducing the likelihood of business continuity issues and security breaches.
2. Adherence to legal and regulatory requirements is streamlined, minimizing the risk of penalties and legal issues.
3. Focused management efforts ensure that resources are allocated efficiently, addressing the most significant threats without spreading efforts too thin.
4. The alignment of risk management practices with business objectives fosters a cohesive approach to cloud governance, supporting overall organizational goals. This allows for more competitive advantage and accelerated growth

There is an increase number of cloud breaches from year to year. Almost all organizations struggle with cloud strategy, and security is among the top reasons for this. It is essential organizations get a grip on their cloud risk (Experts Insights, 2021).

Discussion on using the model

When using the Cloud Risk Governance Maturity Model it is challenging to effectively use it without sufficient knowledge about the organization. It is crucial to recognize the various stakeholders and have knowledge about current processes, and governance structure. To gather this information extensive surveys are often used. However, as this was not part of this study, they are not yet developed. Organization must therefore develop these for themselves, which can be quite challenging.

An import point of discussion during the interviews and validation was the usage of the CMM model. It is a well-known maturity model which knows many different forms. During the interviews there was a lot of discussion on the naming of the second, third and fourth level. Some experts agreed on the current naming scheme while suggested swapping the second and fourth level. There are versions of CMM model who apparently have the following levels: initial, repeatable, defined, managed, and optimizing. This caused confusion, but we decided to stick with the version as described in Section 2.4. We also decided not to discuss it outside this section to avoid confusion.

Relevant studies

Upon examining other research in the field of cloud risks and maturity, several key findings emerge. First, a number of studies have identified similar cloud risks and ranked them. The results of these studies are often comparable, but sometimes take a different angle. Some research focuses more on specific threats, while this study is more directed towards governance. Additionally, there are other non-academic studies that focus on the security process but not on auditing and control (Katz, 2023).

5.3 Implication

Practical implications

The model developed in this research provides organizations with a practical guideline for deploying a risk management strategy tailored to cloud-specific challenges. This can help businesses navigate the complexities of cloud governance more effectively. Awareness on cloud risks is raised which can lead to more informed decision-making, reduced overall risk and enhanced cloud security, with the added benefit of being cost effective due to focus on a selection of topics. This research offers a structured way for organizations to gain control in their cloud risk governance using the Cloud Risk Governance Maturity Model. Together it provides organizations with practical ways of improving their cloud risk management.

Theoretical implications

The study shows how organizations can effectively manage their cloud risk governance, addressing the current gap in literature. Through qualitative insights a lot of industry data was gathered which can be valuable for future studies. We tried to make the data available through using direct quotes from the interviews. There are four interesting theoretical findings. First, this study finds that effective cloud risk governance requires extensive collaboration between stakeholders, often more then with traditional IT. Second, this study contributes to a better understanding of cloud ecosystem within organizational contexts. Third, this research defines 8 Top Risk Topics which can be further investigated on their presence within organizations. Fourth, this research adds to the academic context of maturity model for cloud risk governance. This model can serve as a basis for further research, enabling scholars to refine and expand upon the initial framework.

5.4 Research validity

In Table 8 we discussed several threats to validity and reliability. This section covers all the potential threats, the measures taken, and the effectiveness of the mitigation measures. This section consists of a discussion on threat topic in Table 8.

Construct validity

The study ensured construct validity by applying the three mitigations proposed in Section 3.4.1. During the research we used multiple sources for reasoning. The literature review ensured the concepts are all grounded in literature and that the research method that was used was as well. The interviews provided first hand insights and expert opinions, and the expert validations practical insights from outside perspective. Moreover, E16 provided valuable knowledge about the academic methodology. The triangulation of the three sources benefits the construct validity. Furthermore, during the whole process there was oversight of supervisors reviewing the process and assuring quality by giving feedback. Lastly, experts were asked during the second and third phase of the project to give feedback on the construct itself.

All things considered, the 8 Top Risk Topics can be easily considered to have good construct validity. The Cloud Risk Governance Maturity Matrix however, is more prone. It remains difficult to make a clear distinction between the different levels because requirements can fall into a gray area. Governance may have been established and checked, but how do you know if it is being executed by everyone? A more detailed checklist can contribute to this.

Internal validity

Internal validity was ensured by first trying to reduce bias among interviewees. During the interviews, inquisitive questions were always asked with as little opinion from the researchers as possible. Additionally, input from the experts was always requested before they were shown the information to be discussed. Furthermore, internal validity was ensured by identifying confounding variables and exploring the relationship between possible variables. Factors like industry, organizational size and structure, country, existing governance, and potential personal experience were all considered. A wide range of varying interviewees was selected with very diverse backgrounds. Together they are able to provide wide enough viewpoint.

Other design decisions could have been made to improve the internal validity of the research. More specific areas, control frameworks, and industries could have been considered. However, this would have also hindered the generalizability. It was therefore a conscious decision not to, but given more time it could still be done.

External validity

Generalizability of the findings, or external validity, is accounted for in two different ways. First, several measures were taken to make the findings more generalizable and the research process easier to replicate. The scope of the project is specific and explains from which viewpoint the results should be interpreted. While again the diverse backgrounds of the interviewees ensures the results are applicable in various contexts, organizations, and environments. Cloud risk governance however, is a topic with not that many experts. It requires extensive knowledge of a quickly changing technology and of how large organizations operate. The highest effort was taken to find participants willing to participate in the constrained amount of time for this report. A larger pool of participants would have increased the external validity. Second, the design of the artifacts takes generalizability into account. The artifacts are designed to be applicable in a broad context across many different organizations. The downside of this is that organizations may potentially still have to do the work to tailor the artifact to their specific needs.

Reliability

Reliability is ensured by extensive documentation of the research process. All interview questions are documented and follow a specific protocol. The scope of the project is clearly defined as are other research variables. This ensures that other researchers are able to replicate the results

6 Conclusion

This study investigated how organizations can effectively manage their cloud risk governance. The central question of this thesis was:

How can organizations effectively manage their cloud-specific risk governance?

This was investigated by doing two phases of interviews with subject matter experts and doing three expert validation interviews with industry experts. This chapter describes the results of the three sub-questions and links them to the central research question.

Sub-question 1

Sub-question one focused on assessing cloud risk, the sub-question was:

How can organizations assess their cloud risk governance?

To answer this question we first investigated cloud in itself, and its intrinsic characteristics related so security in Section2. This resulted in a list of cloud risks topics, and stakeholders. During phase 1 of the interviews we discovered the effect of the different cloud service models and existing cloud security frameworks within organizations. We found that there are three important stakeholders, the management, the IT risk department, and the engineers. Also, that organization often do not use existing security frameworks due to their size and complexity. In addition, we discovered that the type of service models does not affect the cloud risk so significantly that the research had to address this. This knowledge feeds into the second sub-question.

Sub-question 2

The second sub-question explored how organizations improve their cloud risk governance, and the sub-question was:

How can organizations improve their cloud risk governance?

During the first phase of the interviews subject matter experts were asked to rank the list of risk topics on what they deemed to be the most important topics. Thus creating a recommendation on which risk topics to focus on. Using both interview coding and a visual analysis of a heatmap of the ranking we found 8 Top Risk Topics. For these topics all risks have to be analyzed within the organization and controls have to be implemented. How this should be done was not specified since we discovered that it can be very organization specific on what works best.

Sub-question 3

Finally, sub-question three considered how organizations could be the most effective in cloud risk governance by researching maturity. The sub-question for this part was:

How can organizations achieve mature cloud risk governance?

To achieve mature cloud risk governance, organizations should follow the structured Cloud Risk Governance Maturity Model. The model describes five maturity levels with three categories per level – policy and governance, process, and implementation. The models helps organizations align and improve the three different perspectives and emphasizes awareness and security-by-design. Were high alignment comes down to alignment between the stakeholders on top of good governance and control processes. The model different stages were inspired by the CMM described in Section 2.4, and the various stages were discovered during the second phase of interviews with subject matter experts. The Cloud Risk Maturity Model is described in Section 4.3 and together with the results of the previous to sub-questions feeds into the main research question.

Main research question

The integrating the results from sub-questions on how to assess cloud risk governance, improve cloud risk governance, and achieve maturity on cloud risk governance we provide an effective approach to managing cloud risk governance. To reiterate the main research question:

How can organizations effectively manage their cloud-specific risk governance?

Organizations can effectively manage their cloud-specific risk governance by analyzing their cloud-specific risks, and defining the three stakeholders within their organization. Then they should implement the 8 Top Risk Topics within the risk frameworks. Finally, to actually implement them effectively, organizations must use the Cloud Risk Governance Maturity Model and evolve in all three different perspectives so to ultimately work from a security first perspective.

7 Limitations

While the research has made significant theoretical contributions, it is not without limitations. The sampling strategy, primarily within EY, may introduce selection bias, potentially limiting the generalizability of the findings. Future research could expand the sampling pool to include a wider range of organizations and industries to enhance the external validity of the artifact. More industries could have been considered, as well as smaller organizations for example. Moreover, during the study mostly qualitative analysis was performed. The results could gain more academic value, especially the 8 Top Risk Topics, if those were also quantitatively tested.

Also, in our research, we made a conscious decision to mostly focus on the management perspective. One potential shortcoming is that the risk topics might not specific enough on the possible issues. For instance, we could have explored which types of APIs are often susceptible to problems, and this could have been made more specific for each CSP. The downside would have been that the model would have had a very narrow application. As it stands, it's more broadly applicable but still requires further specification.

Another limitation of our study is that both the 8 Top Risk Topics and the maturity model are not industry-specific. As a result, they trade off a more specific application for broader applicability. As has been mentioned before, different industries have different regulations regarding cloud usage. For example, the banking sector has much stricter rules than the retail sector. Certain risks may then be more critical, and others less so. This was a deliberate choice to keep the model widely applicable.

The study also considered a broad range of cloud applications. This could have affected the results in many ways. I case studies were performed focusing on various organizations with similar cloud capabilities, the results would have bene more generalizable.

Additionally, the rapid evolution of cloud technologies and risk landscapes suggests that the artifact may require continuous refinement. Future research could focus on the dynamic adaptation of the artifact to ensure its ongoing relevance and effectiveness in cloud risk governance.

7.1 Future work

Future research could enhance this study by delving deeper into the following areas:

1. Maturity assessment model: The current Cloud Risk Governance Maturity Model doesn't yet allow for an assessment to be conducted within an organization. The model could be expanded with a checklist of characteristics for each maturity level and a corresponding questionnaire. With the questionnaire and checklist, an organization can improve in a more targeted manner. Interesting areas of research, would be to do this with generative AI. The maturity model would remain to be broadly applicable while using AI it will be made specific to the desired context.
2. Sector specific: Both the Cloud Risk Governance Maturity Model and the 8 Top Risk Topics could be tailored to specific industries and applications. The various risk topics could be supplemented with concrete vulnerabilities from the MITRE database that may be relevant to the specific sector. Provided the right context, AI models can also help in creating sector specific maturity models.
3. Risk Topics Ranking: Currently, the 8 Top Risk Toics are not ranked. An extended survey could determine the absolute position of these topics. The survey could provide valuable insights in current

issues within organizations. Due to the way the research was conducted, where experts indicate which problems they find important and often see recurring, an assumption can be made about the problems organizations are currently facing, but these findings are not grounded in research.

4. Adapt to future cloud features: Since cloud technology evolves rapidly, it will be necessary to continuously analyze whether the findings remain current. CSPs are increasingly improving their products, which may reduce certain risks. Furthermore, technologies such as Functions as a Service (FaaS) could potentially shift more management responsibilities away from the user in the future, leading to the emergence of different risk priorities. Moreover, cloud organizations are constantly improving there offering, new and improved products in the area of IAM, endpoint management, and security can in the future help mitigate certain risks.
5. Edge computing: As edge computing is advancing, the governance of edge devices and data becomes increasingly important. Future work could investigate how cloud risk governance frameworks can be extended to include edge computing environments.
6. Increased regulations: Regulations on cloud computing usage is changing in a rapid rate al around the world. The impact of new and upcoming regulations should be further researched. An impactful example would be the European Data Act and the EU Cloud Rulebook. Also the European cybersecurity certification scheme for cloud services cloud play an important role in governing cloud in the future, more research should be done in how this integrates in the Cloud Risk Governance Maturity Model.
7. Automated risk analysis tools: Future research should explore automated risk analysis tools, such as EY Cloud Risk View, on their impact within organizations. Study if organizations can effectively manage cloud using automated tools.
8. Zero trust principle: Future research can investigate the integration of the Zero Trust principle into the existing Cloud Risk Governance Maturity Model. This may involves examining how components things as continuous authentication, least privilege access, micro-segmentation, and continuous endpoint protection can be incorporated into cloud governance policies and practices. In addition, it can be explored how zero trust impacts assessment and management of cloud governance.

8 References

Abdalla, P., & Varol, A. (2019). *Advantages to Disadvantages of Cloud Computing for Small-Sized Business* (p. 6). https://doi.org/10.1109/ISDFS.2019.8757549

Abrams, L. (2024, May 10). *Dell API abused to steal 49 million customer records in data breach*. BleepingComputer. https://www.bleepingcomputer.com/news/security/dell-api-abused-to-steal-49-million-customer-records-in-data-breach/

Aguiar, T., Bogea Gomes, S., Rupino Da Cunha, P., & Mira Da Silva, M. (2019). Digital Transformation Capability Maturity Model Framework. *2019 IEEE 23rd International Enterprise Distributed Object Computing Conference (EDOC)*, 51–57. https://doi.org/10.1109/EDOC.2019.00016

Akinsanya, O. O., Papadaki, M., & Sun, L. (2020). Towards a maturity model for health-care cloud security (M2HCS). *Information & Computer Security*, *28*(3), 321–345. https://doi.org/10.1108/ICS-05-2019-0060

Albakri, S. H., Shanmugam, B., Samy, G. N., Idris, N. B., & Ahmed, A. (2014). Security risk assessment framework for cloud computing environments. *Security and Communication Networks*, *7*(11), 2114–2124. https://doi.org/10.1002/sec.923

Aleem, A., & Sprott, C. R. (2013). Let Me in the Cloud: Analysis of the Benefit and Risk Assessment of Cloud Platform. *Journal of Financial Crime*, *20*(1), 6–24. https://doi.org/10.1108/13590791311287337

Alouffi, B., Hasnain, M., Alharbi, A., Alosaimi, W., Alyami, H., & Ayaz, M. (2021). A Systematic Literature Review on Cloud Computing Security: Threats and Mitigation Strategies. *IEEE Access*, *9*, 57792–57807. https://doi.org/10.1109/ACCESS.2021.3073203

Al-Ruithe, M., Benkhelifa, E., & Hameed, K. (2019). A systematic literature review of data governance and cloud data governance. *Personal and Ubiquitous Computing*, *23*(5), 839–859. https://doi.org/10.1007/s00779-017-1104-3

Amah, U., Mart, J., & Oyetoro, A. (2023). *Cloud Security Governance Guidelines* [Preprint]. https://doi.org/10.14293/PR2199.000062.v1

Apeh, A. J., Hassan, A. O., Oyewole, O. O., Fakeyede, O. G., Okeleke, P. A., & Adaramodu, O. R. (2023). GRC STRATEGIES IN MODERN CLOUD INFRASTRUCTURES: A REVIEW OF COMPLIANCE CHALLENGES. *Computer Science & IT Research Journal*, *4*(2), Article 2. https://doi.org/10.51594/csitrj.v4i2.609

AWS. (2024). *Shared Responsibility Model—Amazon Web Services (AWS)*. Amazon Web Services, Inc. https://aws.amazon.com/compliance/shared-responsibility-model/

Becker, J., Knackstedt, R., & Pöppelbuß, J. (2009). Developing Maturity Models for IT Management. *Business & Information Systems Engineering*, *1*(3), 213–222. https://doi.org/10.1007/s12599-009-0044-5

Becker, & Jörg. (2006). *Epistemological Perspectives on Design Science in IS Research*. https://core.ac.uk/reader/301339980

Bennett, K. W., & Robertson, J. (2019). Security in the Cloud: Understanding your responsibility. *Cyber Sensing 2019*, *11011*, 1101106. https://doi.org/10.1117/12.2521821

Bhushan, K., & Gupta, B. b. (2017). Security challenges in cloud computing: State-of-art. *International Journal of Big Data Intelligence*, *4*(2), 81–107. https://doi.org/10.1504/IJBDI.2017.083116

Brandis, K., Dzombeta, S., Colomo-Palacios, R., & Stantchev, V. (2019). Governance, Risk, and Compliance in Cloud Scenarios. *Applied Sciences*, *9*(2), Article 2. https://doi.org/10.3390/app9020320

Cano M., J. J. (2023). Maturity Model for Boards of Directors in Cyber Risk Governance. A Conceptual and Practical Proposal. In Á. Rocha, C. H. Fajardo-Toro, & J. M. Riola (Eds.), *Developments and Advances in Defense and Security* (pp. 39–51). Springer Nature. https://doi.org/10.1007/978-981-19-7689-6_4

Carcary, M. (2013). IT Risk Management: A Capability Maturity Model Perspective. *Electronic Journal of Information Systems Evaluation*, *16*(1), Article 1.

Cayirci, E., Garaga, A., Santana de Oliveira, A., & Roudier, Y. (2016). A risk assessment model for selecting cloud service providers. *Journal of Cloud Computing*, *5*(1), 14. https://doi.org/10.1186/s13677-016-0064-x

Chao, P. G., & Baptista, N. M. (2009). Surfacing ERP exploitation risks through a risk ontology. *Industrial Management & Data Systems*, *109*(7), 926–942. https://doi.org/10.1108/02635570910982283

Chauhan, M., & Shiaeles, S. (2023). An Analysis of Cloud Security Frameworks, Problems and Proposed Solutions. *Network*, *3*(3), Article 3. https://doi.org/10.3390/network3030018

Cloud Security Alliance. (2024). *Cloud Controls Matrix and CAIQ v4 | CSA* (Version v4). https://cloudsecurityalliance.org/artifacts/cloud-controls-matrix-v4

Coates, J. C. (2007). The Goals and Promise of the Sarbanes–Oxley Act. *Journal of Economic Perspectives*, *21*(1), 91–116. https://doi.org/10.1257/jep.21.1.91

De Haes, S., & Van Grembergen, W. (2004). IT governance and its mechanisms. *Information Systems Control Journal*, *1*, 27–33.

De Haes, S., van grembergen, W., & Debreceny, R. (2013). COBIT 5 and Enterprise Governance of Information Technology: Building Blocks and Research Opportunities. *Journal of Information Systems*, *27*. https://doi.org/10.2308/isys-50422

Di Giulio, C., Sprabery, R., Kamhoua, C., Kwiat, K., Campbell, R. H., & Bashir, M. N. (2017). Cloud Standards in Comparison: Are New Security Frameworks Improving Cloud Security? *2017 IEEE 10th International Conference on Cloud Computing (CLOUD)*, 50–57. https://doi.org/10.1109/CLOUD.2017.16

Dillon, T., Wu, C., & Chang, E. (2010). Cloud Computing: Issues and Challenges. *2010 24th IEEE International Conference on Advanced Information Networking and Applications*, 27–33. https://doi.org/10.1109/AINA.2010.187

Djemame, K., Armstrong, D., Guitart, J., & Macias, M. (2016). A Risk Assessment Framework for Cloud Computing. *IEEE Transactions on Cloud Computing*, *4*(3), 265–278. https://doi.org/10.1109/TCC.2014.2344653

Dutta, A., Peng, G. C. A., & Choudhary, A. (2013). Risks in Enterprise Cloud Computing: The Perspective of it Experts. *Journal of Computer Information Systems*, *53*(4), 39–48. https://doi.org/10.1080/08874417.2013.11645649

Experts Insights. (2021, June 14). 50 Cloud Security Stats You Should Know In 2024. *Expert Insights*. https://expertinsights.com/insights/50-cloud-security-stats-you-should-know/

Farrell, R. (2010). Securing the Cloud—Governance, Risk, and Compliance Issues Reign Supreme. *Information Security Journal: A Global Perspective*, *19*(6), 310–319. https://doi.org/10.1080/19393555.2010.514655

Fortis, T.-F., & Munteanu, V. I. (2014). From Cloud Management to Cloud Governance. In Z. Mahmood (Ed.), *Continued Rise of the Cloud: Advances and Trends in Cloud Computing* (pp. 265–287). Springer. https://doi.org/10.1007/978-1-4471-6452-4_11

Gartner. (2023a, February 14). *The Future of Cloud Computing in 2027: From Technology to Business Innovation*. Gartner. https://www.gartner.com/en/doc/768816-the-future-of-cloud-computing-in-2027-from-technology-to-business-innovation

Gartner. (2023b, November 9). *Gartner Says Cloud Will Become a Business Necessity by 2028*. Gartner. https://www.gartner.com/en/newsroom/press-releases/2023-11-29-gartner-says-cloud-will-become-a-business-necessity-by-2028

Gomes, A., & Okano-Heijmans, M. (2024). *Too late to act? Europe's quest for cloud sovereignty*.

Gong, C., Liu, J., Zhang, Q., Chen, H., & Gong, Z. (2010). The Characteristics of Cloud Computing. *2010 39th International Conference on Parallel Processing Workshops*, 275–279. https://doi.org/10.1109/ICPPW.2010.45

Henderson, J. C., & Venkatraman, H. (1999). Strategic alignment: Leveraging information technology for transforming organizations. *IBM Systems Journal*, *38*(2.3), 472–484. https://doi.org/10.1147/SJ.1999.5387096

Hendre, A., & Joshi, K. P. (2015). A Semantic Approach to Cloud Security and Compliance. *2015 IEEE 8th International Conference on Cloud Computing*, 1081–1084. https://doi.org/10.1109/CLOUD.2015.157

Hon, W. K., Millard, C., & Walden, I. (2012). Negotiating Cloud Contracts—Looking at Clouds from Both Sides Now. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2055199

Hong, J., Dreibholz, T., Schenkel, J., & Hu, J. (2019). *An Overview of Multi-cloud Computing* (pp. 1055–1068). https://doi.org/10.1007/978-3-030-15035-8_103

Houidi, I., Mechtri, M., Louati, W., & Zeghlache, D. (2011). Cloud Service Delivery across Multiple Cloud Platforms. *2011 IEEE International Conference on Services Computing*, 741–742. https://doi.org/10.1109/SCC.2011.107

Iivari, J. (2005). Information Systems as a Design Science: Some concerns. In O. Vasilecas, W. Wojtkowski, J. Zupančič, A. Caplinskas, W. G. Wojtkowski, & S. Wrycza (Eds.), *Information Systems Development* (pp. 15–27). Springer US. https://doi.org/10.1007/0-387-28809-0_2

Iivari, J. (2007). *A Paradigmatic Analysis of Information Systems As a Design Science*. https://core.ac.uk/reader/301357840

International Organization for Standardization. (2015). *Information technology—Security techniques—Code of practice for information security controls based on ISO/IEC 27002 for cloud services* (ISO/IEC 27017:2015). https://www.iso.org/standard/43757.html

Irfan, M., Usman, M., Zhuang, Y., & Fong, S. (2015). A Critical Review of Security Threats in Cloud Computing. *2015 3rd International Symposium on Computational and Business Intelligence (ISCBI)*, 105–111. https://doi.org/10.1109/ISCBI.2015.26

ISACA. (2012). *COBIT 5: A business framework for the governance and management of enterprise IT*. https://www.isaca.org/resources/cobit

ISO/IEC 27005:2022. (2022). https://www.iso.org/standard/80585.html

Janet Julia Ang'udi. (2023). Security challenges in cloud computing: A comprehensive analysis. *World Journal of Advanced Engineering Technology and Sciences*, *10*(2), 155–181. https://doi.org/10.30574/wjaets.2023.10.2.0304

Jansen, W., & Grance, T. (2011). *Guidelines on Security and Privacy in Public Cloud Computing* (NIST Special Publication (SP) 800-144). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-144

Jayanthiladevi, A., Ayoobkhan, M. U. A., ThamaraiSelvi, R., Jimmy, L., Mishra, P., & Robert, N. R. (2023). Implementation of multicloud strategies for healthcare organisations to avoid cloud sprawl. *International Journal of Cloud Computing*. https://www.inderscienceonline.com/doi/10.1504/IJCC.2022.128699

Johannsen, A., Kant, D., & Creutzburg, R. (2020). Measuring IT security, compliance and data governance within small and medium-sized IT enterprises. *Electronic Imaging*, *32*(3), 252-1-252–11. https://doi.org/10.2352/ISSN.2470-1173.2020.3.MOBMU-252

Katz, E. (2023, June 2). *What is the Cloud Security Maturity Model, and How mature are you?* Skyhawk Security. https://skyhawk.security/cloud-security-maturity-model/

Khalil, S., Fernandez, V., & Fautrero, V. (2016). Cloud Impact on IT Governance. *2016 IEEE 18th Conference on Business Informatics (CBI)*, 255–261. https://doi.org/10.1109/CBI.2016.36

Kitchenham, B., Pearl Brereton, O., Budgen, D., Turner, M., Bailey, J., & Linkman, S. (2009). Systematic literature reviews in software engineering – A systematic literature review. *Information and Software Technology*, *51*(1), 7–15. https://doi.org/10.1016/j.infsof.2008.09.009

Latif, R., Abbas, H., Assar, S., & Ali, Q. (2014). Cloud Computing Risk Assessment: A Systematic Literature Review. In J. J. (Jong H. Park, I. Stojmenovic, M. Choi, & F. Xhafa (Eds.), *Future Information Technology* (pp. 285–295). Springer. https://doi.org/10.1007/978-3-642-40861-8_42

Le, N. T., & Hoang, D. B. (2017). Capability Maturity Model and Metrics Framework for Cyber Cloud Security. *Scalable Computing: Practice and Experience*, *18*(4), 277–290. https://doi.org/10.12694/scpe.v18i4.1329

Liu, F., Tong, J., Mao, J., Bohn, R., Messina, J., Badger, L., & Leaf, D. (2011). *NIST Cloud Computing Reference Architecture*. https://doi.org/10.6028/NIST.SP.500-292

Luftman, J. (2004). Assessing business-IT allignment maturity. In *Strategies for information technology governance* (pp. 99–128). Igi Global.

Mell, P., & Grance, T. (2011). *The NIST Definition of Cloud Computing*. https://doi.org/10.6028/NIST.SP.800-145

Menasce, D. A., & Ngo, P. (2009). *Understanding Cloud Computing: Experimentation and Capacity Planning*.

Microsoft. (2023, September 29). *Shared responsibility in the cloud—Microsoft Azure*. https://learn.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility

Mikkola, T. (2021). *Extending IT governance with Azure cloud governance*.

Mohanan, S., Sridhar, N., & Bhatia, S. (2022). Comparative Analysis of Cloud Computing Security Frameworks for Financial Sector. In X.-S. Yang, S. Sherratt, N. Dey, & A. Joshi (Eds.), *Proceedings of Sixth International Congress on Information and Communication Technology* (pp. 1015–1025). Springer. https://doi.org/10.1007/978-981-16-2380-6_90

M'rhaoaurh, I., Okar, C., Namir, A., & Chafiq, N. (2018). Challenges of cloud computing use: A systematic literature review. *MATEC Web of Conferences*, *200*, 00007. https://doi.org/10.1051/matecconf/201820000007

Papanikolaou, N., Pearson, S., Mont, M. C., & Ko, R. K. L. (2014). A toolkit for automating compliance in cloud computing services. *International Journal of Cloud Computing*, *3*(1), 45. https://doi.org/10.1504/IJCC.2014.058830

Paré, G., & Kitsiou, S. (2017). Chapter 9 Methods for Literature Reviews. In *Handbook of eHealth Evaluation: An Evidence-based Approach [Internet]*. University of Victoria. https://www.ncbi.nlm.nih.gov/books/NBK481583/

Paulk, M. (2002). Capability Maturity Model for Software. In J. J. Marciniak (Ed.), *Encyclopedia of Software Engineering* (1st ed.). Wiley. https://doi.org/10.1002/0471028959.sof589

Paulk, M. C., Curtis, B., Chrissis, M. B., & Weber, C. V. (1993). Capability maturity model, version 1.1. *IEEE Software*, *10*(4), 18–27. https://doi.org/10.1109/52.219617

Petcu, D. (2013). Multi-Cloud: Expectations and current approaches. *Proceedings of the 2013 International Workshop on Multi-Cloud Applications and Federated Clouds*, 1–6. https://doi.org/10.1145/2462326.2462328

Pöppelbuβ, J., & Röglinger, M. (2011). WHAT MAKES A USEFUL MATURITY MODEL? A FRAMEWORK OF GENERAL DESIGN PRINCIPLES FOR MATURITY MODELS AND ITS DEMONSTRATION IN BUSINESS PROCESS MANAGEMENT. *ECIS 2011 Proceedings*. https://aisel.aisnet.org/ecis2011/28

Porter, M. E. (1985). TECHNOLOGY AND COMPETITIVE ADVANTAGE. *Journal of Business Strategy*, *5*(3), 60–78. https://doi.org/10.1108/eb039075

Qian, L., Luo, Z., Du, Y., & Guo, L. (2009). *Cloud Computing: An Overview* (Vol. 5931, p. 631). https://doi.org/10.1007/978-3-642-10665-1_63

Rashid, A., & Chaturvedi, A. (2019). Cloud Computing Characteristics and Services: A Brief Review. *INTERNATIONAL JOURNAL OF COMPUTER SCIENCES AND ENGINEERING*, *7*, 421–426. https://doi.org/10.26438/ijcse/v7i2.421426

Röglinger, M., Pöppelbuβ, J., & Becker, J. (2012). Maturity models in business process management. *Business Process Management Journal*, *18*(2), 328–346. https://doi.org/10.1108/14637151211225225

Sajid, M., & Raza, Z. (2013). *Cloud Computing: Issues & Challenges*.

Saripalli, P., & Walters, B. (2010). QUIRC: A Quantitative Impact and Risk Assessment Framework for Cloud Security. *2010 IEEE 3rd International Conference on Cloud Computing*, 280–288. https://doi.org/10.1109/CLOUD.2010.22

Sendi, A. S., & Cheriet, M. (2014). Cloud Computing: A Risk Assessment Model. *2014 IEEE International Conference on Cloud Engineering*, 147–152. https://doi.org/10.1109/IC2E.2014.17

Sharma, A., Singh, U. K., Upreti, K., & Yadav, D. S. (2021). An investigation of security risk & taxonomy of Cloud Computing environment. *2021 2nd International Conference on Smart Electronics and Communication (ICOSEC)*, 1056–1063. https://doi.org/10.1109/ICOSEC51865.2021.9591954

Singh, V., & Pandey, S. K. (2014). A comparative study of Cloud Security Ontologies. *Infocom Technologies and Optimization Proceedings of 3rd International Conference on Reliability*, 1–6. https://doi.org/10.1109/ICRITO.2014.7014763

Subramanian, N., & Jeyaraj, A. (2018). Recent security challenges in cloud computing. *Computers & Electrical Engineering*, *71*, 28–42. https://doi.org/10.1016/j.compeleceng.2018.06.006

Tabrizchi, H., & Kuchaki Rafsanjani, M. (2020). A survey on security challenges in cloud computing: Issues, threats, and solutions. *The Journal of Supercomputing*, *76*(12), 9493–9532. https://doi.org/10.1007/s11227-020-03213-1

Taft, T. (2017, April). *The Integration of IT Governance, Information Security Leadership and Strategic Alignment in Healthcare: A Correlational Study*. https://www.proquest.com/openview/a458b48139e5046a971da96c3db1b803/1?pq-origsite=gscholar&cbl=18750

Thuraisingham, B. (2020). Cloud Governance. *2020 IEEE 13th International Conference on Cloud Computing (CLOUD)*, 86–90. https://doi.org/10.1109/CLOUD49709.2020.00025

Tracy, K. W. (2016). Cloud Application Sprawl in Enterprise Applications. *IEEE Potentials*, *35*(2), 26–29. https://doi.org/10.1109/MPOT.2015.2423690

Varghese, B., & Buyya, R. (2018). Next generation cloud computing: New trends and research directions. *Future Generation Computer Systems*, *79*, 849–861. https://doi.org/10.1016/j.future.2017.09.020

Verschuren, P., & Doorewaard, H. (2010). *Designing a Research Project* (Vol. 2). The Hague: Eleven International Publishing.

Weill, P., & Ross, J. W. (2004). *IT governance: How top performers manage IT decision rights for superior results*. Harvard Business School Press.

Wieringa, R. J. (2014). *Design Science Methodology for Information Systems and Software Engineering*. Springer.

Wohlin, C., Runeson, P., Höst, M., Ohlsson, M. C., Regnell, B., & Wesslén, A. (2012). *Experimentation in Software Engineering*. Springer Science & Business Media.

Xie, F., Peng, Y., Zhao, W., Chen, D., Wang, X., & Huo, X. (2012). A risk management framework for cloud computing. *2012 IEEE 2nd International Conference on Cloud Computing and Intelligence Systems*, 476–480. https://doi.org/10.1109/CCIS.2012.6664451

Youssef, A. E. (2019). A Framework for Cloud Security Risk Management based on the Business Objectives of Organizations. *International Journal of Advanced Computer Science and Applications*, *10*(12). https://doi.org/10.14569/IJACSA.2019.0101226

Appendix A – Code book

The following coding scheme was used on all the collected data. Note that the data was first transcribed and then imported into NVIVO for coding. The indented text represents a subcode.

- Assessment
  - Deployment models
  - Service models
  - Frameworks
  - Stakeholders
  - Shared responsibility model
  - Interesting observations
- Topics
  - Account security
  - API security
  - Identity access management
  - Endpoint security
  - Cloud-specific governance
  - Third-party
  - Laws and regulations
  - Compliance
  - Future research
  - Interesting observations
- Maturity matrix
  - Maturity level
    - Level 1
    - Level 2
    - Level 3
    - Level 4
    - Level 5
  - Bottom-up / top-down discussion
  - Control in organization
  - Generalizability
  - Interpretability
  - Maturity definition
  - Naming
  - Design
  - Interesting observations
  - Future work
- Validation maturity
- Validation topics
- Interesting observations