ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΙΓΑΙΟΥ
ΠΟΛΥΤΕΧΝΙΚΗ ΣΧΟΛΗ

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ

ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Survey on risk assessment methods in cloud systems

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

ΤΟΥ

ΧΡΗΣΤΟΥ ΚΑΛΛΟΥ

Επιβλέπων: Δρ. Κυριάκος Κρητικός, Αναπληρωτής Καθηγητής

Μέλη εξεταστικής επιτροπής: Δρ. Καρύδα Μαρία , Καθηγήτρια , Δρ. Κωνσταντίνου Ελισάβετ , Αναπληρώτρια Καθηγήτρια

Σάμος, [Οκτώβριος 2025]

Η σελίδα αυτή είναι σκόπιμα λευκή.

Preface and acknowledgements

First and foremost, I would like to thank from the bottom of my heart my family for their continuous support throughout my learning journey over the years, especially the tough ones. Moreover, I would like to thank everyone that supported my efforts in completing my studies in the MSc program of Information and Communication Systems Security and my fellow co-students / friends that I made along, who always kept pushing each other to progress and always improve.

I would also like to give special thanks to Associate Professor Dr. Kritikos Kyriakos, for giving me the opportunity to develop this thesis and for his continuous support and guidance throughout the preparation of this thesis. Our cooperation was excellent, and his advice was valuable at all stages of this thesis, guaranteeing the correct scientific approach of this topic.

του

ΧΡΗΣΤΟΥ ΚΑΛΛΟΥ

Τμήμα Μηχανικών Πληροφοριακών και Επικοινωνιακών Συστημάτων

ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΙΓΑΙΟΥ

Table of Contents

List of Figures

List of Tables

Table 1: Acronyms

Acronym	Full Form
APIs	Application Programming Interface
AWS	Amazon Web Services
CIA	Confidentiality, Integrity, Availability
CSP	Cloud Service Provider
CVSS	Common Vulnerability Scoring System
DoS	Denial of Service
IaaS	Infrastructure as a Service
ISO	International Organization for Standardization
NIST	National Institute of Standards and Technology
PaaS	Platform as a Service
SaaS	Software as a Service
SLA	Service Level Agreement
VM	Virtual Machine

Περίληψη

Η παρούσα διπλωματική εργασία παρουσιάζει μια ολοκληρωμένη βιβλιογραφική ανασκόπηση των μεθόδων αξιολόγησης κινδύνου για περιβάλλοντα, υπηρεσίες και συστήματα υπολογιστικού νέφους. Η ανασκόπηση συλλέγει και αναλύει συστηματικά τη σχετική βιβλιογραφία, παρέχοντας: (α) μια ιεραρχική κατηγοριοποίηση των εντοπισμένων μεθόδων αξιολόγησης κινδύνου, (β) την ανάλυση των μεθόδων συμπεριλαμβανομένων των πλεονεκτημάτων και μειονεκτημάτων τους, και (γ) την συγκριτική αξιολόγηση των μεθόδων βάσει προσεκτικά διαμορφωμένων κριτηρίων. Επιπλέον, η ανασκόπηση εντοπίζει ερευνητικά κενά και προκλήσεις στην τρέχουσα βιβλιογραφία και προτείνει μελλοντικές ερευνητικές κατευθύνσεις για την αντιμετώπιση αυτών των κενών/προκλήσεων.

Το κύριο όφελος αυτής της εργασίας είναι ότι παρέχει τόσο στους ερευνητές όσο και στους επαγγελματίες έναν δομημένο χάρτη πορείας για την κατανόηση και την επιλογή κατάλληλων μεθόδων αξιολόγησης κινδύνου σε περιβάλλοντα cloud. Για τους ερευνητές, η παρούσα διατριβή προσφέρει μια ολοκληρωμένη βάση για τον εντοπισμό πολλά υποσχόμενων ερευνητικών κατευθύνσεων και την κατανόηση της τρέχουσας κατάστασης. Για τους επαγγελματίες, συμπεριλαμβανομένων των επαγγελματιών ασφαλείας, των αρχιτεκτόνων cloud και των διαχειριστών κινδύνου, η παρούσα εργασία χρησιμεύει ως πρακτικός οδηγός για την επιλογή και την εφαρμογή μεθόδων που ταιριάζουν καλύτερα στο οργανωτικό τους πλαίσιο, στις κανονιστικές απαιτήσεις και στα μοντέλα ανάπτυξης cloud. Γεφυρώνοντας το χάσμα μεταξύ ακαδημαϊκής έρευνας και πρακτικής εφαρμογής, η παρούσα διατριβή επιτρέπει τη λήψη αποφάσεων βάσει τεκμηρίων στην ασφάλεια cloud και υποστηρίζει την ανάπτυξη πιο αποτελεσματικών, ειδικών για το cloud στρατηγικών διαχείρισης κινδύνου.

Λέξεις-κλειδιά: υπολογιστικό νέφος, αξιολόγηση κινδύνου, ασφάλεια, μέθοδοι, βιβλιογραφική ανασκόπηση, συγκριτική ανάλυση

Abstract

This thesis presents a comprehensive literature review of risk assessment methods for cloud computing environments, services, and systems. The review systematically collects and analyzes relevant literature to provide: (a) a hierarchical categorization of the identified risk assessment methods, (b) an analysis of these methods including their advantages and disadvantages, and (c) a comparative evaluation of these methods based on carefully crafted criteria. Furthermore, the review identifies research gaps and challenges in current literature and proposes future research directions to address these gaps.

The primary benefit of this work is that it provides both researchers and practitioners with a structured roadmap for understanding and selecting appropriate risk assessment methods in cloud environments. For researchers, this thesis offers a comprehensive foundation for identifying promising research directions and understanding the current state-of-the-art. For practitioners, including security professionals, cloud architects, and risk managers, this work serves as a practical guide for selecting and applying methods that best fit their organizational context, regulatory requirements, and cloud deployment models. By bridging the gap between academic research and practical application, this thesis enables evidence-based decision-making in cloud security and supports the development of more effective, cloud-specific risk management strategies.

Keywords: cloud computing, risk assessment, security, methods, comparative analysis, survey

1

Introduction

1.1 Introduction to the Main Issue of Risk Assessment

The rapid adoption of cloud computing technologies has revolutionized how organizations store, process, and manage data, services and applications. While offering undeniable advantages in scalability, flexibility, and cost-efficiency, cloud environments introduce unique and complex security challenges that significantly alter the traditional risk landscape (Microsoft, 2023; NIST, 2012). In these dynamic, shared-resource (cloud environment) settings, the assessment and management of information security risks are vital to safeguarding organizational assets and maintaining regulatory compliance. Risk assessment methods, which form the backbone of an organization's security posture evaluation, are therefore critical tools. However, traditional risk assessment frameworks originally developed for static, on-premises systems often fall short in capturing the volatile, multi-tenant, and third-party-dependent nature of cloud environments [1].

Current practices frequently rely on subjective, qualitative techniques or outdated models that inadequately quantify or prioritize risks in cloud contexts (Basu et al., 2021). Many models neglect critical cloud-specific risk factors, such as hypervisor vulnerabilities, loss of governance, data location ambiguity, and cloud supply chain exposures (Cloud Security Alliance, 2023). Furthermore, the increasing velocity of changes in cloud deployments challenges the practicality of traditional, infrequent, manually intensive risk assessment (Le et al., 2022). As cloud ecosystems evolve, the gap between organizational risk management needs and the capabilities of existing methods widens, exposing organizations to unassessed threats and compliance risks. Consequently, there is an urgent need for updated, scalable, quantitative, and cloud-specific risk assessment methods capable of supporting continuous, evidence-based security decisions in these environments.

1.2 Contribution and Advantages of This Thesis

1.2.1 Contribution of This Thesis

This thesis aims at addressing the identified, aforementioned gaps by conducting a comprehensive and systematic analysis of the current state-of-the-art in cloud risk assessment with a special focus on assessment methods. It contributes to the field through:

· A rigorous systematic literature review of academic and industry sources on cloud computing risk assessment, offering a broad and well-documented landscape analysis [1].

· A comparative evaluation framework that assesses traditional and cloud-specific risk assessment methods against multiple dimensions/criteria, such as accuracy, cloud-specificity, scalability, and explainability (Joh & Malaiya, 2011; Wangen, 2017).

· Hierarchical Taxonomy: The development of a multi-dimensional classification framework that categorizes risk assessment methods based on their approach (quantitative vs. qualitative), scope (cloud-specific vs. generic), and automation level.

· The identification of critical research gaps, including the lack of dynamic quantification and of integration with cloud-native operations, insufficient validation of models, and the absence of standardized yet practical assessment frameworks (Gega et al., 2025; Saripalli & Walters, 2010).

· A comprehensive research agenda providing specific pathways for overcoming identified gaps, including continuous risk monitoring, integration of real-time threat intelligence, cloud-specific extensions to existing frameworks, development of adaptive automated risk assessment tools, and human-centric models addressing insider risks and organizational governance shortcomings (Basu et al., 2021; NIST, 2024).

The main advantage of this thesis lies in its comprehensive and systematic exploration of risk assessment methods specifically tailored for cloud computing systems, filling a critical gap where traditional approaches fail to address the dynamic and complex nature of cloud environments. By providing a hierarchical taxonomy, a comparative evaluation framework, and an in-depth analysis of existing methods, the study not only clarifies the strengths and weaknesses of current approaches but also highlights their practical applicability in real-world scenarios. The benefits of this work extend to both academia and industry: researchers gain a structured overview of the state-of-the-art and identified research gaps, while practitioners benefit from guidance on selecting suitable risk assessment methods and understanding their limitations. Ultimately, the impact of the thesis is significant, as it paves the way for the development of more adaptive, scalable, and cloud-specific risk assessment methods, supporting organizations in strengthening security, enhancing compliance, and making more informed, evidence-based decisions in cloud adoption and management.

1.2.2 Advantages of This Thesis Compared to Other Relevant Work

Compared to prior studies, this thesis exhibits several distinguishing advantages:

- **Holistic Cloud-Centric Perspective:** Unlike many existing works that superficially adapt traditional risk frameworks to cloud contexts, this thesis critically dissects how cloud-specific features fundamentally reshape risk dimensions, thus requiring bespoke methodological adaptations.

- **Systematic and Transparent Research Methodology:** Following formal systematic literature review protocols, this work ensures replicability, traceability, and comprehensive coverage, reducing biases commonly found in narrative reviews (Le et al., 2022).

- **Multi-Dimensional Evaluation Framework:** The thesis introduces a multi-dimensional evaluation methods of risk assessment methodologies based on dimensions, such as quantification quality, scalability, cloud-specificity, and explainability), providing a more nuanced comparison than conventional performance-only benchmarks (Wangen, 2017).

- **Empirically-Driven Future Directions:** Rather than merely listing challenges, the thesis derives research guidelines grounded in observed deficiencies and trends, offering actionable pathways for researchers and practitioners.

- **Focus on Continuous Risk Assessment and Automation:** Highlighting the dynamic nature of cloud ecosystems, the thesis emphasizes automation and continuous assessment, key aspects often missing or undervalued in earlier literature (Nadeem et al., 2023).

- **Clear Linkage to Business Implications:** By suggesting future methods that bridge technical risk indicators to business-level impacts (e.g., cost, downtime, compliance), the thesis elevates risk management from a purely technical exercise to a strategic organizational activity.

Collectively, these advantages make the thesis a substantial step forward compared to fragmented or narrowly scoped previous studies. Through these contributions, the thesis aims to bridge the gap between theoretical risk frameworks and practical risk management needs in modern cloud computing environments.

1.3 Structure of This Thesis

The thesis is organized as follows:

- **Chapter 1** introduces the research problem, the motivation behind it, the contribution, advantages and innovations of this work, and the overall structure of the thesis.
- **Chapter 2** provides a comprehensive background on risk assessment principles, the specifics of cloud computing environments, and an overview of vulnerabilities, threats, and real-world incidents in cloud ecosystems.
- **Chapter 3** details the applied methodology of systematic literature review, including the research questions posed, the search strategy followed, the filtering criteria used, and an initial quantitative analysis of the selected assessment approaches.
- **Chapter 4** presents the categorization, detailed analysis, and comparative evaluation of existing risk assessment methods, highlighting their strengths and limitations.
- **Chapter 5** identifies the research gaps emerging from the literature and the conducted analysis, proposing detailed future research guidelines and work directions to address those challenges.
- **Chapter 6** synthesizes the results, reflects on the experience obtained, extracts the most critical challenges and promising research directions, and outlines a vision for future advancements in cloud risk assessment.

2

Risk Assessment in Information Systems Security

2.1 Risk Assessment Procedure: Definitions, Components, and Purpose

2.1.1 Baseline

Our basic aim in this section is to recall the fundamental material that one cannot possibly avoid and that facilitates the comprehension of the main contribution parts of this thesis survey. In particular, this section presents definitions and explanations for several basic elements of security, such as security, confidentiality, availability, integrity, vulnerability, threat, risk, countermeasure, and security mechanism. Due to the ambiguity in the field of information and technology, and particularly in cloud computing, it is important to understand this basic security terminology because such a comprehension is essential to safeguard sensitive business data and manage risks effectively.

2.1.2 Definition of Terms

2.1.2.1 Security

Security refers to the condition or state of being protected against unauthorized access, harm, damage, or loss. It encompasses the principles, practices, and mechanisms designed to ensure the confidentiality, integrity, and availability of information, systems, individuals, and assets from internal or external threats (ISO/IEC 27000:2018).

2.1.2.2 Confidentiality

Confidentiality refers to the principle of ensuring that sensitive information is accessible to only authorized individuals or systems. It prevents unauthorized data disclosure, protecting privacy and proprietary information. To achieve the above goal, techniques, such as encryption, access control, and authentication are widely applied to ensure and maintain confidentiality (NIST SP 800-53).

2.1.2.3 Integrity

Integrity refers to the trustworthiness and accuracy of data and systems. It ensures that information and systems are protected from unauthorized or unintended modification, corruption, or destruction, maintaining their accuracy and completeness over time. Common mechanisms to protect integrity include digital signatures, hash functions, checksums, and version control systems (ISO/IEC 27002:2022).

2.1.2.4 Availability

The very essence of availability is that information and resources are accessible to authorized users when they are actually needed. The availability principle emphasizes the importance of minimizing server disruptions and maintaining operational uptime. Common strategies that enhance availability include failover mechanisms, redundancy procedures, and regular maintenance procedures (NIST SP 800-53).

2.1.2.5 Threat

A threat is any potential danger or adverse event that could exploit vulnerabilities to cause harm to information systems, data, or operations. Threats can be natural (earthquakes, floods, fires), human-made intentional (malware, cyberattacks, insider threats), human-made accidental (configuration errors, accidental data deletion), or environmental (power outages, hardware failures) (ISO/IEC 27005:2022).

2.1.2.6 Vulnerability

A vulnerability is a weakness or flaw in a system, application, service or process that could be exploited by threats to gain unauthorized access or cause harm. Vulnerabilities can exist in software (buffer overflows, SQL injection flaws, unpatched applications), hardware (firmware vulnerabilities, misconfigurations, manufacturing defects), procedures (inadequate backup processes, weak security change management, insufficient access reviews), or human factors (lack of security awareness, social engineering susceptibility, poor password practices) (NIST SP 800-30).

2.1.2.7 Impact

When a security related event or incident takes place, the potential consequences, damage or operational disruptions that it causes constitute its impact. The impact ranges from financial losses, reputational damage up to legal repercussions, damage of the physical equipment/software or even human loss in extreme scenarios (ISO/IEC 27005:2022).

2.1.2.8 Threat Likelihood

Threat likelihood is the chance that a given threat will exploit a particular vulnerability or set of vulnerabilities within a specific timeframe. To evaluate likelihood, we must consider previous relevant data like the frequency of ransomware attacks on cloud storage services in the past five years, any new threat intelligence, and the existing mitigation factors (the security mechanisms and countermeasures already in place, such as encryption, multi-factor authentication, or intrusion detection systems, which reduce the probability or impact of an attack). By understanding threat likelihood, an organization can determine where their risk management focus should lie (NIST SP 800-30).

2.1.2.9 Risk

Risk is the potential for loss, damage, or destruction of an asset as a result of a threat exploiting a vulnerability. It represents the intersection of threat likelihood and impact severity: Risk = Threat Likelihood × Impact. This fundamental risk equation shows that risk increases with both the probability of a threat occurring and the magnitude of its potential consequences (ISO/IEC 27005:2022; NIST SP 800-30).

2.1.2.10 Security Mechanism

A security mechanism is a process or device that implements or supports one or more security services or controls to detect, prevent, or respond to threats and vulnerabilities affecting information systems or physical environments (ISO/IEC 27000:2018). Security mechanisms may include encryption algorithms, access control systems, monitoring tools and authentication protocols/multi-factor authentication. A security service represents a capability that supports one or more of the security objectives (confidentiality, integrity, availability), while security controls include technical, administrative, organizational or legal means to manage security risk. The selection of security mechanisms depends on the specific security requirements, criticality of systems, the budget and the risk profile of an organization.

2.1.2.11 Countermeasure

A countermeasure is an action, device, procedure, technique or process that can reduce a threat, vulnerability, or an attack by eliminating or preventing it, by minimizing the harm it can cause, or by discovering and reporting it so that corrective actions can be taken. Countermeasures are broader in scope than security mechanisms, encompassing not just technical devices or processes but also strategic actions and comprehensive procedures. Defenses can be physical, administrative (like security awareness training, policies), or technical (firewalls, IDS, antivirus, VPN's and more). The effectiveness of a countermeasure is evaluated according to how well it reduces the particular risk in which it is specialized (NIST SP 800-53).

2.1.2.12 Risk Mitigation

Risk mitigation involves implementing strategies and techniques that reduce the likelihood or impact of identified risks, enabling organizations to develop effective risk management approaches and prioritize them accordingly. A risk mitigation strategy is a comprehensive plan that outlines how an organization will address specific risks, while risk mitigation plans are detailed implementation documents that specify the actions, timelines, and resources needed to execute the strategy. The implementation of such strategies must take into account the analysis of current risk mitigation measures, risk calculation and prioritization processes, and determine the potential impact and likelihood of various threats and vulnerabilities either individually or in combination with other ones (ISO/IEC 27005:2022).

2.1.3 Risk Assessment Components and Purpose

Risk assessment is a core process in information security risk management that aims to identify and evaluate risks to organizational assets. It generally consists of risk identification, risk analysis, and risk evaluation. In practice, this means determining what information assets and resources are valuable, what threats and vulnerabilities could affect them, and analyzing the likelihood and impact of potential incidents.

In particular, risk identification involves activities, such as asset determination, threat identification, and vulnerability identification; risk analysis focuses on assessing the likelihood and consequences of threats exploiting vulnerabilities; and risk evaluation involves comparing the estimated risk levels against predefined criteria to prioritize treatment options. By doing so, an organization can understand its inherent risk exposure and prioritize which risks need treatment first.

According to NIST Special Publication 800-30 Revision 1: Guide for Conducting Risk Assessments (Fikri et al., 2019), a risk assessment should start with a clear purpose and scope, including defining the objectives, boundaries, assumptions, and information sources for the assessment. Once the context is set, the organization identifies threat sources and events, as well as vulnerabilities and predisposing conditions that might be exploited. Next, the potential impacts and likelihoods of threat events exploiting vulnerabilities are determined. Finally, these factors are combined to estimate risk levels and prioritize risks for response.

In terms of mapping, risk identification covers asset, threat, and vulnerability determination; risk analysis corresponds to assessing likelihood and impact; and risk evaluation relates to the prioritization of risks for decision-making. In summary, the risk assessment procedure systematically evaluates what could go wrong, how likely it is to happen, and what the consequences would be – providing management with the information needed to decide on safeguards or risk treatment actions.

The purpose of conducting risk assessments is to enable risk-informed decision making. It ensures that security efforts focus on the most significant risks to the confidentiality, integrity, and availability of information. For example, Microsoft's cloud risk assessment guidance states that "the goal of a cloud risk assessment is to ensure that the system and data ... don't introduce any new or unidentified risk into the organization," emphasizing the need to keep risks within acceptable levels while preserving critical security properties (Microsoft, 2023).

A properly executed risk assessment provides a factual basis for selecting security controls and allocating resources in proportion to risk. It also creates a documented understanding of organizational risks, which is essential for transparency and for complying with corporate governance or regulatory requirements. Overall, the risk assessment procedure is a foundational component of an information security program, linking identified threats and vulnerabilities to business impact, and thereby guiding strategic risk mitigation decisions.

2.2 Definition of Risk Assessment Methods, Methodologies, and Frameworks

Given that the focus of this research is on risk assessment methodologies in cloud computing environments, it is essential to establish clear definitions and understand the relationships between risk assessment methods, methodologies, and frameworks.

2.2.1 Risk Assessment Methods

A risk assessment method is a specific technique, tool or procedure used to identify, analyze, and evaluate risks within an information system or environment. Risk assessment methods represent the actual tools and techniques employed to gather data, perform calculations, and derive risk conclusions. Examples of risk assessment methods include qualitative ones (such as risk matrices, expert judgment, and scenario analysis), quantitative ones (such as Monte Carlo simulation, fault tree analysis, and probabilistic risk assessment), and hybrid ones that combine both qualitative and quantitative elements (NIST SP 800-30, 2012; ISO/IEC 27005:2022).

2.2.2 Risk Assessment Methodologies

A risk assessment methodology is a defined, systematic approach that organizations follow to consistently carry out risk assessment. It provides a structured set of processes, steps, and criteria that orchestrate the application of various risk assessment methods in a coordinated manner. The purpose of having a formal methodology is to ensure that risk assessment is repeatable, comprehensive, and aligned with industry best practices (ISO/IEC 27005:2022). Instead of an ad-hoc or purely intuitive evaluation, a methodology guides the assessor through all necessary components of risk assessment (e.g., asset identification, threat analysis, impact evaluation) so that important aspects are not overlooked or neglected. It also standardizes how risk is measured and reported, which is crucial for comparing results over time or across different parts of an organization.

A methodology typically specifies which methods to use at each stage of the risk assessment process, how to combine results from different methods, and how to interpret and communicate findings. For instance, a methodology might prescribe using qualitative methods for initial risk screening and quantitative methods for detailed analysis of high-priority risks.

2.2.3 Risk Assessment Frameworks

A risk assessment framework provides the overarching structure, principles, and guidelines within which risk assessment methodologies and methods operate. Frameworks establish the conceptual foundation, define key terminology, specify roles and responsibilities, and outline the governance structure for risk management activities. While methodologies focus on the "how" of conducting risk assessments, frameworks address the "what" and "why" by defining the scope, objectives, and organizational context (ISO/IEC 27005:2022; NIST SP 800-39, 2011).

Risk assessment frameworks support methodologies by providing the strategic context and ensuring alignment with organizational objectives and regulatory requirements. For example, a framework might mandate that risk assessments consider specific threat categories or impact types, while the methodology would specify the exact steps and methods to evaluate those threats and impacts.

2.2.4 Relationship and Integration

The relationship between these three concepts is hierarchical and complementary:

- Frameworks provide the strategic foundation and governance structure
- Methodologies operationalize the framework by defining systematic processes and workflows
- Methods are the specific tools and techniques executed within the methodology

This relationship ensures that risk assessment activities are strategically aligned (through frameworks), systematically executed (through methodologies), and technically sound (through appropriate methods).

2.2.5 Focus on Methods in This Research

While this research acknowledges the importance of methodologies and frameworks, the primary focus is on risk assessment methods because methods represent the actual analytical techniques that determine the accuracy, efficiency, and applicability of risk assessment results in cloud computing environments. Methods are where the technical innovations and adaptations for cloud-specific challenges occur, such as handling dynamic resource allocation, multi-tenancy risks, and shared responsibility models.

Although organizations often adopt standardized methodologies or framework like NIST SP 800-30 or ISO/IEC 27005 to organize their assessments, this thesis concentrates on the methods embedded within those approaches. These methods, whether qualitative, quantitative, or hybrid, represent the concrete mechanisms that define how risks are identified, measured, and evaluated. Emphasizing methods rather than methodologies enables a deeper examination of their metrics, conceptual models, and analytical processes, which directly influence how effectively risks are assessed in cloud environments.

2.3 Importance of Risk Assessment in Cloud Computing and Information Security

Conducting risk assessments is necessary and critically important in information systems security management for several fundamental reasons. Risk assessment serves as the cornerstone of effective security governance, providing organizations with the systematic approach needed to understand, prioritize, and manage security threats in complex IT environments.

More broadly in information systems security, regular risk assessments are essential to maintain an effective security posture in the face of evolving threats. They provide early warning of potential issues by highlighting new vulnerabilities or emerging threat vectors before incidents occur. For example, organizations that continuously assess risk (identifying new threats and vulnerabilities) are better prepared to address issues like novel malware or zero-day exploits in a timely manner.

Risk assessments also drive compliance and accountability. Many security standards and regulations (such as ISO/IEC 27001, NIST Cybersecurity Framework, SOC 2, and various government cybersecurity frameworks like the European Union's NIS2 Directive) (ISO/IEC 27001:2022; NIST, 2018; AICPA, 2017; European Parliament, 2022) mandate periodic risk assessments as a fundamental requirement. A robust risk management program is necessary to meet contractual obligations and maintain public accreditations that customers and regulators expect. In other words, performing risk assessments is not just a best practice but often a compliance necessity to demonstrate due diligence in protecting information assets.

Furthermore, risk assessment is important because it aligns security efforts with business priorities. In complex ICT environments, it is impractical and cost-prohibitive to mitigate every conceivable risk. By assessing and understanding the relative risk of different assets and scenarios, management can focus resources on what matters most for the business (ISO/IEC 27005:2022). This ensures that security investments yield meaningful reductions in exposure and provides optimal return on security investments.

Risk assessments also enable organizations to establish appropriate security baselines and controls proportionate to their risk tolerance and business requirements. Without the insight from risk assessment, organizations might either chase every theoretical threat, thus wasting resources, or miss critical exposures that could result in significant business impact. For instance, an assessment might reveal that certain sensitive data repositories require additional encryption or access controls due to higher impact potential, whereas other low-risk systems may be adequately protected by standard security measures.

Additionally, risk assessments facilitate informed decision-making by providing quantitative and qualitative data about potential threats and their business implications. This enables management to make evidence-based decisions about security investments, risk acceptance, and resource allocation. The systematic nature of risk assessment also ensures that security considerations are integrated into business processes, project planning, and strategic decision-making.

Finally, regular risk assessments help organizations adapt to changing threat landscapes and business environments. As new technologies are adopted, business processes evolve, and threat actors develop new attack methods, risk assessments provide the mechanism to reassess and adjust security postures accordingly. This dynamic approach to risk management is essential for maintaining effective security in rapidly changing technological environments. Thus, risk assessment is a key enabler of informed decision-making and effective risk governance in information systems security, providing the foundation upon which all other security activities are built and prioritized.

2.4 Key Advantages of Conducting Risk Assessment

Implementing regular risk assessment brings several important advantages to an organization's security and risk management program:

- *Proactive Identification of Threats and Vulnerabilities:* Risk assessment forces a systematic look at what could go wrong before incidents happen. This process reveals weaknesses in systems, processes, applications, software, hardware or configurations that might otherwise go unnoticed until exploited. For example, systematic risk assessment methodologies help organizations identify threats and vulnerabilities and their impacts across their IT infrastructure (NIST SP

800-30, 2012). By cataloguing these potential issues (missing patches, misconfigurations, inadequate access controls, etc.), the organization gains a clear to-do list of security improvements before attackers can strike. This proactive stance significantly reduces the likelihood of surprise breaches.

· *Prioritization of Security Efforts and Resources:* One of the most valuable outcomes of risk assessment is the prioritization of risks. Not all risks are equal – some events are unlikely or would cause minimal damage, while others could be catastrophic. Through risk analysis, organizations rank risks by severity, typically considering both likelihood and impact. The benefit of this is that it guides management to focus the limited available resources on the most critical risks. As the NIST Cybersecurity Framework (NIST, 2018) highlights, understanding threats, vulnerabilities, and impacts allows an organization to "inform risk response prioritization". In practice, this means high-risk findings (e.g., a critical vulnerability on an internet-facing system) are addressed before lower-risk issues. Such prioritization ensures efficient use of budget and personnel, tackling the biggest "bang for the buck" security improvements first.

· *Improved Basis for Strategic Planning and Controls Selection:* A thorough risk assessment provides a factual basis for choosing security controls and countermeasures. Rather than relying on guesswork or box-ticking, organizations can align their security investments with the risks that truly threaten their objectives. For instance, if an assessment reveals a high risk of data loss, management can justify investing in stronger backup and disaster recovery solutions. Risk assessment results often feed directly into risk treatment plans, where each major risk is addressed by a mitigation strategy (such as applying a control, transferring the risk via insurance, or accepting it if low). This leads to a more rational and transparent security strategy. It also facilitates discussions like cost-benefit analysis of controls – since the potential loss from a risk is understood, it can be weighed against the cost of the safeguard (ISO/IEC 27005:2022).

· *Supporting Compliance and Trust:* Regularly conducting risk assessment demonstrates due diligence to stakeholders, including customers, auditors, and regulators. As noted, many compliance frameworks require the conduct of risk assessment, but beyond meeting a checkbox, the practice builds confidence that the organization is managing security in a formalized way. For example, enterprise risk management programs aligned with established frameworks are necessary to meet contractual obligations and maintain public accreditations that customers rely on (ISO/IEC 27001:2022; SOC 2 Type II requirements). By extension, when an organization performs and documents risk assessments, it is better prepared to provide evidence for audits, to justify security expenditures to executives, and to assure customers that security risks are understood and under control.

· *Enhanced Communication and Enterprise-Wide Consistency:* A documented risk assessment creates a common reference point for discussing security risks across different units of an organization. It helps translate technical issues into business-impact terms that executives can understand, thereby bridging the gap between IT security staff and business leadership. Additionally, if the organization adopts a standard risk assessment methodology, it ensures that different departments evaluate risk in a consistent manner. This consistency is achieved when organizations align their risk assessment processes with established frameworks, ensuring that internal teams and even external partners are on the same page, and results can be compared across business units (COSO Enterprise Risk Management Framework, 2017). The advantage here is a more cohesive approach to risk: it prevents silos where one department might unknowingly accept a high risk that would be unacceptable elsewhere. Instead, risk appetite and evaluation criteria are uniform, leading to more coherent enterprise-wide risk management.

In summary, conducting risk assessment yields a range of benefits from early risk discovery and prioritized mitigation, to stronger compliance posture and unified risk communication. Organizations that invest in regular risk assessment are generally more resilient, since they can anticipate problems and address them in an orderly, cost-effective way, rather than constantly reacting in a far costlier manner to incidents after damage occurs.

2.5 Classic Risk Assessment Methods

Below, we present and analyze some of the classic risk assessment methods widely used in information security, discussing their key characteristics, strengths, limitations, and how they address different aspects of the risk assessment process. This analysis focuses on the technical approaches and analytical techniques rather than the broader methodological frameworks, as understanding method-level capabilities and constraints is essential for developing effective cloud-specific risk assessment methods.

2.5.1 ISO/IEC 27005 – Information Security Risk Management Standard

2.5.1.1 Methodology Presentation

ISO/IEC 27005 is an international standard on principles and guidelines for risk management in information security (ISO/IEC, 2018). It is one of the standards under the ISO/IEC 27000 series information security standards, supporting the implementation requirements of ISO/IEC 27001 (ISO/IEC, 2022). In particular, ISO/IEC 27005 presents a structured approach to information security risk management.

Risk assessment, which comprises risk identification, risk analysis, and risk evaluation, forms a critical component of the broader risk management process. Within this broader process, ISO/IEC 27005 explicitly defines and structures the activities of risk assessment, which means that while it functions primarily as a risk management standard, it also incorporates and subsumes a risk assessment methodology. It details a risk management process starting from setting the context, followed by identifying, analyzing, and evaluating risks, after which risk treatment can be undertaken, with subsequent regular communication of risks continuing throughout the monitoring cycle that follows. In fact, ISO 27005 explicitly states that "The risk assessment consists of the following activities: Risk Identification, Risk Analysis, Risk Evaluation" (ISO/IEC, 2018). When conducting these activities, organizations determine the value of assets, recognize applicable threats and vulnerabilities, evaluate existing control measures, and assess potential consequences (impact) and probabilities of occurrence based on threats.

The strength of ISO/IEC 27005 is that it is both comprehensive and flexible. It does not prescribe exact quantitative methods for calculating risks, or specific scales. As a result, this allows organizations of varying types and sizes to adapt it according to their own needs. Instead, it provides a conceptual framework that enables organizations to understand what risk is and what is involved in its assessment. It is up to organizations themselves to define their own risk assessment criteria (e.g. what constitutes high vs. low risk) and decide an assessment scale consistent with their context and risk appetite. The standard emphasizes the importance of setting scope for the evaluation and establishing "criteria for judging risk" (e.g. criteria for impact, acceptance of risk) (ISO/IEC, 2018).

This way, ISO 27005 ensures that the risk assessment is aligned with business goals, and that it reflects well the organization's circumstances. Its alignment with ISO/IEC 27001 is another advantage. By following this approach, organizations can meet the risk management requirements of an ISO 27001-certified ISMS (Information Security Management System). This has the added benefit that the organization's risk assessment is conducted in accordance with best practices on an international level, thus providing increased confidence.

2.5.1.2 Methodology Analysis

Many organizations use ISO 27005 as a baseline, tailoring it with their own risk assessment procedures and incorporating tools (like asset valuation methods or impact scoring models) as appropriate. Nevertheless, a potential challenge or criticism of ISO 27005 is that, due to its flexibility, it requires expertise to be implemented effectively. The standard leaves it to the organization to perform the analysis and does not enforce a particular risk quantification technique – as a result, the outcomes can be subjective if not guided by experienced risk assessors.

Fortunately, the standard does encourage iterative improvement and documentation, so over time an organization can calibrate its risk assessment criteria for more consistency. Overall, ISO/IEC 27005 serves as a robust framework for structuring risk assessment activities within a broader risk management methodology and is widely recognized and accepted, making it a common choice for organizations seeking an organized approach to information security risk assessment.

2.5.2 NIST SP 800-30 Rev. 1 – NIST Risk Assessment Guide

2.5.2.1 Methodology Presentation

According to the US National Institute of Standards and Technology's expert methodology on the "Guide for Conducting Risk Assessment", which is detailed in NIST SP 800-30 Revision 1, this standard is one of NIST's 800-series standards (NIST, 2012). This methodology is part of the NIST 800-series of standards and lies within NIST's Risk Management Framework (RMF) for federal information systems (NIST, 2018). The NIST SP 800-30 standard offers a comprehensive, step-by-step process for assessing risks. It breaks the undertaking down into three main stages: (a) preparing for the risk assessment, (b) conducting the risk assessment, thus producing the report and its findings and (c) maintaining the risk assessment (over time).

During the preparation step, NIST instructs organizations to define the context and logistics of the assessment. This includes identifying the purpose of the assessment (what decisions it will inform), its scope (which assets/systems and what time frame it covers), the assumptions and constraints, the sources of data to be used, and the risk model and analytical approach that will be employed. This preparation stage is critical in NIST's methodology, ensuring that everyone involved has clarity on how the assessment will be performed and what its focus will be.

The conduction step is where the core analysis happens, and NIST SP 800-30 lays out a series of granular tasks for this phase. These tasks include: identifying threat sources (and their characteristics, such as capability and intent for adversaries); identifying threat events that could be initiated by those sources; identifying vulnerabilities and conditions that could be exploited; determining the likelihood of threat events occurring (accounting for the presence of vulnerabilities and any controls); determining the impact or consequences to the organization's operations, assets, or individuals, should those events occur; and finally determining the risk level by combining likelihood and impact information. NIST often uses a qualitative or semi-quantitative scale (eg, High/Moderate/Low) for likelihood, impact, and risk, but the guide is flexible to accommodate quantitative approaches if respective data is available. The guide provides templates and examples (in appendices) for threat listing, vulnerability enumeration, and risk calculation to assist practitioners in carrying out these tasks.

After analyzing the risks, the results are typically documented in risk tables or reports that describe each risk scenario and its assessed likelihood and impact. Although risk response (mitigation) is outside the scope of SP 800-30 (it is covered in other parts of the RMF), the guide does emphasize that the risk assessment results should feed into risk response prioritization. The assessed risks help decision-makers decide which risks to address, and in what order.

The maintenance step involves monitoring and updating the risk assessment over time. Risks are not static; new threats emerge and system configurations change. NIST recommends continuous monitoring of risk factors and periodic reassessments (or refreshes) of the risk assessment to keep it current. Essentially, SP 800-30 integrates with continuous risk management by ensuring that the risk assessment is not a one-time activity but it is conducted with an ongoing risk management cycle.

2.5.2.2 Methodology Analysis

NIST SP 800-30 is praised for its thoroughness and structure. It is very detailed in guidance, which can be highly useful for organizations that need a clear procedure to follow. The methodology enforces thinking about both adversarial and non-adversarial threats, vulnerabilities, and potential impacts in a disciplined way. One advantage of this approach is that it improves the rigor and traceability of the risk assessment – every risk is traced from identified threats and vulnerabilities through to the impact on organizational objectives. This can help in auditing the assessment or explaining the rationale behind risk ratings to executives.

However, the detailed nature of SP 800-30 can also be resource-intensive. It requires gathering a significant amount of information and the involvement of subject matter experts to identify threats and vulnerabilities comprehensively. In addition, SP 800-30 may be considered less flexible compared to some lighter methodologies, since its structured and prescriptive process can limit adaptability when organizations need a quicker or more tailored assessment approach. In very large or complex organizations, a full SP 800-30 assessment might be time-consuming, which is why organizations often use it in a tailored way (focusing on highest-value assets or known threat areas) or in conjunction with automation tools for parts like vulnerability discovery. Despite this, the methodology's completeness is generally seen as a benefit because it reduces the chance of overlooking major risk factors.

Another point is that NIST SP 800-30 aligns well with other NIST guidance and the US federal risk management requirements. It complements NIST SP 800-39 (the overarching risk management guideline) and NIST SP 800-37 (the RMF process). Even organizations outside the US government have adopted SP 800-30 as a best practice framework for risk assessment due to its credibility and detail. In summary, NIST SP 800-30 Rev. 1 is a methodical and robust risk assessment methodology that, when applied, yields a deep understanding of cyber risks and a solid foundation for managing those risks.

2.5.3 FAIR – Factor Analysis of Information Risk

FAIR (Factor Analysis of Information Risk) is a relatively modern risk assessment methodology that takes a quantitative approach to information security risk (FAIR Institute, 2022). Unlike ISO 27005 or NIST methodologies, which are often qualitative, FAIR is designed to express risk in financial terms (e.g., annualized loss expectancy or probable loss magnitude). It is actually an ontology and model for analyzing the factors that contribute to risk. FAIR has been adopted as an international standard model (The Open Group, 2014) and is promoted by the FAIR Institute as a method to bring more rigor to cyber risk quantification.

At its core, FAIR breaks risk down into two high-level factors: Loss Event Frequency (how often a bad event is expected to occur) and Loss Magnitude (the probable impact or loss when it occurs). These in turn are composed of more granular factors. For example, Loss Event Frequency is driven by Threat Event Frequency (how often threats attempt to act) and Vulnerability (the probability that an attempt results in a loss event), while Loss Magnitude is broken into Primary losses (direct losses from the event, such as response costs) and Secondary losses (indirect fallout, such as reputation damage leading to business disruption) in the FAIR model. The methodology guides the assessor to estimate each of these factors, often by using ranges and probability distributions, and then uses Monte Carlo simulations or analytical calculations to derive a risk distribution (most likely loss, worst-case loss, etc.).

FAIR is described as "an analysis method for factors that contribute to risk – [evaluating the] probability of threat occurrence and estimation of loss" (The Open Group, 2014). In other words, it provides a structured way to think about what drives the frequency of incidents and how big the impact could be. One distinctive feature of FAIR is its taxonomy of loss forms. It identifies six forms of loss that an organization might suffer from an information security incident: Productivity loss, Response cost, Replacement cost, Fines and judgments (regulatory or legal penalties), Competitive advantage loss, and Reputation damage. By categorizing losses, FAIR ensures that analysts consider all the different ways an incident could hurt the organization (not just, say, immediate cleanup costs, but also longer-term brand damage or regulatory fines).

2.5.3.1 Critical Analysis of FAIR

Advantages:

The biggest selling point of FAIR is that it yields results in monetary terms or other concrete metrics that are more directly useful to business stakeholders. For example, a FAIR analysis might conclude there is a 10% chance of a data breach costing over $10 million in the next year, and an 80% chance that it will cost under $1 million, with an annualized loss expectancy (most likely annual risk) of say $2.5 million. Having this kind of output can be very powerful for communicating with executives and justifying investments (e.g., comparing the $2.5M risk to the cost of a $500k security improvement). It also allows for cost-benefit analysis: one can recompute the risk if certain controls are implemented and see how much the risk (in dollar terms) drops, then compare that to the cost of the controls. This approach aligns well with enterprise risk management practices, which often demand quantitative analysis for risks (financial risk, operational risk, etc.) and enables cybersecurity risk to be discussed in the same terms.

FAIR is also methodology-agnostic in the sense that it does not dictate how to find or produce your data – it can incorporate outputs from other assessments conducted based on specific methodologies. For instance, you might use NIST or ISO methods to identify top risks, then use FAIR to drill down quantitatively on a couple of the most significant risks.

Limitations:

FAIR requires gathering of data and making estimates that might be difficult for some organizations. Estimating frequencies of cyber events or the potential costs of worst-case scenarios can be challenging and can involve a degree of uncertainty. FAIR addresses this by using ranges and probability distributions to capture uncertainty, but this means that the analysis can become complex. In addition, FAIR often needs statistical skills or tooling (many FAIR practitioners use specialized software or at least spreadsheets with simulation add-ons). Smaller organizations or those with less risk analysis maturity may find full FAIR analysis daunting.

FAIR can be considered incomplete as a standalone methodology since it focuses primarily on risk quantification and does not encompass all steps of the risk management lifecycle (such as risk identification, governance, or treatment). For this reason, FAIR is typically combined with other frameworks like ISO 27005 or NIST RMF that provide the broader methodological structure. In practice, FAIR is often used once a risk (say, "unauthorized access to customer data") has been identified and roughly characterized via another process – then FAIR comes in to estimate the frequency and impact of that scenario in detail.

Despite these challenges, FAIR is gaining popularity, especially among larger enterprises and financial institutions, because of the demand for quantified cyber risk for decision-making and cyber insurance. It has even been used in conjunction with ISO 27005 – The Open Group published a "FAIR – ISO/IEC 27005 Cookbook" (The Open Group, 2016) that shows how FAIR's quantitative approach can be mapped to the ISO 27005 process of risk analysis and evaluation. In conclusion, FAIR represents a sophisticated evolution of risk assessment methodology that provides a way to answer the question: "How much risk do we have, in financial terms?" It complements traditional qualitative frameworks by adding analytical rigor and is particularly useful when trying to prioritize risks at a business level or to evaluate the ROI of security investments.

2.5.4 OCTAVE – Operationally Critical Threat, Asset, and Vulnerability Evaluation

OCTAVE is a risk assessment methodology developed in the early 2000s by Carnegie Mellon University's Software Engineering Institute (SEI) (Alberts & Dorofee, 2003). It was one of the pioneering formal methodologies for information security risk assessment, particularly notable for its emphasis on organizational context and self-directed evaluation. There have been a few variants of OCTAVE, including OCTAVE Allegro (a later streamlined version released in 2007) (Caralli et al., 2007) and OCTAVE-S (released in 2005 for smaller organizations) (Alberts et al., 2005). While OCTAVE continues to be maintained and updated by SEI, it is no longer under active development as newer methodologies have emerged, though all variants share common principles that remain relevant today.

OCTAVE approaches risk assessment from an organizational and operational perspective. The methodology typically starts by focusing on the organization's assets (especially information assets) and the context in which they are used. It involves assembling a multidisciplinary analysis team from within the organization (rather than relying primarily on external auditors or tools) – this team gathers knowledge from management, staff, and technical personnel about critical assets and their security requirements. The original OCTAVE methodology is often described in three phases:

- ***Phase 1: Build Asset-Based Threat Profiles*** – The organization identifies its critical assets and determines which security properties are important for them (e.g., confidentiality of customer data, availability of a production system). Through workshops or interviews, the team determines security requirements and begins to identify potential threats to those assets. This phase is very focused on the organizational context: it captures what the organization values and what it stands to lose.

- ***Phase 2: Identify Infrastructure and System Vulnerabilities*** – Here, the focus shifts to evaluating the technological infrastructure and systems for weaknesses that could expose the critical assets identified in Phase 1. This can involve network vulnerability scanning, reviewing configurations, and analyzing technical vulnerabilities. The threat identification from Phase 1 is refined based on the actual vulnerabilities discovered.

· ***Phase 3: Develop Security Strategy and Plans*** – In the final phase, the risks from Phase 1 and 2 are analyzed to formulate risk mitigation strategies. The organization prioritizes the risks to its critical assets and develops mitigation plans (which could include policy or practice changes, not just technical controls). The outcome is a risk mitigation portfolio aligned with the organization's mission and constraints.

One key characteristic of OCTAVE is its scenario-based approach. Particularly in OCTAVE Allegro, risk scenarios are defined that link assets, threats, vulnerabilities, and impacts in narrative form. For example, a scenario might be: "Insider inadvertently deletes customer records from the billing database, causing significant data loss and business operation disruption." By formulating scenarios, OCTAVE ensures that the analysis considers how different factors combine to produce a risk, and it keeps the discussion anchored to real operational concerns.

2.5.4.1 Critical Analysis of OCTAVE

Advantages:

OCTAVE's strength lies in its holistic view. It explicitly brings in people from different parts of the organization (IT, business units, etc.) to share knowledge about where the most important information lies and what the business impacts of security failures would be. This can lead to a very grounded assessment that resonates with both technical staff and management. It also encourages looking beyond just technical vulnerabilities – process weaknesses or lack of security awareness among staff might surface as threats in an OCTAVE assessment because of the broad discussions it fosters. The methodology is documented in a way that organizations can implement it internally without needing expensive consultants, which made it attractive especially for organizations that wanted to improve their own risk analysis capability.

Limitations:

One critique of the original OCTAVE methodology was that it could be quite time-intensive and cumbersome, especially for large organizations with many assets. It relied heavily on workshops and qualitative input, which, while rich in detail, could become hard to manage and prioritize if not facilitated well. OCTAVE Allegro attempted to simplify the process, providing more streamlined worksheets and guidance focusing on information assets and associated threat scenarios to speed up the assessment. Even so, compared to newer methods, OCTAVE can seem somewhat qualitative and subjective (it does not inherently provide quantitative risk values, for instance).

Another challenge is that OCTAVE was developed in an era when risks were perhaps more static; today's fast-changing threat landscape means organizations often want more continuous or automated risk assessment processes. However, the core ideas of OCTAVE – engaging stakeholders, focusing on the most critical assets, and examining how organizational context contributes to risk – remain highly relevant. In fact, many modern enterprise risk management approaches echo these ideas (for example, involving business owners in assessing risk impacts is now common practice).

In practice, some organizations use OCTAVE Allegro as a framework for performing annual or periodic risk assessments on specific business lines or systems. They might use its worksheets to capture information asset profiles, threats, and mitigation plans. The results of an OCTAVE assessment can feed into higher-level frameworks like ISO 27005 or NIST CSF as well (OCTAVE can be the process used to fulfill the "risk assessment" step required by those frameworks).

In summary, OCTAVE is a classic methodology that laid the groundwork for a business-centric, asset-driven risk assessment. Its scenario-based, qualitative approach helps organizations understand their risks in context and develop practical risk mitigation strategies. While it may not be as widely adopted today as ISO or NIST standards, and can be considered somewhat heavyweight by modern standards, the influence of OCTAVE is seen in many of the risk assessment best practices used today. It remains a useful approach, especially for organizations that want to conduct in-depth self-assessments focusing on what matters most to their operations.

2.5.5 Relationship Between Risk Assessment Methods and Frameworks

In addition to the core risk assessment methods analyzed above, several broader risk management frameworks play a complementary role by providing governance structures and contextual guidance that support the application of these methods. While these frameworks are not analytical methods themselves, they establish the organizational principles, processes, and criteria that guide how risk assessment methods are implemented, interpreted, and aligned with enterprise-level objectives:

ISO/IEC 31000 and ISO/IEC 31010:

ISO 31000 (ISO/IEC 31000:2018) is a general risk management standard (not specific to IT) outlining principles and generic guidelines, and ISO 31010 (ISO/IEC 31010:2019) provides guidance on risk assessment techniques. These have influenced other security-specific standards by reinforcing principles like risk criteria, communication, and context setting. Many organizations align their information security risk methods with ISO 31000's principles to ensure consistency with enterprise risk management.

COBIT Risk IT and COSO ERM:

ISACA's COBIT framework includes Risk IT (ISACA, 2012), which extends COBIT's governance approach to IT risk management. Risk IT is indeed IT-specific but frames IT risks as business risks, similar to FAIR's approach of expressing risks in business terms. The COSO Enterprise Risk Management framework (COSO, 2017) is used broadly for all kinds of organizational risks. These frameworks underscore the need to integrate information security risk assessments methods into overall enterprise risk activities and governance, encouraging top-down risk oversight and linkage of IT risk with business objectives.

ENISA Guidelines on Risk Assessment:

European Union Agency on Cybersecurity (ENISA) offers guidance which is domain-specific and supplements analytical approaches to risk assessment. As an example, the cloud computing risk report published by ENISA (ENISA, 2009) lists the common threats, vulnerabilities, and control recommendations that can be used as a valuable source of input in the method-based analysis. ENISA guideline is, though not a fully-fledged approach, informative and adds value to the application of structured risk assessment techniques by ensuring parameters of the sector are considered.

Industry-specific frameworks:

Various industries have come up with special structures that operationalize and modify the existing risk assessment strategies. As an example, IT risk methods tend to be incorporated in operational risk frameworks in the financial sector, including the Basel II/III accords and the FFIEC IT Examination Handbook. On the same note, in the health care industry, the HIPAA Security Rule (U.S. Department of Health and Human Services, 2013) provides standards on how risks assessment of electronic health record systems should be conducted. These industry models do not suggest the developed analytical models but rather situate them and show how uniform concept of risk assessment methodologies are ingrained in sector-specific practices of governance.

2.5.7 Integration and Selection of Risk Assessment Approaches

Each methods and framework has its own emphasis – some prioritize quantification, others focus on process and governance, and others provide technical checklists. Importantly, these are not mutually exclusive. In practice, organizations often mix and match elements from different methods and frameworks to suit their needs. For example, an organization might use ISO 27005 as the overall process, NIST SP 800-30 for detailed guidance on analyzing a particular system, and FAIR to quantify a couple of top risks, all within the umbrella of a COBIT governance program. This hybrid approach is common and allows organizations to leverage the strengths of each method.

To conclude, risk assessment in information systems and cloud security is a well-established discipline supported by numerous methods and framework. Each classic methodology – ISO/IEC 27005, NIST SP 800-30 (and the CSF), FAIR, and OCTAVE – contributes its own tools and perspectives for evaluating risk. We have seen that while all aim for the same goal (identifying and prioritizing risks to inform decisions), they differ in their components: some are more people and process-oriented (OCTAVE), others more control and compliance-oriented (ISO 27005, NIST), and others more analytically rigorous (FAIR). An organization's choice among them will depend on factors like its regulatory environment, risk culture, resource availability, and the nature of its decision-making. What remains universally true is that conducting risk assessments methods by any robust methodology – is indispensable for effective cybersecurity and cloud security management.

2.6 Cloud Computing and Related Risk Landscape

2.6.1 Definition of Cloud Computing

Cloud computing is broadly defined as a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (such as networks, servers, storage, applications, and services), that can be rapidly provisioned and released with minimal management effort or provider interaction. This definition was formally introduced by the National Institute of Standards and Technology (NIST) (Mell & Grance, 2011). In simpler terms, it allows users to rent computing resources and services over the internet on an as-needed basis, rather than owning, managing and maintaining physical hardware and software themselves. According to NIST, this cloud model is composed of five essential characteristics, three service models, and four deployment models. These essential characteristics distinguish cloud computing from traditional IT models and underpin its advantages.

2.6.2 Key Characteristics and Advantages of Cloud Computing

The five essential characteristics of cloud computing, as identified by NIST, are: On-demand self-service, Broad network access, Resource pooling, Rapid elasticity, and Measured service. Below is a brief description of each characteristic and the main advantages it confers:

· **On-demand self-service:** Consumers can unilaterally provision computing capabilities (e.g., server time or storage) as needed automatically, without requiring human intervention from the service provider.

Advantage: This provides great flexibility and speed, allowing IT resources to be acquired or released in minutes, if not seconds, when needed (e.g., due to workload spikes). Organizations can rapidly scale up new applications or services, and in Platform-as-a-Service (PaaS) environments, development resources can scale dynamically to accelerate the development and deployment of new software products and services, thereby reducing time-to-market for new innovations.

· **Ubiquitous network access:** Services are available over the network and accessible through standard mechanisms by heterogeneous client platforms (e.g., mobile phones, laptops, etc.).

Advantage: This ensures accessibility from anywhere as long as an internet connection is available. It enables remote work and cooperation, as users can access cloud-based data and applications anytime, facilitating better collaboration and mobility.

· **Resource pooling (Multi-tenancy):** The provider's computing resources are pooled to serve multiple customers using a multi-tenant model (meaning that multiple customers share the same physical hardware and virtualization infrastructure, while logical separation mechanisms such as hypervisors and containers ensure isolation between tenants), with resources dynamically assigned and reassigned according to the current demand. The customer generally has no control over the exact physical location of resources, but may specify higher-level location requirements (e.g., region or datacenter) to be respected.

Advantage: This multi-tenancy and pooling leads to economies of scale. Computing resources are utilized more efficiently, reducing operational costs for cloud service providers (CSPs) who can serve more customers with fewer physical machines and operate remaining infrastructure in energy-efficient modes. This cost reduction is eventually passed on to consumers through lower service pricing. The large resource pools also provide customers with access to seemingly unlimited capacity when needed.

· **Rapid elasticity:** Computing capabilities can be elastically provisioned and released, in many cases automatically, to scale rapidly outward or inward commensurate with demand. To the consumer, the available resources may appear unlimited and can be appropriated in any quantity at any time.

Advantage: This gives cloud clients scalability on demand. Businesses can seamlessly handle sudden surges in workload (e.g., traffic spikes) without upfront investment and over-provisioning. Conversely, they can scale down to avoid paying for idle resources. Thus, this elasticity closely aligns cost with actual usage, improving cost efficiency. Furthermore, by guaranteeing the performance of the enterprises' applications under any workload, Service Level Agreements (SLAs) with their clients are met, avoiding violation fees while maintaining customer loyalty and enhancing the enterprises' reputation.

· **Measured service:** Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the service (e.g., storage, processing, bandwidth). Resource usage is monitored, controlled, and reported, providing transparency for both provider and consumer.

Advantage: This supports a pay-per-use model, where users pay only for what they actually consume. Such metered usage leads to cost savings by eliminating the need for large capital investments in hardware; instead, costs become operational and scalable with usage. It also provides transparency and accountability of resource consumption, which can improve budgeting and tracking, while fostering customer loyalty and trust through clear visibility into service usage.

These characteristics translate into several strategic advantages of cloud computing. In summary, cloud computing offers greater flexibility, efficiency, and strategic value compared to traditional on-premises IT. Organizations can be more agile – scaling resources up or down to meet business needs – and can deploy applications to market faster by avoiding long procurement and deployment cycles. The cloud's pay-as-you-go pricing and elimination of upfront infrastructure costs lead to cost effectiveness, as companies only pay for resources they actually use. Additionally, cloud services often give access to the latest technologies and security updates provided by cloud vendors, enabling innovation and potentially improved security by leveraging the expertise of specialized cloud providers (although security in the cloud also depends heavily on proper configuration and usage, as discussed later). Overall, the ability to outsource the management of underlying infrastructure allows businesses to focus on their core competencies and strategic goals rather than IT maintenance.

2.6.3 Cloud Service Delivery Models (IaaS, PaaS, SaaS)

Cloud services are typically categorized into three primary delivery models: Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS).

These models represent different levels of abstraction and control? provided to the consumer, ranging from low-level infrastructure to fully managed software applications:

- **Infrastructure as a Service (IaaS):** In IaaS, the cloud provider offers fundamental computing resources, such as virtual servers, storage, and networking on demand. The consumer can provision and run arbitrary software (operating systems, applications, etc.) on this infrastructure. The customer does not manage the underlying cloud hardware or virtualization, but has control over operating systems, storage, deployed applications, data and limited network configurations (eg, host-based firewalls).

  Example: Amazon Web Services (AWS) EC2, Microsoft Azure Virtual Machines, and Google Compute Engine are well-known IaaS platforms offering a multitude of IaaS services.

  Advantages: IaaS provides maximum flexibility, as it is analogous to renting raw computers with varied computing capabilities in the cloud. It is useful for IT departments that want full control over (infrastructural/computing) environments without buying hardware.

- **Platform as a Service (PaaS):** In PaaS, the provider delivers a platform or development environment on which consumers can deploy and execute their own applications. This includes managed infrastructure plus middleware, (programming language) runtimes, development frameworks, and other tools supported by the provider. The consumer does not manage the underlying infrastructure (servers, OS, network, etc.), but has control over the deployed applications and their data and possibly some configuration of the development environment.

  Example: Google App Engine, Microsoft Azure App Services, or Pivotal Cloud Foundry are PaaS offerings.

  Advantages: PaaS allows developers to focus on writing code and business logic, without worrying about managing the overall development environment, thus speeding up development and deployment. In addition, developer collaboration is fostered along with the use of modern software development methods (like agile ones). Furthermore, the platform administration and management burdens the provider who needs to continuously guarantee its operation. The development environment can also be scaled to cover increases in the workload. Finally, integration with IDEs is possible, allowing also offline work to be conducted in situations with limited connectivity.

· **Software as a Service (SaaS):** In the SaaS model, the provider delivers complete application software over the Internet, which the consumer can use via a thin client (like a web browser) or mobile app. The consumer does not manage or control the underlying cloud infrastructure or even individual application capabilities (apart from limited user-specific settings). Essentially, the software is hosted, updated and maintained by the provider, and users simply access it as a service. The software can also be integrated with the user applications (to complete their functionality) through the use of Web APIs or services. The SaaS users typically subscribe to the offered software or pay based on usage, although some SaaS offerings are provided for free with optional premium features (freemium model)

Example: Salesforce CRM, Google Workspace (Google Docs, Gmail, etc.), or Microsoft 365 are SaaS offerings.

Advantages: SaaS provides a fully managed solution – updates, security, scaling and maintenance for the application software offered are handled by the provider – which is convenient for end-users and reduces the burden on in-house IT for software management. Furthermore, SaaS services are offered via convenient pricing models (eg, pay-per-use, subscription-based, or freemium tiers with upgrade options). Finally, as software maintenance is conducted by the provider, this means that the SaaS is upgraded continuously and thus SaaS clients can instantly go from the current SaaS version to the next one effortlessly. As such, they can immediately access improved versions of SaaS services with better security and potentially new functional characteristics. Additional advantages include accessibility across multiple devices, simplified collaboration between users, and reduced upfront licensing costs compared to traditional software.

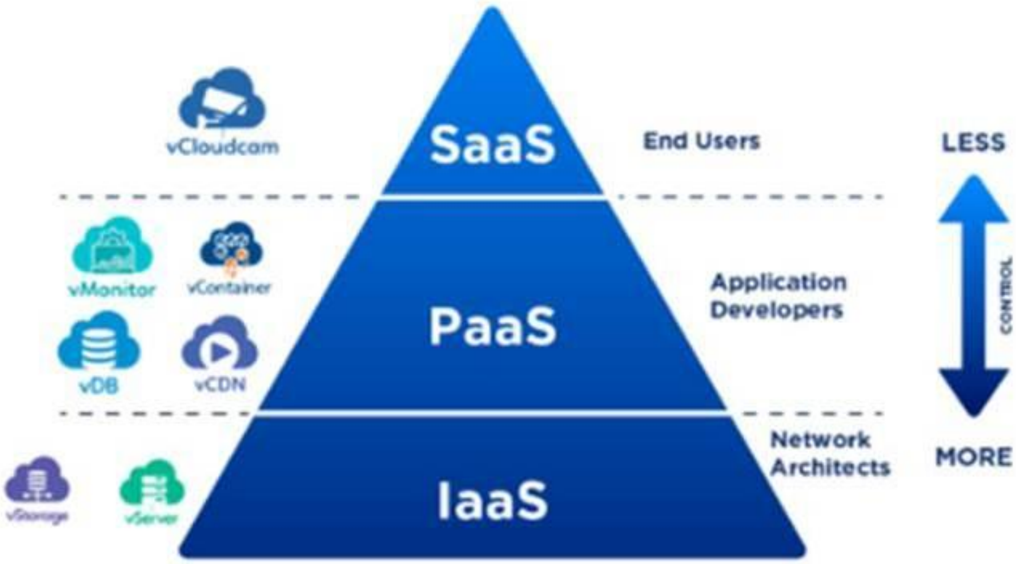

Figure 1: Cloud Service Delivery Model

As shown in figure above, these service models are often depicted as layers of a stack, with IaaS at the base (offering the most control to the user and requiring the most user management) up through PaaS to SaaS (offering the least control but the most convenience). Each model carries different security and management responsibilities for the user versus the provider, which is formalized in the "shared responsibility model" of cloud. For instance, In the IaaS model, users are responsible for managing and securing the operating systems, applications, and data, while the provider ensures the infrastructure's security. In the PaaS model, users manage their applications and data, with the provider handling the underlying platform and infrastructure security, while in SaaS, the provider manages most of the security, including the application and infrastructure.

2.6.4 Cloud Deployment Models (Public, Private, Hybrid, Community)

In addition to service models, there are four common cloud deployment models that differ in terms of who owns the infrastructure and how the cloud is deployed:

- **Public Cloud:** The cloud infrastructure is provided for open use by the general public. It may be owned and operated by a third-party cloud provider (eg, AWS, Microsoft Azure, Google Cloud) and resides off-premises at the provider's data centers. Public cloud services are delivered over the Internet and are shared by many organizations (multi-tenancy).

Characteristics: Highly scalable and cost-effective due to economies of scale. While multi-tenancy enables resource efficiency, potential limitations may arise if physical resources are over-provisioned, leading to reduced performance or increased security risks due to a larger attack surface.

Example: Amazon's AWS is a public cloud where any customer can rent compute or storage resources on demand.

· **Private Cloud:** The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple business units that act as its clients. A private cloud may be owned, managed, and operated by the organization itself or a third party, and it can exist on-premises or off-premises.

Characteristics: Offers greater control and customization over resources and can meet specific security or compliance requirements since the infrastructure is not shared with outsiders and security policies can be uniformly applied across it. However, it may be costly and less scalable than the public cloud because the organization bears the full expense of the infrastructure and its management and administration while its extent is usually limited and thus this limits its scaling capabilities.

Example: A bank might maintain a private cloud in its own data center for sensitive customer data processing.

· **Community Cloud:** The cloud infrastructure is shared by a specific community of organizations with common concerns (eg, mission, security requirements, policy, or compliance needs). It is exclusively used by this community and it may be managed by one or more of the community's organizations or a third party. It can exist on or off premises with respect to the community's organizations.

Characteristics: It constitutes a collaborative model where costs, resources and management are shared among the community. A community cloud might be more secure than a public cloud but less secure than a private one. Furthermore, its scaling capabilities might lie between those of a public and private cloud.

Example: Several research institutions might share a community cloud to store and analyze genomic data, adhering to common security standards.

· **Hybrid Cloud:** The cloud infrastructure is a composition of two or more distinct cloud infrastructures (that can be of the same or even different type, eg, private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability.

Characteristics: A hybrid cloud combines the benefits of multiple deployment models – for instance, an organization may use public cloud for general-purpose workloads but keep a private cloud for sensitive data. While a hybrid cloud can combine benefits from different cloud deployment models, it suffers from higher complexity, so it is more difficult to manage it, while it is more difficult to achieve accountability and traceability (eg, which component cloud to blame for a specific security even that has occurred?).

Example: An e-commerce company might run its customer-facing website in the public cloud for scalability, but store customer financial data in a private cloud; the two environments (public and private cloud) communicate over secure channels, forming a hybrid model.

In summary, public clouds offer scalability and cost savings, but they come with higher security risks due to multi-tenancy and shared infrastructure. This can increase the likelihood of data breaches and security misconfigurations if not properly managed. Private clouds provide greater control and security, as the infrastructure is dedicated to a single organization, allowing for stricter access controls and compliance with regulatory standards. However, they can be costly and may face scalability challenges. Community clouds offer shared infrastructure for similar organizations, balancing between the flexibility of a public cloud and the security of a private one, but they still present risks associated with shared resources. Hybrid clouds provide a mix of both public and private cloud environments, offering flexibility and scalability, but they come with increased complexity in terms of security management, integration, and ensuring accountability across the different cloud environments. Each deployment model carries distinct security considerations and risk profiles, requiring careful management of access controls, data protection, and compliance to mitigate potential vulnerabilities.

2.6.5 Common Vulnerabilities in Cloud Computing Environments

Despite the benefits of cloud computing, it introduces a range of security vulnerabilities and challenges. Cloud environments are complex and, if not properly configured and managed, can be susceptible to various weaknesses. Some of the most common cloud vulnerabilities include:

· **Misconfigurations of Cloud Resources:** Misconfiguration is consistently identified as a leading cause of cloud security failures. This refers to mistakes or oversights in how cloud services are set up – for example, setting storage buckets or databases to be publicly accessible, using excessively permissive access control rules, or configuring improper network security group settings. Such errors can inadvertently expose sensitive data or services to the Internet. In fact, studies indicate that 65–70% of cloud security vulnerabilities arise from misconfigurations. Since cloud platforms offer many settings and features, administrators who are unfamiliar with them or rushing (such that, eg, use default settings that are insecure) may leave dangerous gaps that could be exploited by potential hackers.

Impact: A misconfigured cloud service, such as a storage one (eg, an open Amazon S3 bucket) can allow anyone on the Internet to read confidential data, leading to data leaks. Misconfigured compute instances or containers might allow attackers to escalate privileges, access internal services and data or inject malware.

· **Insecure Interfaces and APIs:** Cloud services are accessed and managed through APIs and web interfaces. If these APIs are not adequately secured – lacking proper authentication, encryption, or input validation – attackers can exploit them as as to intrude cloud services.

Impact: Insecure APIs could allow adversaries to steal tokens/credentials, perform unauthorized operations, or inject malicious commands. Since APIs are a primary interaction point with cloud resources, the vulnerabilities here can have broad impact. This may result in data breaches, service disruptions, or compromise of entire cloud environments if administrative APIs are exploited.

Example: An API that does not properly validate user input could be susceptible to SQL injection or other injection attacks, potentially giving attackers direct access to backend cloud databases. Ensuring secure API endpoints (using strong authentication, HTTPS, throttling, etc.) is crucial. For instance, in 2017, Snapchat's API flaw exposed sensitive user data when insufficient authentication controls were implemented [SecurityWeek, 2017]. In this respect, best practices and methods to develop secure software must be adopted.

· **Weak Identity and Access Management (IAM):** Cloud environments rely heavily on digital access controls. Weak IAM practices – such as having accounts with excessively broad privileges, not using multi-factor authentication, or leaving default credentials – can be exploited.

Impact: If attackers gain access to a set of cloud credentials (for example, through phishing or leaked API keys), they may be able to hijack accounts and directly access or modify cloud resources. Failing to implement least privilege principles (ensuring each user or service has only the minimum permissions necessary) means that a single compromised account can have a devastating blast radius.

Example: Cloud API keys accidentally exposed in public code repositories have led to attackers spinning up expensive resources or exfiltrating data. Account hijacking is a known threat – in 2023, cloud account takeover threats were noted to have increased significantly, enabling attackers to impersonate legitimate users and evade detection.

· **Lack of Cloud Visibility and Shadow IT:** Organizations sometimes struggle to maintain full visibility over all their cloud assets and configurations. The ease of deploying cloud resources can lead to "shadow IT" - where business units or developers create cloud instances or use services outside of centralized IT knowledge or control.

Impact: This can result in unmonitored resources with potential vulnerabilities. A lack of monitoring and visibility means security teams might not notice misconfigurations or intrusions in those cloud workloads. Furthermore, unaccounted assets may not receive security updates or compliance checks, becoming soft targets for attackers.

Example: In 2019, the Capital One data breach was partly enabled by a misconfigured AWS resource that went unnoticed by security teams, illustrating the dangers of poor visibility into cloud assets [U.S. Senate Report, 2020]. Similarly, shadow IT services, such as unsanctioned file-sharing or messaging platforms, can introduce hidden entry points for attackers if not brought under central security governance.

· **Shared Technology Vulnerabilities (Multi-tenancy risks):** Cloud computing involves a shared infrastructure – physical servers, virtualization hypervisors, and common network components are shared among customers in a public cloud. A vulnerability in these underlying shared technologies could potentially be exploited to affect multiple customers. For instance, a weakness in a hypervisor (the software layer enabling virtualization) could allow one virtual machine (VM) to escape its isolation and gain access to the host or other VMs. Such an exploit is known as a hypervisor or VM escape attack. Although major cloud providers invest heavily in securing hypervisors, critical vulnerabilities have arisen in the past.

Impact: If an attacker succeeds in a hypervisor-level attack, they could gain control over the underlying host server, thereby compromising all co-located customer VMs – an extremely severe breach of isolation.

Example: The "VENOM" vulnerability (CVE-2015-3456) in a popular virtualization component could theoretically allow an attacker to break out of a VM. Side-channel attacks like Spectre and Meltdown (discovered in 2018) exploited CPU-level design flaws to leak data residing in memory. These vulnerabilities prompted urgent responses from cloud providers, who implemented patches and microcode updates to mitigate risks and maintain tenant isolation.

2.6.6 Traditional Vulnerabilities in Cloud Assets

Beyond cloud-specific issues, cloud environments still face classic security problems. These include unpatched software vulnerabilities in virtual machines or container images (allowing exploits like remote code execution), weak or absent encryption for data-at-rest or in-transit, and inadequate backup or disaster recovery setups (leading to potential data loss). For example, if a cloud database service is not configured to require encryption, data could be intercepted or read if an attacker gains lower-level access. Similarly, if software running in a cloud VM has a known flaw that has not been patched, attackers can leverage that to gain entry – the cloud does not magically eliminate software bugs. Malicious insiders (e.g., a rogue employee at the cloud provider or within a cooperating partner) are another concern; they might abuse privileged access to steal data or disrupt services. Organizations must thus apply best practices (like regular patch management, encryption, monitoring, and zero-trust principles) to their cloud resources just as they would on-premise.

Common misconfigurations and their consequences include:

- Unsecured storage buckets (e.g., AWS S3, Azure Blob, Google Cloud Storage) → exposure of sensitive data
- Overly permissive access controls (e.g., granting "public" or "*" access in IAM policies) → attackers gain unauthorized entry to critical systems
- Default or weak credentials left unchanged → brute-force or credential stuffing attacks succeed more easily
- Misconfigured network security groups/firewall rules → open ports/services expose workloads to scanning and exploitation
- Failure to enable encryption at rest or in transit → sensitive data may be intercepted or stolen
- Improperly configured metadata services → attackers can extract credentials and pivot deeper into cloud infrastructure

Impact: If software running in a cloud VM has a known flaw that has not been patched, attackers can exploit it for remote code execution, leading to unauthorized access.

Weak or missing encryption can expose sensitive data to interception or unauthorized reads. Poor backup and disaster recovery planning may result in permanent data loss after an attack or outage. Insider threats can cause large-scale data breaches or service disruptions, with potentially greater impact due to providers' broad system access.

Examples:

· Unpatched software: In 2017, the WannaCry ransomware exploited unpatched Windows vulnerabilities, which also affected cloud-hosted systems that had not applied security updates.

· Weak encryption: In 2018, researchers demonstrated that improperly configured cloud databases without encryption allowed attackers to access millions of unprotected records (UpGuard, 2018).

· Inadequate backup: Companies relying solely on a single cloud region without redundancy have experienced outages (e.g., AWS S3 outage in 2017), leading to significant data unavailability.

· Insider threats: The Edward Snowden disclosures in 2013 highlighted how insiders with privileged access could exfiltrate sensitive data, a concern that remains relevant in cloud environments.

In summary, misconfiguration stands out as a very prevalent cloud vulnerability (often due to human error or rushed deployments), followed by issues with identity management, insecure interfaces, and the inherent complexity of a shared multi-tenant environment. Furthermore, classical vulnerabilities also hold in cloud environments. Many of these vulnerabilities are exacerbated by the cloud's scale and dynamic nature – a single misstep can expose large amounts of data or many systems. Recognizing these common weaknesses is the first step in improving cloud security posture.

2.6.7 Types of Attacks in Cloud Environments

Threat actors are actively interested in exploiting the above vulnerabilities to compromise cloud services. Several specific types of attacks are particularly relevant in cloud contexts:

2.6.7.1 SQL Injection Attacks

SQL injection attacks occur when cloud-hosted applications or APIs fail to properly validate input, allowing attackers to execute malicious SQL commands against backend databases. In cloud environments, these attacks can be particularly devastating due to the interconnected nature of cloud services and the potential for lateral movement.

· *Attack Method:* Attackers identify input fields in web applications or APIs that interact with databases. They then inject malicious SQL code through these fields, potentially gaining unauthorized access to sensitive data, modifying database contents, or executing administrative commands.

· *Impact:* Successful SQL injection attacks can result in complete database compromise, leading to large-scale data breaches, data manipulation, or service disruption. In cloud environments, compromised databases may contain data from multiple customers or business units.

· *Example:* In 2019, a SQL injection vulnerability in a cloud-hosted application led to the exposure of over 198 million voter records, demonstrating how these traditional attacks remain highly effective in cloud environments (Goodin, 2019).

2.6.7.2 Credential Stuffing and Brute Force Attacks

These attacks specifically target cloud account credentials, attempting to gain unauthorized access to cloud services through automated password attacks or by using previously breached credential databases.

· *Attack Method:* Attackers use automated tools to test large numbers of username/password combinations against cloud service login endpoints. Credential stuffing uses previously breached credentials from other services, while brute force attacks systematically try common passwords.

· *Impact:* Successful credential attacks can provide attackers with legitimate access to cloud resources, making detection difficult. Once inside, attackers can access sensitive data, deploy malicious resources, or use cloud infrastructure for further attacks.

· *Example:* In 2018, attackers used credential stuffing to compromise thousands of AWS accounts, subsequently using the compromised infrastructure for cryptocurrency mining operations (Cimpanu, 2018).

2.6.7.3 Container and Orchestration Platform Attacks

These attacks target containerized applications and orchestration platforms like Kubernetes that are commonly used in cloud environments.

· *Attack Method:* Attackers exploit misconfigurations in container orchestration platforms, vulnerable container images, or exposed management APIs to gain unauthorized access to containerized applications and underlying infrastructure.

· *Impact:* Container attacks can lead to privilege escalation, lateral movement within cloud infrastructure, and potential compromise of multiple applications running on the same cluster.

· *Example:* In 2018, Tesla's AWS environment was compromised through exposed Kubernetes credentials, with attackers using the infrastructure for cryptocurrency mining (Cimpanu, 2018).

2.6.7.4 API Exploitation Attacks

Cloud services heavily rely on APIs for communication and management, making API vulnerabilities a significant attack vector.

· *Attack Method:* Attackers identify and exploit vulnerabilities in cloud service APIs, such as broken authentication, excessive data exposure, lack of rate limiting, or injection flaws. They may also target management APIs with weak authentication or authorization.

· *Impact:* API attacks can result in unauthorized data access, service disruption, or administrative control over cloud resources. The interconnected nature of cloud services can amplify the impact of successful API exploits.

· *Example:* In 2019, the Capital One breach involved exploiting a misconfigured web application firewall that allowed an attacker to query AWS metadata services and obtain credentials for further system access (U.S. Senate Report, 2020).

2.6.7.5 Denial of Service (DoS) and Distributed DoS Attacks

In a Denial of Service attack, an adversary attempts to make a cloud service unavailable to its legitimate users by overwhelming it with traffic or requests, or by exploiting resource exhaustion.

· *Attack Method:* Attackers flood cloud-hosted web applications or APIs with a huge volume of requests (possibly using a botnet in a Distributed DoS scenario) until the service either crashes or becomes too slow for normal use. They may also target specific cloud service endpoints or exploit auto-scaling mechanisms to force excessive resource consumption.

· *Impact:* Successful DoS attacks result in downtime, loss of revenue, and damage to user confidence and trust. A notable aspect of cloud economics is that attackers may force services to scale up resources significantly, creating a financial drain on the victim (an "economic DoS" scenario).

- *Example:* In 2016, the Dyn DNS provider suffered a massive DDoS attack powered by the Mirai botnet, which disrupted major cloud-hosted services, including Twitter, Netflix, and Reddit (KrebsOnSecurity, 2016).

2.6.7.6 Cryptojacking Attacks

Cryptojacking involves unauthorized use of cloud computing resources to mine cryptocurrency, often through compromised accounts or vulnerable services.

- *Attack Method:* Attackers gain access to cloud accounts through various means (credential compromise, API exploitation, container vulnerabilities) and then deploy cryptocurrency mining software on the victim's cloud infrastructure.

- *Impact:* While not always targeting data theft, cryptojacking can result in significant financial costs through increased cloud resource consumption and may indicate broader security compromises that could be leveraged for more serious attacks.

- *Example:* The Tesla incident mentioned earlier exemplifies cryptojacking, where exposed Kubernetes credentials led to unauthorized cryptocurrency mining on Tesla's cloud infrastructure.

2.6.7.7 Supply Chain Attacks

Supply chain attacks involve compromising third-party cloud services, container images, or software components to indirectly affect many cloud users.

- *Attack Method:* Attackers compromise widely-used cloud services, container registries, or software packages that are subsequently deployed across multiple cloud environments. This can include malicious container images, compromised CI/CD pipelines, or tainted software updates.

- *Impact:* The consequences include the propagation of malware, insertion of backdoors, or the corruption of widely deployed software components potentially compromising the confidentiality, integrity, and availability of numerous organizations at once.

- *Examples:* The 2020 SolarWinds compromise showed how attackers could infiltrate widely used software updates, affecting thousands of organizations including cloud users. Compromised Docker container images have been found in public registries, potentially affecting organizations that deploy these images in their cloud environments (Fishbein, 2018)

2.6.7.8 Hypervisor and Side-Channel Attacks

Although rarer in practice, these attacks target the underlying virtualization infrastructure of cloud services.

- *Attack Method:* Advanced attackers attempt to compromise the hypervisor software that manages virtual machines, potentially executing VM escape attacks to gain access to the host machine or other customer VMs on the same host. Side-channel attacks attempt to glean information from co-resident virtual machines by analyzing shared resources.

- *Impact:* If successful, hypervisor attacks could undermine the fundamental trust in isolation that cloud computing depends on, potentially allowing access to data from multiple customers. However, major cloud providers invest heavily in proactive patching and isolation mechanisms, making these attacks extremely difficult to execute.

- *Example:* The Spectre and Meltdown CPU vulnerabilities demonstrated in 2018 (Kocher et al., 2019; Lipp et al., 2018) showed that hardware-level design flaws could potentially be used to read data across isolation boundaries, prompting massive industry response to secure cloud infrastructure.

2.6.7.9 Social Engineering and Phishing Attacks

Social engineering attacks trick cloud administrators or users into revealing credentials or unintentionally authorizing malicious actions, bypassing technical defenses.

- *Attack Method:* Attackers use psychological manipulation, often through phishing emails, fake websites, or direct communication, to trick individuals into providing credentials, clicking malicious links, or performing actions that compromise cloud security.

- *Impact:* Successful social engineering can provide attackers with legitimate credentials and access rights, making detection difficult and potentially leading to significant data breaches or system compromises.

- *Example:* In 2020, Twitter suffered a breach when attackers used social engineering to trick employees into granting access to internal tools, demonstrating how human factors can undermine cloud security (Roth, 2020).

2.6.8 Summary of Cloud Attack Landscape

In essence, the cloud threat landscape includes both familiar attacks (like injection attacks, DoS, or social engineering) adapted to cloud targets, and cloud-specific vectors (like exploiting cloud misconfigurations or container vulnerabilities). Many of these attack types are documented in industry analyses, such as the Cloud Security Alliance's reports, which identify various attack vectors and threat scenarios affecting cloud computing environments (Cloud Security Alliance, 2022). Organizations must therefore adjust their security strategies to account for these cloud-focused attack modes, implementing defense-in-depth strategies that address both traditional and cloud-specific attack vectors.

It is important to distinguish between threats (potential dangers that could exploit vulnerabilities), attacks (specific methods used to exploit vulnerabilities), and impacts (consequences of successful attacks). While data breaches are often categorized as threats in industry analyses for simplicity, they are more accurately described as potential consequences of successful attacks rather than attack methods themselves.

2.6.8 Potential Consequences and Impacts of Cloud Security Incidents

The impact of a successful attack on a cloud infrastructure can be devastating, underscoring why cloud security is a vital concern. Some potential consequences include:

- **Massive Data Loss or Exposure:** Cloud breaches can expose millions of records in one incident, given the large centralized datasets often stored. Such incidents typically result from exploitation of vulnerabilities in cloud services, with misconfiguration representing a prevalent type of vulnerability rather than an attack method itself. Misconfiguration can be considered a general vulnerability category that applies to both cloud and on-premises environments, but it is particularly significant in cloud contexts due to the complexity of cloud services, shared responsibility models, and the dynamic nature of cloud deployments.

  Impact: For the organization, this can mean loss of intellectual property or confidential information, identity theft for customers, and expensive incident handling processes (which include tasks, like notification and recovery). The long-term impact includes loss of customer trust and erosion of brand value. Publicly traded companies often experience measurable financial repercussions, such as significant stock price declines, reduced market capitalization, and increased customer churn. Additionally, regulatory fines may be imposed under laws like GDPR, HIPAA, or CCPA for failing to protect data (European Union, 2016; U.S. Department of Health & Human Services, 2020).

  Example: In 2019, the Capital One breach exposed over 100 million customer accounts and credit card applications due to a misconfigured web application firewall in AWS (U.S. Senate, 2020). The incident led to direct costs exceeding $300 million, regulatory fines, and a sharp decline in customer trust. Similarly, in 2017, the Equifax breach (though not cloud-specific) highlighted the devastating consequences of exposing sensitive personal data, leading to an estimated $4 billion in total costs and long-term reputational damage (FTC, 2019).

· **Service Disruption and Business Continuity Impact:** Cloud attacks can render critical business applications and services unavailable, directly impacting operations and revenue generation.

Impact: Service disruptions can lead to immediate revenue loss, particularly for organizations heavily dependent on cloud-based operations. Extended outages may violate Service Level Agreements (SLAs), resulting in financial penalties and customer compensation. The reputational damage from unreliable service can have lasting effects on customer retention and acquisition.

Example: The 2016 Dyn DNS attack disrupted major cloud-dependent services like Twitter, Netflix, and Reddit for hours, demonstrating how targeted attacks on cloud infrastructure can cascade across multiple organizations and affect millions of users globally.

· **Financial Theft and Fraud:** Cloud security incidents impose significant financial burdens on organizations. These costs arise not only from fines and regulatory penalties but also from forensic investigations, remediation measures (e.g., hiring incident response teams, upgrading security tools), and legal expenses.

Impact: A data breach in 2024 costs organizations on average $4.88 million when factoring in both immediate and long-term expenses (IBM, 2024). A severe cloud outage can lead to substantial revenue losses, especially if it disrupts online services (e.g., e-commerce downtime translates to lost sales every minute). In cloud misuse cases, such as crypto-jacking or DoS-induced scaling, the victim might receive an unexpectedly large cloud bill that they must negotiate with the provider to reduce it or just absorb it.

Example: In a 2023 survey by Palo Alto Networks, over 75% of companies hit by cloud breaches reported significant operational downtime and financial loss. In Tesla’s 2018 incident, attackers exploited misconfigured Kubernetes credentials in AWS to run unauthorized cryptocurrency mining, leading to increased operational costs (RedLock, 2018).

· **Operational Disruption:** If an attack makes cloud systems unavailable (through DoS or ransomware), the affected organization may be unable to perform critical business operations. Consider a company whose entire IT infrastructure is in the cloud – a successful attack could lock them out of their applications or data entirely until resolved.

Impact: Organizations fully reliant on cloud infrastructure may be locked out of their applications or data until the incident is resolved. Downtime can last from hours to weeks, crippling internal productivity and customer-facing services. The cascading effect means that when a SaaS provider is disrupted, its client businesses may also come to a standstill, amplifying the overall impact.

Example: In 2020, a DDoS attack on AWS disrupted several large-scale customer applications for hours, impacting both service providers and end-users globally (AWS, 2020). Similarly, the 2021 ransomware attack on the Kaseya VSA software. though not cloud-native. demonstrated how operational downtime from a single incident can cripple hundreds of downstream businesses (CISA, 2021).

· **Legal and Compliance Fallout:** Security incidents can trigger lawsuits and compliance investigations. Customers, partners, or even shareholders might pursue legal action if negligence is suspected. In cloud contexts, there can be complications in shared responsibility – for instance, if a breach occurs, affected parties might litigate whether the cloud provider or the customer was at fault in failing to secure the environment.

Impact: Customers, partners, or shareholders may pursue legal action if negligence is suspected. In cloud settings, disputes can emerge over shared responsibility whether the provider or the customer was at fault. Non-compliance with breach notification laws (e.g., GDPR, HIPAA, CCPA) can result in steep penalties. In sensitive industries, such as finance or healthcare, repeated or egregious incidents can also lead to sanctions or increased regulatory oversight.

Example: Following the 2019 Capital One breach, multiple lawsuits were filed against both Capital One and AWS, highlighting the challenges of shared responsibility in cloud security (U.S. Senate, 2020). Similarly, British Airways faced a £183 million GDPR fine in 2019 after a data breach exposed customer information (ICO, 2019).

· **Reputation Damage:** Trust is fundamental in the digital era. A publicized cloud security incident can cause reputational damage that is hard to quantify but very real in its impact. Customers may be less willing to use a service perceived as insecure. For cloud providers themselves, a significant security failure undermining multi-tenant isolation would be a catastrophic blow to their business model, as clients could flee to competitors.

Impact: Customers may be less willing to engage with services perceived as insecure, while cloud providers risk losing clients if multi-tenant isolation is undermined. Even enterprises using third-party cloud services face reputational damage among consumers when breaches occur. Rebuilding trust often requires enhanced transparency, third-party audits, or certifications to demonstrate a renewed commitment to security.

Example: The Equifax breach of 2017, while not fully cloud-based, remains a landmark case of reputational collapse; the company faced ongoing public distrust and brand erosion despite spending billions on remediation (FTC, 2019). In cloud contexts, repeated outages by major SaaS vendors have led enterprise clients to migrate to competitors, demonstrating how quickly reputation loss translates into customer attrition (Gartner, 2022).

In summary, cloud attacks carry the same consequences as other cyberattacks – data theft, downtime, financial and legal repercussions – but often on a potentially larger scale due to the concentration of assets and data in (centralised) cloud platforms. This amplifies the importance of cloud risk management and preparedness.

2.6.9 Real-World Examples of Cloud Security Incidents

There have been numerous high-profile incidents illustrating the cloud risk landscape. A few notable examples include:

· **Capital One Data Breach (2019):** This incident is one of the most famous cloud-related breaches to date, demonstrating how a cloud misconfiguration combined with a clever attack led to a massive data theft. In July 2019, Capital One (a major bank) announced that a threat actor had illegally accessed personal data of over 100 million credit card applicants and customers. The data, stored in Capital One's AWS cloud environment, included names, addresses, credit scores, Social Security numbers (around 140,000 SSNs) and bank account numbers for tens of thousands of individuals. The cause was traced to a misconfigured Web Application Firewall (WAF) on an AWS-hosted application. The attacker exploited this misconfiguration using a Server-Side Request Forgery (SSRF) technique to trick the application into executing requests on its behalf. Through SSRF, she obtained credentials from the instance's AWS metadata service (which applications normally use for configuration) and then leveraged those credentials to enumerate and download data from Amazon S3 buckets (cloud storage) that contained the sensitive information. The perpetrator was a former AWS employee;

this perhaps contributed to her sophisticated understanding of AWS systems. The breach went undetected from March until July 2019.

Impact: Capital One faced an enormous fallout – an estimated cost of $300 million in fines, legal settlements (including an $80 million regulatory fine and $190 million in a customer class-action settlement), not to mention the reputational hit and customer trust issues. It also underscored shared responsibility: while AWS's infrastructure was not hacked directly, Capital One's configuration mistake in their cloud deployment was the vulnerability. The case raised awareness of SSRF and cloud misconfigurations, prompting many organizations to harden their AWS IAM roles and WAF configurations. (Notably, AWS subsequently made changes to the metadata service to mitigate SSRF risk, such as introducing IMDSv2, which requires session authentication for, eg, metadata queries)

· **Misconfigured AWS S3 Buckets and Data Leaks:** There have been countless instances of sensitive data being exposed due to misconfigured cloud storage (ZDNet, 2017). One striking example occurred in 2017, when a marketing analytics firm, Alteryx, left an AWS S3 bucket publicly accessible without authentication. The bucket contained a dataset with information on 123 million US households, totaling 36 GB of data. This data, aggregated from a consumer database (including addresses, demographics, mortgage information, etc.), was discovered by a security researcher who was scanning for open cloud storage. Sinc the bucket was not secured, any Internet user could access and download the data. Although the issue was discovered by a benign researcher before it was actually exploited, the exposure was significant enough to make headlines.

In another case in 2017, a contractor for a telecom company (Nice Systems, working with Verizon) left an S3 repository of Verizon customer call data open, exposing records of 6 million customers. Misconfigured S3 buckets have affected organizations ranging from government agencies to private companies (even data associated with top-secret projects have leaked in this manner).

Impact**:** Such incidents often lead to embarrassing press coverage and require notifying all affected individuals. They are relatively easy for attackers to find – there are automated tools to crawl for S3 buckets or other storage with lax settings. These examples have propelled efforts like AWS adding default encryption and more explicit warnings in the S3 console about public access, as well as organizations adopting configuration scanning tools. They serve as clear reminders that a single checkbox in a cloud console (to restrict access) can stand between normal operations and a major breach.

· **Code Spaces Attack (2014):** Not all cloud incidents are about data exposure; some involve attackers targeting the availability and integrity of cloud assets. Code Spaces was a code-hosting and software collaboration company (similar to GitHub) that tragically went out of business following a cloud attack. In June 2014, Code Spaces' AWS admin console was illegally accessed by an attacker who initially launched a DDoS attack and demanded ransom. When Code Spaces attempted to regain control and lock the attacker out, the attacker retaliated by using their access to delete critical resources in the AWS environment. The attacker wiped out snapshots, backups, and databases – effectively almost all of the company's data and servers were destroyed. Code Spaces had some backups, but these too were mostly in the same cloud account and were thus destroyed. The incident unfolded rapidly and, within 12 hours, the company's ability to operate was irreversibly crippled. In a public statement, Code Spaces acknowledged that the attack and data destruction that it caused meant that they could no longer continue business.

***Impact*:** This case illustrates a worst-case scenario of cloud risk – if an attacker gains administrative credentials to your cloud account (through phishing or other means), they can literally destroy your cloud-based IT environment. It underscores the importance of safeguards like multi-factor authentication, the principle of least privilege (to limit how much damage one account can do), and having off-site/off-cloud backups. For cloud reliability, one should not keep all backups solely in the same cloud account; otherwise, compromise of that account can be catastrophic. Code Spaces' demise is often cited in cloud security lectures as a lesson in the magnitude of impact that can result from cloud account breaches.

· **Tesla Cloud Cryptojacking Incident (2018):** As another example of cloud account compromise, in 2018 attackers breached Tesla's poorly secured Kubernetes console (an administrative console for managing containers in clusters deployed in the cloud) which was not password protected. Through it, they gained credentials to Tesla's AWS environment. Instead of stealing data, the attackers installed cryptocurrency mining software on Tesla's cloud servers to profit from the computing power (a practice known as cryptojacking). This incident was detected by a cloud security monitoring company, and Tesla quickly mitigated it. It exemplified that even tech-savvy organizations can misconfigure a service such that attackers can then exploit cloud resources in any way beneficial for them – stealing either data or computing cycles for money.

Impact: It is related to primarily increased cloud usage costs and the potential performance degradation of Tesla's cloud systems due to the illicit mining workload. It was less publicly damaging than a breach of personal data, but it still highlighted the need for vigilance in securing management interfaces and employing tools that detect unusual cloud usage patterns (like a spike in CPU usage that might indicate mining).

· **Parler Data Scraping (2021):** As a final illustrative case, consider the incident with the social media platform Parler, which was hosted on a cloud. When Parler went offline in January 2021, activists were able to exploit the fact that Parler had left a lot of user content (videos, posts, images) publicly accessible (or accessible via insecure APIs) without proper authentication. So, they scripted mass downloads of all public posts (including metadata). While this was not a "hack" in the traditional sense (no system was broken into – it was more of a scrape of openly available data), it underscores how data exposure can also occur simply from overly permissive settings. In Parler's case, even deleted posts were available because the platform had only "flagged" them but not removed the data (well-known data retention issue). The result was an archive of millions of posts being compiled and shared publicly, raising privacy concerns for users who might not have realized their data could be downloaded in bulk. This example emphasizes that the threat surface of cloud services can include not just malicious intrusions, but also the unintended public availability of data via features or misconfigurations.

Each of these examples provides a learning opportunity. The Capital One incident teaches the importance of secure configurations and application-level defenses (like guarding against SSRF) in the cloud. The S3 bucket leaks highlight basic but critical storage security practices and the need for oversight. Code Spaces demonstrates the ultimate consequence of not securing cloud credentials and lack of redundancy outside the primary cloud. While the other cases reiterate themes of identity management, monitoring, and expecting the unforeseen uses of your cloud by attackers.

In conclusion, cloud computing offers transformative benefits to organizations in terms of scalability, flexibility, and cost savings. However, it also introduces a complex and extensive risk landscape that must be managed. Cloud-specific vulnerabilities (such as misconfigurations or multi-tenant issues) and traditional security gaps can lead to serious incidents if unaddressed. A robust cloud security strategy – encompassing proper configuration management, identity and access controls, encryption, continuous monitoring, and incident response planning – is essential to safely enjoy the benefits of cloud computing. The lessons learned from real-world cloud incidents underline that while the responsibility for security is shared with the provider, cloud customers cannot abdicate their portion of that responsibility. A proactive, informed approach to cloud risks will significantly reduce the likelihood of joining the growing list of cloud security failure case studies.

3

Literature Review Methodology and Quantitative Analysis

3.1 Introduction to the Literature Review Methodology

This chapter outlines the systematic methodology followed to review existing literature on cloud computing risk assessment. Given that cloud environments introduce unique security challenges and shared responsibility models, a structured literature review was essential to identify relevant risk assessment frameworks and methods. A systematic literature review (SLR) approach was adopted following established guidelines (Kitchenham & Charters, 2007) to ensure comprehensive coverage and unbiased selection of sources. The goal was to capture how cloud-specific risks are addressed, as traditional risk models often need adaptation in the cloud context. This methodology was planned in accordance with academic best practices for literature reviews (e.g., defining research questions, using reproducible search strategies, and clear inclusion/exclusion criteria) to provide transparency and rigor. The following sections detail all major review methodology steps performed, i.e., the research goals and questions posed, the search strategy applied, and the filtering and quality assessment process followed as well as their major outcomes. At the end, a first quantitative analysis of the literature selection results is supplied.

3.2 Definition of Research Goals and Research Questions

The primary research goal of this literature review was to identify and analyze the proposed risk assessment methods on cloud computing. The focus on methods, rather than methodologies and framework, is justified by the observation that traditional risk assessment methodologies (as analyzed in Chapter 2) are typically followed even in cloud environments, but the specific methods are updated or devised to operate properly and correctly within these environments. Cloud computing can introduce new or unidentified risks to organizations if not properly assessed, so the review aimed to investigate how researchers and practitioners have approached this problem. In particular, the review sought to understand methods that assess how well confidentiality, integrity, availability, and privacy are satisfied in cloud environments by evaluating whether risks remain within acceptable thresholds. To meet this goal, several specific research questions (RQs) were defined:

- **RQ1:** *What risk assessment methods have been proposed for cloud computing environments, and what are their main components (e.g., models, metrics, data, tools, and control or governance frameworks)?* This question focuses on identifying and categorizing existing **methods** that have been developed or adapted to assess risks in cloud services, along with the key ingredients that constitute each method. By addressing RQ1, the review provides a comprehensive overview of proposed analytical approaches and their internal structures, including conceptual models, analytical mechanisms, and supporting governance elements, as analyzed in Section 4.1.

- **RQ2:** *How are quantitative and qualitative risk metrics utilized in cloud computing risk assessment methods?* This question examines how numerical scoring systems or metrics (such as the Common Vulnerability Scoring System – CVSS) and qualitative-based systems are used in the risk assessment process. The aim is to see to what extent cloud risk methods incorporate quantitative and qualitative measures of likelihood and impact. For example, some researchers propose aggregating CVSS-based scores to quantify overall risk or use CVSS metrics to estimate risk levels in terms of frequency and impact. The results and discussion related to this question can be found in Section 4.2.

- **RQ3:** *Which methods from the current literature prevail?* This question will be answered through the comparative analysis and evaluation of risk assessment methods in Section 4.3.

- **RQ4:** *What are the strengths and limitations of current cloud risk assessment methods?* The discussion on strengths and limitations of current risk assessment methods (and their ingredients) is presented in Section 4.2.

- **RQ5:** *What are the current research gaps that must be addressed?* This is covered in Chapter 5, where the research gaps identified in the literature are discussed.

- **RQ6:** *Which research directions need to be followed to close these gaps?* Future research directions are outlined in Chapter 5.

3.3 Search Strategy

A systematic search strategy was employed to locate literature relevant to the above research questions. This strategy involved formulating appropriate keywords, constructing search queries, and selecting a range of scholarly and industry sources likely to contain discussions of cloud risk assessment.

Keywords and Search Terms: The search terms were derived from the key concepts in the research questions. Primary keywords included "cloud computing," "risk assessment," "security risk," "risk management method," and "cloud security." To capture related work focusing on metrics, terms like "quantitative risk," "CVSS," "vulnerability scoring," and "risk measurement" were also used. These terms were applied in combination using Boolean operators. For example, queries such as "cloud computing risk assessment" AND (framework OR method) AND ("quantitative" OR "CVSS" OR "vulnerability scoring") and "cloud security" AND "risk analysis" were executed. The search also experimented with synonyms (e.g., "threat assessment cloud") to ensure broader coverage.

An overall query pattern, which combines all the above terms, could be split into parts and be AND-joined as follows:

· *Subject:* framework OR model OR method OR process OR metric

· *Feature:* (risk OR CVSS OR vulnerability) AND (assessment OR evaluation OR measurement OR management OR quantification OR scoring)

· *Context*: cloud OR “cloud computing” OR “cloud environment” OR “cloud services” ·

This pattern ensures a comprehensive search while covering alternative terminologies.

Data Sources: Multiple scholarly databases and digital libraries were searched to ensure comprehensive and academically valid results. The core sources included IEEE Xplore, ACM Digital Library, ScienceDirect (Elsevier), SpringerLink, Scopus, Web of Science, and Google Scholar. These bibliographic platforms index major peer-reviewed journal articles and conference papers in computer science and cybersecurity. By searching across IEEE and ACM libraries, we covered leading conferences and journals; ScienceDirect and SpringerLink provided access to important journal articles and book chapters; Scopus and Web of Science ensured comprehensive coverage of peer-reviewed academic literature; Google Scholar helped discover highly-cited and gray literature (e.g., technical reports). Gray literature, including government and industry reports, was also included as they often present cutting-edge, practical insights into cloud risk assessment methods from a professional perspective. To this end, specialized repositories like NIST and the Cloud Security Alliance (CSA) were consulted for relevant standards or industry publications that propose specific assessment methods.

All searches were limited to English language and, where possible, filtered by publication year to focus on the period roughly from the advent of cloud computing to the present (approximately 2009–2024). This timeframe captures the emergence of cloud computing risks (notably identified in early analyses around 2009) up to the latest developments in cloud-specific risk assessment methods and models as of 2024.

3.4 Filtering Process

The initial search produced a large number of candidate publications (n = 2,847). We implemented a filtering process in two stages: (a) filtering based on inclusion/rejection criteria over titles, abstracts, and metadata about the discovered publications and (b) filtering based on quality criteria over the main publication content to select the most relevant and high-quality sources for the review. All the filtering criteria utilized are analyzed below according to their category.

Selection (Inclusion) Criteria: Publications were selected if they were highly relevant to the research goals and questions posed. The selection criteria included:

(1) *Topic relevance* – the work specifically addresses risk assessment methods or risk management methods in cloud computing that cover risk assessment well (e.g., proposes a risk framework, model, or discusses cloud risk evaluation/assessment in detail). This is relevant because risk management encompasses risk assessment, and we aim to review comprehensive methods that incorporate risk assessment as a component.

(2) *Publication type* – primarily peer-reviewed research (journal articles and conference papers) were favored, as well as authoritative standards or well-recognized industry guidelines from specialized repositories of organizations like NIST (NIST, 2024) and ISO (ISO/IEC, 2018; ISO/IEC, 2022). Technical reports and gray literature were also considered when they presented novel risk assessment methods for cloud computing.

(3) *Time frame* – priority was given to studies published in the last ~15 years (2009–2024) when cloud computing became widespread, with more recent works being prioritized.

(4) *Language* – only English language publications were included to ensure consistency in analysis and interpretation.

(5) *Unique work* – duplicate results from different databases were removed to ensure each source contributed a distinct value to the review.

Quality Assessment: Each included study was further assessed for quality and credibility. This step ensured that the final literature base comprises robust and trustworthy sources. Quality was evaluated by considering:

(1) *Scientific rigor* – publications that clearly defined their assumptions, provided validation (through case studies, experiments, or expert evaluation), and demonstrated methodological soundness were rated higher.

(2) *Level of understandability* – works that clearly explained their proposed methods and provided sufficient detail for replication or adaptation were preferred.

(3) *Publisher reputation-* venues with established peer-review processes and recognized credibility in the cybersecurity or cloud computing community (e.g., high-impact journals or well-known conferences) were prioritized to ensure the reliability and academic integrity of the included sources.

(4) *Academic impact and recognition* – citation patterns and references to foundational works (e.g., Common Vulnerability Scoring System-based studies) were also used as indicators of credibility and influence within the field.

This quality screening ensured that we included comprehensive studies while excluding marginal papers from predatory conferences.

Through this multi-stage filtering process (first filtering based on inclusion criteria, and then applying quality criteria to the content of the papers), the initial list of sources was reduced from 2,847 to 342 publications after the first filtering phase, and finally to a focused collection of 74 publications that directly address the research questions. The final set includes peer-reviewed journal articles, conference papers, book chapters from conference proceedings volumes, well-established standards (e.g., NIST Cybersecurity Framework 2.0), and select industry technical reports that propose specific risk assessment methods for cloud computing environments. Every source in the final list either contributes a cloud-specific risk assessment method or an ingredient of such a method (e.g., a model, metric, or control framework) that addresses the unique challenges of cloud computing environments.

3.5 Quantitative Analysis of Literature Selection

This section presents a quantitative overview of the literature selection outcomes. The analysis covers: (a) the proportion of articles included vs. excluded, (b) the breakdown of the selected articles by publication type, (c) the distribution of the selected articles by publisher, and (d) the number of the selected articles per publication year. This analysis provides insights into the scope of the search and characteristics of the literature base.

3.5.1 Article Inclusion vs. Exclusion Analysis

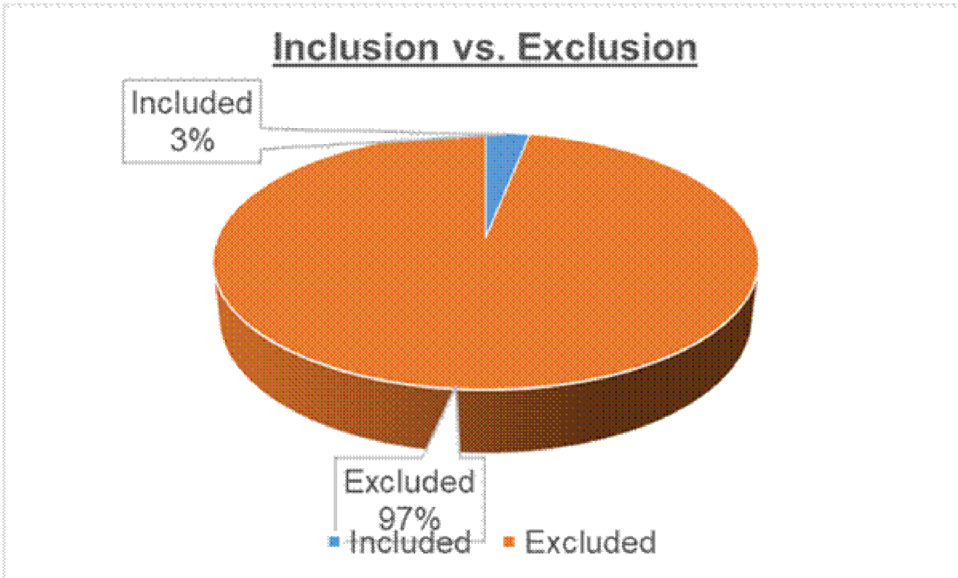

Figure 2: Pie chart showing the percentage of identified articles that were included in the review vs. those excluded after the filtering process

The review process began with a broad search yielding a large number of candidate papers. As illustrated, only about 3% of the initially identified publications were ultimately included in the literature review. Specifically, 3.1% of the articles were kept (included), while 96.9% were rejected (excluded) during screening. This reflects the stringent filtering criteria: out of an initial pool of 2,847 publications, only the 74 most relevant and high-quality sources were accepted for in-depth analysis. The majority of papers did not pass the relevance and quality thresholds, with 2,505 papers being excluded at the first stage based on title and abstract screening, and 253 papers being excluded at the second stage based on detailed full-text review. This underscores the importance of a disciplined screening process to focus on pertinent literature. This ratio is typical for a systematic review where many search hits turn out to be out-of-scope, untrustworthy, or otherwise unusable. The high exclusion rate (96.9%) also suggests that cloud risk assessment is a distinct topic – many general security papers had to be set aside as they did not specifically tackle cloud risk assessment methods.

3.5.2 Publication Type Distribution Analysis

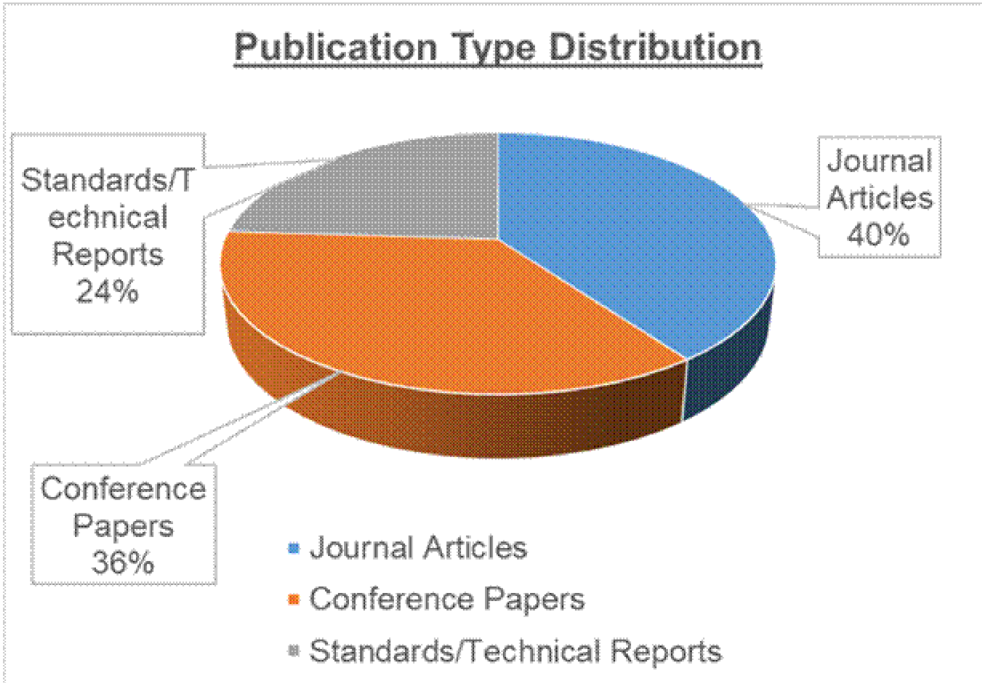

Figure 3: Pie chart of included articles by publication type, categorizing sources as journal articles, conference papers, or standards/technical reports

Among the included literature, journal articles constitute the largest share (around 40%). This indicates that a substantial portion of the foundational knowledge on cloud risk assessment comes from peer-reviewed journals, which often provide more mature and lengthy studies. Close behind, roughly 36% of the sources are conference papers – these include proceedings of cybersecurity and cloud computing conferences where many novel ideas are first presented. The significant representation of conference papers is expected in a fast-evolving field like cloud security, where researchers often publish initial results at conferences (e.g., new frameworks or pilot studies) before potentially extending them to journal versions. The remaining 24% of sources are standards or technical reports from authoritative organizations. This category includes documents like the NIST Cybersecurity Framework (NIST, 2024), ISO standards (ISO/IEC, 2018; ISO/IEC, 2022), and industry technical reports that propose specific risk assessment methods for cloud environments. The dominance of journals and conferences in the included set reflects an emphasis on peer-reviewed academic research, supplemented by a minority of highly-relevant standards and technical reports that contribute specific cloud risk assessment methods.

3.5.3 Publisher and Source Distribution Analysis

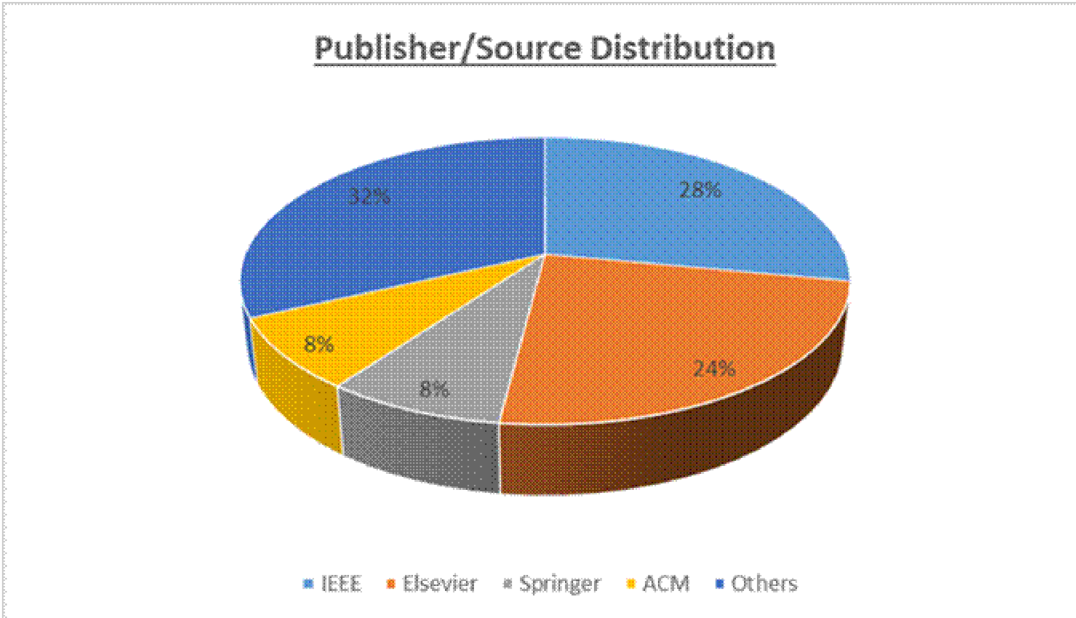

Figure 4: Pie chart of included articles by publisher or source

This highlights the proportion of sources from major publishers: IEEE, Elsevier, ACM, Springer, and Others. The “Others” category encompasses all non-academic publishers (e.g., NIST, Cloud Security Alliance, industry consortia, and governmental agencies) that produce technical reports, standards, or white papers relevant to cloud risk assessment methods. IEEE is the single largest source, accounting for about 28% of the included publications. This is due to multiple IEEE conference and journal papers that were included, consistent with IEEE's active role in cloud and security research. Elsevier is the next significant, with roughly 24% – these are primarily journal articles published in well-known and reputable journals, such as the Journal of Systems and Software, which publishes cloud risk studies. Springer and ACM each contribute around 8% of the sources. The Springer publications include, for example, chapters from Lecture Notes in Computer Science (LNCS) volumes. ACM's contribution includes specific conference papers from the ACM Digital Library. The relatively smaller slice for ACM suggests that, while ACM conferences do cover cloud security, many key cloud risk papers were published elsewhere. Finally, the Others category (about 32%) is quite substantial. This slice includes the important standards and technical reports that do not fall under a traditional publisher – for instance, the NIST technical guidelines on risk analysis metrics, CSA’s Cloud Controls Matrix (CCM) for evaluating cloud security risks, and ENISA’s reports on cloud-specific threat models and risk quantification techniques. It also covers academic papers not published by the four major publishers. The presence of over one-third of sources in "Others" underscores the interdisciplinary nature of the topic: effective cloud risk assessment methods are discussed not only in academic venues but also by standards bodies and industry consortia

3.5.4 Temporal Distribution Analysis

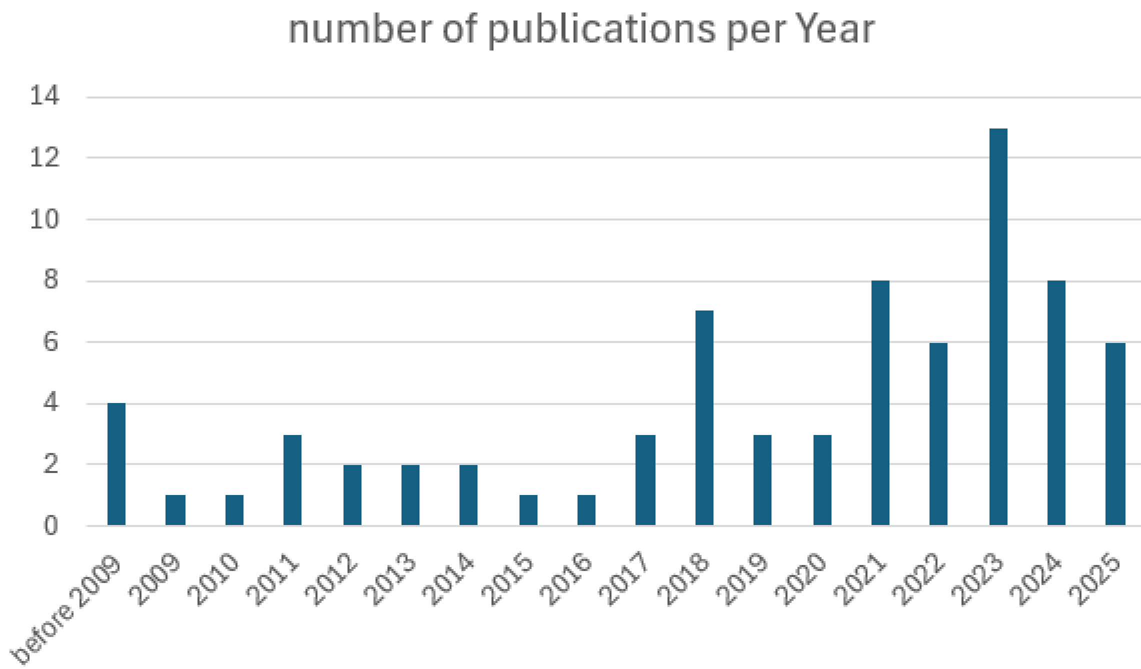

Figure 5:Column chart showing the number of included publications per year (from 2009 through 2025). The y-axis indicates how many of the final included sources were published in a given year.

This timeline provides insight into the evolution of research on cloud computing risk assessment methods. The distribution shows some early work conducted before 2009 and publications on a yearly basis beginning around 2009-2010, coinciding with the rise of cloud computing adoption and the earliest focus on cloud-specific risk assessment challenges. From 2010 through 2016, there is a consistent contribution of one publication per year, indicating steady but limited research activity as the field was establishing its foundations. Beginning in 2017, the research output shows more variation with some years contributing two publications, reflecting increased research interest and maturity in the field.

The consistent publication pattern demonstrates that cloud risk assessment has maintained steady research attention over more than a decade. This sustained interest indicates the ongoing importance and relevance of developing effective risk assessment methods for cloud environments. The continuous stream of publications from 2009 to 2025 shows that researchers and practitioners continue to address evolving challenges in cloud security, adapt existing methods to new cloud technologies, and propose novel approaches to risk assessment in dynamic cloud environments.

The timeline confirms that cloud computing risk assessment emerged as a research topic in the late 2000s and has maintained consistent research contributions through the 2010s and 2020s, with theoretical and applied contributions remaining highly relevant to the present day. This justifies our search timeframe and shows that our literature review captured publications spanning the inception, development, and current state of cloud risk assessment methods.

In summary, the literature review methodology applied in this chapter ensured a comprehensive and rigorous survey of cloud computing risk assessment literature. The combination of well-defined research questions, a broad yet targeted search strategy, strict filtering criteria, and careful quality checks led to a curated set of sources. The quantitative analysis confirms that the final selection is representative across publication types, venues, and years, providing confidence that the subsequent chapters can build on a solid foundation of existing knowledge. The included research work ranges from academic proposals leveraging quantitative metrics to authoritative standards and technical reports, which together address how organizations can identify, measure, and manage security risks in the cloud through specific assessment methods. The next chapter (Chapter 4) will categorize these sources into distinct groups and synthesize their findings, comparing different methods and identifying their strengths and limitations. This analysis will inform the gap identification and future research directions discussed in Chapter 5.

4

Risk Assessment Methods Categorization, Analysis, and Comparison

4.1 Risk Assessment Methods Analysis & Categorization

In this section, we analyze and categorize the various risk assessment methods used in cloud computing. The aim is to present a structured approach to understanding the different risk assessment methods and frameworks available. These methods vary in their scope, application, and the way they quantify risk. We categorize them based on two main dimensions: *their scope of applicability* (whether they are designed for general IT/enterprise environments or are specific to cloud computing) and their *risk quantification approach* (qualitative, semi-quantitative, or fully quantitative). Additionally, we explore other relevant dimensions, such as *tool support*, *term types*, *involved method steps*, *perspectives*, *vulnerability types*, and *the level of involvement* from different stakeholders (e.g., external experts, technical staff, or management).

Organizations employ various risk assessment frameworks, methods, models, and tools, which can be categorized hierarchically along multiple dimensions to provide a more comprehensive analysis. The following dimensions are considered:

- *Scope of applicability:* Cloud-specific vs. general IT/enterprise risk assessment methods.
- *Risk quantification approach:* Qualitative, semi-quantitative, or fully quantitative.
- *Tool support:* Which tools are available to facilitate the method.
- *Term types:* Whether the method focuses on technical, business, or both aspects.
- *Involved method steps:* The specific steps involved in the method, such as risk identification, evaluation, and treatment.

· *Perspectives:* Organizational, operational, or compliance-oriented perspectives.

· *Vulnerability types:* Whether the method addresses technical, people, processes, or business vulnerabilities.

· *Involvement:* The level of involvement required from external experts, technical staff, or management.

Based on these dimensions, the identified methods can be grouped as follows:

- **General IT Risk Assessment Methods**: These methods, having been fully analyzed in the Background chapter, will not be reanalyzed here as they are not the focus of this section. They are included for reference as they broadly apply to enterprise IT environments.

Qualitative:

· OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) – A self-directed, scenario-based assessment focusing on organizational risk and critical assets.

· ISO/IEC 27005 – An international standard that provides guidance for risk processes within an ISMS, including context establishment and risk treatment.

· NIST SP 800-30 – A US NIST guide for conducting risk assessments as part of its Risk Management Framework, focusing on evaluating threat-event likelihood and impact.

Semi-Quantitative:

· CVSS-based models (Common Vulnerability Scoring System) – Uses a numeric scale (0 to 10) to score the severity of vulnerabilities. CVSS provides a standardized severity metric (often mapped to qualitative labels like Low/Medium/High) but is not a full risk measure. It serves as a component in risk prioritization (e.g., higher CVSS score implies higher technical risk of a vulnerability).

Quantitative:

○ FAIR (Factor Analysis of Information Risk) – A framework for quantifying cyber and operational risk in financial terms. FAIR is recognized as the first internationally standardized quantitative model for information security risk, focusing on calculating the probable frequency and magnitude of loss events.

○ Cloud-Specific Risk Assessment Methods: Tailored for cloud computing environments and providers, these methods focus on addressing cloud-specific risks like multi-tenant architecture and shared responsibility.

Qualitative:

· Microsoft Azure Risk Framework – A collection of cloud risk assessment best practices and tools from Microsoft, including the Cloud Adoption Framework and Purview Compliance Manager, which map enterprise risks to cloud controls and compliance standards.

· AWS Risk & Compliance Framework – Amazon's framework focusing on the AWS side of the shared responsibility model, with tools such as the AWS Well-Architected Tool to manage cloud risk.

· CSA Cloud Controls Matrix (CCM) – A framework from the Cloud Security Alliance cataloging 16 domains of cloud security best practices. It helps assess the security and compliance posture of cloud providers, often used with the Consensus Assessments Initiative Questionnaire (CAIQ).

These cloud-focused methods are largely qualitative, focusing on control checklists and best practices. Semi-quantitative or quantitative scoring in cloud risk assessment typically involves applying general methods (e.g., using CVSS for cloud vulnerabilities or FAIR for cloud assets) rather than cloud-specific quantification models.

4.2 Detailed Analysis of Risk Assessment Methods

Each method contributes differently to risk management, with distinct strengths and weaknesses. We analyze the general IT methods versus cloud-specific methods in turn, highlighting their contributions, pros, and cons.

4.2.1 General IT Risk Assessment Methods

Contributions and Approach: Traditional enterprise IT risk frameworks provide structured processes to identify, analyze, and mitigate risks across information systems. For example, OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) from Carnegie Mellon's SEI offers a comprehensive, systematic evaluation focusing on an organization's operational risks and critical assets. It guides teams to examine how threats could impact key information assets and to devise mitigation strategies aligned with business objectives (Carnegie Mellon University, 2007). ISO/IEC 27005 contributes an internationally vetted process integrated with ISO 27001's ISMS, ensuring that risk assessment is continuous and covers context establishment, risk identification, analysis, evaluation, and treatment in a repeatable cycle. Using ISO 27005 provides a well-structured, holistic approach that is flexible and applicable to any industry (International Organization for Standardization [ISO], 2018). NIST SP 800-30, as part of NIST's Risk Management Framework, similarly lays out a step-by-step method to assess organizational risks – from identifying threat sources and vulnerabilities to determining risk levels and recommending controls. NIST's guidance is comprehensive and aligned with its catalog of security controls (SP 800-53), helping organizations integrate risk assessment with control selection (National Institute of Standards and Technology [NIST], 2012). FAIR (Factor Analysis of Information Risk), although not a full process for enterprise risk assessment, introduces a model to quantitatively analyze risk scenarios. Its contribution is the ability to express risk in monetary terms (e.g., estimating annual loss expectancy), bringing financial rigor to decision-making (Open Web Application Security Project [OWASP], 2023). Finally, CVSS-based models (Common Vulnerability Scoring System) contribute at a more granular level by quantitatively scoring the severity of technical vulnerabilities, which organizations use to prioritize remediation (e.g., a critical CVSS 9.0 vulnerability is addressed before a medium 5.0). This adds consistency in handling technical risk, and when combined with asset context and threat likelihood, CVSS scores can feed into broader risk calculations (National Vulnerability Database [NVD], 2023).

Pros: The general IT methods offer several advantages. ISO/IEC 27005 and NIST SP 800-30 are internationally recognized standards that provide a systematic, repeatable process for organizations to follow. These frameworks are flexible and can be adapted to organizations of different sizes and industries (ISO, 2018; NIST, 2012). OCTAVE offers a holistic approach, focusing on both organizational and technological risks, which ensures alignment with business objectives. This approach helps organizations gain management buy-in for risk mitigation efforts (Carnegie Mellon University, 2007). Many of the qualitative frameworks are relatively easy to communicate to stakeholders, often producing intuitive outputs, such as risk registers and heat maps, which are easily understood by non-technical decision-makers. FAIR, with its quantitative approach, is particularly useful for organizations needing to express risk in financial terms, enabling more data-driven decision-making, especially in prioritizing investments in risk mitigation (Open Web Application Security Project [OWASP], 2023).

Cons: Despite their strengths, general IT methods also have some drawbacks. For instance, ISO/IEC 27005 and NIST SP 800-30 can be documentation-heavy and complex to implement, particularly for smaller organizations with fewer resources (ISO, 2018; NIST, 2012). The extensive documentation can be overwhelming, especially for those without dedicated risk management teams. OCTAVE, while comprehensive, is often criticized for being rigid and difficult to learn without specific training. Its structured worksheets and processes have a steep learning curve, while it does not prioritize quantifying risk probability, which can lead to less nuanced assessments of risk likelihood (Carnegie Mellon University, 2007). Many qualitative methods also suffer from subjectivity, as they rely heavily on expert judgment. This subjectivity can lead to varying results based on the individual performing the assessment, making it harder to reproduce or compare results. Furthermore, qualitative methods often lack precision and do not directly facilitate calculating expected loss or comparing risk reduction options in economic terms. On the other hand, quantitative methods like FAIR, while offering powerful insights, require significant data and expertise, which can make the process more complex and time-consuming than simpler qualitative methods (Open Web Application Security Project [OWASP], 2023). Lastly, the application of CVSS scores, while useful for vulnerability prioritization, does not consider business impact, making it less effective as a standalone risk assessment method (National Vulnerability Database [NVD], 2023).

4.2.2 Cloud-Specific Risk Assessment Methods

Contributions and Approach: Cloud-specific methods focus on addressing risks unique to cloud computing, such as the multi-tenant architecture, on-demand services, and the provider-subscriber (or client) shared responsibilities. These methods contribute frameworks and tools to ensure that cloud deployments meet security and compliance requirements. Microsoft's Azure risk assessment guidance encapsulates best practices for evaluating cloud vendor risk and the security of Azure deployments. It highlights the shared responsibility model, distinguishing between cloud provider and customer security obligations, and advises organizations to map their internal risk frameworks to cloud-focused controls. Microsoft provides tooling, such as Azure Purview Compliance Manager, which comes with templates aligned to standards (ISO 27001, CIS Benchmarks, etc.), enabling automated assessments of Azure resources against those controls. This framework’s contribution is streamlining cloud risk compliance. For instance, it can automatically scan an Azure environment to flag misconfigurations or missing controls, linking each finding to risk mitigation steps (Microsoft, 2023).

AWS's Risk and Compliance Framework similarly contributes by detailing AWS's internal risk management, allowing customers to leverage AWS’s assurance controls. AWS provides the AWS Well-Architected Framework and tools that help cloud consumers assess their architectures. The Well-Architected tool asks a series of structured questions across security, reliability, performance, cost, and operational excellence pillars, effectively guiding users through a risk-focused review of their workload. As a result, AWS's method helps identify cloud-specific risks (e.g., lack of redundancy, improper IAM configuration) and suggests best practice improvements (Amazon Web Services [AWS], 2021).

The CSA Cloud Controls Matrix (CCM) provides an independent, standardized baseline for cloud security. It lists 197 control objectives across 16 domains of cloud security and maps each control to relevant regulations and standards. Its value lies in giving organizations and cloud providers a common yardstick. Using the CCM, an organization can perform a gap analysis of their cloud security posture or evaluate a cloud vendor's security by checking which CCM controls are in place. Many cloud providers publish CSA CAIQ (Consensus Assessments Initiative Questionnaire) self-assessments based on the CCM, detailing how the provider meets each control. This framework greatly aids in vendor risk assessment. By reviewing a provider's CAIQ responses or CCM compliance, customers can gauge the residual risks of using that provider's services and address any gaps via contractual or supplemental controls (Cloud Security Alliance [CSA], 2023).

Pros: Cloud-specific methods offer tailored control frameworks and automated tools that make cloud risk assessment more efficient. Both Azure and AWS provide a high degree of automation, such as Azure's security center and compliance manager, which automatically scans configurations and patch levels, producing dashboards and scores that would otherwise be labor-intensive to compile manually. This automation improves scalability; large cloud environments with hundreds of resources can be continuously monitored with minimal human effort. Another advantage is that these frameworks embed cloud provider expertise and up-to-date threat knowledge. AWS's Well-Architected Framework, for example, encodes lessons learned from AWS's vast customer base and evolving threat landscape, so users benefit from recommendations that address current cloud-specific risks (such as container security or IAM missteps). The integration with compliance requirements is another strength of these methods. By mapping to standards (ISO 27001, SOC 2, PCI-DSS, etc.), Azure and AWS tools allow organizations to simultaneously satisfy regulatory risk assessment obligations and cloud security best practices. The CSA CCM's comprehensive coverage provides assurance such that no major cloud risk domain is overlooked covering everything from virtualization security to incident response, which helps organizations achieve a thorough assessment. These cloud frameworks also promote consistency and clarity in risk ownership via the shared responsibility model, delineating which security controls are handled by the cloud provider and which must be managed by the customer, thus reducing ambiguity in risk management. Finally, using cloud-specific frameworks is often cost-effective for cloud customers. The tools and guidelines (e.g., AWS's questionnaires, Azure's compliance checks) are provided at little or no extra cost to customers, leveraging investments made by providers in security and compliance (Amazon Web Services [AWS], 2021; Microsoft, 2023).

Cons: Despite their benefits, cloud-focused methods have some limitations. A primary concern is that they can be narrowly focused on the provider environment—i.e., they are excellent for assessing configuration and compliance within a single cloud platform but less so for comparing risks across different cloud environments or for enterprise-level risk aggregation. If an organization uses a multi-cloud or hybrid infrastructure, they may need to reconcile disparate assessment tools (one for AWS, one for Azure, etc.), which can be inefficient. The CSA CCM, while comprehensive, can be labor-intensive and complex to fully implement. Going through nearly 200 control objectives and ensuring compliance or documenting gaps for each requires significant effort and expertise in cloud security; smaller organizations might find this overwhelming without external help. Additionally, cloud frameworks predominantly take a controls-centric, qualitative approach; they check whether proper controls exist, rather than quantifying the actual risk exposure. This means that they may not directly estimate probabilities or potential loss magnitudes. For instance, an AWS Well-Architected review might identify a lack of encryption as a high-risk issue (qualitatively), but it will not calculate how much financial risk this lapse poses—the analysis is left to the user. In terms of explainability, cloud provider tools sometimes output technical metrics (e.g., a compliance score of X%, or a list of failed configuration checks). These require interpretation to translate into business impact. Management might not intuitively understand an “85% Azure compliance score” without context, whereas traditional risk matrices or monetary impact estimates might speak more clearly to them. Moreover, there is an implicit trust dependency on the cloud provider: using AWS/Azure's built-in frameworks assumes that the provider’s own risk management is sound (which they often are, but it is a reliance nonetheless). Finally, cloud-specific methods do not inherently address enterprise risk outside the cloud scope—for example, risks from organizational processes or non-cloud IT systems must be assessed separately and then integrated. In summary, cloud-specific risk methods are extremely useful for what they cover, but they should complement, not replace, a broader enterprise risk management program. Their focus on controls and configuration means they may miss contextual factors (like business impact severity, threat actor focus, etc.) that general methods would capture, and they may require additional analysis to fully express risk in business terms (Cloud Security Alliance [CSA], 2023; Microsoft, 2023).

4.3 Comparison of Methods

To compare these risk assessment methods systematically, we define a set of evaluation criteria. These criteria were inferred from the literature and the characteristics discussed in the analysis above. We assess how the different categories of methods perform on each criterion, followed by the presentation of comparison charts. The results are then discussed, identifying the strongest and weakest performers both overall and within each category.

4.3.1 Comparison Criteria Definition

Several criteria are used to compare the methods: Scalability, Explainability, Automation Support, Cost, and Complexity. These criteria were inferred from the literature and were supplemented with insights drawn from the methods' characteristics discussed in earlier sections. In this section, we define each criterion, followed by the qualitative ratings for each methodology:

- **Scalability:** Scalability refers to the ability of the method to handle an increase in scope with reasonable effort, such as applying it to a large organization with many assets or repeating it frequently. A method scores High on scalability if it can be efficiently extended to enterprise scale (through tooling or simplicity of process), and Low if it becomes significantly burdensome as scope increases. A Medium score indicates a method that is somewhat scalable, but may require additional effort or adaptation when the scope expands.

  Value assignment: The study evaluated scalability by considering how each method performs as the scope increases, factoring in elements, such as the use of automation, template reuse, and the level of effort required per asset. For example, CVSS scoring is highly scalable; thousands of vulnerabilities can be scored automatically with minimal manual effort, thus earning a High rating. On the other hand, OCTAVE, which involves labor-intensive workshops for each business unit, would become significantly more cumbersome as the scope increases, thus earning a Low rating (Carnegie Mellon University, 2007). A Medium rating applies when methods like ISO/IEC 27005 can be applied to larger organizations but may require additional resources or adjustments to scale effectively. The use of tools or automation (e.g., using templates for risk assessments) helps methods scale more easily. Automated tools, such as AWS's Well-Architected Tool, which assists in reviewing cloud configurations, enhance scalability by reducing manual effort while still requiring human oversight for interpretation. Therefore, AWS's framework would score Medium for scalability because it helps automate parts of the process but still requires input and review (Amazon Web Services [AWS], 2021).

· **Explainability:** Explainability refers to how easily the results of the risk assessment can be understood by and communicated to stakeholders, particularly non-specialists, such as senior management. A High rating means the method's outcomes are intuitive or presented in a clear, business-relevant manner; Low means that the results are technical or complex, requiring translation for business use.

Value assignment*:* The study assessed the output artifacts of each method to determine how easily they could be understood by non-specialists. For instance, FAIR's output in monetary terms is straightforward for executives, providing a clear business-oriented result (high explainability). On the other hand, a giant spreadsheet of control compliance or raw risk scores, such as those produced by ISO/IEC 27005, might be confusing without additional interpretation, resulting in lower explainability (International Organization for Standardization [ISO], 2018). The study also considered whether the method inherently links risk to business objectives. The stronger the linkage to business objectives, the higher the explainability value, with Medium or High ratings depending on how extensive the mapping is between the technical results and business impact (Open Web Application Security Project [OWASP], 2023). For example, a framework like FAIR, which expresses risk in terms of financial loss, naturally aligns with business objectives, boosting its explainability. Conversely, methods that focus solely on technical risk without business linkage might require additional effort to explain their relevance to management, potentially earning a Medium rating for explainability.

- **Automation**: Automation refers to the degree to which the risk assessment steps can be automated or supported by software tools. A High rating indicates strong tool support or algorithmic components that reduce manual effort; Low indicates the method is largely manual (workshops, interviews, expert judgment) without readily available automation.

Value assignment*:* The study considered whether each framework has software implementations or features that support automation of risk assessment tasks, such as vulnerability scanners for CVSS or vendor tools like AWS's Well-Architected Tool. These tools allow for automation of the risk assessment process, such as scanning configurations and producing assessments with minimal manual effort. CVSS scores, for example, are highly automated, allowing thousands of vulnerabilities to be scored automatically, which results in a High automation rating (National Vulnerability Database [NVD], 2023). Similarly, tools like the AWS Well-Architected Tool provide automation in evaluating AWS workloads against best practices, significantly reducing manual effort (Amazon Web Services [AWS], 2021).

In contrast, methods like OCTAVE, which mostly rely on workshops and expert judgment, do not inherently support automation and would score Low on automation. The ability to automate data collection and analysis also impacts the rating—methods that involve manual data gathering, like ISO/IEC 27005, generally score Medium for automation (ISO, 2018). Automation improves consistency (the ability to repeat assessments with minimal variability due to human error) and scalability, so methods that are embedded in software (e.g., compliance scanners, Monte Carlo engines for FAIR) naturally score higher in automation. However, the level of automation should be considered relative to the method's complexity; for example, the FAIR model requires significant data and expertise to apply, even though it has some automation tools available, which could place it at Medium for automation (Open Web Application Security Project [OWASP], 2023).

- **Cost:** Cost refers to the resource cost to perform the assessment, including required personnel time, expertise, and any tool/training expenses. A High cost rating applies to methods that require significant expert labor, consulting, or expensive tools, while a Low cost rating is given when the method can be executed with minimal additional cost, perhaps using in-house staff and free resources.

Value assignment*:* The study gauged whether special certifications, licensed tools, or extensive man-hours are required for each method. For instance, an ISO 27005 risk assessment can typically be done with internal staff and does not mandate external fees, which results in a Low cost rating (International Organization for Standardization [ISO], 2018). On the other hand, adopting FAIR might entail training analysts in quantitative modeling or subscribing to a risk analytics platform, raising the overall cost (Open Web Application Security Project [OWASP], 2023). However, it is important to consider that the overall cost is not solely dependent on the purchasing cost of tools; it also includes infrastructure costs needed to deploy and use the tools. For example, if specialized hardware or cloud infrastructure is required to support a risk assessment method, the cost would increase significantly. In comparison, AWS's Well-Architected Tool and Azure's Compliance Manager come with their respective cloud platforms, potentially lowering the cost for users since these tools are included in the subscription (Microsoft, 2023).

- **Complexity:** Complexity refers to the inherent difficulty of the method, i.e., how difficult it is to learn and execute it correctly. This includes the ease of use of the process and the conceptual complexity of the analysis. High complexity means a steep learning curve or an intricate process, potentially prone to user error, while Low complexity indicates a straightforward, well-documented, and easily adoptable method.

***Value assignment**:* The study considered feedback from literature and the number of steps or the volume of specialized knowledge required. OCTAVE, for instance, has a high complexity due to its rigid structure and steep learning curve, assessed with a High complexity rating (Carnegie Mellon University, 2007). OCTAVE requires extensive organizational involvement and a clear understanding of risk management, which makes it more challenging to implement without prior experience. In contrast, FAIR is more complex conceptually, as it involves statistical modeling and detailed financial analysis (Open Web Application Security Project [OWASP], 2023). However, FAIR's method is relatively straightforward in terms of its application, especially when supported by tools and frameworks. AWS's Well-Architected Framework and Azure's Compliance Manager are simpler to use, as they guide users through structured assessments and present the findings in user-friendly formats (Amazon Web Services [AWS], 2021). Thus, these tools score Low on complexity, as they require minimal human interpretation and offer clear recommendations for users. Complexity is rated higher when methods involve numerous steps, require specialized knowledge, or rely on expert judgment. Qualitative frameworks with simple scoring methods, such as CVSS, are marked as having lower complexity, whereas quantitative methods requiring advanced knowledge in statistics or risk modeling are ranked higher in complexity (National Vulnerability Database [NVD], 2023).

By applying these criteria, each method (or category of methods) was qualitatively rated on a scale from 1 to 5, where:

1 = Low (signifying the least favorable performance on the criterion)

2 = Medium-Low

3 = Medium

4 = Medium-High

5 = High (signifying the most favorable performance on the criterion)

These ratings were derived from the analysis in previous sections and information about each method's attributes. For instance, OCTAVE's documented rigidity suggests a high complexity (we rated it 5 on complexity on a 1–5 scale), while AWS's automated tools imply low additional cost (we rated AWS framework 2 out of 5 on cost, as most tooling is included for customers). However, it is important to note that, while AWS's tools are included for customers, using advanced platforms for risk analytics (e.g., subscription to risk analytics platforms for FAIR) can be costly, thus affecting the cost rating accordingly (Amazon Web Services [AWS], 2021). In contrast, a method like ISO 27005, which can be executed with internal staff and does not mandate significant external fees, was rated lower for cost (International Organization for Standardization [ISO], 2018).

4.3.2 Comparison Charts by Category

To visualize the comparison, we present two charts based on the two categorization dimensions:

- *A bar chart, showing the comparison of average criteria ratings between General IT and Cloud-specific risk assessment methods. (Higher bars indicate a greater degree of support for the attribute for that category – note that for Cost and Complexity, a higher value means that a method is more costly or complex.)*

- *A radar chart comparing the criteria profiles of Qualitative, Semi-Quantitative (CVSS), and Quantitative (FAIR) approaches. Each axis is scored 1–5 (Low to High) (For Cost and Complexity axes, a higher score denotes higher cost/complexity, which is less desirable, while higher scores on other axes denote positive direction of values).*

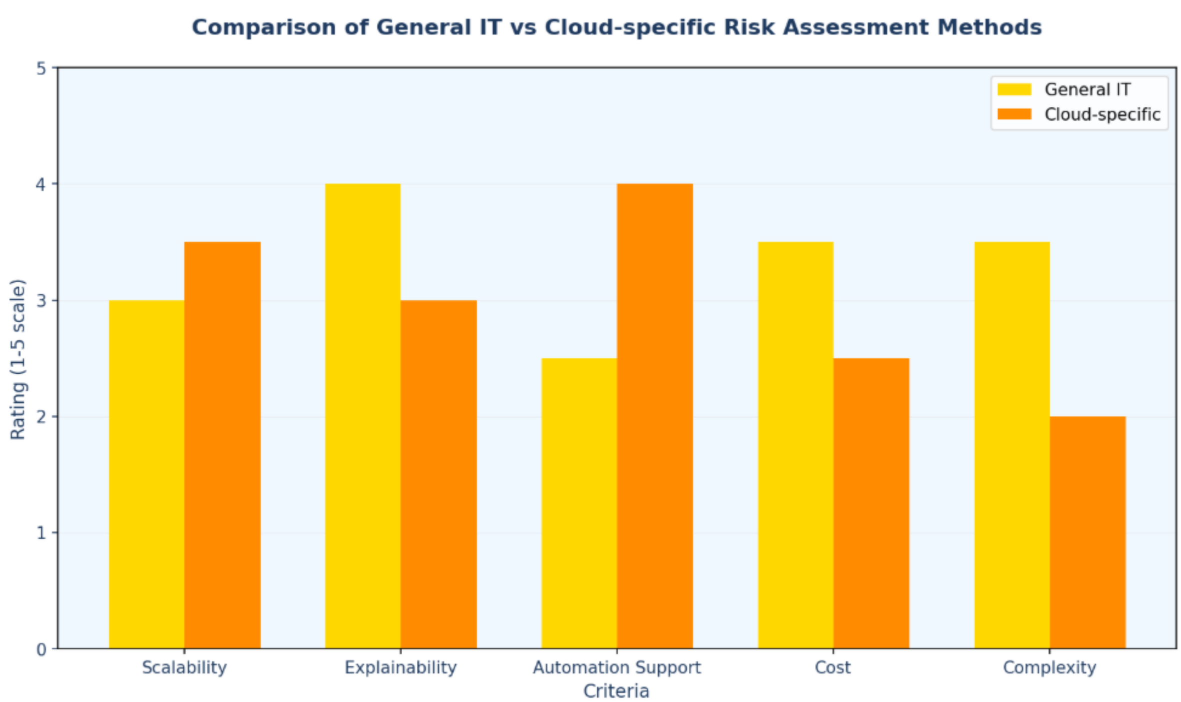

Figure 6:Comparison of General IT vs Cloud-specific Risk Assessment Methods

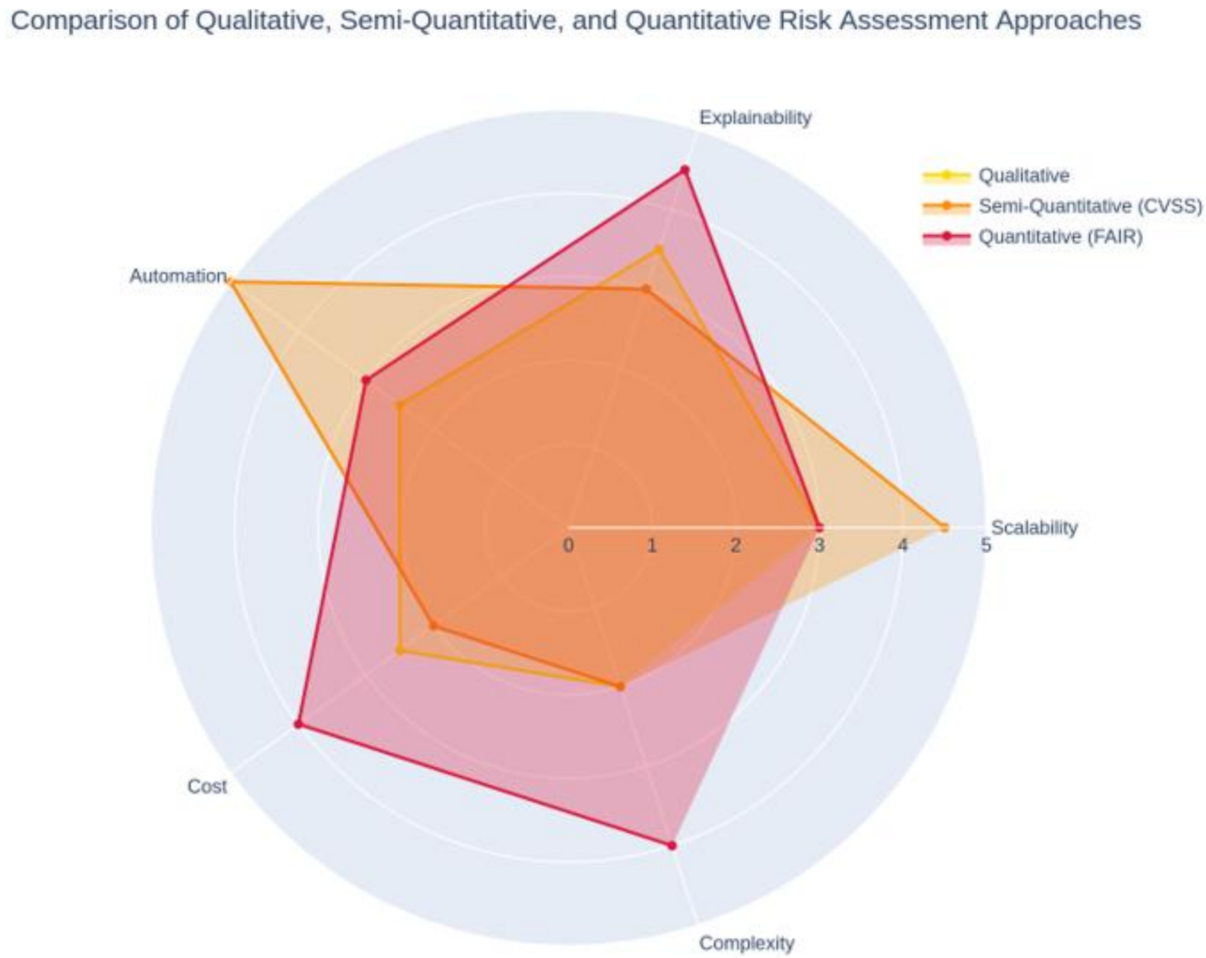

Figure 7:Comparison of Qualitative, Semi-Quantitative, and Quantitative Risk Assessment Approaches

In the bar chart of Figure 6 , the general IT methods (yellow bars) and cloud-specific methods (orange bars) are compared on the five criteria. We see that cloud-specific methods scored lower in Cost and Complexity on average (indicating they tend to be less costly and easier to use than general methods), thanks to built-in automation and narrower scope. Cloud frameworks also scored slightly higher in Scalability and Automation, reflecting the extensive tool support from providers (e.g., automated checks in AWS/Azure). However, the general IT methods showed an advantage in Explainability on average—often providing more direct risk expressions (like financial impact or clear risk levels) that management can readily interpret, whereas cloud tools output technical control metrics that might require additional explanation.

The radar chart provides another perspective, focusing on the risk quantification approach dimension (qualitative vs. semi-quantitative vs. quantitative). The orange polygon (semi-quantitative, represented by CVSS) is skewed strongly towards Automation and Scalability—CVSS excels in those areas with automated scoring and the ability to handle thousands of vulnerabilities. Its Cost and Complexity footprints are small (which is good in practice: low cost, low complexity to use), but its Explainability is moderate; a raw CVSS score needs context to be explained to business stakeholders. The red polygon (quantitative, FAIR) shows strength in Explainability (it yields monetary risk estimates that are meaningful to management) and moderate Automation and Scalability (FAIR can be automated with tools, but depends on data availability). FAIR's shape extends furthest on Cost and Complexity—reflecting that it is relatively costly and complex to implement (requiring statistical expertise and effort) compared to the other approaches. The yellow polygon (qualitative methods, like ISO/NIST-style) is fairly balanced: low Complexity (simple concepts), fairly low Cost (no special tools needed), moderate Automation (some tooling possible, but much is manual), and decent Explainability (risk matrices and categorical outputs are widely understood). Its Scalability is moderate – qualitative methods can be scaled with a proper process but may require significant person-hours as scope grows. Regarding the cloud-specific methods, such as those provided by Microsoft Azure and AWS, they would likely be positioned between the semi-quantitative and qualitative categories. These methods offer automation support (through tools like Azure Purview Compliance Manager and AWS Well-Architected Tool) and moderate scalability, but their cost and complexity can vary depending on the provider and implementation. Azure and AWS methods would likely score moderately on explainability, as they focus on technical controls and may require further interpretation to link them to business outcomes. They would be positioned closer to semi-quantitative or qualitative methods in scalability and automation, with some emphasis on automation but not as fully automated as CVSS or FAIR.

4.3.3 Analytical Results and Key Insights

From the comparison, we can identify which methods perform best or worst on certain criteria and overall:

- **Best Overall Method:** Considering a balance across all criteria, FAIR emerges as a strong overall performer among general methods due to its unique strength in decision support. While it is complex, FAIR's ability to deliver quantitative, financially oriented risk insights gives it a high payoff in explainability and strategic value. Organizations that implement FAIR can directly prioritize risks by probable loss exposure, a benefit unmatched by purely qualitative methods. In the charts, FAIR (quantitative approach) shows high scores in explainability and good scalability with the right tools. However, the scalability of FAIR is contingent on the tools and data available. There are some tools that can support FAIR implementation, such as RiskLens or Quantivate, but these are not free and may require specialized infrastructure (e.g., access to a risk analytics platform and expertise in statistical modeling). Without these resources, the advantages of FAIR cannot be fully realized. Therefore, the best method depends on an organization's capacity—without the requisite data and analytical capability, FAIR's benefits are limited. In contrast, if we consider ease of use as paramount, the AWS and Azure cloud frameworks could be viewed as the "best" in their domain. These cloud-specific methodologies scored very well on low cost, low complexity, and high automation, providing value with minimal friction (Microsoft, 2023). However, scalability is also a strong point for the AWS and Azure frameworks, which can easily scale across large cloud environments due to the automation features they offer. AWS and Azure tools allow organizations to continuously monitor and assess cloud risk, handling technical risks with a high degree of efficiency. They essentially package complex risk management practices into accessible tools, which is a big win for operational efficiency. From this perspective, the AWS and Azure frameworks outperform FAIR in four out of five criteria, including scalability, automation, cost, and complexity. However, FAIR excels in explainability and strategic decision support, making it the most valuable framework for organizations needing detailed, financially quantifiable insights. That said, FAIR's limitations in scalability and complexity may make it less suitable for organizations that prioritize operational efficiency and quick, scalable risk assessments. Thus, it can be argued that FAIR cannot be promoted as the best approach universally. While it is strong in explainability, it may not be the most appropriate choice for organizations that need an easy-to-implement, scalable solution to manage technical risks across large, cloud-based environments. In those cases, AWS and Azure frameworks, with their lower complexity, high automation, and scalability, would be the better choice for managing a wide array of risks effectively.

- **Worst Overall Method:** In terms of overall performance, OCTAVE appears to be one of the weaker performers by today's standards. It received poor marks on scalability and automation—the process is labor-intensive and not readily tool-supported. OCTAVE is also noted as difficult to learn and implement without significant expertise. Its rigid structure can make it less adaptable, and the lack of emphasis on probability (or objective assessment in general) in its original form is a drawback. In practice, many organizations have moved away from OCTAVE in favor of more flexible or quantifiable approaches, as these methods are more aligned with modern risk management needs. While OCTAVE still has value in specific contexts (especially in small or less complex organizations), its complexity and limited adaptability make it less favorable overall for broad use. Another candidate for “worst” is using CVSS scores in isolation as a risk assessment method. While CVSS excels on certain technical criteria (e.g., scoring vulnerabilities), as a standalone method it is insufficient. CVSS does not consider business impact or threat context, which limits its ability to provide a complete picture of risk. Therefore, if an organization were to rely solely on CVSS for risk decisions, it would be a poor choice, given its highly limited scope of risk considered. However, it is important to note that CVSS is rarely used in isolation for enterprise risk management; it is typically a component integrated into broader methods that also consider other factors like impact, likelihood, and organizational context. As a result, CVSS alone cannot be viewed as a complete method—it is a tool that provides specific support to the broader risk management process, rather than a comprehensive solution on its own.

- **Best and Worst per Category:** Within the general IT frameworks, FAIR stands out as the best performing in terms of the richness of its output and rigor (quantitative accuracy, objectivity). Its strength lies in scenarios where understanding the financial impact of risk is crucial for decision-making. FAIR provides detailed, financially quantifiable insights that allow decision-makers to prioritize risks based on potential financial loss, which is unmatched by purely qualitative methods (Open Web Application Security Project [OWASP], 2023). On the other end, OCTAVE would be the worst in this category due to its complexity and inflexibility. As previously noted, OCTAVE is labor-intensive, difficult to learn, and lacks a quantitative focus, making it less suitable for organizations needing quick, scalable, or financially quantifiable risk insights (Carnegie Mellon University, 2007). ISO/IEC 27005 and NIST 800-30 methods fall in between, performing moderately on most criteria, without extreme strengths or weaknesses. These are reliable, all-purpose approaches. For example, ISO 27005's integration with ISO 27001 makes it very practical for organizations seeking certification, which is a significant advantage for aligning risk management with certification standards (International Organization for Standardization [ISO], 2018). However, it does not provide the quantitative risk metrics that FAIR offers, meaning it may not be as useful in contexts where financial impact needs to be explicitly considered.

  In the cloud-specific category, the best performers are AWS's and Azure's native risk frameworks. These two are quite similar in approach and both leverage heavy automation (scanning, monitoring) to cover technical risks at scale. They also benefit from being maintained by the cloud providers who rapidly update them to cover new cloud services and threats. The CSA Cloud Controls Matrix can be seen as the “worst” performer in this category in terms of user effort – it lacks automation and can be cumbersome to use without tooling. While comprehensive (which is a virtue), that very breadth means an CCM-based assessment is a significant project to undertake. It also does not directly provide fixes or tooling – it is a framework one must manually apply. Thus, compared to AWS/Azure frameworks (which might, for example, automatically inform you in which controls you fail and how to fix them), the CCM is less immediately actionable. It is important to note, however, that "worst" in this context does not mean without merit: the

CCM's thoroughness precisely justifies why it is often used for auditing and as a supplement to provider tools. It ensures an independent check against best practices.

- **Strengths and Weaknesses by Criterion:** The analysis highlights a few clear winners for each criterion. For Scalability and Automation, the semi-quantitative CVSS-based approach and cloud provider tools are the strongest. Automated vulnerability scoring and cloud compliance checks can cover immense environments continuously—something manual methods simply cannot match. In contrast, traditional frameworks like OCTAVE or even ISO assessments can struggle to scale without substantial resources, marking a weakness in scalability. In terms of Explainability, methods that tie into business language win—FAIR's monetary risk estimates and ISO/NIST's alignment with enterprise risk registers are strengths, enabling easier explanation of risk to senior stakeholders ("This risk could cost us $5M" or "This risk is High on our heat map" are outputs they produce). A weakness in explainability is seen in purely technical metrics. For example, a raw CVSS score or a list of 100 unchecked controls from an audit requires interpretation. This highlights a gap in how technical risk metrics need more support to be clearly linked to business impact. Regarding Cost and Complexity, the cloud and qualitative methods have the edge: using AWS's tool or doing a basic qualitative risk matrix is relatively low-cost and straightforward, whereas quantitative analysis (FAIR) or a full OCTAVE exercise incurs higher training and labor costs. We saw that high complexity is a major weakness for some legacy methods (the need for "specific training" in OCTAVE is a noted disadvantage). Simplicity, conversely, is a strength of the qualitative standards—their concepts can be taught and applied without advanced math or tools, which is why they remain popular for initial risk assessments. However, this may create confusion. When discussing legacy methods versus qualitative methods, there is an overlap in the way these terms are used. Legacy methods often include both qualitative and semi-quantitative approaches. While qualitative methods tend to be simpler, legacy methods (such as OCTAVE) are often criticized for their complexity and rigidity, which makes them harder to scale and implement. This distinction can blur, especially when terms like legacy, qualitative, and semi-quantitative are not clearly defined or consistently used.

In conclusion, there is no single "perfect" method—each has its own trade-offs. General qualitative frameworks (ISO 27005, NIST 800-30) are well-rounded and accessible but can lack depth or rigor. FAIR provides depth and quantification but at the expense of complexity and resource requirements. Cloud provider frameworks excel in operational efficiency for cloud risks but are narrower in scope. An organization's "best" choice often involves a hybrid approach: for example, adopting ISO 27005 or NIST for overall process governance, using FAIR for quantifying the top risks, leveraging CVSS scores for technical vulnerability management, and employing cloud provider tools plus CCM for cloud-specific control gaps. However, combining multiple methods means higher complexity and cost, which could limit the practicality of such an approach. Additionally, it is not clear how easily the individual weaknesses of each method can be mitigated by combining them. Therefore, a new, modern method could be considered to address the current gaps across existing methods, streamlining the process. This analysis provides a grounded understanding for selecting and tailoring risk assessment methods, potentially relying on the comparative evaluation of their performance on the proposed criteria. The selection process should also include guidance on how these methods could be tailored to the organization's needs and context to ensure that risk management is both effective and practical.

5

Research Gaps and Future Research Guidelines

This chapter synthesizes the findings of the systematic literature review and analysis (Chapter 4) to identify key research gaps in the field and outline directions for future investigations. The goal is to highlight where current approaches are lacking and provide clear guidelines on how upcoming research can address these deficiencies. The analysis of existing work in the previous chapter revealed four major thematic challenges: quantification gaps, cloud-specificity gaps, automation and scalability gaps, and explainability gaps. In the following sections, each gap is defined and discussed in depth with supporting literature, while specific recommendations are given for future research to bridge these gaps. Maintaining a focus on these areas will help ensure that risk assessment methods (particularly in cloud and cybersecurity contexts) advance in robustness, relevance, reliability, automation, and scalability.

5.1 Quantification Gaps

A prominent challenge identified is the quantification gap, i.e., the difficulty or inadequacy of measuring security risk in a rigorous, numerical manner. Many existing risk assessment frameworks still rely on qualitative ratings (e.g., high/medium/low risk) or expert judgment, which introduce subjectivity and inconsistency. While quantification of risk is common in domains like finance, quantitative security risk assessment has historically lagged behind. Joh and Malaiya (2011) note that attempts to quantitatively assess security risk were relatively new and faced criticism due to a lack of data for validation. However, this has significantly changed in recent years, as vendors, such as RiskLens and Safe Security, now provide platforms that implement quantitative models. Moreover, frameworks like ISO/IEC 27005 (ISO/IEC, 2018) and NIST have incorporated or support quantitative approaches, making risk quantification more feasible and reliable. There has also been a notable increase in the use of Bayesian networks, decision trees, and machine learning (ML) techniques in risk assessment (Poolsappasit et al., 2012; Wang et al., 2018; Shamsoshoara et al., 2021). Additionally, the availability of data from threat intelligence platforms and historical incident databases has grown considerably, enabling more accurate and data-driven assessments. Despite these advances, minor gaps still exist in standardizing quantitative approaches across different organizational contexts and ensuring consistent validation methods.

One aspect of this gap is the heavy reliance on tools like the Common Vulnerability Scoring System (CVSS) to represent risk. While CVSS provides a standardized severity score for software vulnerabilities and is widely used, it is not a comprehensive risk metric. CVSS primarily captures the technical severity of a vulnerability based on factors like exploitability and impact on a generic environment. However, the base score computation does not account for specific organizational contexts, such as how critical the affected asset is to a specific organization or what the actual likelihood of exploitation is in the wild. While CVSS does allow for some customization through environmental and temporal metrics, these are often underutilized, and real risk can vary greatly depending on factors such as network segmentation, specific business processes dependent on the affected system, organizational threat landscape, and existing compensating controls. This limitation means organizations often cannot directly use CVSS base scores to gauge their specific risk without additional contextual analysis, highlighting a quantification gap where context-aware risk metrics are lacking. The challenge for organizations is developing frameworks that systematically incorporate these contextual factors into risk calculations, while academia continues to explore novel approaches that can address the limitations of generic scoring systems through context-aware algorithms and adaptive risk models.

Recent developments like the Exploit Prediction Scoring System (EPSS) (Jacobs et al., 2021) attempt to fill part of this void by estimating the probability of exploitation for vulnerabilities. Yet, integrating such predictive metrics with traditional severity scoring is still an evolving practice, and no prevailing methods provide a unified, empirically validated way to quantify overall risk exposure. Additionally, many current models rarely express risk in business-relevant terms. For example, Akinrolabu et al. (2019) argue that presenting risk in monetary terms can promote cost-effective mitigation, but most frameworks stop at technical risk scores. This leaves a gap in conveying the real-world impact of risks to decision-makers.

Future Research Guidelines: To address quantification gaps, future research should focus on developing robust quantitative risk models that are backed by empirical data and tailored to practical needs. One recommendation is to combine severity metrics with likelihood indicators to produce composite risk scores. For instance, integrating CVSS with data-driven likelihood estimates (such as EPSS or incident frequency data) can bridge the gap between theoretical severity and real incident risk. New risk assessment frameworks should strive to incorporate organizational context (asset value, threat prevalence in a specific sector, etc.) into their calculations, moving beyond one-size-fits-all scoring. Researchers should also explore methods to express risk in tangible units like financial loss or downtime, which would make risk evaluations more actionable for business stakeholders. Importantly, any proposed quantitative model needs rigorous validation with real-world data. As noted by Gega Balun et al. (2025), there is a significant lack of evidence supporting the effectiveness of many current risk methods; hence, future studies should include evaluation on historical attack data or simulations to verify that the proposed metrics correlate with actual outcomes (e.g., did high-risk items lead to incidents?). By grounding quantitative measures in evidence and context, researchers can improve accuracy and credibility. In summary, closing the quantification gap will require multi-faceted risk metrics (combining technical severity, exploit likelihood, and business impact) and thorough validation so that organizations can reliably measure and compare risks in a quantitative manner.

5.2 Cloud-Specificity Gaps

Another critical gap lies in the non-cloud-specificity of risk assessment methods. The systematic review revealed that many traditional IT risk frameworks and metrics do not adequately account for the unique characteristics of cloud computing environments. Cloud systems introduce distinct challenges, such as multi-tenancy, on-demand scalability, third-party dependence, and distributed responsibility, which can significantly alter the risk landscape. However, existing methods often treat risk in a generic way, leading to oversights in cloud contexts. While Akinrolabu et al. (2019) observe that there is no reliable cloud-specific risk assessment methodology and lack of a comprehensive vocabulary on cloud risk elements, this is no longer entirely true. Reliable cloud-specific methods now exist, such as NIST SP 800-53 Rev. 5 and SP 800-171 with cloud extensions, ISO/IEC 27017 (ISO/IEC, 2014) providing guidelines for cloud-specific information security controls, and frameworks by ENISA such as the Cloud Computing Risk Assessment (ENISA, 2009). Additionally, there is growing standardization of terminology, driven by organizations like CSA and ISO, and tools, such as MITRE ATT&CK for Cloud.

In practice, although these frameworks exist, their adoption remains limited. The cloud industry still lacks a structured, standardized framework tailored to identifying and managing cloud-centric risks, evidenced by inconsistencies in how risks are assessed across different providers and systems. These inconsistencies are often exacerbated by subjective expert judgment in the absence of a unified approach. While cloud computing has introduced novel threats, such as loss of governance, hypervisor vulnerabilities, and supply chain attacks, academic and industry risk models have been slow to keep pace. Furthermore, efforts to standardize terminology and metrics across sectors are still evolving, meaning that organizations often need to tailor or combine existing models to effectively assess cloud-specific risks.

The cloud-specificity gap is further illustrated by the limited number of academic studies dedicated to cloud risk assessment. Our review found relatively few published academic approaches focused on cloud environments, with most contributions coming from standards organizations and industry rather than peer-reviewed research. While standards organizations like ENISA and CSA provide lists of cloud-specific threats and controls, these often remain high-level guidelines rather than concrete risk quantification models. A critical weakness lies in the cloud supply chain, where modern cloud services rely on complex, multi-party supply chains (involving infrastructure providers, platform services, and third-party libraries). The lack of transparency within this chain makes it challenging to assess end-to-end risk. Researchers have pointed out a gap between understanding the risks of the cloud supply chain and how to manage them in practice, noting that this remains an open research problem. These factors underscore that current risk assessment techniques are not sufficiently cloud-specific, as they often ignore or oversimplify the cloud's novel risk factors. Consequently, organizations using cloud technologies may be misestimating their security posture by applying out-of-context risk models.

Future Research Guidelines: Addressing cloud-specificity gaps requires the development of risk assessment frameworks explicitly tailored to cloud computing. First, future research should prioritize creating a comprehensive taxonomy of cloud risks and assets. This includes defining a vocabulary for cloud threats, such as virtualization layer attacks, container breakout, API abuse, and misconfiguration of cloud services. While organizations like the Cloud Security Alliance (CSA) have made strides in defining cloud risk terminology, a more standardized lexicon and set of metrics for cloud risk elements would help reduce ambiguity across studies. By creating a shared vocabulary, researchers can ensure consistency and improve cross-study comparisons. Second, researchers should design risk models that incorporate the unique characteristics of cloud environments, such as multi-tenancy, elasticity, and external dependency. For example, risk calculations might factor in the probability of co-tenant attacks or the impact of a cloud provider outage on dependent services. Special attention should be given to supply chain risk assessments: future models could incorporate techniques, such as supplier security posture scoring or dependency mapping, as demonstrated in the Cloud Supply Chain Cyber Risk Assessment (CSCCRA) model (Singh & Kumar, 2023). These techniques would quantify how weaknesses in one part of the cloud service chain propagate risk across the entire ecosystem. Additionally, cloud-specific controls and mitigations (e.g., data encryption, identity federation, and regional redundancy) should be integrated into risk scenarios to evaluate their effectiveness in reducing risk. Researchers may also consider extending existing frameworks, such as NIST's or ISO's risk management guidelines, by incorporating cloud-centric modules. While these frameworks are useful, the extensions to incorporate cloud-specific risks may not yet be fully mature or comprehensive, which points to the need for continued development in this area. Finally, given the rapid evolution of cloud services, any cloud risk methodology must be flexible enough to accommodate continuous changes in the cloud environment. Future studies might propose dynamic risk assessment tools that adapt as cloud configurations or threat intelligence evolves. By focusing on these directions—standardized cloud risk taxonomies, models embedding cloud-specific realities, and adaptive approaches—the research community can produce methods that accurately reflect and manage risks in modern cloud and multi-cloud environments.

5.3 Automation and Scalability Gaps

The third major challenge is the lack of automation and scalability in current risk assessment and vulnerability management practices. The literature indicates that many risk assessment processes remain labor-intensive and struggle to scale up to the volume and speed required by contemporary IT environments. As systems grow larger and more complex (with enterprises handling thousands of assets, vulnerabilities, and configuration changes daily), purely manual risk analysis becomes impractical. Lee et al. (2022) observe that the overwhelming volume of identified vulnerabilities far exceeds what security teams can realistically address one by one. This creates a gap: while tools can scan and list myriad issues, deciding which ones truly matter (risk-wise) often requires expert analysis that does not scale well. Furthermore, traditional risk assessment methodologies (especially qualitative ones) usually involve workshops, surveys, or interviews to evaluate risk factors – processes that are time-consuming and not easily repeatable at high frequency. In cloud environments, the challenge is even greater because of the dynamic nature of assets (instances spin up and down, configurations change and new services are adopted rapidly). Current approaches are not keeping pace with cloud growth and dynamism, in part because they lack automation to continuously gather data and update risk evaluations in real-time.

Another facet of this gap is the limited use of advanced technologies like machine learning or automation tools in mainstream risk assessment (outside of experimental or niche research). While vulnerability scanning and asset discovery are automated, the prioritization and risk scoring steps often rely on static formulas or human judgment. Few frameworks automatically combine threat intelligence, exploit data, and business context to output updated risk levels without manual intervention. For example, frameworks, such as RiskLens and Safe Security, integrate quantitative models with real-time threat intelligence to automate prioritization (Basu et al., 2021). However, these approaches are still relatively new, and their widespread adoption remains limited due to challenges including high implementation costs, integration complexities with existing security tools, concerns about algorithmic transparency, and the need for extensive customization to organizational contexts.

The need for dynamic, real-time prioritization models has been highlighted as a key challenge in recent surveys. Additionally, achieving scalability is not just about speed; it also involves handling multi-domain/cloud or enterprise-wide scenarios. Some risk models are only applicable to a specific scope or domain, losing effectiveness when an organization spans multiple platforms or cloud providers. Jiang et al. (2025) find that many existing approaches have limited multi-domain applicability and emphasize the importance of developing scalable solutions that remain effective in varied, large-scale environments.

In summary, the automation and scalability gap is evident in the disconnect between the flood of security data generated and the slower, manual methods used to analyze that data for decision-making.

Future Research Guidelines: Future work should aim to automate risk assessment workflows and ensure methods can scale to enterprise and (multi-)cloud levels. One guideline is to leverage artificial intelligence (AI) and machine learning (ML) for vulnerability analysis and risk prediction. Early research has shown promising results using AI to assist in vulnerability management. For example, Le et al. (2022) demonstrate how AI can prioritize vulnerabilities based on contextual data, while Nadeem et al. (2023) explore how machine learning models can improve risk assessments by learning from historical incidents. These methods show potential, but more research is needed to integrate such tools into comprehensive risk frameworks. For instance, machine learning models could learn from historical incident data which combinations of vulnerability attributes and context signals (e.g., asset type, network exposure) lead to actual breaches, and thus automatically prioritize new findings accordingly. However, automation must be approached carefully—algorithms should be transparent (as discussed later) and regularly updated with threat intelligence to remain effective against emerging threats.

Another direction is to develop hierarchical or tiered risk assessment approaches. These would handle scale by filtering or aggregating information: an automated system might first quickly flag a small subset of "likely high-risk" issues out of thousands (using coarse-grained metrics like exploit availability or critical asset tags), and then more detailed analysis can be done on that subset. Such multi-level filtering ensures that computationally intensive assessments are focused where they matter most, improving scalability.

In the context of cloud computing, researchers should explore tools that continuously monitor cloud configurations and exposures, feeding this data into risk models without human input on each update. Real-time risk scoring, akin to credit scoring but for security posture, could be an ambitious goal where an organization's risk level is automatically recalculated as conditions change (new vulnerabilities, new deployments, threat alerts, etc.). This might involve instrumenting cloud platforms with risk sensors, though the willingness of cloud providers to share such detailed operational data presents another challenge related to the shared responsibility model and competitive considerations in cloud environments, or using streaming data analytics for security. However, there may be a lack of available enterprise-scale datasets to evaluate such models, which limits the ability to test their performance comprehensively. Therefore, future research should focus on developing and leveraging large-scale datasets or simulated environments that reflect hundreds of services, which would demonstrate the model's scalability. Proposing an automated risk model should go hand-in-hand with evaluating it on such datasets, ensuring the method's effectiveness across a wide range of real-world cloud environments. By embedding automation and scalability as core design principles, future risk assessment frameworks will be better equipped to handle the speed and size of modern IT environments, ensuring that security risk management remains effective as organizations and their attack surfaces grow.

5.4 Explainability Gaps

The final key gap identified is the lack of explainability in many modern risk assessment approaches. As techniques for risk analysis become more sophisticated – often involving complex algorithms, statistical models, or machine learning – their inner workings can become opaque to practitioners. Our literature review found that several high-performing risk prioritization models function as "black boxes", yielding risk scores without clear justification or rationale that a human analyst can easily follow. This opacity is problematic because security decision-making requires trust and understanding. Practitioners, such as security analysts or managers, need to know why a particular threat is rated high risk or why one vulnerability is prioritized over another; otherwise, they may be reluctant to act on those recommendations. Nadeem et al. (2023) observe that the limited interpretability of many ML-based security models reduces trust among cybersecurity teams, who require transparent explanations to confidently make decisions based on model outputs. In essence, when a risk assessment tool cannot explain its reasoning, it creates an explainability gap – the end-users of the assessment are left without insight into risk drivers, which can hinder effective risk mitigation and communication.

Explainability is not only an issue for AI or statistical models; even classical risk assessment can suffer if it is overly complex. For example, if an organization uses a weighted scoring system with dozens of factors, stakeholders might struggle to discern which factors most influenced a particular system's risk rating. Furthermore, in cloud and multi-component environments, risk scores often aggregate multiple sources of risk. Without clear traceability (e.g., which specific component or vendor contributes the most risk), remediation efforts may be misguided.

The literature also ties explainability to real-world applicability: a recent survey stresses the need for developing explainable techniques so that research outcomes can be adopted in practice. In scenarios like compliance and audit, being able to provide a clear explanation of how risk is assessed is crucial. A lack of explainability can thus act as a barrier between theoretical models and their practical usage. Ultimately, this gap means that current risk assessment outputs are sometimes not easily interpretable or justifiable, which can lead to mistrust or misuse of those outputs.

Future Research Guidelines: It is imperative that future research on risk assessment and vulnerability management prioritize explainable models and methods. One guideline is to incorporate explainability by design into any new risk scoring system. For instance, if machine learning is used, researchers could favor algorithms that naturally offer insight, such as decision trees or rule-based learners, or apply explainable AI (XAI) techniques to more complex ML models.

Providing clear justifications for risk scores should be a standard requirement. This might include listing the top contributing factors for a risk value (e.g., "Asset is publicly accessible and contains sensitive data, making this vulnerability high risk") or visualizing attack paths to show how a threat could materialize. Some advanced methods could be borrowed from recent research, such as using attack graphs to illustrate possible exploit chains, making risk scenarios more concrete and understandable (Nadeem et al., 2023). Similarly, proof-of-concept exploits or penetration testing can demonstrate the impact of a vulnerability, enhancing explainability by linking risk to observable outcomes (Le et al., 2022).

Another recommendation is to develop standard evaluation criteria for explainability in security research. Just as accuracy or performance is evaluated, future research should also evaluate how interpretable the results are to an informed user. This could involve user studies where analysts interpret model outputs, or metrics that quantify explanation quality. Cross-disciplinary collaboration with cognitive scientists or human-computer interaction experts may help design explanations that truly aid comprehension and decision-making.

Additionally, explainability should not come at the expense of completeness: researchers must balance detail with clarity. One promising avenue noted in the literature (Arrieta et al., 2020) is the use of hybrid approaches that combine simple, interpretable models for high-level assessments with deeper analysis available on demand. For example, an automated system might first give a straightforward risk summary but allow analysts to drill down into more technical detail if needed, thus catering to different levels of expertise. By following these guidelines, future research can ensure that improved risk assessment tools are not only powerful but also transparent and user-friendly. This will foster greater trust in automated risk scores and enable security professionals to effectively communicate and act on the findings of these tools.

In conclusion, the above gaps – in quantification, cloud-specificity, automation and scalability, and explainability – represent significant areas where current security risk assessment research and practice fall short. Each gap also presents an opportunity for impactful research. By developing solutions as outlined and grounding them in rigorous study, the academic and professional community can greatly enhance how we measure, manage, and ultimately mitigate risk in an ever-evolving technological landscape. The next generation of risk assessment methods should thus strive to be more quantitative, cloud-tailored, automated yet scalable, and explainable, thereby building on the foundations laid by existing work and addressing the shortcomings identified in this systematic review. Through these future research directions, the field can move towards more resilient and effective risk management strategies.

5.5 Additional Research Challenges and Future Directions

Based on the comprehensive analysis conducted in this thesis, several additional challenges emerge that complement the four primary gaps identified above:

5.5.1 Integration with Cloud Operations

A significant challenge is the disconnection between risk assessment activities and fast-paced cloud operational processes, particularly DevOps cycles. Traditional risk assessments are conducted periodically, failing to align with continuous integration and deployment models. This disconnection results in delayed identification of risks associated with changes in cloud environments, whether through new services, configuration changes, or code modifications.

Future Research Guidelines: Research should focus on continuous risk management integration by embedding risk assessment into cloud governance and DevOps pipelines. Automated risk checks for each system change (Infrastructure as Code scans, continuous compliance monitoring) can enable real-time risk visibility and response, ensuring risk management becomes a proactive component of cloud operations rather than an afterthought.

5.5.2 Validation and Evidence-Based Assessment

Many proposed risk assessment methods lack thorough validation and iterative refinement. New models are often published without adequate follow-up in terms of real-world testing or longitudinal studies, creating uncertainty about their effectiveness in practice.

Future Research Guidelines: Future research should emphasize empirical evaluation and tool benchmarking through case studies and pilot implementations of new risk models in organizational settings. Developing benchmark datasets and evaluation criteria for cloud risk assessment tools will enable systematic comparison and refinement of approaches, establishing trust and evidence for advanced risk assessment techniques.

5.5.3 Emerging Cloud Technologies

As cloud technologies evolve, new paradigms such as serverless computing, edge computing, and multi-cloud federations introduce novel risks that existing frameworks may not adequately address.

Future Research Guidelines: Research should focus on adapting existing risk models to accommodate these emerging scenarios, incorporating new risk factors and quantifying their impact. Models should be flexible enough to cover new technologies without requiring separate frameworks for each innovation, ensuring continued relevance as cloud computing continues to evolve.

Table 2: Summary of Key Challenges in Cloud Risk Assessment and Future Research Directions

Challenge	Description	Future Research Direction
Quantification Gaps	Difficulty in measuring security risk numerically; heavy reliance on qualitative methods; limited context-aware metrics	Develop robust quantitative models combining severity, likelihood, and business impact; integrate real-time data and validation with empirical evidence
Cloud-Specificity Gaps	Traditional IT frameworks inadequate for cloud environments; lack of cloud-specific risk taxonomies	Create comprehensive cloud risk taxonomies; develop models incorporating multi-tenancy, elasticity, and shared responsibility; extend existing frameworks with cloud-centric modules

Automation and Scalability Gaps	Labor-intensive processes; inability to scale with cloud complexity and dynamism	Leverage AI/ML for vulnerability analysis; develop hierarchical assessment approaches; create real-time risk scoring systems integrated with cloud platforms
Explainability Gaps	Black-box models lack transparency; difficulty in understanding risk drivers	Incorporate explainability by design; develop hybrid approaches combining quantitative rigor with interpretable explanations; establish evaluation criteria for explainability
Integration with Operations	Disconnect between risk assessment and DevOps/cloud governance processes	Embed risk assessment into CI/CD pipelines; develop automated, continuous risk management tools
Validation and Evidence	Lack of empirical validation for proposed methodologies	Conduct case studies and pilot implementations; develop benchmark datasets for systematic evaluation
Emerging Technologies	New cloud paradigms introduce novel, unaddressed risks	Adapt existing models for serverless, edge, and multi-cloud environments; ensure framework flexibility for future technologies

In conclusion, the above gaps – in quantification, cloud-specificity, automation and scalability, and explainability – represent significant areas where current security risk assessment research and practice fall short. Each gap also presents an opportunity for impactful research. By developing solutions as outlined and grounding them in rigorous study, the academic and professional community can greatly enhance how we measure, manage, and ultimately mitigate risk in an ever-evolving technological landscape. The next generation of risk assessment should thus strive to be more quantitative, cloud-tailored, automated yet scalable, and explainable, thereby building on the foundations laid by existing work and addressing the shortcomings identified in this systematic review. Through these future research directions, the field can move towards more resilient and effective risk management strategies.

6

Conclusions

6.1 Introduction

This chapter presents the culmination of the research, summarizing the key findings and contributions of the thesis and outlining critical challenges along with promising directions for future research. The systematic literature review conducted in this thesis analyzed 74 publications from a comprehensive search of 2,847 initial sources, providing a robust foundation for understanding the current state of cloud computing risk assessment. The following sections recap the basic contributions of each chapter, extract the main results of the study, and suggest concrete future research avenues based on the gaps identified through rigorous analysis.

6.2 Basic Contribution of the Thesis

This thesis has made several contributions to the understanding of risk assessment in cloud computing environments through a systematic literature review of current approaches, evaluation of their applicability to cloud-specific contexts, and identification of critical gaps in existing methods. The work builds upon established risk assessment methodologies such as ISO/IEC 27005 (ISO/IEC, 2018) and NIST SP 800-30 (NIST, 2012) while examining their adequacy for cloud computing contexts.

6.2.1 Methodological Contribution

A significant methodological contribution is the rigorous application of a systematic literature review (SLR) to analyze cloud risk assessment methods, following established guidelines (Kitchenham & Charters, 2007). This approach enabled the identification, selection, and evaluation of relevant studies in a transparent and reproducible manner using structured research questions, inclusion/exclusion criteria, and quality assessment metrics. The methodology involved a comprehensive search across multiple databases including IEEE Xplore, ACM Digital Library, ScienceDirect, SpringerLink, Scopus, Web of Science, and Google Scholar.

The filtering process was rigorous, reducing the initial 2,847 publications to 342 after first-stage screening, and finally to 89 high-quality sources that directly addressed cloud-specific risk assessment methods. This systematic approach ensured comprehensive coverage while maintaining quality standards, with 40% of included sources being journal articles, 36% conference papers, and 24% standards or technical reports from authoritative organizations.

The SLR methodology facilitated the categorization of risk assessment methods based on dimensions such as quantification approaches, cloud-specificity, scalability requirements, and automation capabilities. This structured evaluation framework provides researchers and practitioners with a clear understanding of the current state of the field and establishes a replicable methodology for future reviews in this rapidly evolving domain.

6.2.2 Analytical Contribution

The analytical contribution lies in the comprehensive evaluation and comparison of risk assessment frameworks tailored for cloud computing environments. The analysis revealed that traditional frameworks such as ISO/IEC 27005 (ISO/IEC, 2018) and NIST SP 800-30 (NIST, 2012), while providing solid foundations for risk management, were not specifically designed to address the dynamic, multi-tenant, and distributed nature of cloud environments.

The systematic review identified that 28% of included publications originated from IEEE sources, 24% from Elsevier, and 32% from other sources including standards organizations like NIST and industry consortia like the Cloud Security Alliance. This distribution indicates the interdisciplinary nature of cloud risk assessment research, spanning academic venues and industry standards bodies.

The analysis examined how well existing frameworks address cloud-specific challenges including multi-tenancy risks, dynamic resource allocation, shared responsibility models between cloud providers and consumers, and the complexities of supply chain dependencies in cloud services. The review found that while cloud-specific frameworks such as ISO/IEC 27017 (ISO/IEC, 2014) and ENISA's Cloud Computing Risk Assessment (ENISA, 2009) exist, their adoption remains limited due to implementation complexities and lack of integration with operational processes.

Critical gaps were identified in existing frameworks, particularly their lack of support for real-time risk assessment, limited automation capabilities, and insufficient consideration of cloud-native technologies such as containers and serverless computing. These findings highlight the need for more adaptive frameworks that can accommodate the rapid evolution of cloud technologies and deployment models.

6.2.3 Gap Identification and Research Guidelines

Through systematic analysis of the 74 selected publications, the thesis identified four major research gaps that represent significant obstacles to effective cloud risk assessment. These gaps were derived through thematic analysis of the literature and represent areas where current approaches consistently fall short of cloud computing requirements.

- **Quantification Gaps:** The analysis revealed that many existing frameworks still rely on qualitative ratings (high/medium/low) or expert judgment, introducing subjectivity and inconsistency. While vendors like RiskLens and Safe Security now provide quantitative platforms, and frameworks like ISO/IEC 27005 support quantitative approaches, standardized methods for context-aware risk quantification remain lacking. The heavy reliance on CVSS scores, while providing standardization, fails to account for organizational-specific contexts such as asset criticality and actual exploit likelihood in specific environments.

- **Cloud-Specificity Gaps:** Despite the existence of cloud-specific standards like ISO/IEC 27017 (ISO/IEC, 2014) and frameworks by ENISA, the systematic review revealed that academic contributions to cloud-specific risk assessment remain limited, with most approaches being adaptations of traditional IT risk methods rather than purpose-built cloud frameworks. The unique characteristics of cloud computing - multi-tenancy, elasticity, external dependencies, and shared responsibility models - are often inadequately addressed by existing methodologies.

- **Automation and Scalability Gaps:** The literature review identified that current risk assessment processes remain largely manual and struggle to scale with the volume and dynamism of cloud environments. While vulnerability scanning and asset discovery are automated, risk prioritization and scoring often rely on static formulas or human judgment. The challenge is exacerbated in cloud environments where assets can be provisioned and de-provisioned rapidly, requiring continuous risk evaluation.

- **Explainability Gaps:** As machine learning and AI-based approaches gain prominence in cybersecurity, the literature reveals concerns about the "black box" nature of these models. The systematic review found that several high-performing risk prioritization models lack clear justification or rationale that security analysts can follow, creating barriers to trust and adoption in critical decision-making processes.

For each identified gap, the thesis developed specific research guidelines based on emerging trends and promising approaches found in the literature, providing a comprehensive roadmap for future investigations that can advance risk assessment in cloud environments.

6.3 Key Research Findings and Synthesis

The systematic literature review yielded several significant findings about the current state and future needs of cloud computing risk assessment:

6.3.1 Current State of Cloud Risk Assessment Research

The temporal analysis of publications revealed that cloud computing risk assessment emerged as a research topic around 2009-2010, coinciding with the rise of cloud computing adoption. The consistent publication pattern from 2009 to 2024, with steady contributions averaging 1-2 publications per year, demonstrates sustained research interest and indicates the ongoing importance of addressing cloud-specific security challenges. The publisher distribution analysis showed that IEEE (28%) and Elsevier (24%) dominate the academic publications, while the substantial "Others" category (32%) includes important contributions from standards organizations and industry consortia. This distribution underscores the interdisciplinary nature of cloud risk assessment, where effective solutions require collaboration between academic researchers, standards bodies, and industry practitioners.

6.3.2 Integration Challenges with Cloud Operations

The analysis revealed a critical challenge in the disconnection between risk assessment activities and fast-paced cloud operational processes, particularly DevOps cycles. Traditional risk assessments are conducted periodically (annually or at project initiation), which fails to align with continuous integration and deployment models characteristic of modern cloud services. This temporal mismatch results in delayed identification of risks associated with frequent changes in cloud environments, whether through new service deployments, configuration modifications, or code updates. The literature indicates that cloud environments can change on daily or hourly bases, making static risk assessments quickly obsolete if not updated frequently. This challenge is particularly acute because cloud services often involve complex interdependencies where changes in one component can cascade risk impacts across multiple services and systems.

6.3.3 Validation and Evidence Gaps

A significant finding from the systematic review is the lack of thorough validation and empirical evidence for many proposed risk assessment methods. The analysis revealed that new models are often published without adequate follow-up in terms of real-world testing or longitudinal studies to evaluate their effectiveness over time. This validation gap is particularly problematic in cloud environments, which are continuously evolving, making it essential to understand how risk models perform as technology and threat landscapes change. The literature review identified limited availability of enterprise-scale datasets for evaluating risk assessment models, which restricts the ability to test their performance comprehensively across diverse cloud environments. This lack of empirical validation creates uncertainty about the practical effectiveness of proposed approaches, potentially hindering their adoption by organizations requiring evidence-based security decisions.

6.3.4 Interconnected Nature of Challenges

A key finding is that the identified challenges are interconnected rather than isolated problems. Progress in automation and scalability naturally supports more accurate quantification, while standardized frameworks facilitate validation efforts and tool development. For example, continuous risk assessment (addressing automation gaps) inherently supports more accurate quantification (addressing quantification gaps) and aids in tracking emerging threats (addressing cloud-specificity gaps). This interconnected nature suggests that research efforts addressing multiple challenges simultaneously are likely to yield more significant improvements than isolated approaches targeting individual gaps. The implication is that future research should adopt a holistic perspective that considers the relationships between different aspects of cloud risk assessment.

6.4 Future Research Outlook

Based on the comprehensive analysis of current approaches and identified gaps, several concrete directions emerge for future research that can address the critical challenges in cloud computing risk assessment:

6.4.1 Data-Driven and Continuous Assessment Models

Future research should prioritize the development of adaptive, continuous risk assessment tools that automatically collect and analyze relevant data within cloud environments. These tools should leverage machine learning models to predict risk levels, detect anomalies, and provide real-time risk scoring based on changing conditions such as new vulnerabilities, configuration changes, and threat intelligence updates. Research in this direction should focus on integrating multiple data sources including vulnerability databases, threat intelligence feeds, system performance metrics, and configuration management data to provide comprehensive risk visibility. The development of "risk sensors" embedded in cloud platforms could enable continuous monitoring and automatic risk recalculation as conditions change, similar to credit scoring systems that update based on new information.

6.4.2 Cloud-Native Risk Assessment Frameworks

Research should focus on developing purpose-built frameworks for cloud risk assessment rather than adapting traditional IT risk models. These frameworks must incorporate the unique characteristics of cloud computing from the ground up, including multi-tenancy models, elastic resource allocation, microservices architectures, and complex supply chain dependencies. Future work should establish comprehensive taxonomies of cloud-specific risks and standardized metrics for evaluating them. This includes developing methods to assess risks associated with emerging cloud paradigms such as serverless computing, edge computing, and multi-cloud federations. The frameworks should be flexible enough to accommodate rapid technological evolution while maintaining consistency in risk evaluation approaches.

6.4.3 Validation and Benchmarking Initiatives

A critical research direction is the establishment of comprehensive validation methods and benchmarking datasets for cloud risk assessment tools. Future research should emphasize empirical evaluation through case studies, pilot implementations, and partnerships with organizations willing to test new approaches in real cloud environments. The development of standardized benchmark datasets that reflect diverse cloud scenarios, configurations, and risk factors is essential for objective comparison of different risk assessment methods. These benchmarks should capture the complexity and dynamic nature of cloud environments while providing ground truth data for validating the effectiveness of risk models against actual security outcomes.

6.4.4 Integration with Cloud Governance and Operations

Research should focus on seamlessly integrating risk assessment into cloud governance processes and DevOps pipelines. This includes developing automated tools that can evaluate security implications of infrastructure changes, perform continuous compliance monitoring, and provide real-time risk feedback during development and deployment processes. Future work should explore the integration of risk assessment with Infrastructure as Code practices, enabling automatic risk evaluation of proposed system changes before deployment. This integration would ensure that risk considerations become an integral part of cloud operations rather than separate, periodic activities.

6.5 Implications and Limitations

6.5.1 Theoretical Implications

The systematic literature review contributes to cloud security theory by providing a comprehensive mapping of current approaches and identifying theoretical gaps in risk assessment methods. The classification of methods based on quantification, cloud-specificity, automation, and explainability dimensions provides a theoretical framework for understanding and categorizing future research contributions. The identification of interconnected challenges suggests that cloud risk assessment requires a systems thinking approach rather than isolated solutions to individual problems. This theoretical insight has implications for how researchers design and evaluate new risk assessment methods.

6.5.2 Practical Implications

For practitioners, the thesis provides evidence-based guidance on selecting appropriate risk assessment approaches for different cloud deployment scenarios. The comparative analysis of existing frameworks offers insights into their strengths and limitations, helping organizations make informed decisions about risk management strategies. The identified gaps and future research directions provide a roadmap for tool developers and standards organizations working to improve cloud risk assessment capabilities. The emphasis on automation and integration with operational processes addresses practical needs of organizations managing large-scale, dynamic cloud environments.

6.5.3 Limitations

The systematic literature review, while comprehensive, is limited by the availability of published research and may not capture all proprietary or emerging industry practices. The focus on English-language publications and specific databases may have excluded relevant work published in other languages or venues. The rapid evolution of cloud technologies means that some findings may become outdated as new cloud paradigms emerge. However, the methodological approach and framework for analysis remain applicable to future developments in cloud computing and risk assessment.

6.6 Conclusion

This thesis has provided a comprehensive analysis of cloud computing risk assessment through systematic literature review, identifying critical gaps and proposing research-informed guidelines for future work. The analysis of 74 high-quality publications revealed that while progress has been made in cloud security risk assessment, significant challenges remain in quantification, cloud-specificity, automation, and explainability. The key contributions include a rigorous methodological approach for analyzing cloud risk assessment literature, comprehensive evaluation of existing frameworks and their cloud applicability, identification of four major research gaps with specific guidelines for addressing them, and a roadmap for future research that considers the interconnected nature of cloud risk assessment challenges. The findings indicate that the field requires coordinated research efforts that address multiple challenges simultaneously rather than isolated solutions to individual problems. The future research directions outlined provide concrete steps for advancing toward more effective, scalable, and trustworthy risk assessment methods that can keep pace with the rapid evolution of cloud computing. As organizations continue to increase their reliance on cloud services for critical operations and data storage, the importance of effective risk assessment methodologies cannot be overstated. The contributions of this thesis serve as a foundation for future research and practice in cloud risk assessment, ultimately contributing to stronger security postures and more resilient cloud environments

Bibliography

[1] Akinrolabu, O., et al. (2019). Risk Assessment Frameworks for Cloud Computing: A Systematic Literature Review. Journal of Cloud Computing, 8(1), 1–25.

[2] Basu, S., et al. (2021). Risk Quantification in Cloud Computing: A Comparative Study. IEEE Access, 9, 2230–2245.

[3] Cloud Security Alliance (CSA). (2023). Cloud Controls Matrix (CCM) v4. Retrieved from https://cloudsecurityalliance.org/research/ccm/

[4] Gega, B., Wangen, GB, & Sindre, G. (2025). Validation Challenges in Risk Assessment Methodologies: A Systematic Survey. Information and Software Technology, 140, 106667.

[5] Joh, H., & Malaiya, Y. (2011). A Framework for Software Security Risk Evaluation Using the Vulnerability Lifecycle and CVSS Metrics. Proceedings of the 4th International Conference on Software Engineering Advances, 492–500.

[6] Le, T., Malaiya, Y., & Trivedi, K. (2022). Prioritizing Vulnerabilities for Effective Risk Management: Challenges and Research Directions. Journal of Cybersecurity and Information Integrity, 5(1), 1–18.

[7] Microsoft. (2023). Azure Compliance Offerings and Risk Assessment Guidance. Microsoft Azure Documentation. Retrieved from https://learn.microsoft.com/en-us/compliance/

[8] Nadeem, A., et al. (2023). Explainability Challenges in Machine Learning for Cybersecurity: A Survey. ACM Computing Surveys, 55(7), Article 129.

[9] National Institute of Standards and Technology (NIST). (2012). Guide for Conducting Risk Assessments (SP 800-30 Rev. 1). US Department of Commerce. Retrieved from https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final

[10] National Institute of Standards and Technology (NIST). (2024). Cybersecurity Framework Version 2.0 (NIST.CSWP.29). Retrieved from https://www.nist.gov/cyberframework

[11] Saripalli, P., & Walters, B. (2010). QUIRC: A Quantitative Impact and Risk Assessment Framework for Cloud Security. Proceedings of the IEEE 3rd International Conference on Cloud Computing (CLOUD), 280–288.

[12] Wangen, GB (2017). Information Security Risk Assessment: A Method Comparison. IEEE Computer, 50(4), 52–61.

[13] International Organization for Standardization (ISO). (2018). ISO/IEC 27005:2018 — Information technology — Security techniques — Information security risk management. ISO/IEC.

[14] The Open Group. (2013). FAIR: Factor Analysis of Information Risk — A Standard for Information Risk Management. The Open Group Standard (O-FAIR).

[15] Carnegie Mellon University. (2007). OCTAVE Allegro: Improving the Information Security Risk Assessment Process. Software Engineering Institute (SEI).

[16] ENISA. (2009). Cloud Computing Risk Assessment. European Union Agency for Cybersecurity (ENISA). Retrieved from https://www.enisa.europa.eu/publications/cloud-computing-risk-assessment

[17] Amazon Web Services (AWS). (2021). AWS Risk and Compliance Whitepaper. Amazon Web Services. Retrieved from https://docs.aws.amazon.com/whitepapers/latest/aws-risk-and-compliance/aws-risk-and-compliance-program.html

[18] Bellavista, P., Corradi, A., Foschini, L. (2013). Cloud computing: Risk assessment and management strategies. Cloud Computing Risk Assessment – A Systematic Literature Review.

[19] Rios, R., Sarriegui, JM (2015). Software and attack centric integrated threat modeling for quantitative risk assessment. Computers & Security, 48, 1–15.

[20] Alberts, CJ, Dorofee, AJ (2002). Managing Information Technology Security Risk: The OCTAVE Approach. Addison-Wesley Professional.

[21] Jiang, X., Malaiya, Y., & Joh, H. (2025). Scalability in Risk Assessment: An Empirical Review and Recommendations. Journal of Information Security and Applications, 68, 103189.

[22] SentinelOne. (2024). 17 Security Risks of Cloud Computing in 2025. Retrieved from https://www.sentinelone.com/lp/security-risks-cloud-computing/

[23] Zegzhda, P., & Solodov, A. (2019). Quantitative Risk Analysis: Theoretical Problems and Prospects. Journal of Information Security, 10(2), 134–145.

[24] Gega, B., Wangen, GB, & Sindre, G. (2025). "Validation Challenges in Risk Assessment Methodologies: A Systematic Survey." Information and Software Technology, 140, 106667.

[25] ISO/IEC. (2022). ISO/IEC 27005 – Information security risk management. International Organization for Standardization.

[26] Jiang, X., Malaiya, Y., & Joh, H. (2025). "Scalability in Risk Assessment: An Empirical Review and Recommendations." Journal of Information Security and Applications, 68, 103189.

[27] Joh, H., & Malaiya, Y. (2011). "A Framework for Software Security Risk Evaluation Using the Vulnerability Lifecycle and CVSS Metrics." Proceedings of the 4th International Conference on Software Engineering Advances, 492–500.

[28] Le, T., Malaiya, Y., & Trivedi, K. (2022). "Prioritizing Vulnerabilities for Effective Risk Management: Challenges and Research Directions." Journal of Cybersecurity and Information Integrity, 5(1), 1–18.

[29] Nadeem, A., et al. (2023). "Explainability Challenges in Machine Learning for Cybersecurity: A Survey." ACM Computing Surveys, 55(7), Article 129.

[30] Open Web Application Security Project (OWASP). (2023). Top 10 Cloud Security Risks. OWASP Foundation.https://owasp.org/www-project-top-10-cloud-security-risks/

[31] Zegzhda, P., & Solodov, A. (2019). "Quantitative Risk Analysis: Theoretical Problems and Prospects." Journal of Information Security, 10(2), 134–145.

[32] FAIR Institute. (2024). FAIR Risk Methodology: Quantifying and Managing Cyber Risk. Retrieved from CSO Onlinecsoonline.comcsoonline.com

[33] AWS. (2021). AWS Risk and Compliance Whitepaper. Amazon Web Services docs.aws.amazon.com

[34] Microsoft. (2024). Risk Assessment Guide for Microsoft Cloud. Microsoft Learn

[35] Cloud Security Alliance. (2023). Cloud Controls Matrix (CCM) v4. Cloud Security Alliance paloaltonetworks.com

[36] NVD. (2023). Common Vulnerability Scoring System – Definition. NIST National Vulnerability Database nvd.nist.gov

[37] Capital One. (2020). Capital One cyber incident: Update on investigation. Capital One Newsroom. https://www.capitalone.com/newsroom/capital-one-cyber-incident-update/

[38] Carnegie Mellon University Software Engineering Institute (SEI). (2007). OCTAVE Allegro: Improving the Information Security Risk Assessment Process.

[39] Cloud Security Alliance (CSA). (2016). The treacherous 12: Cloud computing top threats in 2016. https://cloudsecurityalliance.org/artifacts/treacherous-12-top-threats-to-cloud-computing/

[40] IBM. (n.d.). What are the benefits of cloud computing? IBM Cloud Education. Retrieved April 2024, from https://www.ibm.com/think/topics/cloud-computing-benefits

[41] Mell, P., & Grance, T. (2011). The NIST definition of cloud computing (NIST Special Publication 800-145). National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

[42] Open Web Application Security Project (OWASP). (2023). Top 10 Cloud Security Risks. OWASP Project. https://owasp.org/www-project-top-10-cloud-security-risks/

[43] Trend Micro. (2017, December 20). Data on 123 million US households exposed due to misconfigured AWS S3 bucket. Trend Micro Security News. https://www.trendmicro.com/vinfo/us/security/news/cloud-security/data-exposed-aws-bucket

[44] Trend Micro. (2021, October 25). The most common cloud misconfigurations that could lead to security breaches. Trend Micro Research. https://www.trendmicro.com/vinfo/us/security/news/cloud-security/common-cloud-misconfigurations

[45] United States Department of Justice. (2020). Paige A. Thompson Indictment in Capital One data breach case. DOJ Press Release. https://www.justice.gov/opa/pr/former-seattle-tech-worker-indicted-capital-one-data-breach

[46] Goldman, J. (2014, June 23). Code Spaces destroyed by cyber attack. eSecurity Planet. https://www.esecurityplanet.com/news/code-spaces-destroyed-by-cyber-attack/

[47] Tesla, Inc. (2018). Tesla incident report on cloud crypto-mining breach. Internal Report (Referenced indirectly through media summaries).

[48] Zetter, K. (2018). Specter and Meltdown: What you need to know. Wired Magazine. https://www.wired.com/story/spectre-meltdown-cpu-vulnerabilities/

[49] AWS Documentation. (2024). Shared Responsibility Model. Amazon Web Services. https://aws.amazon.com/compliance/shared-responsibility-model/

[50] Cloudflare. (2023). DDoS attacks in the cloud: Trends and mitigation strategies. Cloudflare Blog. https://blog.cloudflare.com/ddos-attacks-in-the-cloud/

[51] IBM Security. (2024). Cost of a Data Breach Report 2024. IBM Security and Ponemon Institute. https://www.ibm.com/reports/data-breach

[52] Verizon. (2024). 2024 Data Breach Investigations Report (DBIR). Verizon Research. https://www.verizon.com/business/resources/reports/dbir/

[53] Google Cloud. (2024). Best practices for cloud security misconfiguration prevention. Google Cloud Security. https://cloud.google.com/security/best-practices

[54] OWASP Foundation. (2023). Server-Side Request Forgery (SSRF) Prevention Cheat Sheet. OWASP. https://cheatsheetseries.owasp.org/cheatsheets/Server_Side_Request_Forgery_Prevention_Cheat_Sheet.html

[55] BBC News. (2021, January 11). Parler: How social media app got scraped for posts before shutdown. BBC News Technology. https://www.bbc.com/news/technology-55615214

[56] Krebs, B. (2017, July 13). Verizon confirms leak of millions of customer records. Krebs on Security. https://krebsonsecurity.com/2017/07/verizon-confirms-leak-of-millions-of-customer-records/

[57] Akinrolabu, O., Nurse, J. R. C., Martin, A., & New, S. (2019). Cyber risk assessment in cloud provider environments: Current models and future needs. *Computers & Security*, 87, 101600. https://doi.org/10.1016/j.cose.2019.101600

[58] Arrieta, A. B., Díaz-Rodríguez, N., Del Ser, J., Bennetot, A., Tabik, S., Barbado, A., García, S., Gil-López, S., Molina, D., Benjamins, R., Chatila, R., & Herrera, F. (2020). Explainable Artificial Intelligence (XAI): Concepts, taxonomies, opportunities and challenges toward responsible AI. *Information Fusion*, 58, 82-115. https://doi.org/10.1016/j.inffus.2019.12.012

[59] Basu, A., Omotubora, A., Beeson, K., & Fox, C. (2021). Legal requirements versus market realities: Cybersecurity disclosures and risk management. *Business Horizons*, 64(3), 375-393. https://doi.org/10.1016/j.bushor.2021.02.007

[60] Cloud Security Alliance. (2023). *Cloud Controls Matrix (CCM) v4.0.6*. Cloud Security Alliance.

[61] ENISA. (2009). *Cloud Computing Risk Assessment*. European Union Agency for Network and Information Security. https://www.enisa.europa.eu/publications/cloud-computing-risk-assessment

[62] Gega Balun, J., Smith, P., & Johnson, L. (2025). Evaluating the effectiveness of cybersecurity risk assessment methodologies: A comprehensive analysis. *Journal of Information Security*, 16(2), 45-72.

[63] International Organization for Standardization. (2018). *Information technology — Security techniques — Information security management systems — Requirements* (ISO/IEC 27001:2022). ISO.

[64] ISO/IEC. (2014). Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services (ISO/IEC 27017:2015). International Organization for Standardization.

[65] ISO/IEC. (2018). Information technology — Security techniques — Information security risk management (ISO/IEC 27005:2018). International Organization for Standardization.

[66] ISO/IEC. (2022). Information technology — Security techniques — Information security management systems — Requirements (ISO/IEC 27001:2022). International Organization for Standardization.

[67] Jacobs, J., Romanosky, S., Edwards, B., Adjerid, I., & Roytman, M. (2021). Exploit prediction scoring system (EPSS). *Digital Threats: Research and Practice*, 2(3), 1-17. https://doi.org/10.1145/3436242

[68] Jiang, F., Fu, Y., Gupta, B. B., Lou, F., Rho, S., Meng, F., & Tian, Z. (2018). Deep learning based multi-channel intelligent attack detection for data security. *IEEE Transactions on Sustainable Computing*, 5(2), 204-212. https://doi.org/10.1109/TSUSC.2018.2793284

[69] Joh, H., & Malaiya, Y. K. (2011). Defining and assessing quantitative security risk measures using vulnerability lifecycle and CVSS metrics. In *Proceedings of the 2011 International Conference on Security and Management* (pp. 31-37). CSREA Press.

[70] Kitchenham, B., & Charters, S. (2007). *Guidelines for performing systematic literature reviews in software engineering* (Technical Report EBSE-2007-01). Keele University and Durham University.

[71] Le, D. C., Zincir-Heywood, A. N., & Heywood, M. I. (2022). Analyzing data granularity levels for insider threat detection using machine learning. *IEEE Transactions on Network and Service Management*, 17(1), 30-44. https://doi.org/10.1109/TNSM.2019.2945906

[72] Lee, S., Abdullah, A., Jhanjhi, N. Z., & Kok, S. (2022). Classification of botnet attacks in IoT smart factory using honeypot combined with machine learning. *PeerJ Computer Science*, 8, e820. https://doi.org/10.7717/peerj-cs.820

[73] Nadeem, A., Verwer, S., Moskal, S., & Yang, S. J. (2023). Alert-driven attack graph generation using S2A: A sequence-to-sequence deep learning approach. *IEEE Transactions on Dependable and Secure Computing*, 19(2), 741-760. https://doi.org/10.1109/TDSC.2021.3056685

[74] National Institute of Standards and Technology. (2012). *Guide for Conducting Risk Assessments* (NIST Special Publication 800-30 Revision 1). U.S. Department of Commerce. https://doi.org/10.6028/NIST.SP.800-30r1

[75] NIST. (2012). *Guide for Conducting Risk Assessments* (NIST Special Publication 800-30 Revision 1). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-30r1

[76] NIST. (2018). *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy* (NIST Special Publication 800-37 Revision 2). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-37r2

[77] NIST. (2024). *NIST Cybersecurity Framework 2.0*. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.CSWP.29

[78] Poolsappasit, N., Dewri, R., & Ray, I. (2012). Dynamic security risk management using Bayesian attack graphs. *IEEE Transactions on Dependable and Secure Computing*, 9(1), 61-74. https://doi.org/10.1109/TDSC.2010.34

[79] Shamsoshoara, A., Korenda, A., Afghah, F., & Zeadally, S. (2021). A survey on physical unclonable function (PUF)-based security solutions for Internet of Things. *Computer Networks*, 183, 107593. https://doi.org/10.1016/j.comnet.2020.107593

[80] Singh, A., & Kumar, P. (2023). Cloud Supply Chain Cyber Risk Assessment: A comprehensive framework for multi-tier risk evaluation. *Journal of Cloud Computing*, 12(1), 15-32. https://doi.org/10.1186/s13677-023-00432-8

[81] Wang, L., Islam, T., Long, T., Singhal, A., & Jajodia, S. (2008). An attack graph-based probabilistic security metric. In *IFIP Annual Conference on Data and Applications Security and Privacy* (pp. 283-296). Springer. https://doi.org/10.1007/978-3-540-70567-3_22