Assessing the Security Risks of Multicloud SaaS Applications: A Real-World Case Study

1st Olusola Akinrolabu
Department of Computer Science
University of Oxford
Oxford, UK
olusola.akinrolabu@cs.ox.ac.uk

2nd Steve New
Saïd Business School
University of Oxford
Oxford, UK
steve.new@sbs.ox.ac.uk

3rd Andrew Martin
Department of Computer Science
University of Oxford
Oxford, UK
andrew.martin@cs.ox.ac.uk

***Abstract*—Cloud computing is widely believed to be the future of computing. It has grown from being a promising idea to one of the fastest research and development paradigms of the computing industry. However, security and privacy concerns represent a significant hindrance to the widespread adoption of cloud computing services. Likewise, the attributes of the cloud such as multi-tenancy, dynamic supply chain, limited visibility of security controls and system complexity, have exacerbated the challenge of assessing cloud risks. In this paper, we conduct a real-world case study to validate the use of a supply chain-inclusive risk assessment model in assessing the risks of a multicloud SaaS application. Using the components of the Cloud Supply Chain Cyber Risk Assessment (CSCCRA) model, we show how the model enables cloud service providers (CSPs) to identify critical suppliers, map their supply chain, identify weak security spots within the chain, and analyse the risk of the SaaS application, while also presenting the value of the risk in monetary terms. A key novelty of the CSCCRA model is that it caters for the complexities involved in the delivery of SaaS applications and adapts to the dynamic nature of the cloud, enabling CSPs to conduct risk assessments at a higher frequency, in response to a change in the supply chain.**

***Index Terms*—Cloud, SaaS, Quantitative Risk Assessment, Supply Chain, Transparency, Case study.**

I. Introduction

Cloud computing has changed the way IT services are delivered and consumed. It is a set of disruptive technologies that have facilitated new business models and a new industry architecture [1]. Organisations look to take advantage of its agility, functionality, scalability, and cost benefits. The cloud enables modularisation, standardisation, and concentration of core competencies, maximising value for all actors involved [2]. Although the cloud model has many economic and functionality advantages, the increased external interactions of its applications have resulted in a rise in architectural complexity. The ubiquity of the cloud also introduces new risks and assessing these risks remains a challenge for CSPs and their customers.

The increased growth experienced in the cloud industry has led to the development of multi-cloud systems (MCS), where a variety of vendors provides cloud-based services and each service relies on more than one CSP [3]. We define a MCS as an architecture made up of a mashup of cloud services, runs in a complex ecosystem that connects components from different organisations, and is written in different technology stacks. In multicloud systems, the CSP's ability to secure customer data and assure customers of the compliance of other suppliers involved in the provision of the service becomes more complicated due to the many moving parts. The further away the CSP is from the cloud customer, the coarser the customer's view of the CSP's security policies and processes [4]. As the growth of cloud computing and adoption continue to increase, the move to the cloud will gradually change from being a tactical means for cost reduction, into a strategic tool for business transformation. This trend calls for a matured risk assessment process for the cloud, ideally one that can become an industry standard [5].

Furthermore, in today's world, the challenge of assessing risks in a MCS is evident. While many of the recent research efforts (e.g., Cayirci et al. [6] and Islam et al. [7]) have concentrated on cloud adoption risk assessment, there seems to be a lack of studies targeted at the assessment of cloud service provision risks. Therefore, selecting the best provider for each service or evaluating the security risks of cloud collaborations, remains a challenge to CSPs. Some of the past studies which have proposed risk assessment model for CSPs include QUIRC [8], OPTIMIS [9] and SEBCRA [10]. Despite best intentions, these models have many shortcomings ranging from the risk analysis method, the limited scope of assessment, expert subjectivity, and inapplicability of the models in real-world scenarios.

In this study, we explore the utility of the CSCCRA model in assessing the risk of a SaaS provider (CSP-A). The CSCCRA model is a supply chain-inclusive risk assessment model that aims to structurally analyse the interdependence between the components of a cloud service, assess the cybersecurity posture of its suppliers, and comprehensively identify and analyse cloud risks. It presents CSP's cloud risk in a format that is consistent, repeatable, traceable and understandable, one which encourages proactive mitigation of cloud risks [11].

The remainder of the paper is organised as follows. First, we present background information on cloud risk assessment, which also includes a brief review of the CSCCRA model. After that, we describe the design of our case study where we used the CSCCRA model to assess the risk of a SaaS CSP. In section 4, we present the results of the assessment and discussion. Finally, section 5 concludes the paper and presents our plan for future work.

II. Background and Related Work

According to a report by the European Agency for Network and Information Security (ENISA), the features of cloud computing, particularly its economies of scale and flexibility, are both a friend and a foe [12]. Cloud services rely on a multi-tiered and often global supply chain, where services are sub-contracted based on expertise. Cloud computing lowers the entrance barrier to service provision, especially for small and medium businesses (SMBs), who now have access to compute-intensive applications, hardware resources with no upfront cost, a platform for innovation and IT scalability [13]. The cloud supply chain is extremely complex and highly diverse; the variety of parties involved in the delivery of a cloud service widens its attack surface [14]. Studies into the supply chain of cloud services 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 [15]. With 1.8 billion vulnerable open source components downloaded in 2015 and at least 26% of the most common open source component having high-risk vulnerabilities, the risks of multicloud systems would seem to be on an ever-increasing trajectory [16].

Numerous scholars have developed *conceptual* models [6], [7], [17] to assess cloud risk. While some of these have concentrated on cloud adoption risk assessment, others have followed the traditional route to security assessment, adapting the traditional frameworks, e.g. ISO 27005, ISO 31000 and NIST 800-30v1. Being predominantly qualitative or at best semi-quantitative, these exhibit serious limitations, including the subjectivity of risk evaluation and the inability to cope with the dynamic cloud infrastructure [18], [19]. We have argued elsewhere that the lack of CSP transparency is also perceived to be a contributing factor to the use of qualitative methods in assessing cloud risks [20]. According to Bellandi et al. [21], new approaches targeted at improving these qualitative methods, accounting for the opacity of the cloud environment, have largely fallen short. Likewise, traditional assessment frameworks may not be well suited to dynamic cloud risks.

Furthermore, the traditional risk assessment approach concentrates only on a focal organisation and its critical assets, while neglecting the supplier network. So far, very little research has looked into the inherent cloud supply chain as a source of these risks [9]. This limitation calls for a more dynamic and inclusive approach that considers the transparency of the supply chain, accountability of suppliers and provides a basis for trust.

The approach examined here is an attempt to devise a quantitative and data-driven process, where the value of a cloud risk is based on the decomposition of a risk scenario into its various elements and expressing risk in financial terms. The vulnerabilities of the individual components can help identify where the weak spots exist in the supply chain.

A. The CSCCRA Model

We developed the CSCCRA model [11] to address the gap in cloud supply chain transparency, particularly how the lack of visibility of supplier's security controls has contributed to the inadequate level of cloud risk assessment. It aims to present the CSP's cloud risk in a format that is consistent, repeatable, traceable and understandable, allowing for the proactive mitigation of cloud risks.

Targeting SaaS CSPs, the model follows a systematic approach to cloud risk assessment, decomposing a cloud service into its component services (managed by different suppliers), mapping its supply chain, and using a multi-criteria decision support tool to assess the cybersecurity posture of the suppliers [22]. The model reflects the systems thinking approach, which gives cloud risk assessors the ability to see the cloud service as a complex system and understand the interconnectedness of its networks [23]. This approach requires us to analyse the interdependencies of a cloud service while making use of modelling and simulation techniques to draw the result of the assessment [24]. The CSCCRA model is made up of three components and builds on existing risk standards and guidance documents such as ISO 27005:2011, ISO 31000:2009, NIST 800-30v1 and FAIR risk assessment [11]. The components are:

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

The steps taken to assess cloud provisioning risks using the CSCCRA model are as follows:

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 compile a comprehensive list of cloud security risks.
4) Enable stakeholders within the CSP to make reasonable estimates of risk values.
5) Input risk values to the CSCCRA quantitative simulation tool, to arrive at the risk value in monetary terms.

III. Research Design

One of the limitations of existing cloud risk assessment models is that they only exist as proposals or prototypes, providing no real measurement of their effectiveness when applied in real-world scenarios [25]. In contrast, we sought to validate the CSCCRA model using a case study approach to help generate an in-depth understanding of how a cloud provider carried out risk assessment using the proposed model in a natural setting, where participant's behaviour cannot be manipulated [26], [27]. This allows for a thorough and detailed evaluation of the model's features in a real setting.

For this case study, we opened up the workings of the model to critical review by technical and business professionals who know the intricacies of managing, supporting and assessing the risks of cloud applications. We engaged in an open process in which the researcher, and business and technical stakeholders

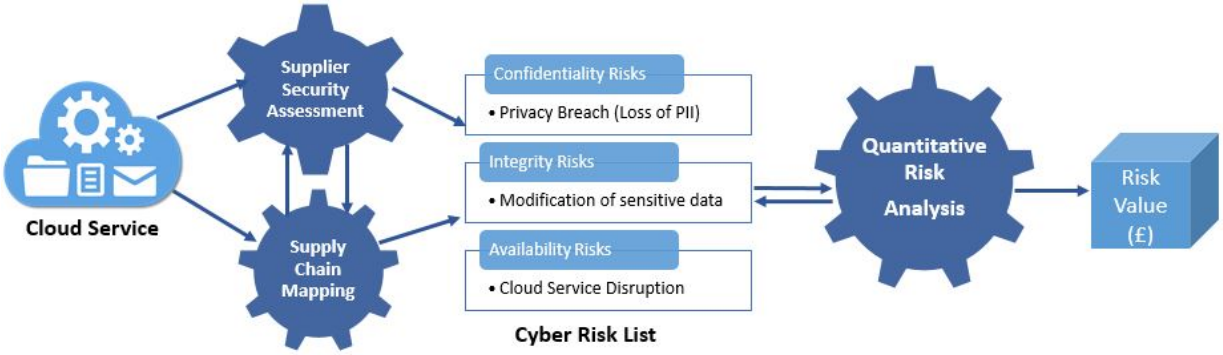
Cloud Service
Supplier Security Assessment
Supply Chain Mapping
Confidentiality Risks
• Privacy Breach (Loss of PII)
Integrity Risks
• Modification of sensitive data
Availability Risks
• Cloud Service Disruption
Cyber Risk List
Quantitative Risk Analysis
Risk Value (£)

Fig. 1. Overview of the CSCCRA Model

within the SaaS company sit down to review the cloud service supply chain, assess its weak spots, and evaluate risks. In recruiting the case organisation, we leveraged our existing relationships with respondents to our previous surveys and interviews. The case organisation was assured of anonymity and aggregation of data [27]. This approach complies with the ethical approval for this study, given by the University of Oxford Central University Research Ethics Committee, under Ref No: SSD/CUREC1A CS_C1A_18_026.

In Figure 2, we show the different phases of stakeholder participation based on the CSCCRA risk assessment method.

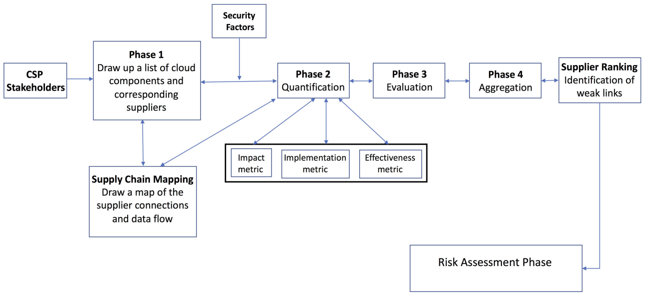

Fig. 2. Steps taken by case study participants using the CSCCRA model

A. Background of CSP-A

Due to confidentiality reasons, the case organisation is referred to as CSP-A. CSP-A is an innovative and rapidly growing software company in the UK. They are involved in the development of software products used in the health, engineering, and science industries. They also work with local government authorities to deliver services required for social care delivery. In 2016, CSP-A developed a not-for-profit SaaS application aimed at curbing social isolation across different age groups, which is the focus of this case study.

We approached CSP-A to take part in the study because a principal member of their team had participated in our previous study. However, it seems they obliged because at the time of our asking, they were also preparing to conduct a risk assessment of the application in compliance with a European Union (EU) grant. We met with the stakeholders before the assessment day to introduce the model and confirm it was a good fit for their application. Following the approval by management, the case study was completed on the 21st of September 2018. A total of six participants took part in the risk assessment exercise; three participated in all the exercises, while the other three were called upon during the risk estimation stages since they were more aware of the business impacts of risks.

IV. Findings and Discussion

In this section, we present our findings from the assessment of CSP-A's SaaS risks, using the CSCCRA model. We give an overview of the steps taken to arrive at the estimated values of CSP-A's top ten risks, followed by a brief discussion on the applicability of the model to assessing multicloud SaaS.

A. Application of CSCCRA to CSP-A SaaS

Conducting a case study can be an intensive process, one that requires a detailed process [28], part of which involves data collection before the exercise. Our initial data collection saw us gather data on the SaaS applications' components including services such as DNS, Web hosting, E-mail, Database, Payment, Identity and Access management etc., and identify their suppliers. We collected this information from external information sources such as the technology lookup website, builtwith.com [29], and Google.

1) Supply Chain Mapping: The risk assessment process using the CSCCRA model followed the steps identified in Figure 2. Presenting the stakeholders with the initial information collected, we got them to provide the other components, which were not externally visible. Figure 3 presents the anonymised supply chain map of CSP-A-SaaS (i.e. the SaaS application). Likewise, in Table I, we identify the cloud components, suppliers and services, their criticality, and the data storage or processing responsibilities of the supplier.

As shown in Figure 3, 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. However, for CSP-A-SaaS, we did not go into greater detail on the lower tier suppliers due to the unavailability of information, and because most of the component providers were themselves IaaS

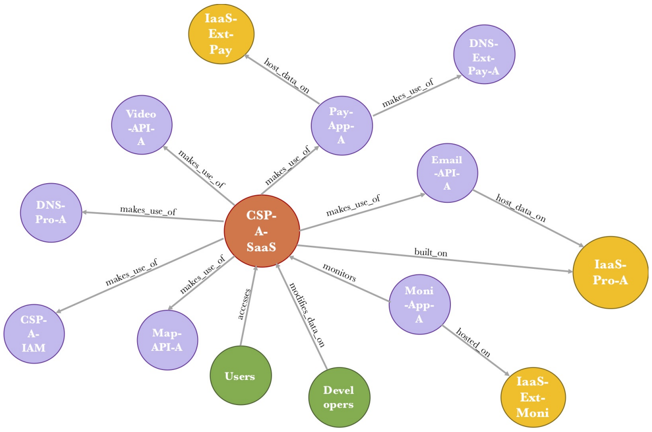

Fig. 3. Supply Chain mapping of CSP-A-SaaS using the CSCM tool

TABLE I
CSP-A SUPPLIER LIST

Anonymised Supplier	**Component**	**Service Category**	**System Criticality**	**Data Proce-using (Y/N)**	**Data Stora-ge (Y/N)**
IaaS-Pr-A	Hosting (Web, Code), Database & Backups	Application/ Infrastructure	Very Critical	Y	Y
CSP-A	*IAM & Software code*	*IAM, Software development*	*Critical*	*Y*	*Y*
Email-API-A	E-mail	Application	Critical	Y	Y
Video-API-A	Video	Application	Not Critical	N	N
Map-API-A	Maps	Application	Critical	N	N
DNS-Pro-A	DNS	Infrastructure	Very Critical	Y	Y
Moni-App-A	Monitoring	Application	Not Critical	N	N
Pay-App-A	Sales and Billing	Application	Not Critical	Y	Y

providers, who are assumed to host the applications internally. Nonetheless, the Figure shows the dependence of CSP-A-SaaS application on IaaS-Pro-A which another component provider (Email-API-A) also depends on for data hosting. The use of a visual structural model helps to illustrate the interdependencies between the components and accurately visualise the cloud information flow. Mapping the supply chain ensures that relevant information that can be used to assess the criticality, threat, and vulnerabilities of suppliers such as IaaS-Pro-A, are transparent to the CSP during an assessment.

2) Supplier Security Assessment: Using the information identified in Table I and aided with a visual structure of the SaaS's supply chain (Figure I), we assessed the cybersecurity posture of the suppliers. The process assists CSPs to evaluate each supplier's security posture by presenting them with a consistent approach to assessing and comparing suppliers based on nine (9) security target dimensions. Assessing suppliers based on dimensions such as their availability of service (AoS), data & system hosting (DSH), data security controls (DSC), the maturity of security assessment (MSA), the maturity of operational security (MOS), encryption & key management(EKM), identity & access management (IAM) etc., assist CSPs in the identification of weak suppliers readily susceptible to cyber attack or those with a high risk of failure. See [30] for more information on the target dimensions.

In this study, the CSSA process took longer than expected, because the participants did not have enough information on their suppliers, and had to rely on observation and publicly available information. While this experience supports the lack of visibility of provider controls, which we have argued has contributed to the lack of comprehensive cloud risk assessments [20], it also confirms an element of blind trust with cloud customers. According to Chan et al. [31], the challenge organisations face in obtaining the desired information for a thorough risk assessment has led many cloud customers to blindly trusting the provider and passively accepting providers' report on the security of their service. Cloud customers on finding out that the information suppliers provide on their website does not translate to the actual implementation of security controls have resolved to use other factors for supplier selections. Some of the factors CSP-A considered included "availability of free credit", "provider reputation", "past working experience", "recommendation" & and "ease of setup".

The result of the supplier security assessment using the CSSA tool is presented in Table II.

As shown in Table II, the participants' scoring rated CSP-A as the weakest link of the supply chain, one with a high susceptibility to a cyber attack. While this strengthened the objectivity of the participants, it also reiterates the idea of increased subjectivity in assessment when customers do not have details of a supplier's security control or operational process. CSP-A scored themselves low in areas where they lacked adequate controls around the components they managed. Some specific areas where gaps were noticed included Disaster Recovery (DR), backup and storage, authentication (No Multi-Factor Authentication (MFA)), encryption, and continuous security assessment. However, it is worth noting that based on the information asymmetry gap, the supplier assessment was made to best-effort.

Overall, the participants found this supplier assessment enlightening, considering its rigorous approach which required them to look through their documentation, of which there was little, and search online for details about their suppliers. From our observation, it seems the details most providers have about their suppliers are restricted to compliance, availability and other SLA-related information. Information on technical or operational security is often limited. However, we believe that the exercise made CSP-A aware of their lack of information on suppliers that were critical to their application. One of the participants even suggested that they would look into including all their suppliers in their upcoming ISO 27001 assessment. This recognition is a positive outcome of this study and one that meets our goal of causing CSPs to step back cognitively from their usual approach to risk assessment.

3) Quantitative Risk Analysis: Following the structured approach of the CSCCRA model, we progressed to the quantitative risk assessment stage. This phase began with a short powerpoint presentation on quantitative risk analysis and risk estimations to a 90% Confidence Interval (CI), after which we presented participants with a short calibration exercise to prepare them for making reasoned estimates about risk factors. Hubbard [32] and Freund & Jones [33] gave insights into conducting proper risk estimations by calibrating the expert

TABLE II

ASSESSING CSP-A SUPPLIER LIST USING CSSA

Anonymised Supplier	**AoS**	**DSH**	**DSC**	**MSA**	**MOS**	**SGC**	**IAM**	**EKM**	**AS**	**Combined Z-Score Value**
IaaS-Pr-A	8	10	10	10	10	10	10	9	9	-0.20
CSP-A	*7*	*9*	*9*	*8*	8	*8*	*9*	*9*	*9*	*1.28*
Email-API-A	10	9	10	10	9	9	10	10	9	-0.17
Video-API-A	9	10	10	9	7	7	9	9	9	0.65
Map-API-A	9	10	9	10	8	10	10	10	9	-0.07
DNS-Pr-A	10	10	10	10	10	10	9	10	10	-0.71
Moni-App-A	10	10	10	9	10	10	10	10	9	-0.46
Pay-App-A	8	10	10	10	9	10	10	10	9	-0.31

team.

Considering that this application is for a non-profit purpose, CSP-A prioritised confidentiality risks over availability and integrity ones. CSP-A acknowledged the impact attacks such as customer data breach could have on their brand name, reputation, and continuous patronage from their other paying customers. The risk identification step of the process looked to identify and prioritise the risks of CSP-A-SaaS, such that, at any given moment, ten or less high priority risks are being tracked on the risk register. So, from the vantage point of the just concluded supplier security assessment and the supply chain mapping, the participants were able to visualise their areas of weakness and begin to identify vulnerabilities, threats and probable risk events.

Table III is an abridged version of CSP-A's risk register. We realised our inability to conduct a 100% comprehensive measurement of risk, hence we settled for pragmatically reducing uncertainty around risk events and having enough information to mitigate the top risks. We focused on the asset-level controls put in place to prevent risk or reduce the effect of its occurrence and discussed ways of improving the controls.

To estimate the value of each identified risk, participants were reminded to consider the results of the initial stages of the assessment in their estimations, to improve their objectivity. Each participant provided an independent estimation of the probability, frequency, impact cost and evaluation of countermeasures for each risk item. Similar to the Factor Analysis of Information Risks (FAIR) method, some of the factors accounted for in the estimation of impact cost include: productivity cost, response costs, replacement costs, and other legal and public relations (PR) costs [33]. The uncertainties in the experts' estimates are presented as a probability distribution, including a Lower Bound (LB), Most Likely (ML) and an Upper Bound (UB), made to a 90% CI.

$$\begin{aligned} RiskValue = PERT(Probability) * PERT(Impact\_Cost) \\ * Poison(Frequency) \end{aligned} \tag{1}$$

After the participants provided their estimates, we gathered the data and analysed each risk item using our Monte Carlo simulation tool. We built models of possible risk results based on the estimations of the risk factors. Each risk result was calculated over five (5) simulations of a hundred thousand (100,000) iterations each, producing a distribution of possible risk values for a particular risk item. Additionally, and as a rule of thumb during our analysis, we applied a mental litmus test to verify if the result of the CQRA simulation appears to be credible considering the participants' estimations. See Figure IV for the estimated risk values.

In Table IV, we present the estimated risk value in rounded numbers for easy analysis, which according to Freund & Jones [33] is also a good way of presenting a risk to decision makers. Our evaluation of the estimated risk value based on existing controls, saw us consider values ranging between the 65% to 90% percentile of the risk value continuum. We did this for a couple of reasons: First was the level of uncertainty around the estimations echoed by a majority of the stakeholders; some of this uncertainty was around the cost of data breach fines (e.g. General Data Protection Regulation (GDPR)) and their limited knowledge of supplier security controls. Secondly, a majority of the risks involved external attackers whose threat capability could be said to be higher than average and an assessment of the existing controls, which in some cases are less optimal. For the brevity of this report, we have not listed each stakeholder's estimation of the various risk factors, neither have we shown the calculation of each risk value.

B. Discussion

This case study set out to assess the risk of a SaaS application using the CSCCRA model. The evaluation is aimed at demonstrating the applicability and feasibility of the model, and validating its use within a real-world context.

In the course of the assessment, we identified some opportunities for security control improvements, some of which are common across multiple asset types (e.g. Logging and MFA). We discovered that the CSP did not conduct a comprehensive evaluation before selecting their critical suppliers. Instead, suppliers were chosen based on the "availability of free credit", "provider reputation", "recommendation" & and "ease of setup". The CSP's limited knowledge of their supplier controls was evident during the cybersecurity posture assessment. Taking a look at the list of identified risks, we see that a majority of them lie within the confidentiality and availability risks and had a reputational impact on CSP-A. CSP-A, however, prioritised confidentiality risks over availability and integrity ones because of its financial impact on their business, either as part of a fine or loss of reputation. This perhaps resulted in the noticeably high impact estimations of specific risk items even though their probability of occurrence were quite low.

TABLE III
LIST OF SECURITY RISKS IDENTIFIED BY THE CSP-A STAKEHOLDERS

Risk No	Risk Description	Supplier	Vulnerability Name	Threat Agent	Threat Type
1.	Loss of CSP-A-SaaS assets due to an unauthorised access to the hosting platform	IaaS-A-Pr, CSP-A	Insufficient Identity and Access Management (No Two factor (2FA), misconfigured access control), No encryption at rest	Malicious Outsiders, Privileged Insiders, CyberCriminals	Sabotage, Social Engineering, Unauthorised Activity, Abuse of Authorisation
2.	Unavailability of service due to DDoS	DNS-Pr-A, IaaS-Pr-A, Pay-App-A	Inadequate resource provisioning, Publicly available service	Malicious Outsider	Denial of Service
3.	Data Breach of customer PII data	IaaS-Pr-A, CSP-A	Unencrypted storage of data, Weak encryption of archives and data in transit, Poor key management procedures,	Malicious Outsiders, Privileged Insiders, Accidental Insider	Information leak/sharing
4.	Loss of SaaS application data	IaaS-Pr	Unencrypted storage of data at rest, Inadequate data archiving procedures (Application and backup storage stored with the same provider)	Provider , malicious outsider, privileged insiders, accidental insider, environmental, political,	Loss due to administrative error, Sabotage, Theft, Failure of system
5.	Data breach of customer sensitive and PII data	Email-API-A, Pay-App-A	Insufficient Identity and Access Management (No Two factor (2FA), misconfigured, Access control), Insufficient Log auditing	Malicious Outsider	Information leak/ sharing
6.	Data breach of customer Payment Card Industry (PCI) data	Pay-App-A	Application/Platform vulnerability, Misconfiguration,	Malicious Outsider	Information leakage
7.	Unavailability of service for 6 hours due to software code bug	CSP-A	Non-optimal change and configuration management procedures, Poor patch management, Limited support staff	Insiders	Service outage,
8.	Malware distribution from SaaS website	CSP-A, IaaS-Pr-A	Application vulnerabilities or poor patch management, limited control for file upload	Malicious Outside, Privileged Insiders	Abuse and Nefarious use of cloud service, Malicious code
9.	Replacing SaaS web video with unsuitable content	CSP-A/ Video-API-A	Insufficient Identity and Access Management (No Two factor (2FA), misconfigured access control), No audit log of video API activity	Malicious (outside, insider)	Abuse and Nefarious use of cloud service, website defacement
10	SaaS application users unable to access platform for 6 hours due to a Service outage	IaaS-Pr-A	Provider misconfiguration, No redundancy, shared platform vulnerabilities	Insider (privileged, accidental), Malicious outsider	Service outage

TABLE IV
CSP-A RISK ANALYSIS RESULT BASED ON CQRA CALCULATION

Risk No	Probability of Occurence			Impact Cost (£) Estimate			Frequency (per year)	Risk Value (£) Estimates			Risk Value (£)
	LB	ML	UB	LB	ML	UB		LB	ML	UB	
R1.	0.50%	2.20%	4.40%	91,852.07	193,996.04	391,144.05	0.10	0.00	1,909.50	10,144.17	4,610
R2.	1.00%	4.20%	9.20%	897.85	3,308.36	6,289.69	2.00	0.00	2,832.79	12,344.24	5,383
R3.	1.70%	4.40%	7.50%	71,471.74	375,472.04	818,307.88	0.50	0.00	9,546.45	45,704.15	22,350
R4.	1.10%	3.90%	7.40%	97,167.81	193,264.91	390,186.33	0.58	0.00	4,379.42	21,102.72	5,815
R5.	3.09%	5.80%	5.80%	2,487.19	7,265.28	14,657.43	0.50	0.00	211.99	1,052.93	906
R6.	1.03%	4.86%	12.40%	24,703.13	152,406.47	386,531.26	0.45	0.00	3,272.94	19,080.34	8,187
R7.	5.23%	10.08%	16.32%	918.83	3,351.24	7,066.79	1.28	0.00	436.14	1,522.44	716
R8.	1.14%	3.25%	7.81%	24,926.22	135,635.75	375,441.62	0.52	0.00	2,328.89	12,054.02	9,945
R9.	**0.50%**	**5.67%**	22.56%	**42,280.34**	**262,761.77**	**771,711.31**	**0.46**	**0.00**	**6,156.74**	**30,040.49**	**27,513**
R10.	1.06%	4.11%	11.39%	907	3,270	6,551	0.80	0.00	109.37	515.77	325

Risk **R1**, which is categorised as a LOW risk, based on the difficulty for an attacker to pull off, is one risk that could disrupt the entire cloud service. Seeing that CSP-A lacks some best practice controls around authentication, logging and encryption, which exposes them to some of the 2018 OWASP top 10 web application vulnerabilities, this assessment justifies the need for the improvement of the existing controls. Also, the risk value estimations of risks **R5** & **R6**, which are data breach attacks on the payment provider (Pay-App-A), is worth discussing. While one would think these two risks should ideally command a high impact cost estimation, they have been rated relatively low, due to the arrangement in place for the delivery of the service. For risk **R6**, CSP-A relies solely on the controls in place at Pay-App-A, which in some cases might not be sufficient. Furthermore, when asked about the low impact cost estimations, one of the stakeholders confirmed that they were not going to be liable for the fines against the payment provider, and they will most likely be hit by reputational loss and other public relations (PR) cost. This is because, post-GDPR, data processors (e.g. payment provider) can now be held accountable by the Information Commissioners Office (ICO) and the data subject, for certain aspects of personal data processing [34].

Other risks related to the defacement of the SaaS website (**R9**), unavailability of the service (**R7** & **R10**) and **R8** - a risk scenario where malicious actors using CSP-A-SaaS as an attack vector, were considered. Risk **R8** was a surprising addition to the risk register, seeing that it is an often overlooked phenomenon in IT risk assessment, i.e. a risk event where the focal asset (item of value) is a threat agent. In this case, CSP-A-SaaS spreading malicious content could easily hurt other members of the supply chain and CSP-A's business.

In presenting the risk assessment result to the CSP, we included risk treatment recommendations which incorporated controls that could mitigate or eliminate the identified risks, and improve CSP-A's operations in the cloud. We consulted cloud security best practice documents [35], [36], identifying corrective actions for each risk item. Based on CSP-A's existing controls, some of our suggested improvements included (i) Improving on the privileged access management; (ii) Improving operational security (redundancy, event notification); (iii) Improving data classification, protection and encryption processes; (iv) Deploying Web Application Firewalls (WAF); and (v) Conducting privacy impact assessment etc.

In summary, these results provide further support for the hypothesis that the CSCCRA model enables CSPs to understand, manage, and make well-informed decisions about their cloud risks. The participants validated the risk assessment process and confirmed the applicability of the model to a SaaS CSP and the effectiveness of its decision-making framework. Their acceptance of the risk assessment results and willingness to continue using aspects of the model for future risk assessments validated the model and its claims of bridging some of the existing cloud risk assessment gaps, e.g. supply-chain and uncertainty quantification. A significant takeaway from this study is the effect of supply chain mapping on stakeholder estimations. According to Beatson [37], protecting an organisation from supplier slip-ups means taking a big-picture view of the information architecture of the cloud service and its underlying infrastructure. This level of transparency is one area where the CSCM and CSSA components of the model, provided valuable input into the risk assessment process.

Another advantage of the CSCCRA methodology is that it demands visibility into the vulnerability of the chain and elicits information sharing, which is key to conducting a comprehensive risk assessment. Likewise, the risk values calculated from the expert's estimations showed that the application of quantitative simulation to reasoned risk factor estimates made by adequately calibrated experts, combined with appropriately communicated assumptions is capable of producing realistic risk values.

V. Conclusion and Future Work

In this study, we validated the applicability of the CSCCRA model in assessing the risk of a multicloud SaaS application through a case study. The result of the case study showed that the structured and systematic application of our proposed model within SaaS organisations yields objective and defensible risk assessment results. Also, the presentation of the risk value in monetary terms promotes cost-effective risk mitigation and optimal risk prioritisation. The model not only caused the participants to step back cognitively from their usual approach to risk assessment, but we believe it made them to fundamentally question and rethink their established interpretations of cloud risks and mitigations. Despite the lack of historical data, CSCCRA's use of controlled experimentation, clearly defined model, peer reviews, and calibration of the expert judges, help CSPs address some of the valid arguments that have limited the use of quantitative risk analysis methods in the information systems domain.

While the CSCCRA process is a long way from being fully automated, it gives CSPs visibility into their cyber-threat landscape, thereby identifying areas of weakness within the supply chain. The CSCM & CSSA components of the model, help stakeholders to gather initial data on their supply chain and understand the potential risks posed by their suppliers. The process of identifying the components that make up a cloud service, their suppliers, mapping the supply chain and assessing these suppliers, compel the CSP to gather more information on the supply chain security, thereby building an understanding of their security posture and the nature of potential risks masked in the supply chain. Over time, the model reduces the time and effort CSPs expend in carrying out comprehensive risk assessments.

However, as with every research project, this study has its limitations. First, we have only validated the model in one CSP environment, and this evaluation was based on the participant's feedback on the workings of the model. Second, we have not compared our assessment process with another model in assessing the risks of CSP-A, which would have provided more convincing results. In addressing these limitations, our future work will see us conduct two more real-world case studies with SaaS cloud providers to validate the applicability of our model to multicloud systems. We will also use other models to assess the identified risks and compare the results. Lastly, we are currently working on developing the CSCCRA model into a web-based application that can be accessed by CSPs over the internet.

Acknowledgment

The authors thank the anonymous reviewers for their helpful and constructive comments. The authors will also like to thank the SaaS CSP that participated in the case study. This research project has been possible thanks to a research grant from EPSRC and Kellogg College, via the Centre for Doctoral Training in Cyber Security at the University of Oxford.

References

[1] M. G. Jacobides, T. Knudsen, and M. Augier, "Benefiting from innovation: Value creation, value appropriation and the role of industry architectures," *Research policy*, vol. 35, no. 8, pp. 1200–1221, 2006.

[2] R. Heininger, M. Böhm, and H. Krcmar, "Managing Heterogeneity in IT Service Management: Towards a Research Agenda," *SIG Service Science (SIG SVC) pre-ICIS Workshop*, no. August 2016, 2013.

[3] S. Gupta, V. Muntes-Mulero, P. Matthews, J. Dominiak, A. Omerovic, J. Aranda, and S. Seycek, "Risk-Driven Framework for Decision Support in Cloud Service Selection," *2015 15th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing*, pp. 545–554, 2015. [Online]. Available: http://www.scopus.com/inward/record.url?eid=2-s2.0-84941248061&partnerID=tZOtx3y1

[4] J. Luna, N. Suri, M. Iorga, and A. Karmel, "Leveraging the Potential of Cloud Security Service-Level Agreements through Standards," *IEEE Cloud Computing*, vol. 2, no. 3, pp. 32–40, 2015.

[5] C. Colwill and A. Gray, "Creating an effective security risk model for outsourcing decisions," *BT Technology Journal*, vol. 25, no. 1, pp. 79–87, 2007.

[6] E. Cayirci, A. Garaga, A. Santana, and 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.

[7] S. Islam, S. Fenz, E. Weippl, and H. Mouratidis, "A Risk Management Framework for Cloud Migration Decision Support," *J. Risk Financ. Manag.*, vol. 10, no. 2, p. 10, 2017. [Online]. Available: http://www.mdpi.com/1911-8074/10/2/10

[8] P. Saripalli and 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.

[9] K. Djemame, D. J. Armstrong, M. Kiran, and 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.

[10] J. O. Fitó, M. Macías, and 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.

[11] O. Akinrolabu, S. New, and 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.

[12] D. Catteddu, H. Giles, H. Thomas, and L. Dupre, "Cloud Computing: Benefits, Risks and Recommendations for Information Security," *Computing*, vol. 72, no. 1, pp. 17–17, 2010. [Online]. Available: http://link.springer.com/10.1007/978-3-642-16120-9_9

[13] S. Marston, Z. Li, S. Bandyopadhyay, J. Zhang, and A. Ghalsasi, "Cloud computing - The business perspective," *Decision Support Systems*, vol. 51, no. 1, pp. 176–189, 2011. [Online]. Available: http://linkinghub.elsevier.com/retrieve/pii/S0167923610002393

[14] S. Bleikertz, T. Mastelić, W. Pieters, S. Pape, and T. Dimkov, "Defining the cloud battlefield: Supporting security assessments by cloud customers," *Proceedings of the IEEE International Conference on Cloud Engineering, IC2E 2013*, pp. 78–87, 2013.

[15] O. Akinrolabu, A. Martin, and S. New, "Assessing cloud risk: The supply chain perspective," pp. 14–16, 2018. [Online]. Available: https://www.bcs.org/content/conWebDoc/59876

[16] M. Sherman, "Risks in the Software Supply Chain," *Software Solutions Symposium*, pp. 1–36, 2017.

[17] Y. Sivasubramanian, S. Z. Ahmed, and V. P. Mishra, "Risk Assessment for Cloud Computing," *International Research Journal of Electronics and Computer Engineering*, vol. 3, no. 2, p. 7, 2017. [Online]. Available: http://researchplusjournals.com/index.php/IRJECE/article/view/292

[18] M. Theoharidou, N. Tsalis, and D. Gritzalis, "In Cloud We Trust: Risk-Assessment-as-a-Service," *Trust Management VII*, vol. 401, pp. 100–110, 2013. [Online]. Available: http://link.springer.com/10.1007/978-3-642-38323-6_7

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

[20] O. Akinrolabu and 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)*, vol. 10, no. 3, pp. 877–892, 2016.

[21] V. Bellandi, S. Cimato, E. Damiani, G. Gianini, and A. Zilli, "Toward economic-aware risk assessment on the cloud," *IEEE Security and Privacy*, 2015.

[22] O. Akinrolabu, S. New, and A. Martin, "Cyber supply chain risks in cloud computing - bridging the risk assessment gap," *Open Journal of Cloud Computing (OJCC)*, vol. 5, no. 1, pp. 1–19, 2018.

[23] J. D. Sterman, "Business dynamics: System thinking and modeling for a complex world," *MIT - Engineering Systems Division Working Paper Series*, no. January 2000, p. 982 pp, 2002.

[24] A. Ghadge, S. Dani, M. Chester, and R. Kalawsky, "A systems approach for modelling supply chain risks," *Supply chain management: an international journal*, vol. 18, no. 5, pp. 523–538, 2013.

[25] S. Gadia, "Cloud Computing Risk Assessment: A Case Study," *ISACA journal*, vol. 4, pp. 11–16, 2011. [Online]. Available: http://www.isaca.org/Journal/Past-Issues/2011/Volume-4/Pages/Cloud-Computing-Risk-Assessment-A-Case-Study.aspx

[26] R. Yin, *Case Study Research: Design and Methods*. SAGE Publications, 2013. [Online]. Available: https://books.google.co.uk/books?id=OgyqBAAAQBAJ

[27] I. Benbasat, D. K. Goldstein, and M. Mead, "The case research strategy in studies of information systems," *MIS quarterly*, pp. 369–386, 1987.

[28] S. Soy, "The case study as a research method," 2015.

[29] BuiltWith, "BuiltWith Technology Lookup," https://builtwith.com/. [Online]. Available: https://builtwith.com/

[30] O. Akinrolabu, S. New, and A. Martin, "Cloud Service Supplier Assessment : A Delphi Study," in *Proceedings of the Eighth International Conference on Innovative Computing Technology (INTECH),2018, Luton, UK*, no. Intech, 2018, pp. 142–150.

[31] W. Chan, E. Leung, and H. Pili, "Enterprise risk management for cloud computing," *Committee of Sponsoring Organizations of the Treadway Commission*, p. 4, 2012.

[32] D. W. Hubbard, *The Failure of Risk Management: Why It's Broken and How to Fix It*. John Wiley & Sons, 2009.

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

[34] L. Maxfield, "Managing commercial risk within the supply chain post - GDPR.Report," 2018. [Online]. Available: https://gdpr.report/news/2018/08/31/managing-commercial-risk-within-the-supply-chain-post/

[35] C. Eric, D. Chris, E. Mike, and G. Jonathan, "Security for Cloud Computing 10 Steps to Ensure Success," *Cloud Standards Customer Council*, pp. 1–35, 2015.

[36] R. Samani, B. Honan, and J. Reavis, *CSA Guide to Cloud Computing*, 2015, no. November 1996.

[37] E. Beatson, "How to Manage Third-Party Risk," 2018. [Online]. Available: https://blogs.infosecurityeurope.com/how-to-manage-third-party-risk/