Cyber risk assessment in cloud provider environments: Current models and future needs

Olusola Akinrolabu[a,*], Jason R. C. Nurse[b], Andrew Martin[a], Steve New[c]

[a]*Department of Computer Science, University of Oxford*
[b]*School of Computing, University of Kent*
[c]*Saïd Business School, University of Oxford*

Abstract

Traditional frameworks for risk assessment do not work well for cloud computing. While recent work has often focussed on the risks faced by firms adopting or selecting cloud services, there has been little research on how cloud providers might assess their own services. In this paper, we use an in-depth review of the extant literature to highlight the weaknesses of traditional risk assessment frameworks for this task. Using examples, we then describe a new risk assessment model (CSCCRA) and compare this against three established approaches. For each approach, we consider its goals, the risk assessment process, decisions, the scope of the assessment and the way in which risk is conceptualised. This evaluation points to the need for dynamic models specifically designed to evaluate cloud risk. Our suggestions for future research are aimed at improving the identification, assessment, and mitigation of inter-dependent cloud risks inherent in a defined supply chain.

Keywords: Cloud computing, Risk assessment, Conceptual model, Cloud risks, Quantitative and Qualitative assessment, Supply chain

1. Introduction

Cloud computing is a resources management model that enables convenient, on-demand access to a shared pool of computing resources [1]. Cloud

*Olusola Akinrolabu
Email addresses: olusola.akinrolabu@cs.ox.ac.uk (Olusola Akinrolabu), j.r.c.nurse@kent.ac.uk (Jason R. C. Nurse), andrew.martin@cs.ox.ac.uk (Andrew Martin), Steve.new@sbs.ox.ac.uk (Steve New)

technology is evolving at a rapid rate while also becoming more ubiquitous. This ubiquity gives rise to many opportunities but also introduces new risks. While the cloud model has many economic and functional advantages, the increased external interactions of its applications have expanded the complexity of cloud architectures and reshaped the backbone of infrastructures and supply chains [2]. According to a report by ENISA on cloud security, the benefits of cloud computing, particularly its economies of scale and flexibility are both a friend and a foe [3]. Cloud users put their most sensitive assets directly on the Internet, which is why cloud security has become a significant topic both for research and in practice.

A risk is defined as the effect of uncertainty on objectives [4]; while risk assessment is the process of identifying, evaluating and prioritising risks [5]. Information security risks lead to a deviation from the expected results for which security controls were implemented, and they impact the objectives of the information asset including its financial, safety or productivity goals. The concept of risk varies in interpretation and significance to organisations. Therefore, the risk management and risk assessment approach for each organisation will vary based on their predisposition, in-house expertise, and risk appetite. Due to their broad applicability, most of the popular risk assessment and management (RA/RM) frameworks, e.g. ISO/IEC 27005, ISO/IEC 31000 and NIST 800-30, describe risk assessment at an abstract level and do not offer sufficient practical guidelines for completing each step. They introduce a certain level of ambiguity into the interpretation of security risks making it difficult for them to be used in understanding and assessing cloud risks, mainly because cloud environments are highly connected, rapidly changing, and inter-dependent [6]. Being predominantly qualitative or semi-quantitative, the prevalent use of these traditional frameworks in assessing cloud risks has further exacerbated the cloud risk assessment challenge.

Cloud risks vary with deployment, and the effect of risk on an organisation is dependent on factors such as data sensitivity, cloud architecture, and implemented security controls. The responsibilities of each stakeholder vary with each cloud service model, and the trust among the communicating parties plays a pivotal role in determining the appropriate risk level of a cloud application. In multicloud systems (MCS), where cloud architectures use services from more than one cloud service provider (CSP), the challenge of risk assessment is evident. While many of the recent research efforts (e.g., Busby et al. [7], Cayirci et al. [8], and Islam et al. [9]) have concentrated on cloud adoption risk assessment, others (e.g., Sendi & Cheriet [10] and

Sivasubramanian et al. [11]) have followed the traditional route to security risk assessment, concentrating on the focal organisation, their critical assets, threats, and likelihood of impact, without paying attention to the supplier network nor fully understanding its interrelated consequences. This problem has also been highlighted and evidenced in the works of Johnson [12], Bartol [13], Boyens et al. [14], Lewis et al. [15] and Motta et al. [16]. Based on the complexity of cloud service provisioning, there is, therefore, a need for more research aimed at improving cloud risk assessment.

In this paper, we review the extant literature on risk assessment frameworks for cloud service provisioning. Our decision to address security risk assessment from a cloud provider perspective was influenced by the scarcity of studies in this area, and on the practical need for cloud providers to assess security risks to assure secure cloud delivery to customers. As such, we also describe our novel quantitative model for cloud providers: Cyber Supply Chain Cloud Risk Assessment (CSCCRA) [17]. Here we highlight its strengths, which include its systematic analysis of cloud risks, the visual representation of the cloud supply chain, and the assessment of the cybersecurity posture of cloud suppliers.

Based on a set of defined selection criteria, we identify three conceptual models developed for assessing cloud service provision risks and systematically evaluate them against the CSCCRA model. We assess each of the models based on their goal, risk assessment steps, decisions supported, the scope of assessment and conceptualisation of risk. Given the scarcity of initiatives for the practical implementation of a quantitative risk assessment of a cloud computing service, the CSCCRA model contributes towards improving the state of the art knowledge around the transparency of the cloud supply chain, cyber supply chain risks, supply chain mapping and the quantitative risk assessment of cloud services.

The contributions of this paper are the identification of gaps in cloud risk assessment, an analysis of current models, and a more detailed presentation of the proposed CSCCRA model we introduced in [17] which is meant to address some of the identified gaps. Furthermore, we present directions for future research by outlining areas where the theory and practice of cloud provisioning risk assessment can be improved including the application of dynamic modelling based on defined boundaries and the development of automated models for the proactive mitigation of cloud risks.

The remainder of the paper is organised as follows. First, in Section 2, we present background information on risk assessment and cloud risk assessment

models. Next, Section 3 examines well-known cloud risk models according to a set of defined criteria; this also includes a reflection on our own CSCCRA model. In Section 4, we evaluate the models and discuss our findings; while in Section 5, we identify several outstanding needs for cloud risk assessment approaches. This article is concluded in Section 6, where we also present avenues for future research.

2. Background and Literature Review

2.1. Risk Assessment

Risk Management (RM) is the general process of managing risk to an acceptable level within an organisation and typically consists of two main stages known as risk assessment and risk treatment [5]. Risk Assessment (RA) is a central part of information security management, and it enables organisations to identify vulnerabilities and threats while also informing the choice of cost-effective controls (safeguards & countermeasures) to address potential threats [18]. Ionita [19] describes RA as a structured or semi-structured approach of analysing the security of a system, identifying weak spots, and selecting adequate controls.

According to the ISO/IEC 27005:2011 standard [4], risk assessment consists of two processes, Risk Analysis & Risk Evaluation. RA involves a continuous iterative process which revolves around identifying, analysing, prioritising, mitigating and monitoring security risks. In assessing the risk of an IT system, several factors are taken into consideration, including identifying the asset, threat, vulnerability and impact. The objective of a risk assessment is to understand the existing system and environment and identify risks through analysis of the information/data collected, which helps organisations to make security decisions consistent with their risk management strategy, despite the level of uncertainty inherent in the evaluation process [20]. Risk assessments are conducted to inform decision-makers and support risk responses, either as part of a security audit, compliance initiative, or to support security budget decisions [19, 20]. Therefore, in assessing risks, it is practical to implement a risk assessment framework that employs a rigorous process in determining the risk factors and promotes increased objectivity through the use of controlled experimentation. Also, the process followed by the risk assessment model in evaluating initial risks and informing security decisions should be repeatable, understandable, and traceable.

Overall, the main result of a risk assessment exercise is the quantitative or qualitative evaluation of the possible impact of threat sources on a given system and its vulnerability, while considering the context of such risk scenarios. This assessment, however comprehensive, does not assure a fully secure system; instead, it assists organisations in implementing cost-effective risk treatment processes with the aim of achieving an acceptable level of risk, which is sometimes referred to as "good enough" security [21].

2.2. Assessing Cloud Risks versus Traditional IT Risks

Thus far, and despite a significant number of scholars who have grappled with the issue of cloud computing risks, there is currently no industry established consensus on assessing cloud risks [9] and no standard measurement unit for cyber risk [2]. According to ISACA [22], this difficulty is down to the lack of a structured framework for cloud risk identification and assessment, coupled with the cloud's highly dynamic and flexible nature. In the absence of a standardised risk assessment framework for cloud computing, the industry has continued to use existing IT risk frameworks to address cloud risks [23, 24]. However, while the cloud faces some of the threats applicable to any information system, it also faces unique threats and vulnerabilities involving multiple parties including cloud providers (employees, facilities, systems), technology (interfaces, API), external attackers and other cloud co-tenants.

Traditional IT risks differ from cloud computing risks. The risk involved with the migration of internal IT data and applications, or hosting customer data in the cloud varies according to the sensitivity of the asset, cloud service/delivery model, cloud architecture and security controls. Cloud computing leverages many technologies (Service Oriented Architecture, virtualisation, Web 2.0, Internet) and inherits the security risks of these underlying systems, introducing an extra layer of complexity [25, 26]. The virtual flows of data through the cloud is layered on top of physical network media such as fibre optics and other technologies which are old, slower to change and centripetal in nature [27]. As such, the security concerns associated with the Internet also threatens the existence of cloud, but in the case of the cloud, the risk is overwhelmingly high, because of the vulnerabilities of the individual components, and the co-location of large amounts of valuable data [28, 29]. Interestingly, while some of the cloud risks are as a result of the dynamic supply chain of the cloud, others are down to the immature offering from service providers, limited transparency, and the subjective nature of expert claims [30].

Furthermore, the traditional IT risk assessment frameworks, e.g.ISO/IEC 27005, which were developed before the evolution of cloud computing, cannot cater to the complexity or pervasiveness of these dynamic and automated systems of systems. According to Albakri et al. [31], the most popular risk assessment standards assume that an organisation's assets are managed in-house. These frameworks are structured based on security control domains [2]. Applying risk assessment frameworks developed with these assumptions to the cloud, therefore, leads to increased vulnerabilities and inadequate implementation of security controls. Some of the other concerns often raised about the traditional risk assessment frameworks includes the shortcomings of periodic assessment, limited knowledge of the Target of Assessment (ToA), and inability to measure cyber risk in dynamic systems [32, 33, 34].

The process of conducting periodic assessments, naturally assumes that systems will not significantly change over a short period [35]. Cloud computing exacerbates this issue because a dynamic infrastructure and flexible links are central to its paradigm. Due to its automated nature, the stream of interactions between connected systems in the cloud is not always capable of being scoped and fully characterised a priori. As such, organisations are increasingly likely to have limited knowledge about their systems and their interactions with external systems. With cloud services susceptible to increasing exposure to disruptions, especially from the supply chain, it is vital to assess the risks of any cloud service proactively [36].

Collectively, we maintain that the process of manually fitting the traditional risk assessment frameworks to address dynamic cloud risks is counterproductive. Therefore, a more effective approach will be for new cloud risk frameworks to be built from the ground up to address the various shortcomings of the current risk models, and in the same vein, improve the rigour of security provisions in the cloud.

2.3. Cloud Risk Assessment Models

Cloud risk assessment is defined as a dynamic, step by step, repeatable process used to produce an understanding of cloud risks associated with relinquishing control of data or management of services to an external service provider [37]. It is considered to be one of the most significant enterprise security weaknesses worldwide [38]. Tang et al. [39] argue that two significant problems that have contributed to relatively low turnout of cloud computing risk assessment research, one of which is the lack of systematic study on the whole process of cloud assessment. While many studies have been conducted

to investigate and address cloud consumer risks and issues, the perspective of the CSPs is rarely discussed in the literature [40].

We define cloud risk assessment model as a tool designed for cloud stakeholders to assess the risks they face from the adoption, creation or operation of a particular service. It helps to understand the problem area, analyse various risk scenarios, and improve the defensibility of risk result. A cloud model could be used to evaluate the various background information obtained from members of the supply chain and other public sources [8]. The application of a well-founded risk model to cloud assessment ensures that the process follows a particular methodology and is repeatable, understandable and traceable. A risk model defines the risk factors to be assessed, and the relationship between the risk factors, with these factors used as input to determine the risk level during assessments. Risk factors include vulnerability, impact, threat, likelihood, probability, exposure factors, and predisposing condition [20].

Some of the advantages of applying a risk model to assessing cloud risks include the structured and systematic approach to understanding risks, and the ability to deliver objective and effective decision-making and risk evaluations while saving the stakeholders time and effort as they mature into the use of the model. Examples of proposed cloud risk assessment models include SECCRIT [7], CARAM[8], CSPRAM [31], QUIRC [41], OPTIMIS [42] and SEBCRA[43]. While each of these models addresses risks relating to the provisioning, adoption or migration of cloud resources, we will be concentrating on models which address cloud provider risks in this study.

3. Conceptual Risk Assessment Models for Cloud Provisioning Risks

A reality of traditional risk assessment methodologies is that they concentrate on providing organisations with general principles and guidelines of risk assessment and may offer fewer details on their implementation. As such the cloud industry stands to benefit from the development of conceptual models that address different cloud stakeholder needs. Conceptual models are tools composed of concepts and relationships, designed to help make sense of complex issues [44], such as those faced in cloud risk assessment.

Cloud risk assessment requires domain-specific knowledge, and a deep understanding of the ToA, i.e. cloud service, to ensure one can arrive at reasonable risk estimates [44]. Seeing that a key novelty of cloud computing in comparison to other IT service is its dynamic supply chain, assessing the risk of a cloud service requires capturing a snapshot of its shifting landscape. The

dynamic supply chain, which is an adaptable ecosystem of people, processes, capital assets, technology and data, enables businesses to strike a balance between the opportunities that drive economic growth and the downside risks of disruptive events within the chain [45]. One approach to addressing this evolving landscape is to ensure that the cloud stakeholders and IT components that make up the cloud service are viewed as belonging to the same socio-technical system.

The current state-of-the-art in cloud risk assessment is presented in the works of Alturkistani et al. [46], and Drissi & Benhadou [47], where the authors classified the current cloud risk assessment approaches into five and seven categories respectively. Our survey work differs from both works in that, while theirs provides an overview of cloud risk assessment models applicable to both customers and providers based on the assessment methods (i.e. quantitative, qualitative, graph analysis, hierarchical etc.), ours provides greater detail on cloud provisioning risk assessment models. We investigate models that are targeted at cloud providers to enable them to address the risks of designing, deploying, configuring, or managing the cloud.

3.1. Selection Method and Result

In this section, we examine a set of established service-driven conceptual models that can be used by CSPs' to assess cloud risk. To identify conceptual models proposed for the assessment of cloud provisioning risks which could also serve as a reference to the cloud community, we conducted a systematic review. We adopted a three-staged literature review process similar to that of Fernandez-Aleman et al. [48]. An overview of the review's main stages of our systematic review is presented in Figure 1.

Before beginning the search, we identified the eligibility criteria to include:

1. Articles published in English (CR1)
2. Articles on cloud risk assessment (CR2)
3. Articles proposing cloud risk assessment models for CSPs (CR3)

We considered only peer-reviewed articles, journals and conference proceeding, and limited our search to well-regarded online databases such as the IEEE Xplore, SpringerLink, ACM Digital Library, ScienceDirect, Elsevier and Google Scholar. Due to the nascent nature of cloud provider risk assessment and owing to the limited research in this area of cloud computing,

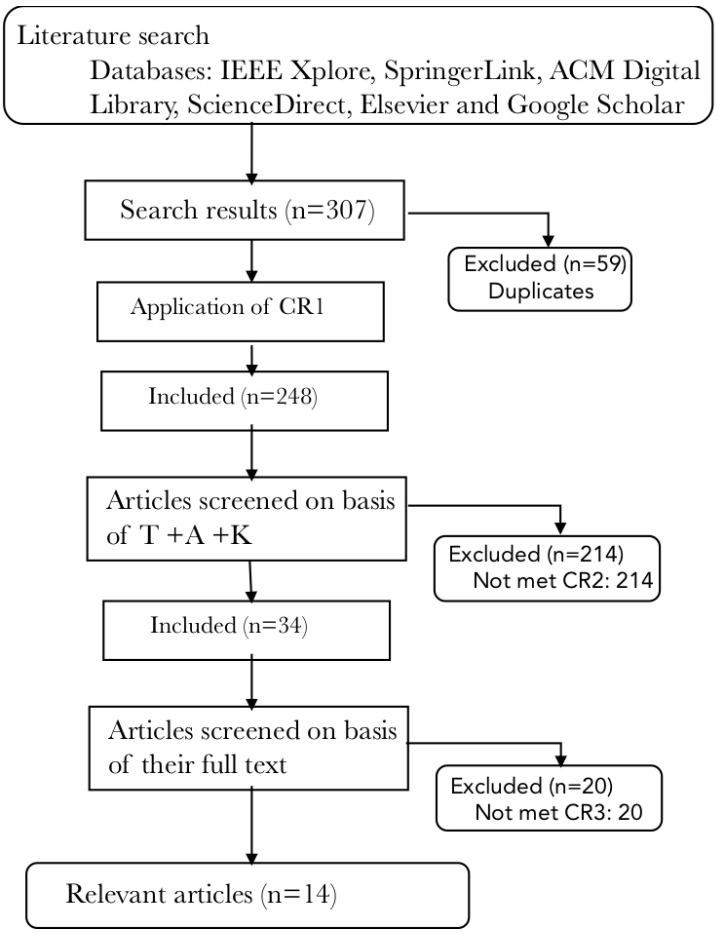

Figure 1: Flow Diagram of Inclusion/Exclusion and Literature Analysis Process

we narrowed our search to articles published between 2010 and 2018. The keywords used in our search criteria included "Cloud service provider risk assessment" OR "Cloud provider risk assessment" OR "cloud risk model" OR "Cloud risk assessment". We explored the title, abstract and keywords (T+A+K) of identified articles to determine their eligibility. Next, we carried out a partial or complete reading of the articles that had not been eliminated in the T+A+K stage, and in some cases scanned the reference list of the articles to discover new studies that satisfied our inclusion criteria.

A total of 14 articles were selected for this review. These were derived as follows. Through our database search using the predefined keywords, we

Table 1: Comparison of Cloud Risk Assessment Models (Proposed)

Author/ Year	**Cloud Risk Assessment Description**	**Method**	**Cope with dynamic cloud**	**Risk value**	**Use of Experts**	**Supply chain**
(Albakri et al., 2014)[31]	They proposed a model that considers both the cloud customer and the CSP during its risk assessment process.	Qualitative	No	Risk Matrix	No	Yes
(Chih-An & Huang 2015)[49]	Authors proposed an Adjustable Cloud Risk Assessment systeM (ACRAM) for CSPs and users. The tool assesses the risk of a cloud environment based on the historical or runtime software vulnerabilities of virtual machines or network devices.	Semi-quantitative	Partial	Risk Score	No	Yes
(Djemame et al., 2011) [42]	Risk assessment framework with methodologies for the identification, evaluation,mitigation & monitoring of cloud risks during the various stages of cloud provision.	Semi-quantitative	Partial	Risk Score	No	Yes
(Fito et al., 2010)[43]	A cloud risk assessment model for analysing the data security risks of confidential data. It prioritises cloud risks according to their impact on Business Level Objectives(BLO).	Semi-quantitative	No	Risk Score	No	No
(Liu & Liu, 2011)[50]	The model assesses cloud risks based on eight kinds of threats to security principles and their corresponding factors.	Qualitative	No	Risk Score	Yes	No
(Saripalli & Walters, 2010) [41]	A quantitative risk and impact assessment of cloud risk events based on six key security objectives.	Semi-quantitative	No	Risk Score	Yes	Yes
(Sendi & Cheriet, 2014)[10]	The model uses fuzzy multi-criteria decision-making technique to assess cloud risks. Linguistic variables are used to obtain expert opinions for weighting security risk criteria.	Quantitative	No	Risk Score	No	No
(Sivasubramanian et al., 2017)[11]	The model measures cloud risks in terms of impact, occurrence and disclosure, to arrive at a Risk Priority Number (RPN).	Semi-quantitative	No	Risk Score	No	No
(Zhang et al ., 2010)[51]	The framework was developed for a better understanding of critical areas in cloud computing environments and the identification and mitigation of cloud risks.	Qualitative	No	Risk Score	No	No

were able to identify a total of 307 studies/articles. Of these, 59 were first excluded as they represented duplicates of existing articles. Next, CR1 was applied, and all of the 248 articles passed this criterion. The T+A+Ks of the remaining 248 articles were then examined, and 214 of these were discarded because they did not meet criterion CR2. While most of them contained elements of cloud risk assessment, it was not the core area of the study. The remaining 34 studies were examined in greater detail, based on partial or full reads of their text. Of the 34 articles, 20 were excluded for not meeting criterion CR3. Some of the articles excluded in the final phase of the review included that of Cayirci et al. [8], Islam et al. [9], and Tang & Liu [29]. While they discussed cloud risk assessment in great detail, they only concentrated on cloud consumer risks.

In Table 1, we present a cross-section of proposed cloud risk assessment methods applicable to CSP risks, highlighting their assessment method, use of experts and evaluation of supply chain. The choice of these criteria for comparison is based on the existing gaps in the use of traditional risk assessment frameworks to assess cloud risks. The criteria can be further described as follows:

- **Assessment Method** – This highlights the risk assessment method adopted by the model, i.e. Quantitative, Qualitative or Semi-quantitative.
- **Cope with Dynamic Cloud** – This assess the model's ability to cope with assessing the ever-changing risks of the dynamic cloud infrastructure.
- **Risk Value** –This identifies the format in which the risk value is presented to decision-makers, e.g. risk score, risk matrix or monetary value.
- **Use of Experts** – This considers whether the model requires the participation of external risk experts during the risk assessment exercise.
- **Supply Chain Inclusion** – This assesses if the model considers the supply chain in its risk assessment steps, e.g. involving customers or providers in risk identification and estimation.

With these criteria, we expect to gather key characteristics of each model.

3.2. Limitations and Gaps

The amount of research into the assessment of cloud provisioning risks is limited. Examination of the literature relevant to cloud risk assessment so far has identified that there is more research into cloud consumer risks [52, 53, 9, 54], compared to cloud provider risks. The lack of studies targeted at assessing cloud service provision risks has also resulted in less agile cloud environments [55]. While all of the models described in Table 1 were developed in the cloud era, their principally traditional approach to risk assessment, application of qualitative methods, and the limited knowledge of the ToA make them unsuitable for measuring cyber risk in dynamic cloud environments. According to Sendi & Cheriet [10], applying qualitative models which lack granularity and objectivity to assessing cloud risks is a challenging undertaking, due to the lack of trust in CSPs and limited visibility of security control.

Similarly, none of the models presented in Table 1 estimated the value of a cloud risk in monetary terms, which according to Freund & Jones [56], is known to promote cost-effective risk mitigation and optimal risk prioritisation. Also, we see that the majority of the models adopted a silo (traditional) approach to assessing risks (i.e. limiting the assessment to the focal CSP) [2]. Considering that CSPs rely on a dynamic and complex supply chain, where the perceived level of the security risk of the cloud service increases with each additional component integrated into the offering, a supply chain inclusive approach would be valuable [7, 55]. It would have been fitting for the model to assist the CSP to understand the vulnerabilities each component supplier introduces to the cloud service. This remains a gap with provider-based risk assessment, and in our bid to address it, we proposed the CSCCRA model [17].

4. Systematic Evaluation of CSCCRA with other Conceptual models

In this section, we systematically evaluate three other conceptual models that have been proposed to address cloud service provision risks, comparing them with the CSCCRA model. To determine which of the models identified through our literature review in section 3.1 will be most suitable for this evaluation, we defined two new criteria. First, it was important that the selected model included information on the parties involved in the development, hosting, management, monitoring or use of the cloud services

(i.e. the supply chain); this criterion was necessary to ensure the selected models were inclusive in their assessment of cloud provisioning risks and did not just concentrate on the focal CSP. Second, we were interested comparing our proposed model with established models that had a good citation record and their risk assessment approach aligned with information security standards. Three of the models listed in Table 1 met these criteria and they are CSPRAM [31], QUIRC [41] and OPTIMIS [42].

To begin our evaluation, we describe the CSCCRA giving details on its components and risk assessment process. Next, we provide a brief description of the three other conceptual models. Consequently, we compare each model with the CSCCRA highlighting their goals, risk assessment process, decisions, assessment scope, and risk conceptualisation (see Table 8).

4.1. CSCCRA Model

Seeing that the challenge of cloud risk assessment can be summed up as the application of mental models which are static, narrow and reductionist, the CSCCRA model adopts a systems thinking approach to assessing cloud risks [36]. The model takes a multi-disciplinary approach to assessing the dynamic, evolving and interconnected risks in the cloud, applying different knowledge areas in the identification, analysis, and evaluation of these risks [17]. It combines factors such as security, supplier selection, systems thinking, decision support systems, quantitative risk modelling, and supply chain mapping in a multi-stage approach. The structured approach of CSCCRA allows for a more exhaustive analysis of cloud risk through the identification of the various components that make up a cloud service and the evaluation of their impact when assessing the risk of the cloud service. CSCCRA also enables the risk assessor to focus on critical components of a cloud service and evaluate them for technology weakness as part of the risk assessment process.

The CSCCRA model builds on existing risk assessment standards and guidance documents such as ISO/IEC 27005:2011 [4], NIST 800-30v1 [20], ISO/IEC 31000:2009 [57] and Factor Analysis of Information Risks (FAIR) methodology [56, 58]. The model is made up of three components [17]:

1. Cloud Quantitative Risk Analysis (CQRA)
2. Cloud Supplier Security Assessment (CSSA)
3. Cloud Supply Chain Mapping (CSCM)

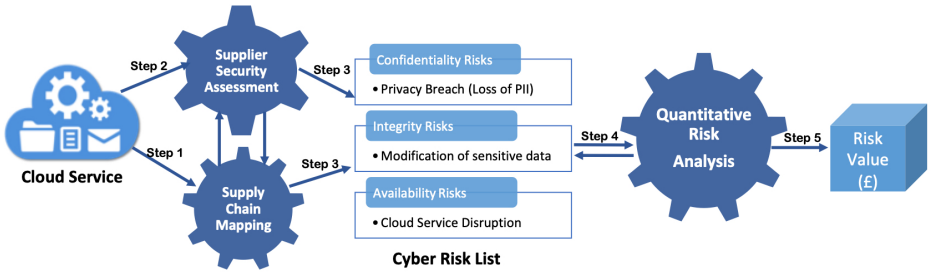

Figure 2: Overview of the CSCCRA Model

The CSCCRA steps for assessing cloud provisioning risks are as follows and as shown in Figure 2:

1. Decompose the cloud application into its component services and map out the supply chain.

2. Assess the security of the supplier of each service component using a multi-criteria decision support system.

3. Identify the weak link(s) within the chain and draw a comprehensive list of cloud security risks.

4. Stakeholders within the CSP make reasonable estimates of risk factors.

5. Input risk factor estimate to CQRA simulation tool, to arrive at the risk value in monetary terms.

The primary goal of the CSCCRA model is to be used by CSPs in the identification, analysis, and evaluation of cloud risks based on the dynamic supply chain. The CSCM and CSSA tools are to be used by CSPs in conducting enterprise-wide socio-technical assessments of the cloud services' supply chain and in the process, identify suppliers with weak security controls or processes. The result of these processes provides the CSP with an increased knowledge of their security weakness and assists them in drawing up a comprehensive list of risks to the cloud service, which are evaluated quantitatively and the result presented in dollar value. The visualisation techniques employed in the CSCCRA simplifies the detection of weak spots within the supply chain during risk identification, evaluation and prioritisation processes.

The use of the model is not heavily reliant on expert's experience or intuition. To assess a cloud service, the CSP establishes the context of the

assessment, which includes identifying the ToA (cloud service), evaluation criteria, duration of the exercise, and initial security concerns. We now describe the three main components of the CSCCRA model.

1. ***Cloud Supply Chain Mapping:*** Using the CSCM, the risk assessor through the help of the CSP decomposes a cloud service into its component services (managed by different suppliers), and creates a comprehensive map of the different tiers of suppliers for the cloud service, beginning with the Level 1/Tier 1 suppliers. The team gains an understanding of the cloud service data flow, components and the list of stakeholders. This process enables the risk assessor to visualise the cloud service through the lens of its supply chain, identifying its vulnerabilities, hidden dependencies, and critical suppliers who might exist as a single point of failure (SPOF). The process of graphically representing the inherent risk in the supply chain also helps to counter any documented biases and increases the justifiability of the risk evaluation results, making it easy to understand, and provides a basis for making the risk assessment a transparent and collaborative process.

2. ***Cloud supplier security assessment:*** The CSSA allows the CSP to assess the cybersecurity posture of cloud suppliers. Using the CSSA tool, the CSP evaluates each supplier's security posture based on a combined implementation, effectiveness and impact metric. Being a Multi-criteria security assessment tool, the CSSA presents a consistent approach to assessing and comparing cloud suppliers based on 52 security criteria grouped into nine (9) security target dimensions which were achieved through Delphi study with cloud experts [55] (see Figure 3). The CSSA tool is based on Dawes's z-score method of unit-weighted regression. Our choice of this approach is influenced by the research of Dawes et al. [59], which showed that the unit (equal) weights of variables could yield predictions that correlate highly with optimally weighted composites if the direction (+1 or -1) in which each predictor is related to the criterion is known.

    - Availability of Service (AoS)
    - Data & System Hosting (DSH)
    - Data Security Controls (DSC)
    - Maturity of Security Assessment process (MSA)

- Maturity of Operational Security (MOS)
- Security Governance and Compliance (SGC)
- Identity and Access Management (IAM)
- Encryption & Key Management (EKM)
- Application Security (AS)

Assessing suppliers based on these security dimensions assist CSPs in the identification of weak suppliers readily susceptible to a cyber attack or those with a high risk of failure. Improving the risk assessment process with this identification of potential weak spots in the supply chain also helps to capture the vulnerabilities of the cloud service and promote proactive mitigation of risks.

3. ***Cloud quantitative risk analysis:*** The third and final component of the CSCCRA model is the risk analysis tool. With uncertainty being a primary factor in risk analysis, the CQRA makes use of a probabilistic estimate of risk factors, e.g. threat frequency, vulnerability and impact, and represents stakeholder estimates as a probability distribution (e.g. PERT, Poisson). We chose to represent experts' estimate of the probability of risk and impact factors with the Program Evaluation Review Technique (PERT) continuous probability distribution because studies have shown that in situations where there is a lack of real data, it is safe enough to assume that the variable of interest follows a normal distribution [56, 60]. Likewise, we adopted the Poisson distribution for the attack frequency factor, since this distribution expresses the probability of a given number of events occurring within a fixed time, with a known average rate, where the occurrence of events are independent of one another [61]. These estimates are then run through a Monte Carlo simulation engine using different scenarios to arrive at a reasonable estimate of the risk. The Monte Carlo simulation is a computerised mathematical technique that allows people to account for risk in quantitative analysis and decision making. It is a stochastic modelling tool based on a computerised mathematical technique and is used to provide estimates for complex problems where there are significant uncertainty [56, 60].

   Applying quantitative methods to risk analysis is suitable for the decomposition of risk into its various risk variables, as it takes away part

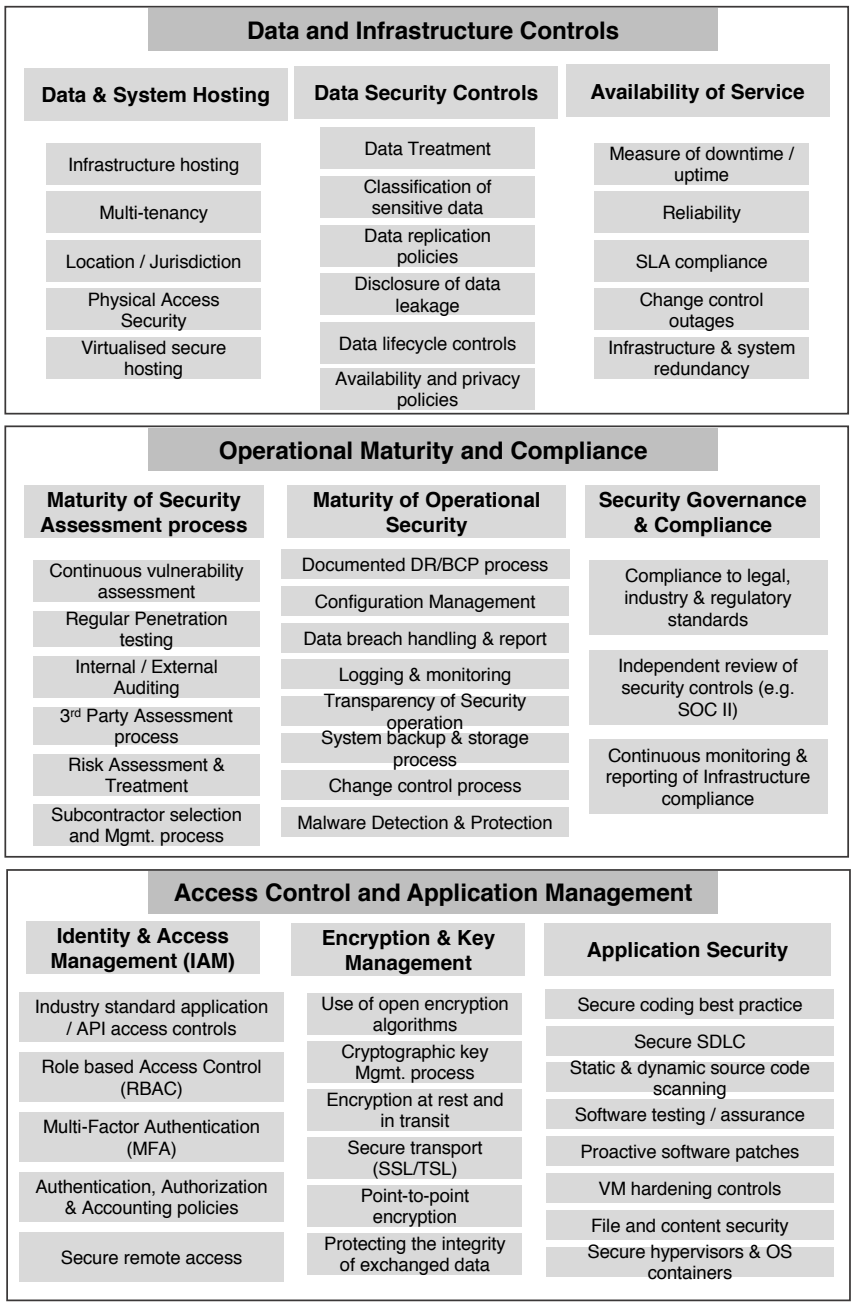

Figure 3: Target security dimensions for assessing cloud suppliers [55]

> of the subjectivity of the risk estimates. While we are conversant with the argument against quantitative risk analysis, primarily as relating to the lack of reliable data, complexity of computation, duration of exercise and the lack of efficiency [2], we maintain that the quantitative method is more applicable to cloud risk assessment. Its use of a rigorous data-driven process allows for a deeper understanding of the inter-connectedness of cloud risks. Furthermore, we argue that the application of quantitative simulation to reasoned risk factor estimates made by a properly calibrated expert team combined with appropriately communicated assumptions will yield realistic risk values [56, 62].

Within the CSCCRA model, stakeholders estimate the values of each of the risk factors according to their knowledge of the cloud service. Despite the lack of historical data, the CSCCRA increases the objectivity of expert estimates through the *use of controlled experimentation, clearly defined model, peer reviews and calibration of the experts* [56, 62]. Before each assessment, experts are given a short calibration exercise to prepare them for making reasoned estimates about the risk factors identified during the assessment. Factors such as the probability of a threat occurrence are estimated twice (i.e. with or without security controls), while the estimation of the impact of a threat source considers different criteria ranging from lost revenue from operational outages to loss of customer market share, or loss of reputation. Combining these expert estimates, summarises the accumulated information and enables the risk assessor to present condensed information to decision-makers [63].

The application of the CSCCRA model to cloud risk assessment also helps to decompose cloud risk data into a clear, observable and useful format. Its quantitative approach also provides a better platform for risk analysts to defend their result and explain the rationale behind it, thus helping decision makers to trust the analysis process and its suggestions of risk mitigation strategies. While the model is currently targeted at cloud service providers (particularly Software-as-a-Service (SaaS)), its iterative, inclusive and rigorous approach makes it applicable to assessing the risks of many composite services. Our primary targets are SaaS providers because studies have shown that at least 80% of a typical SaaS application is made up of assembled parts, with each component representing a different level of risk [64]. SaaS applications, therefore, presents an excellent scope for our work, seeing that the more the components combined to deliver a SaaS service, the supposed in-

crease in the risk of the service and the higher its dependence on the supply chain.

4.1.1. Sample Risk Assessment with CSCCRA model

To illustrate the steps of the CSCCRA model, we present an abridged version of a real-world case study where the model was used to assess the risk of a SaaS Service. For confidentiality reasons, we refer to the case organisation as CSP-B. CSP-B hosts and manages an asset tracking application (CSP-B-SaaS) used by organisations to remotely manage the inventory of their PCs, servers, network and internet-of-things (IoT) devices. In the following steps, we are going to apply the components of the CSCCRA model in assessing the risks of the SaaS application.

- **Step 1 - Supply Chain Mapping:** In complying with our assessment framework, we decompose CSP-B-SaaS into its component services, while also identifying their suppliers and service category, their criticality, and the data storage or processing responsibilities of the supplier (see Table 2). We leveraged technology lookup websites such as builtwith.com [65] and Google to gather additional data on the lower tiers of the supply chain, identifying the providers used for the Infrastructure hosting, Domain Name System (DNS) and Identity and Access Management (IAM) etc. The resulting map (see Figure 4) provides a comprehensive view of the supply chain, which assists CSP-B in assessing the criticality, threat and vulnerabilities of their direct and indirect suppliers.

  Visualising a supply chain helps to detect convergence risks, where a critical supplier in the second, third or fourth tier could represent a single point of failure for multiple components of the cloud service. Figure 4 provides a visualisation of CSP-B-SaaS supply chain and identifies SPOFs within the chain. One of the suppliers that immediately stands out is IaaS-Pro-B, the infrastructure provider for CSP-B, who also provides infrastructure and/or hosts data for all other suppliers involved in the delivery of CSP-B-SaaS. Here, we see that the use of mapping tools to illustrate the interdependencies between the components helps to visualise the cloud information flow and promotes transparency, thereby assisting CSPs to implement controls proactively.

- **Step 2 - Supplier Assessment:** Following the supply chain mapping, the stakeholders appraise the security posture of CSP-B-SaaS's supply

Table 2: CSP-B Supplier list

Anonymised Supplier	Component	Service Category	System Criticality	Data Proce-using (Y/N)	Data Stora-ge (Y/N)
Serv-Desk-Pr-B	Service Desk	Application	Not Critical	Y	Y
CSP-B	*SaaS Integration/ Software development*	*Application/ Platform*	*Critical*	*Y*	*Y*
Code-Repo-Pro-B	Code Repository	Application	Not Critical	N	Y
PAM-Pro-B	Privileged access management	Application	Critical	Y	N
IaaS-Pro-B	Database, IaaS, DNS, Backups	Infrastructure/ Application	Very Critical	Y	Y
AD-SaaS-Pr-B	Active Directory	Application	Critical	N	Y
IAM-Pro-B	Identity Management	Application	Very Critical	Y	N
Perf-Mon-Pro-B	Application Performance Management	Application	Not Critical	Y	Y
MFA-Pro-B	Multi-Factor Authentication	Application	Critical	Y	N
Log-Pro-B	Log Management	Application	Not Critical	Y	Y

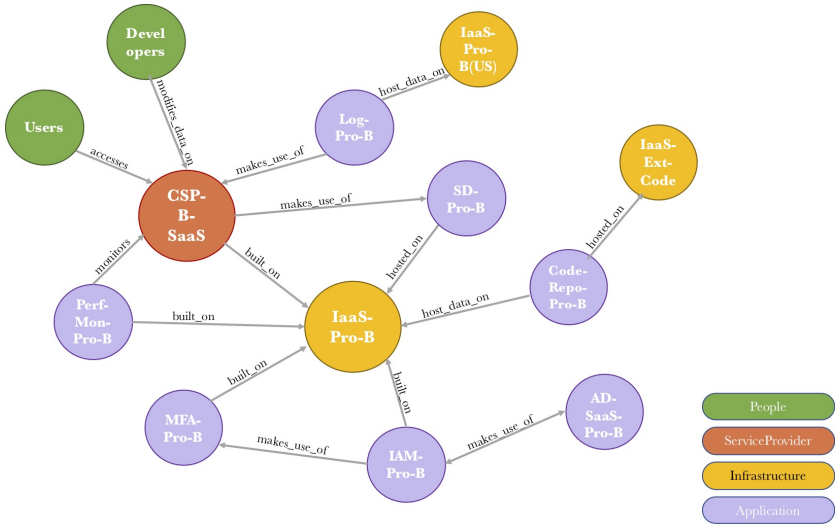

Figure 4: Supply Chain mapping of CSP-B-SaaS using the CSCM tool

chain, to identify suppliers who based on their lack of transparency or limited security control implementation, could be referred to as weak links. The process facilitates the conduct of comprehensive due diligence on the security controls of the CSP's suppliers. Assessing the security processes of suppliers makes the stakeholders investigate their supplier controls such as personal data encryption, data breaches detection & communication, data storage and location, and how supplier's use of sub-processors impact these controls.

Table 3 presents the participants' assessment of each supplier's security posture. The CSP stakeholders score each component supplier based on the nine security target dimensions on a scale of 1(least secure) to 10 (most secure). A z-score is calculated for each target dimension, and the z-scores are summed up in the last column. The z-score (Z_i) is a statistical measurement of a score's relationship to the mean in a set of scores. It measures how many standard deviations (σ), a score (y_i) is above or below the population mean (y) [66]. The power of the z-score lies in the appropriate integration of distinct dimensions weighted to form a single performance measure. Formally, the score can be defined as follows:

$$Z_i = \frac{(y_i - y)}{\sigma} \tag{1}$$

So, the combined z-score (CZ-score) for a supplier, e.g. IAM-Pro-B, is a summation of the suppliers' z-score for each of the nine security factors and is depicted as follows:

$$CZ\text{-}score = \sum_{i=1}^{9} Z_i \tag{2}$$

The use of colour and values are considered as suitable methods for communicating information in a visual framework [67]. The colour in each of the cells in the last column of Table 3, conveys the degree of risk that particular component has, comparative to the rest of the chain. A green cell has the best risk score (least risky), followed by yellow and then red.

As shown in Table 3, Perf-Mon-Pro-B was assessed to be the weakest link in this supply chain, followed by CSP-B themselves, and then

Table 3: Assessing CSP-B Supplier list using CSSA

Anonymised Supplier	**AoS (1 -10)**	**DSH (1 -10)**	**DSC (1 -10)**	**MSA (1 -10)**	**MOS (1 -10)**	**SGC (1 -10)**	**IAM (1 -10)**	**EKM (1 -10)**	**AS (1 -10)**	**Combined Z-Score Value**
Service-Desk-Pro-B	9	9	7	9	10	10	9	8	9	-0.43
CSP-B	*8*	*7*	*8*	*8*	8	*5*	*9*	*8*	*6*	*0.63*
Code-Repo-Pro-B	8	9	9	10	9	9	9	8	9	-0.34
IaaS-Pro-B	9	9	9	9	8	10	10	9	8	-0.69
AD-SaaS-Pro-B	9	9	9	9	9	10	10	9	8	-0.78
IAM-Pro-B	8	6	7	10	9	10	10	9	9	-0.25
Perf-Mon-Pro-B	9	9	5	7	6	7	7	8	3	1.02
MFA-Pro-B	8	8	8	7	7	7	9	9	6	0.39
Log-Pro-B	8	9	8	8	7	7	8	8	7	0.46

Log-Pro-B. For the performance monitoring provider, they scored low on data security controls (DSC) and application security (AS), because they provided limited information on their website on the implemented controls that assure these factors. Although they provided more information on their Cloud Security Assurance's (CSA) Consensus Assessments Initiative Questionnaire (CAIQ) self-assessment report [68], much of the information was referencing the controls in place at their hosting provider (IaaS-Pro-B). Likewise, Perf-Mon-Pro-B scored the lowest score for AS, and this was due to the basic level of protection they had in place for virtual machines and the limited information on their coding practices, which they claim to be proprietary. CSP-B, despite their detailed and secure architecture, scored low in security governance and compliance (SGC), due to their reliance on suppliers for the compliance of their service. Some other suppliers had traditional security measures in place, which in the face of changing risk landscape and growing sophistication of attackers, was judged insufficient.

The need for CSPs to search through online resources and in-house documentation for supplier controls and processes, and the need for stakeholders within a CSP organisation to discuss their controls and identify weak spots are some of the benefits of the supplier assessment process.

- **Step 3 - Risk Identification:** In this phase, the participants build on the results of the supply chain mapping and supplier security assessment, to identify the weak areas the SaaS platform and identify rele-

vant vulnerabilities, threats and probable risk events. Table 4 presents CSP-Bs risk register with the top ten risks identified in the course of the exercise. The register includes a short description of each risk, the asset at risk, suppliers involved, vulnerability, threat agent and type, and available control. The threat, vulnerability, asset taxonomy complies with ENISA's method of structuring risk information [8, 69].

- **Step 4 - Risk Factor Estimation:** Following the identification of their top ten cloud risks, CSP-B stakeholders are given a short calibration exercise on how to estimate risk factors using confidence intervals (CI). Uncertainty is inherent in the evaluation of risk, due to the imperfect or incomplete knowledge of the threat, the ever-increasing discovery of vulnerabilities and the unrecognised dependencies that can lead to unforeseen impacts [20]. Therefore, for each risk item, the CSCCRA model expresses the participants' degree of uncertainty quantitatively using probability distributions. Each of the factors (Probability with controls (PwCE), Probability without controls (PwoCE) and Impact cost) are represented by a PERT distribution, where the assessors are required to provide estimates to a 90% CI, i.e. lower bound (5%), most likely, and upper bound (95%) estimate of the factors. A Poisson distribution is used to represent the frequency (freq) of attack since it expresses the probability of a given number of events occurring within a fixed time. Acknowledging our inability to eliminate risks, we settle for pragmatically reducing uncertainty around risk events and having enough information to mitigate the top risks.

- **Step 5 - Risk Value Calculation:** The CQRA tool is used to combine stakeholders' estimation of the various risk factors and compute the risk value. The lower bound, most likely and upper bound risk factor estimates of each of the experts (Exp) is combined as shown in *equations 3 to 6*. After which, we generate a discrete distribution based on each expert's estimates and the weighting of their opinion, using the Monte Carlo Simulation tool. As shown in Table 5, we calculated two sets of risk values, one with controls and the other without controls, based on the combined stakeholder estimates for each scenario. This risk value calculation then informs our estimated risk value based on existing controls. For this case study, the estimated value of the identified risks ranged from £90 to £36,357, which represents between 65%

Table 4: List of Security Risks identified by the CSP-B Stakeholders

Risk No	Risk Description	Asset at Risk	Supplier	Vulnerability Name	Threat Agent	Threat Type	Security Effect	Existing Controls
R1.	Disgruntled employee disrupts CSP-B-SaaS by polluting or corrupting critcal data	Database, Source code	IaaS-B-Pro, CSP-B	Application/Platform vulnerability, System or OS vulnerabilities, Unclear roles and responsibilities, Poor integrity or backup controls	Privileged Insider	Sabotage, Data Loss/Manipulation, Website defacement	Integrity, Availability	Backup, privileged management (PAM), Logging, HR Termination process & Employment screening
R2.	Accidental misconfiguration of access control exposes CSP-B-SaaS data	Customer PII in DB and AD, Intellectual Property (IP)	CSP-B, Code-Repo-Pro-B, IaaS-Pro-B	Insufficient IAM controls, Poor key management, Weak encryption, Non-optimal change control, Unavailable or misconfigured security controls, shared platform vulnerabilities	Accidental Insider	Information/Data leakage, Service outage, Data Loss /Manipulation, Loss of governance	Confidentiality, Integrity	Backup, Logging, Awareness and Training, Penetration testing
R3.	Malicious/accidental attack of privileged access control locks out CSP-B-SaaS Admin	Privileged Access Management	PAM-Pr-B, CSP-B	Application/platform vulnerability, Failure of configuration management, system or OS vulnerabilities	Accidental Insider, Malicious Outsider, Privileged Insider	Sabotage, Lock-in, Loss of governance	Availability	Penetration testing, MFA, Backup, Code repository
R4.	Compromise of IAM-Pro-B facility to obtain privileged access to CSP-B-SaaS	Identity & Access Mgmt, Database	IAM-Pro-B, CSP-B	Insufficient IAM controls, shared platform vulnerabilities, Weak authentication mechanism, Insiders on provider side, hidden application dependency	Malicious Outsider, Political	Malicious Probes or scans, Cross-site scripting, Social Engineering, Management interface compromise, Lock-in	Confidentiality, Integrity, Availability	MFA, Third party supplier selection, Logging
R5.	Malicious outsider inserting malware into CSP-B-SaaS code repository	Code repository (IP)	Code-Repo-Pro-B, CSP-B	Insufficient IAM controls, Failure of configuration Mgmt, shared platform vulnerabilities, Unavailable or misconfigured security controls, lack of monitoring mechanism	Malicious Outsider	Sabotage, Data Loss/ Manipulation, Loss of governance	Integrity, Availability	Change (+release) process, code scanning
R6.	Non targeted DDoS attack affecting Asset tracking SaaS	CSP-B-SaaS (front -end, Database)	CSP-B, IaaS-Pro-B	Inadequate resource provisioning, Limited redundancy, multi-tenancy, Bandwidth under-provisioning, Lack of resource isolation, Lack of supplier redundancy	Malicious Outsider, Political , Environmental	Malicious Probes or scans, Denial of Service, Fraudulent resource consumption attack	Availability	N/A (rely on supplier controls)
R7.	Loss of customer PII due to inadequate security controls	Service Desk, Database, Active Directory	Service-Desk-Pro-B, IaaS-Pro-B, AD-SaaS-Pro-B, CSP-B	Insufficient IAM controls, Weak encryption, Non-optimal change control, weak physical security measures, Unclear roles& responsibilities	Malicious Outsider, Privileged Insider	Information/Data leakage, Social Engineering, Brute force and Dictionary attacks, Data Loss/Manipulation, Loss of governance	Confidentiality	PAM, MFA, Logging
R8.	Service outage due to vendor supply chain failure affecting CSP-B-SaaS	AD, Database, IAM, CSP-B web fronted	AD-SaaS-Pro-B, IAM-Pro-B, CSP-B	limited redundancy, system or OS vulnerabilities, Poor provider selection, Lack of supplier redundancy, hidden application dependency	Environmental, Accidental Insider	Service outage, Supply chain failure	Availability	Supplier Selection
R9.	Data Breach of customer PII data	Database, Active Directory	AD-SaaS-Pro-B, IAM-Pro-B, CSP-B	Insufficient IAM controls, Failure of configuration management, Unavailable or misconfigured security controls, insecure systems database	Privileged Insider	Information/Data leakage, Data Loss/Manipulation, Supply chain failure	Confidentiality, Reputation	Encryption, PAM, Incident management, Logging (SIEM)
R10	Leakage of admin credentials including second factor	IAM, PAM	CSP-B, IAM-Pro-B, MFA-Pro-B	weak physical security measures, Training and awareness	Malicious Outsider, Insiders	Non-compliance, Abuse and Nefarious use of cloud service, Data Loss/Manipulation, Information/Data leakage	Confidentiality, Reputation	Least Privilege, RBAC

to 95% percentile of the risk value continuum. The risk value is calculated based on *equations 7 & 8,* where ERV_WC is the estimated risk value with controls, and ERV_WoC is the estimated risk value without controls.

$$Exp_nPwCE = RiskPert(LB_n, ML_n, UB_n) \tag{3}$$

$$Exp_nPwoCE = RiskPert(LB_n, ML_n, UB_n) \tag{4}$$

$$Exp_nImpact = RiskPert(LB_n, ML_n, UB_n) \tag{5}$$

$$Exp_nFreq = RiskPoisson(Mean) \tag{6}$$

$$ERV\_WC = Impact * Freq * PwCE \tag{7}$$

$$ERV\_WoC = Impact * Freq * PwoCE \tag{8}$$

4.1.2. Merits of the CSCCRA model

The structured and systematic approach of the CSCCRA to assessing cloud provider risks yields objective and defensible risk assessment results. Its use of the CSCM to identify the components of a cloud service and their corresponding suppliers helps to present stakeholders with complex supply chain information using maps. The CSSA component of the model is a supplier rating service, which uses a multi-criteria decision-making method to rank suppliers cybersecurity posture [70]. The CSSA is designed to bring transparency to the security risk rating of cloud suppliers, providing a quantitative measurement of security performance across the chain, identifying the inherent risks and comparing suppliers based on their cybersecurity posture. The risk analysis phase allows multiple stakeholders to participate in risk identification, estimation and evaluation process and presents cloud risk values in monetary terms to promote optimum and effective decision-making. According to Keyun [2], the economic implications of cyber risk have to be quantified in monetary value for cyber risk management to transform from a compartmentalised technical issue into a business issue.

Table 5: CSP-B Risk Analysis result based on CQRA calculation

Risk No	Probability of occurrence (without control)			Probability of occurrence (with control)			Impact Cost Estimate (£)			Frequency (per year)	Risk Value (£) Estimates (without controls)			Risk Value (£) Estimates (with controls)			Estimated Risk Value (£) based on Existing Controls
	LB	ML	UB	LB	ML	UB	LB	ML	UB		LB	ML	UB	LB	ML	UB	
R1.	3.80%	11.03%	23.86%	2.59%	5.17%	9.00%	£15,302.00	£253,982.75	£851,633.99	0.71	£0.00	£20,886.11	£106,279.92	£0.00	£9,418.21	£49,919.98	**£36,357**
R2.	6.12%	11.79%	19.01%	3.44%	6.07%	9.87%	£4,834.60	£35,125.95	£78,186.20	0.23	£0.00	£1,001.42	£6,530.93	£0.00	£523.72	£3,362.18	**£2,039**
R3.	1.33%	4.35%	7.39%	1.37%	2.57%	3.95%	£857.32	£7,396.28	£20,710.54	0.08	£0.00	£25.80	£145.73	£0.00	£14.90	£90.48	**£90**
R4.	3.00%	7.31%	12.36%	2.01%	4.30%	7.05%	£41,352.19	£390,737.32	£996,565.61	0.05	£0.00	£1,627.97	£3,189.58	£0.00	£989.64	£2,108.03	**£2,108**
R5.	5.50%	10.44%	15.66%	1.79%	3.64%	6.83%	£23,7999.61	£273,549.06	£807,160.17	0.06	£0.00	£1,627.90	£5,031.18	£0.00	£592.05	£1,547.85	**£1,627**
R6.	3.87%	8.35%	12.72%	2.62%	7.90%	12.73%	£276.28	£4,408.03	£14,537.86	0.35	£0.00	£129.51	£778.49	£0.00	£122.87	£725.48	**£778**
R7.	6.12%	10.24%	15.11%	2.85%	5.20%	7.84%	£12,004.97	£131,768.82	£623,029.49	0.17	£0.00	£2,322.46	£7,425.09	£0.00	£1,142.07	£3,952.33	**£1,667**
R8.	5.53%	10.71%	16.59%	5.53%	10.70%	16.57%	£1,745.41	£8,835.75	£19,533.57	0.23	£0.00	£225.57	£1,306.26	£0.00	£222.60	£1,289.76	**£1,306**
R9.	6.08%	10.26%	15.39%	2.79%	5.47%	8.76%	£12,101.94	£133,537.78	£625,461.21	0.17	£0.00	£2,329.39	£8,510.21	£0.00	£1,235.80	£4,549.27	**£4,549**
R10.	2.98%	5.32%	7.93%	2.01%	4.49%	7.60%	£8,995.93	£115,822.80	£323,703.30	0.08	£0.00	£524.29	£3,211.94	£0.00	£444.84	£2,535.47	**£3,211**

The novelty of the CSCCRA is that it is an effective and efficient cloud risk assessment framework which provides visibility into the supply chain and supports comprehensive risk identification, analysis, evaluation and a cost-benefit analysis for security control implementation. It fills the supply-chain and uncertainty quantification gaps of both the generic and domain-specific risk assessment frameworks.

4.2. QUIRC

Saripalli et al. [41] proposed the quantitative risk and impact assessment framework (QUIRC) model for assessing security risks associated with cloud computing platforms based on six key security objectives (SO): confidentiality, integrity, availability, multiparty trust, mutual auditability and usability. The proposed model is based on the premise that most of the typical attack vectors and events, map to one of these six categories. With the model being semi-quantitative, the authors maintain that their approach enables stakeholders to comparatively assess the robustness of different cloud offerings in a defensible manner.

The steps taken to assess cloud risks with QUIRC requires a trained team to perform risk estimations. The risk assessment process is divided into two phases: impact assessment and probability assessment. The impact assessment employs a wide-band Delphi method [71] in collecting external experts' estimate of the impact (I) of a threat to a security objective. This approach is suggested as a scientific method of ensuring that there is a consensus among the expert team on the estimate of impact values. Also, due to the lack of historical data on cloud outages, QUIRC relies on security reports (e.g. SANS Institute report [72]) in an attempt to evaluate the probability (P) of threat events.

QUIRC defines risk as a product of the Probability (Pe) of a security compromise, i.e. a threat event, e, occurring, and its potential Impact Ie, where Ie is assigned a value on a numerical scale based on the Federal Information Processing Standards (FIPS) model [73] of Low (1-5), Moderate (6-10) or High (11-15). The calculation of the risk of an application based on a single security objective is represented by Rs, which is the average over the cumulative weighted sum of n threats which map to a particular SO category.

$$R_s = \frac{1}{n} \sum_{i=1}^{n} P_e I_e \tag{9}$$

So for example, in assessing the risk of a cloud service, let us assume that three threat events were identified and they all related to the confidentiality SO, i.e. cross-site scripting (XSS) attack, malicious access to API keys, and man-in-the-middle attack. These threats were estimated to have impact (I) values of 3, 7, 10, and the probability (P) of their occurrence are 0.08, 0.1, 0.24. Therefore, the risk value for the cloud system under the confidentiality SO would be [0.08(3) + 0.1(7) + 0.24(10)]/3 or **1.11**. Due to the combined value of risk under the same SO, the confidentiality risk of the cloud service will be classed as a low risk, seeing that it is far below the maximum potential risk value of [1.00(10) + 1.00(10) + 1.00(10)]/3 or **10**.

Furthermore, the net security risk (R) for the cloud application will be represented below as the weighted average of the risk calculated for the CIAMAU objectives.

$$R = \sum_{s=1}^{6} w_s R_s \tag{10}$$

where the ws for the CIAMAU SOs could have values similar to [0.3, 0.1, 0.1, 0.2, 0.1, 0.2].

In summary, the RA steps identified in the QUIRC model promote communication on risk factors between external experts and internal stakeholders. The model also enables CSPs to consider how identified threats, impact business objectives. The QUIRC is adaptable, and its use can be extended beyond cloud computing to other IT and technology industries, where there is access to subject matter experts (SMEs) and industry-specific knowledge-base. However, its use of a Delphi method for impact estimation is bound to slow down the risk assessment process, and the ability of the CSP to adapt to risks in the dynamic cloud. It is easy to see RA exercises taking over a month to complete since issues relating to expert consensus, and expert/ stakeholder availability need to be considered. Also, the QUIRC model fails to consider the direct and indirect consequences of an impact from their suppliers.

4.3. CSPRAM

In [31], Albakri et al. proposed a security risk assessment method for cloud computing environments. This framework contains several components including a cloud service provider risk assessment manager (CSPRAM). It is designed to be used by CSPs in assessing the security risks in their cloud computing environment and is complemented by the inclusion of customers' evaluation of security risk factors [31]. This study addresses the challenge of

defining the risk criteria according to the organisation's security objectives and considering these criteria when evaluating the value of a risk event. The model also includes cloud customers (CC) in the risk assessment process. The inclusion of customers is limited to processes that define the security risk factors, such as asset value, the likelihood of a threat, vulnerability, and impact of the incident, as well as determining the legal and regulatory framework. However, the authors maintain that including all CCs can quickly become unmanageable if all their objectives are included in the risk evaluation.

The CSPRAM model follows the ISO/IEC 27005 standard in defining its main risk assessment steps. The authors defined risk as a combination of the likelihood of a threat and the impact of the incident. The framework is made up of two main parts: The CSP and CC assessments. It attempts to achieve a balance between the *realistic result* obtained from the contribution of the customer, and the complexity of the risk assessment process due to the inclusion of the CC. The risk analysis phase takes into consideration the information provided by the CC and CSP's knowledge of their threats, vulnerabilities and controls. Subsequently, the CSP determines the risk level based on the likelihood of the incident scenario and its consequences and compares the risk levels with the risk evaluation and risk acceptance criteria set at the beginning of the process, producing a prioritised list of risks.

CSPRAM is designed to assess the risk of a cloud service (particularly Software-as-a-Service), and it uses a risk analysis matrix for rating risk factors. The range of both likelihood and business impact are: very low, low, medium, high, and very high. The combination of likelihood and impact values is represented on a risk scale that ranges from 0 to 8. The risk scale is mapped to a simple overall risk rating of LOW (0-2), MEDIUM (3-5), and HIGH (6-8). For example, using table 6 to assess the risk of a Distributed Denial of Service (DDoS) attack disrupting the availability of a cloud service requires the assessor to estimate the business impact of the threat and the likelihood of the attack. Estimating the *Business impact* as a Medium and the *Likelihood* of the incident as Low, will give us a *Risk value of 3*, same as an event with an impact of Very low, and a Likelihood of High.

Overall, the CSPRAM model promotes trust between the CSP and customer based on customer involvement in the RA process. Although, determining which customer to pick for the exercise, and deciding on how to manage different customer preferences and risks, could lead to the increased complexity of the cloud hosting infrastructure. The process is also reliant on customers providing accurate feedback, and could also be slow in adapt-

Table 6: CSPRAM Risk Analysis Matrix

	Likelihood of incident scenario				
Business Impact	Very low	Low	Medium	High (likely)	Very high
Very low	0	1	2	3	4
Low	1	2	3	4	5
Medium	2	3	4	5	6
High	3	4	5	6	7
Very high	4	5	6	7	8

ing to the dynamic changes in the cloud ecosystem. The compliance of the model with the ISO/IEC 27005 standard helps with the scope and boundary definition, but its use of a risk matrix in evaluating different risk scenarios could lead to unprioritised high impact risk events.

4.4. OPTIMIS

Djemame et al. [42] proposed the Service Provider Risk Assessment Tool (SPRAT) and Infrastructure Provider Risk Assessment Tools (IPRAT) for cloud service provisioning, and as part of the EU-funded project, OPTIMIS (Optimized Infrastructure Services). The SPRAT and IPRAT are independent parts of the risk assessment framework. The objective of the OPTIMIS project is to enable an open and dependable cloud service ecosystem, which provides technological assurances. These should consequently lead to higher confidence of cloud consumers and promotes the cost-effective and reliable productivity of CSPs and resourcefulness of Infrastructure Providers (IP). The framework aims to deliver flexible, auditable, reliable, sustainable, secure and economical cloud services.

The risk assessment process follows a use case scenario to determine which assets will be involved in the assessment and their interactions. Risks are also assessed by categories (e.g., technical, legal, policy, and general) to streamline the mitigation strategies. Using this framework, the different business level objectives of the SP and IP actors, play a part in deciding the importance of cloud risk. The model supports the assessment of cloud risks involved in the outsourcing of a service to an external provider, e.g. infrastructure hosting. Another decision supported by the model is the evaluations of the reliability of IP offerings and their ability to meet stipulated SLA. The suggested use-cases supported by the risk assessment framework include: i) Private cloud,

Table 7: Presenting a risk event with SPRAT

Risk Category:	**General**
Asset identified	Security
Vulnerability of Asset	Unprotected password
Threat to the Asset	Unrestricted access to data
Resulting risk item	Data leaks
Risk Likelihood	High (4) [Range 1-5]
Risk Impact	High (4) [Range 1-5]
Resulting Risk level	Risk Likelihood * Risk Impact = 4*4 = 16 [Range 1-25]
Risk Event	System hacks
Resulting Risk Mitigation	Encrypting data

ii) Bursting, iii) Multi-Cloud, iv) Federated cloud, and v) Brokerage. Each risk assessment exercise conducted by the SP will incorporate provider reliability into the risk model, to verify the expected integrity of the provider's guarantee when making SLA offer.

The OPTIMIS model defines risk as the combination of the likelihood of an event occurring, and the negative consequence/impact of the undesirable event. For each risk event, the assessors estimate the risk level based on the impact and likelihood of that risk. The likelihood and impact values are labelled from 1 to 5 according to their intensity (1-very low, 2- low, 3- medium, 4- high, 5-very high), and the resulting risk level ranged from 1-25. In Table 7, we present an example of a cloud risk event involving the unauthorised access to data due to access to unprotected passwords. Here, the risk assessors estimate the likelihood of the risk as High, which is equivalent to a value of 4, and the impact also estimated as High (4). The resulting risk is a product of the impact and likelihood, which yields a risk level of **16**, with the maximum being **25**.

In summary, the OPTIMIS model provides a good foundation for a reliable and trustworthy cloud environment, seeing that it involves the infrastructure and service provider in the RA process. Using the toolkit, the model can support the dynamic assessment of cloud provisioning risk. However, its assessment of cloud risks using use-case scenarios means that any scenario not identified in the risk identification stage, will not be considered. This model requires a significant level of transparency between the IP and SP, as

part of determining the reliability of providers and their ability to meet SLA.

5. Discussion

This study aims to evaluate conceptual cloud risk assessment models, developed for assessing cloud service provision risks. In Table 8, we compare our proposed model *(CSCCRA)* with other selected models *(QUIRC, CSPRAM, and OPTIMIS)*. Based on the high-level comparisons of the cloud models, we discuss some of our key findings, emphasising how the models differ, and the improvements built into the CSCCRA model. As part of the discussion, we also evaluate some of the emerging factors from our description of the models, including their risk assessment methodology, participating cloud stakeholders, use of experts, presentation of risk value, evaluation of supply chain, and the ability of each model to be dynamic.

5.1. Reflecting on Current Models

As one can imagine, the three cloud risk assessment models compared in this study, are not the only conceptual models available to CSPs. Nevertheless, they were chosen because they were the only ones that met our criteria as mentioned earlier. The work of Fito et al. [43] stands out as another suitable alternative, except for their concentration on business level objectives and the lack of emphasis on security risks in the application of the SEmi-quantitative BLO-driven Cloud Risk Assessment (SEBCRA) model in a CSP environment. Some of the excluded papers did not give a practical example of the model's application [50, 51], while others did not explicitly consider the supply chain [10, 11] in their risk assessment process.

While each of the discussed models was developed for assessing cloud service provisioning risks, they differ in their primary goal and the process involved in achieving these goals. We draw particular attention to the CSPRAM model [31], which identified the need for involving cloud customers in the risk assessment process. This was based on the understanding that although the CSP owns the cloud infrastructure and software used to process data, the data is owned by the CC, and only them can provide a realistic estimate of the impact cost. CSPRAM authors, however, were cautious not to involve users in all stages of the assessment to avoid process becoming unmanageable.

Furthermore, the comparison of the models strengthened the notion of a predominance of qualitative risk matrix and semi-quantitative risk scoring

Table 8: Systematic evaluation of cloud risk assessment models

Criterion ——— **Models**	**Goal**	**Risk Assessment steps**	**Decisions supported by the model**	**The scope of risk assessment**	**Risk Conceptualisation**
QUIRC	Assessing cloud risks based on security objectives	The RA process is split into two phases: impact assessment using wide-band Delphi method, & probability assessment based on security reports	The model supports business-driven assessment of the security of cloud services	The CSP conducts the assessment with help from experts. The model is applicable to other IT systems beyond the cloud.	Risk (score) = Impact * Probability
CSPRAM	Assessing the risk of cloud services, with inputs from cloud consumers (CC)	The model follows the steps defined in the ISO/IEC 27005 standard and is split into two aspects: CSP and CC	Supports the implementation of appropriate security controls based on changing customer requirements	The scope is reliant on the CSP and how much they choose to include customers in the assessment. The model also includes elements of risk management processes.	Risk (score) = Impact * Likelihood
SPRAT	To enable cloud providers analyse and address risk factors in a cloud ecosystem	The RA process follows a use-case scenario in determining the assets and actors required to conduct the assessment. It addresses two cloud stakeholder risks : SP & IP	The model supports the assessment of risks involved with the outsourcing of a cloud service to an external provider	The assessment involves both service provider and infrastructure provider. The model extends beyond RA to include risk mitigation and monitoring steps	Risk (score) = Impact* Likelihood
CSCCRA	To enable CSPs identify, analyse, and evaluate cloud risks from a dynamic supply chain perspective.	The model builds on existing RA standards and involves the mapping of a cloud supply chain, supplier assessment, before the risk analysis phase.	The presentation of cloud risks in dollar value promotes cost-effective risk mitigation and optimal risk prioritisation.	The CSP conducts the assessment following the assessment of the security posture of their suppliers. The model is extensible to any composite IT service.	Risk (cost) = Impact * Probability* Frequency

in cloud risk assessments [34, 74]. A possible explanation for this approach is that their proponents are interested in simplifying the model. However as noted in [20], qualitative approaches can be subjective, and assessments conducted with such methods may often fail to maintain internal and external consistency with the meanings and proportionality of the values used for risk estimation. Such assessments will need to include organisationally-meaningful annotations since their values and meanings are not maintained across other contexts.

A significant aspect of the models discussed is their use of experts. Of the four models discussed in this study, only QUIRC actively makes use of external experts during the impact assessment of cloud risks. Although the deductive risk modelling approach is valuable to the risk analysis process, since it relies on experts' experience, logic, and critical thinking, the QUIRC's wide-band Delphi format (which requires a consensus among experts) makes this model inflexible to address the dynamic cloud risks. Likewise, on the subject of involving members of the supply chain in the assessment of risks, both OPTIMIS and CSCCRA involved suppliers of the cloud service, while CSPRAM involved the customers. Arguments for both approaches can be made. However, a more significant concern will be for CSPs to consider data processing and treatment, particularly when in possession of third-party vendors, given the limited insights CSP's have about vendor security controls. We, therefore, conclude that the CSPRAM model would have been more convincing if the authors had also considered the "upstream" supply chain.

Similarly, considering the flexibility and adaptability of the models to different cloud scenarios, it would appear that QUIRC is the least flexible. The main reason for this conclusion is because of its need for Delphi participants, which is less adaptable for the cloud. However, the RA approach described in CSPRAM, which the authors claim will be tested in a public cloud SaaS application, does not seem to fit that environment. We maintain that the approach will be more suited to a private cloud setting, where the CSP has a working relationship with cloud customers and can rely on them to be involved in such a rigorous cloud assessment. Lastly, proposing a risk assessment model without a measure of its capability does not assure its effectiveness. As such, we commend the implementation of the OPTIMIS model as a tool and the illustration of its use in the risk assessment of a cloud service provision.

Given that one of the primary purposes of risk assessment is to prioritise cloud risks, that is, deciding before a security event which systems are critical

to cloud operation, and presenting this information to the business owners, it is only appropriate for the value of risk to be presented in a format that decision-makers can understand. The CSCCRA model presents decision-makers with a pictorial representation of their risk landscape and helps them to identify weak suppliers within the chain. In their review of a dynamic model, Ghadge et al. [36], maintain that the process of identifying the potential weak spots through the implementation of dynamic models capable of capturing the vulnerability in the supply chain is beneficial to practitioners in proactively mitigating the risks. Additionally, while other risk assessment models ignored uncertainty and its associated challenges to simplify their decision-making, the CSCCRA explicitly considered uncertainty in its risk factor estimation, making it an integral part of the model.

Overall, this study has found that conceptual models increase justifiability by making the inner operations of the risk assessment easier to understand for both the assessors and external stakeholders. Since cloud risk assessments often involve internal and external stakeholders with expertise in the different domain, the best approach to conducting cloud assessments will be to have all assumptions about the asset and environment documented, to enhance the justifiability of the risk results and ensure its transparency, repeatability, and understandability.

5.2. Future Needs

Information security risk in the cloud has remained a cross-cutting concern for cloud consumers and providers, seeing that it integrates other factors such as trust, transparency, accountability, and cost [75]. The importance of assessing cloud risks has mainly been motivated by the dynamic context in which the services and application are implemented. However, the silo approach of most cloud risk assessment models, where the focus of the assessment is limited to a single environment (focal CSP/customer), instead of within the context of its supply chain, has been identified as a critical failure of cloud risk models. Due to the dynamic and rapidly advancing nature of the cloud, it would seem that our risk assessment practices are failing to keep pace, creating greater risk exposures. Furthermore, most organisations due to their resource constraint, fail to conduct due diligence on their third and fourth party vendors, even though there is an ever-increasing dependence on these vendors.

We, therefore, anticipate the need for technology-enabled automation and proactive solutions in addressing the need for continuous risk assessment in

the cloud [76, 77]. The cloud is amenable to *automated risk assessment and mitigation*, where the members of its supply chain can be dynamically monitored for risk and vulnerabilities within the system and vulnerabilities can be remediated before getting exploited by attackers. Due to the numerous indirect assets (i.e. assets harmed through the impact on other assets) involved in the provision of cloud services, *CSPs should proactively assess the risk of dealing with all known suppliers* to allow them to identify their limitations and improve their performance [78, 79]. This approach involves the application of structural analysis of the cloud environment and the use of visual structural models to illustrate the interdependencies between the components and assess the cause and effect relations within the supply chain.

Seeing that the physical boundaries of the cloud supply chain are blurred due to interconnectedness, the impact of information security risks through the supply chain is magnified. CSPs are therefore encouraged to *dynamically model their cloud risk assessment process based on defined boundaries*, and proactively monitor this boundary for cyber threats. Automating all or most aspects of cloud risk assessment allows for repeatable processes which yield valuable outputs, while also allowing humans to focus on the most significant risks [77, 80]. This approach also limits the need for external expert judgement on metrics and estimation of risk factors, since experts engagement has been known to delay the assessment process.

Furthermore, while the causes of *cybersecurity incidents may be technical, their impact directly concerns the business*, with links to the reputation and continued viability of the CSP. Therefore, proposals for *cloud risk assessment models should look towards quantitative risk methodologies* to enable them present cloud risks based on its impact to the business (i.e. loss of business or cost to recover), factoring the value of the asset into the risk estimations [17, 81]. According to some authors, asset characterisation and valuation, which should be considered as key components of cloud security risks assessment, have not been well discussed in the existing frameworks [82]. With this in mind, we suggest that new cloud models should embrace quantitative methods in assessing cloud risks with the aim of presenting the value of the risk as an actual dollar amount or 'bottom line', which we believe will be helpful to decision-makers in evaluating and treating cloud risks.

Lastly, researchers and practitioners within the *cloud community should strive to develop assessment tools targeted at cloud provisioning risks*, which are both useful for science and practice alike, to enable CSPs deal effectively with the risks involved in the design, deployment, configuration, or opera-

tion of the cloud [83]. We anticipate that this will improve the agility, and reliability of cloud services, helping CSPs to handle predicted and unforeseen changes, while also assisting them in meeting their SLAs. Also, researchers should endeavour to implement their proposed models, to measure its capability and assure its effectiveness in addressing the cloud risk assessment challenges. The reason for this suggestion is because, to date, many of the proposed models stay in the prototype realm, and have not been applied to real-world scenarios [84].

6. Conclusion and Future Work

Security is interrelated with trust, and trust is essential for cloud survival. The increased dependence on suppliers and the seeming lack of visibility of CSP security controls have made it difficult for cloud customers to assess the risk of their cloud services. This inability to conduct a comprehensive risk assessment has also prevented others from migrating their data to the cloud and reaping any efficiency benefits. Assessing cloud risks requires us to proactively identify security risks, up and down the supply chain, and implement the best safeguards to reduce them. The limitations of the current risk assessment frameworks, therefore call for a more dynamic and inclusive approach to cloud risk assessment, one that considers the transparency of the supply chain, accountability of suppliers, and improves the trust of the customer.

In this study, we conducted an in-depth review of the extant literature to identify models proposed for cloud provisioning risk assessment. Using a set of criteria, we identified and described three of the existing models and later compared them with our proposed model. We highlighted each models' goal, risk assessment steps, decisions, the scope of assessment, and risk conceptualisation while also suggesting their applicability and reproducibility. Our detailed comparison of the models highlighted the strengths, weaknesses, applicability, and reproducibility of each model. While the findings are based on our interpretation of each risk assessment model, we believe that the information presented will enhance the research community's understanding of different approaches to modelling and assessing cloud risks.

Furthermore, we found that despite the multiplicity of approaches targeted at addressing cloud risks, there remains a considerable gap in the research of cloud risk assessment models, with emphasis on the inherent risk in the supply chain. As such, it has become essential for more study to be

conducted in this area. However, in the meantime, CSPs need to adopt a more rounded approach to dealing with cloud risks. This new approach ultimately requires CSPs to complement the abstract knowledge of risks from the more traditional frameworks like ISO/IEC 27005, with the specific technical factors that drive cloud risks, which the lower-level conceptual model provides.

In conclusion, this study should be seen as a foundation for researchers looking to build new conceptual models for assessing cloud risks. As for the CSCCRA model, our future work will see us validate and demonstrate the suitability of the proposed framework in assisting CSPs to assess the risks of their cloud service and efficiently mitigate them. We are currently conducting case studies with SaaS CSPs within the UK to establish the value of the model with regards to structuring the risk assessment conversation across the supply chain. The finalised model will also be implemented as part of a cloud risk assessment web-based application.

7. Acknowledgement

This research project has been possible thanks to a research grant from the UK EPSRC (Engineering and Physical Research Council) and Kellogg College, via the Centre for Doctoral Training in Cyber Security at the University of Oxford, UK.

References

[1] K. E. Kushida, J. Murray, J. Zysman, Cloud Computing: From Scarcity to Abundance, Journal of Industry, Competition and Trade 15 (1) (2015) 5–19.

[2] K. Ruan, Introducing cybernomics: A unifying economic framework for measuring cyber risk, Computers & Security 65 (2017) 77–89.

[3] D. Catteddu, H. Giles, H. Thomas, L. Dupre, Cloud Computing: Benefits, Risks and Recommendations for Information Security, Computing 72 (1) (2010) 17–17. arXiv:S0167739X10002554, doi:10.1007/978-3-642-16120-9˙9.
URL http://link.springer.com/10.1007/978-3-642-16120-9-9

[4] ISO 27005, BS ISO / IEC 27005 : 2011 BSI Standards Publication Information technology – Security techniques – Information security risk management 1 (2011) 1–68.

[5] R. Bojanc, Quantitative Model for Information Security Risk, Engineering Management Journal 25 (2) (2013) 267–275.
URL http://www.tandfonline.com/doi/abs/10.1080/10429247.2013.11431972

[6] A. Shameli-Sendi, R. Aghababaei-Barzegar, M. Cheriet, Taxonomy of information security risk assessment (ISRA), Computers & Security-doi:10.1016/j.cose.2015.11.001.

[7] J. Busby, L. Langer, M. Schöller, N. Shirazi, P. Smith, AIT, SEcure Cloud computing for CRitical infrastructure IT, "Methodology for Risk Assessment and Management", SECCRIT Consortium 3 (5) (2014) 1–92.

[8] E. Cayirci, A. Garaga, A. Santana, Y. Roudier, A cloud adoption risk assessment model, in: Utility and Cloud Computing (UCC), 2014 IEEE/ACM 7th International Conference on, IEEE, 2014, pp. 908–913.

[9] S. Islam, S. Fenz, E. Weippl, H. Mouratidis, A Risk Management Framework for Cloud Migration Decision Support, J. Risk Financ. Manag. 10 (2) (2017) 10.
URL http://www.mdpi.com/1911-8074/10/2/10

[10] A. S. Sendi, M. Cheriet, Cloud computing: A risk assessment model, in: Cloud Engineering (IC2E), 2014 IEEE International Conference on, IEEE, 2014, pp. 147–152.

[11] Y. Sivasubramanian, S. Z. Ahmed, V. P. Mishra, Risk Assessment for Cloud Computing, International Research Journal of Electronics and Computer Engineering 3 (2) (2017) 7. arXiv:arXiv:1011.1669v3.
URL http://researchplusjournals.com/index.php/IRJECE/article/view/292

[12] C. W. Johnson, You Outsource the Service but Not the Risk : Supply Chain Risk Management for the Cyber Security of Safety Critical Systems . In : 34th International System Safety Conference , Orlanda , FL , USA , 8-12 This is the author ' s fi (November) (2016) 8–12.

[13] N. Bartol, Cyber supply chain security practices DNA - Filling in the puzzle using a diverse set of disciplines, Technovation 34 (7) (2014) 354–361. doi:10.1016/j.technovation.2014.01.005.

[14] J. M. Boyens, C. Paulsen, R. Moorthy, N. Bartol, Supply Chain Risk Management Practices for Federal Information Systems and Organizations, NIST Special publication.
URL http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161.pdf

[15] R. Lewis, P. Louvieris, P. Abbott, Cybersecurity Information Sharing : a Framework for Information Security, Twenty Second European Conference on Information Systems (2014) 1–15.

[16] G. Motta, L. You, N. Sfondrini, D. Sacco, T. Ma, Service level management (SLM) in cloud computing-third party SLM framework, Proceedings of the Workshop on Enabling Technologies: Infrastructure for Collaborative Enterprises, WETICE (2014) 353–358.

[17] O. Akinrolabu, S. New, A. Martin, CSCCRA: A Novel Quantitative Risk Assessment Model for Cloud Service Providers, in: European, Mediterranean, and Middle Eastern Conference on Information Systems, Springer, 2018, pp. 177–184.

[18] Y. Cherdantseva, P. Burnap, A. Blyth, P. Eden, K. Jones, H. Soulsby, K. Stoddart, A review of cyber security risk assessment methods for scada systems, Computers & security 56 (2016) 1–27.

[19] D. Ionita, Current established risk assessment methodologies and tools, Master's thesis, University of Twente (2013).

[20] R. S. Ross, Guide for conducting risk assessments, Special Publication (NIST SP) - 800-30 Rev 1 1 (September) (2012) 95.
URL http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

[21] J. Luna, N. Suri, M. Iorga, A. Karmel, Leveraging the Potential of Cloud Security Service-Level Agreements through Standards, IEEE Cloud Computing 2 (3) (2015) 32–40.

[22] D. Vohradsky, Cloud Risk – 10 Principles and a Framework for Assessment, ISACA Journal 5 (2012) 31–41.

[23] M. Theoharidou, N. Tsalis, D. Gritzalis, In Cloud We Trust: Risk-Assessment-as-a-Service, Trust Management VII 401 (2013) 100–110.
URL http://link.springer.com/10.1007/978-3-642-38323-6

[24] S. Drissi, S. Benhadou, H. Medromi, Evaluation of risk assessment methods regarding cloud computing, in: The 5th Conference on Multidisciplinary Design Optimization and Applicaton no, 2016.

[25] K. Hashizume, D. G. Rosado, E. Fernández-Medina, E. B. Fernandez, An analysis of security issues for cloud computing, Journal of internet services and applications 4 (1) (2013) 5.

[26] A. Singh, K. Chatterjee, Cloud security issues and challenges: A survey, Journal of Network and Computer Applications 79 (2017) 88–115.

[27] T.-H. Hu, A Prehistory of the Cloud, MIT Press, 2015.

[28] S. Subashini, V. Kavitha, A survey on security issues in service delivery models of cloud computing, Journal of Network and Computer Applications 34 (1) (2011) 1–11. arXiv:S0167739X10002554, doi:10.1016/j.jnca.2010.07.006.
URL http://linkinghub.elsevier.com/retrieve/pii/S1084804510001281

[29] C. Tang, J. Liu, Selecting a trusted cloud service provider for your SaaS program, Computers and Security 50 (2015) 60–73. doi:10.1016/j.cose.2015.02.001.

[30] O. Akinrolabu, S. New, Can Improved Transparency Reduce Supply Chain Risks in Cloud Computing, Proceedings of the 7th International Conference on Operations and Supply Chain Management (OSCM) 10 (3) (2016) 877–892.

[31] S. H. Albakri, B. Shanmugam, G. N. Samy, N. B. Idris, A. Ahmed, Security risk assessment framework for cloud computing environments, Security and Communication Networks 7 (11) (2014) 2114–2124. arXiv:0806.0557.

[32] J. R. C. Nurse, S. Creese, D. De Roure, Security risk assessment in internet of things systems, IEEE IT Professional 19 (5) (2017) 20–26.

[33] J. R. C. Nurse, P. Radanliev, S. Creese, D. De Roure, If you can't understand it, you can't properly assess it! the reality of assessing security risks in internet of things systems, in: Living in the Internet of Things: Cybersecurity of the IoT-2018, IET, 2018, pp. 1–9.

[34] O. Akinrolabu, S. New, A. Martin, Cyber Supply Chain Risks in Cloud Computing – Bridging the Risk Assessment Gap, Open Journal of Cloud Computing (OJCC) 5 (1) (2018) 1–19.

[35] U. M. Ismail, S. Islam, M. Ouedraogo, E. Weippl, A framework for security transparency in Cloud Computing, Future Internet 8 (1).

[36] A. Ghadge, S. Dani, M. Chester, R. Kalawsky, A systems approach for modelling supply chain risks, Supply chain management: an international journal 18 (5) (2013) 523–538.

[37] B. Ribbeck, Cloud Service Provider Risk Assessment (2014).
URL `https://events.educause.edu/annual-conference/2014/proceedings/cloud-service-provider-risk-assessment`

[38] Tenable Network Security, 2017 Global Cybersecurity Assurance Report Card 1 (2017) 19.
URL `http://static.tenable.com/whitepapers/2016-global-cybersecurity-assurance-report-card.pdf`

[39] H. Tang, J. Yang, X. Wang, Q. Zhou, A Research for Cloud Computing Security Risk Assessment, The Open Cybernetics & Systemics Journal 10 (1) (2016) 210–217.
URL `http://benthamopen.com/ABSTRACT/TOCSJ-10-210`

[40] R. Hentschel, C. Leyh, A. Petznick, Current cloud challenges in germany: the perspective of cloud service providers, Journal of Cloud Computing 7 (1) (2018) 5.

[41] P. Saripalli, B. Walters, Quirc: A quantitative impact and risk assessment framework for cloud security, in: Cloud Computing (CLOUD), 2010 IEEE 3rd International Conference on, IEEE, 2010, pp. 280–288.

[42] K. Djemame, D. J. Armstrong, M. Kiran, M. Jiang, A risk assessment framework and software toolkit for cloud service ecosystems, in: in 2nd International Conference on Cloud Computing, GRIDs, and Virtualization, Citeseer, 2011.

[43] J. O. Fitó, M. Macías, J. Guitart, Toward business-driven risk management for cloud computing, in: Network and Service Management (CNSM), 2010 International Conference on, IEEE, 2010, pp. 238–241.

[44] D. Ionita, Model-driven information security risk assessment of socio-technical systems, Ph.D. thesis (2018).

[45] S. Pearson, V. Tountopoulos, D. Catteddu, M. Sudholt, R. Molva, C. Reich, S. Fischer-Hubner, C. Millard, V. Lotz, M. G. Jaatun, R. Leenes, C. Rong, J. Lopez, Accountability for cloud and other future Internet services, CloudCom 2012 - Proceedings: 2012 4th IEEE International Conference on Cloud Computing Technology and Science 3 (2012) 629–632. doi:10.1109/CloudCom.2012.6427512.

[46] F. M. Alturkistani, A. Z. Emam, A Review of Security Risk Assessment Methods in Cloud Computing, in: New Perspectives in Information Systems and Technologies, Vol. 1, 2014, pp. 443–453. doi:10.1007/978-3-319-05951-8.

[47] S. Drissi, S. Benhadou, H. Medromi, Evaluation of risk assessment methods regarding cloud computing, in: The 5th Conference on Multidischiplinary Design Optimization and Applicaton, no, 2016.

[48] J. L. Fernández-Alemán, I. C. Señor, P. Á. O. Lozoya, A. Toval, Security and privacy in electronic health records: A systematic literature review, Journal of biomedical informatics 46 (3) (2013) 541–562.

[49] C.-A. Chih, Y.-L. Huang, An adjustable risk assessment method for a cloud system, in: Software Quality, Reliability and Security-Companion (QRS-C), 2015 IEEE International Conference on, IEEE, 2015, pp. 115–120.

[50] P. Liu, D. Liu, The new risk assessment model for information system in Cloud Computing Environment, Procedia Engineering 15 (2011) 3200–3204.

[51] L.-J. Zhang, J. Zhang, J. Fiaidhi, J. M. Chang, Hot Topics in Cloud Computing, IT Professional 12 (5) (2010) 17–19.
URL http://ieeexplore.ieee.org/document/5593035/

[52] A. Khajeh-Hosseini, I. Sommerville, J. Bogaerts, P. Teregowda, Decision support tools for cloud migration in the enterprise, in: Cloud Computing (CLOUD), 2011 IEEE International Conference on, IEEE, 2011, pp. 541–548.

[53] P. Jamshidi, A. Ahmad, C. Pahl, Cloud migration research: a systematic review, IEEE Transactions on Cloud Computing 1 (2) (2013) 142–157.

[54] F. Fowley, C. Pahl, Cloud migration architecture and pricing ? Mapping a licensing business model for software vendors to a SaaS business model, Commun. Comput. Inf. Sci. 707 (September) (2018) 91–103.

[55] O. Akinrolabu, S. New, A. Martin, Cloud Service Supplier Assessment : A Delphi Study, in: Proceedings of the Eighth International Conference on Innovative Computing Technology (INTECH),2018, Luton, UK, 2018, pp. 142–150.

[56] J. Freund, J. Jones, Measuring and managing information risk: a FAIR approach, Butterworth-Heinemann, 2014.

[57] ISO31000-2009, ISO31000:2009 - Risk management: Principles and guidleines (2009). doi:10.5594/J09750.

[58] G. The Open, Technical Standard Risk Taxonomy (2009).
URL http://pubs.opengroup.org/onlinepubs/9699919899/toc.pdf

[59] R. Dawes, D. Faust, P. Meehl, Clinical versus actuarial judgment, Science 243 (4899) (1989) 1668–1674. doi:10.1126/science.2648573.
URL http://www.sciencemag.org/cgi/doi/10.1126/science.2648573

[60] Jonathan Greer, Taking a Chance with Monte Carlo (2015).
URL https://www.panaseer.com/2015/09/30/taking-a-chance-with-monte-carlo/

[61] W. Koehrsen, The Poisson Distribution and Poisson Process Explained (2019).
URL https://towardsdatascience.com/the-poisson-distribution-and-poisson-process-explained-4e2cb17d459

[62] D. W. Hubbard, R. Seiersen, Risk Matrices, Lie Factors, Misconceptions, and Other Obstacles to Measuring risk, in: How to Measure Anything in Cybersecurity Risk, 2016.

[63] R. T. Clemen, R. L. Winkler, Combining probability distributions from experts in risk analysis, Risk analysis 19 (2) (1999) 187–203.

[64] M. Sherman, Risks in the Software Supply Chain, Software Solutions Symposium (2017) 1–36.

[65] BuiltWith, BuiltWith Technology Lookup, https://builtwith.com/ (2018).
URL https://builtwith.com/

[66] R. Hogan, Introduction to Statistics for Uncertainty Analysis, http://www.isobudgets.com/introduction-statistics-uncertainty-analysis/ (2016).
URL http://www.isobudgets.com/introduction-statistics-uncertainty-analysis/

[67] D. Gresh, L. a. Deleris, L. Gasparini, Visualizing Risk, Proc. IEEE Symp. Inf. Vis. 25293.

[68] CSA, Consensus Assessments : Cloud Security Alliance (2016).
URL https://cloudsecurityalliance.org/group/consensus-assessments/{\#}{_}overview https://cloudsecurityalliance.org/group/consensus-assessments/

[69] L. Marinos, ENISA threat taxonomy: A tool for structuring threat information. Initial report., ENISA (January) (2016) 1–24.
URL https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/enisa-threat-landscape/etl2015/enisa-threat-taxonomy-a-tool-for-structuring-threat-information

[70] O. Akinrolabu, A. Martin, S. New, Assessing cloud risk: The supply chain perspective (2018).
URL https://www.bcs.org/content/conWebDoc/59876

[71] H. A. Linstone, M. Turoff, et al., The delphi method, Addison-Wesley Reading, MA, 1975.

[72] SANS Institute, SANS Institute - Critical Security Controls (2016).
URL https://www.sans.org/critical-security-controls/

[73] NIST, Standards for security categorization of federal information and information systems, Tech. rep., National Institute of Standards and Technology, Gaithersburg, MD (feb 2004).
URL https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.199.pdf

[74] B. Karabacak, I. Sogukpinar, ISRAM: Information security risk analysis method, Computers and Security 24 (2) (2005) 147–159.

[75] D. Nuñez, C. Fernández-Gago, J. Luna, Eliciting metrics for accountability of cloud systems, Computers & Security 62 (2016) 149–164.

[76] A. Amini, N. Jamil, A comprehensive review of existing risk assessment models in cloud computing, in: Journal of Physics: Conference Series, Vol. 1018, IOP Publishing, 2018, p. 012004.

[77] Bitsight, Resources - Cybersecurity & Vendor Risk Management — BitSight (2018).
URL https://www.bitsighttech.com/resources?topic=all\resource=data-sheet\usecase=all

[78] E. Doherty, M. Carcary, G. Conway, Risk Management Considerations in Cloud Computing Adoption (August).

[79] I. Agrafiotis, J. R. C. Nurse, M. Goldsmith, S. Creese, D. Upton, A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate, Journal of Cybersecurity 4 (1).

[80] M. Adelmeyer, L. Beike, M. Buggenthin, S. Osada, F. Teuteberg, Riscc - a risk management tool for cloud computing environments.

[81] R. Schmittling, A. Munns, Performing a security risk assessment, ISACA Journal 1 (2010) 18.

[82] S. Tweneboah-Koduah, W. J. Buchanan, Security risk assessment of critical infrastructure systems: A comparative study, The Computer Journal 5.

[83] K. Djemame, D. Armstrong, J. Guitart, M. Macias, A Risk Assessment Framework for Cloud Computing, IEEE Transactions on Cloud Computing 4 (3) (2016) 265–278.

[84] S. Gadia, Cloud Computing Risk Assessment: A Case Study, ISACA journal 4 (2011) 11–16.
URL http://www.isaca.org/Journal/Past-Issues/2011/Volume-4/Pages/Cloud-Computing-Risk-Assessment-A-Case-Study.aspx