



## Article

# CSCCRA: A Novel Quantitative Risk Assessment Model for SaaS Cloud Service Providers

Olusola Akinrolabu <sup>1,\*</sup> , Steve New <sup>2</sup> and Andrew Martin <sup>1</sup> <sup>1</sup> Department of Computer Science, University of Oxford, Oxford OX1 2JD, UK; andrew.martin@cs.ox.ac.uk<sup>2</sup> Saïd Business School, University of Oxford, Oxford OX1 2JD, UK; steve.new@sbs.ox.ac.uk

\* Correspondence: olusola.akinrolabu@cs.ox.ac.uk

Received: 3 July 2019; Accepted: 5 September 2019; Published: 8 September 2019



**Abstract:** Security and privacy concerns represent a significant hindrance to the widespread adoption of cloud computing services. While cloud adoption mitigates some of the existing information technology (IT) risks, research shows that it introduces a new set of security risks linked to multi-tenancy, supply chain and system complexity. Assessing and managing cloud risks can be a challenge, even for cloud service providers (CSPs), due to the increased numbers of parties, devices and applications involved in cloud service delivery. The limited visibility of security controls down the supply chain, further exacerbates this risk assessment challenge. As such, we propose the Cloud Supply Chain Cyber Risk Assessment (CSCCRA) model, a quantitative risk assessment model which is supported by supplier security posture assessment and supply chain mapping. Using the CSCCRA model, we assess the risk of a SaaS application, mapping its supply chain, identifying weak links in the chain, evaluating its security risks and presenting the risk value in monetary terms (£), with this, promoting cost-effective risk mitigation and optimal risk prioritisation. We later apply the Core Unified Risk Framework (CURF) in comparing the CSCCRA model with already established methods, as part of evaluating its completeness.

**Keywords:** cloud computing; quantitative risk assessment; supply chain; transparency; security rating service; decision support analysis

## 1. Introduction

Cloud computing is widely believed to be the future of computing [1]. The use of cloud resources has changed the way data is stored, shared and accessed. However, as compelling as cloud computing is for organisational productivity, understanding its information security risks and mitigation strategies is critical [2]. The security challenges of cloud computing are even more formidable in the public cloud, where infrastructure and computational resources are owned, managed and operated by third parties [3]. The use of the public cloud typically means that organisation's data and applications are managed outside their *trust boundary* and require a dynamic supply chain, which invariably introduces a new set of risks, changing the probability of success for a threat source and increasing the impact of an attack. The variety of parties involved in the delivery of a cloud service widens its attack surface [4]. While we argue that the cloud is often more secure, compared to many enterprise networks, the extent of this security is hard to verify, seeing that Cloud Service Providers (CSPs), who should be more aware of cloud risks, find it difficult to audit or assess risks due to limited visibility of security controls and lack of supplier transparency [5].

The multi-tenancy characteristics of the cloud, coupled with its dynamic supply chain, have been identified as two areas of challenge to cloud risk assessment. Studies into the supply chain of cloud services have shown that at least 80% of a typical software-as-a-service (SaaS) application is made up of assembled parts, with each component representing a different level of risk [6]. Also, 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. In an attempt to address the challenges of assessing cloud risks, numerous scholars have developed conceptual models [7–11]. While some of these studies have concentrated on cloud adoption risk assessment, others have followed the traditional route to security risk assessment, adapting the traditional risk frameworks, for example, ISO/IEC 27005, ISO/IEC 31000 and NIST 800-30v1. Being predominantly qualitative or at best semi-quantitative, the prevalent use of these traditional methodologies in assessing cloud risks presents a wide range of limitations including the subjectivity of risk evaluation and the inability to cope with the dynamic cloud infrastructure [12,13].

The limitations of current risk assessment frameworks, therefore, calls 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. Cloud computing risk assessment requires domain-specific knowledge and a deep understanding of the Target of Assessment (ToA), that is, cloud service, to ensure one can arrive at reasonable risk estimates. The risk landscape of a cloud service is constituted of the security risks introduced during the development, implementation, operation and maintenance phases of the service [14]; hence, with traditional frameworks, decision-making has often been based on incomplete information. Therefore, 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.

This study extends the work presented in [15] by providing a more detailed description of the Cloud Supply Chain Cyber Risk Assessment model (CSCCRA) model. Using the CSCCRA model, we assess the risk of a SaaS application, mapping its supply chain, identifying weak links in the chain, evaluating its security risks and presenting the risk value in monetary terms, with this, promoting cost-effective risk mitigation and optimal risk prioritisation. Following this, we apply the Core Unified Risk Framework (CURF) in comparing the CSCCRA model with already established risk assessment methods, as part of evaluating its completeness.

The CSCCRA model is built out to empower CSPs to make reliable inferences about the risk of their cloud service and the performance of their component suppliers, based on a deep understanding of their underlying structure. Through its conduct of an attack surface analysis, the CSCCRA enables cloud providers to identify suppliers who might pose a threat to the cloud service, with this reducing the exposure to the CSP. It builds on existing risk assessment standards and guidance documents such as ISO/IEC 27005 [16], ISO/IEC 31000 [17], NIST 800-30v1 [18] and FAIR risk assessment [19].

The structure of the paper is as follows—we present the literature on cloud risk assessment, supply chain and transparency in Section 2. Then we articulate the CSCCRA model in Section 3. The CSCCRA is used to assess the risk of a SaaS application in Section 4, after which we compare the model with other established methods in Section 5. Section 6 concludes the paper and presents our plans for future work.

## 2. Literature Review

This section focuses on a review of existing cloud risk assessment models, the cloud supply chain and the effect of transparency on cloud risks.

### 2.1. Cloud Risk Assessment

Cloud risk assessment is defined as a 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 [20]. Currently, and despite the very many discourses about cloud computing risks, there is no reliable cloud-specific risk assessment methodology, neither is there a comprehensive vocabulary on cloud risk elements [21]. The cloud industry lacks a structured framework for identifying, assessing and managing cloud risks [8,22]. The lack of a systematic approach and expert subjectivity, synonymous with risk assessments, particularly qualitative, has led to inconsistencies in cloud risks [23,24].

There are relatively few published studies in the area of cloud computing risk assessments both from the academic and industrial communities. Seeing that cloud deployments are rapidly evolving based on new service provider offerings and changing compliance and regulatory landscape, risk assessment solutions would seem not to be keeping pace with cloud growth. Nevertheless, we acknowledge the efforts of international standard and regulatory organisations such as the Cloud Security Alliance (CSA), a not-for-profit organisation, whose mission is to promote the use of best practices that provide security assurance in the cloud [25]. Their work on cloud security, privacy and trust, have formed an excellent foundation for new research. The current state-of-the-art in cloud risk assessment is presented in works of Alturkistani et al. [26] and Drissi et al. [13], where the authors classified recent cloud risk assessment approaches into five and seven categories respectively.

In Table 1, we present a cross-section of other proposed cloud risk assessment methods, highlighting their assessment method, use of experts and evaluation of supply chain.

**Table 1.** Existing Cloud Risk Assessment Models.

Author/Year	Cloud Risk Assessment Description	Method	Implementation	Risk Value	Use of Experts	Supply Chain
(Albakri et al., 2014) [27]	They proposed a model that considers both the cloud customer and the CSP during its risk assessment process.	Qualitative	Yes	Risk Matrix	No	Yes
(Busby et al., 2014) [11]	SECCRIT is a risk assessment model developed to assist organisations in determining the risk associated with cloud adoption.	Qualitative	No	Risk Score	No	Yes
(Djemame et al., 2011) [28]	Risk assessment framework with methodologies for the identification, evaluation, mitigation & monitoring of cloud risks during the various stages of cloud provision.	Semi-quantitative	No	Risk Score	No	Yes
(Fito et al., 2010) [29]	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	Yes	Risk Score	No	No
(Liu & Liu, 2011) [30]	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) [31]	A quantitative risk and impact assessment of cloud risk events based on six key security objectives.	Semi-quantitative	No	Risk Score	Yes	No

Table 1. Cont.

Author/Year	Cloud Risk Assessment Description	Method	Implementation	Risk Value	Use of Experts	Supply Chain
(Sendi & Cheriet, 2014) [9]	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	Yes	Risk Score	No	No
(Sivasubramanian et al., 2017) [10]	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) [32]	The framework was developed for a better understanding of critical areas in cloud computing environments and the identification and mitigation of cloud risks.	Quali-tative	No	Risk Score	No	No

## 2.2. Cloud Supply Chain Risks

The supply chain of a cloud service can be defined as a complex system of two or more parties that work together to provide, develop, host, manage, monitor or use cloud services [33]. The typical cloud supply chain is made up of five essential elements, which are: Cloud Service Providers, Hosting Infrastructure, Delivery Platform, Cloud Control Systems and the Cloud Customers [33]. The cloud supply chain employs “aggressive sourcing” based on free-market principles rather than collaboration, which increases cloud risks. Risks associated with the processes, procedures and practices used to assure the integrity, security, resilience and quality of cloud services increases with the on-demand, automated, and multi-tenanted cloud, down the supply chain [34]. Cloud services are exposed to new threats capable of exploiting the technology, process and organisational vulnerabilities associated with the cloud service delivery.

The supply chain of a cloud service involves multi-level networked relationships among a heterogeneous group of organisations, many of which are small and medium enterprises (SMEs). Lindner et al. [35] believe the application of the supply chain concept to cloud computing to be innovative and suggest the possibility of a new research field. According to Jenks [36], there is a gap between the ‘what’ and ‘how’ processes of managing cloud supply chain cybersecurity risks, and seeing that only a few recommendations have been made to bridge this gap, it remains an open research problem [37,38].

## 2.3. Transparency, Trust and Risk Assessment

Numerous scholars have written extensively about the in-depth connection between transparency and trust [39,40]. Other research works have also considered the effect of transparency on risk [41,42]. However, only a few of these studies have addressed issues in the technology sector, particularly cloud computing. According to Pearson [43] and Schneier [44], the low level of consumer trust resulting from the lack of cloud provider transparency have resulted in new and unquantifiable security risks.

In Reference [45], Ismail et al. described cloud security transparency as the disclosure of security-related practices and controls used for the protection of customer data and applications hosted in the cloud environment. Similarly, Werff et al. [46] defined trust as a three-stage process consisting of positive expectation, the decision to make oneself vulnerable to another party and a risk-taking act. In Reference [47], the author makes a distinction between contractual, competence and goodwill trust, while the work of Sung & Kang [48] lists long-term and repeated interaction, information sharing and reciprocity, and interdependence and asset specificity as the determinants of trust level between firms. In cloud supply chains, trust is one of the fundamental cooperation factors [49]. To establish the interconnectedness between transparency, trust and risk assessment, Kaliski-Jr and Pauley [20] point out that an increased level of trust improves disclosure and reduces perceived risk, while Pearson [43] concludes that risk assessments provide significant value in increasing trust in commercial services. In Figure 1, we show how each element contributes to improving consumer perception of cloud adoption risks.

According to the Centre for the Protection of National Infrastructure (CPNI), the awareness or visibility of third-party risks is the key to effective risk management [50]. The lack of cloud provider data on cloud risks, which is hindered by concerns for reputational risks [51], remains a primary challenge for the cloud industry. An example of this lack of transparency is found in CSA’s report on cloud outages between 2008 and 2013. The report listed 172 unique cloud incidents, but only 129 (75%) providers declared the cause of the outage, while 43 (25%) failed to attribute their outage to a particular vector [52].

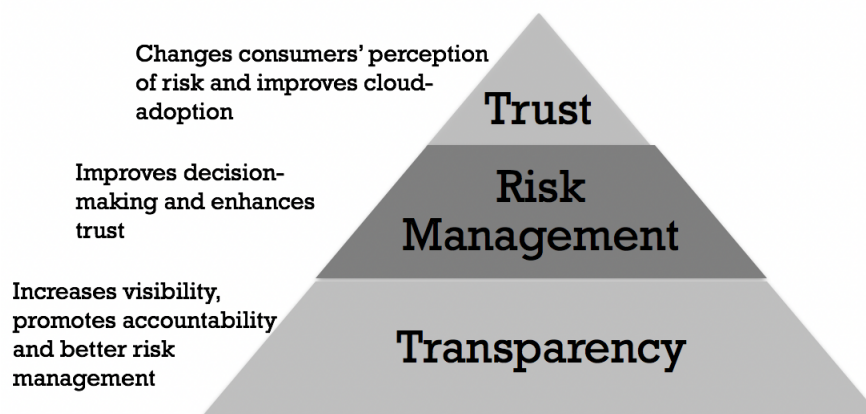


Figure 1. Transparency, Trust and Risk Management between Cloud Stakeholders.

#### 2.4. Research Gap and Proposal

As shown in Table 1, only a few cloud risk assessment models have considered the inherent risks in the supply chain. Furthermore, due to the lack of a structured framework for cloud assessment, many of the existing studies continue to adopt the traditional IT risk assessment methods, which are predominantly qualitative, static and unable to adapt to the dynamic cloud supply chain. With the cloud supply chain made up of SMEs, whose vulnerability to cyber attacks magnifies into the supply chains, there is a need to assess cloud risks from a supply chain perspective, identifying the sub-providers involved in service delivery and evaluating their security controls. This remains a gap with provider-based risk assessment, one which if addressed, is capable of promoting visibility into the vulnerability of the chain and information sharing, both of which are key to conducting a comprehensive RA.

As such, we propose the CSCCRA model, which we argue, partially addresses the problem of supply chain risks in cloud computing. Currently, no other study has addressed this problem, and since information security is all about decisions, we believe that this quantitative and iterative approach to cloud risk assessment, will provide CSPs with an objective risk result, that is consistent, easy to understand and encourages continuous mitigation of cloud risks.

### 3. The CSCCRA Model

The CSCCRA model (see Figure 2) considers the dynamism of the cloud supply chain and looks to address the gap of cloud supply chain transparency, and how the lack of visibility of supplier's security controls have contributed to the inadequate level of cloud risk assessment. Knowing that this can be a difficult undertaking, not least because of the inherently unpredictable and chaotic cloud supply chain, we adopt the systems thinking approach to solving complex system problems as suggested by Ghadge et al. [53]. Systems thinking provides the ability to see the world as a complex system and understand the interconnectedness of networks [54]. Using this approach, we conceptualise and analyse the interdependencies of a cloud service during the risk assessment and make use of modelling and simulation techniques to draw the result of the assessment.

Given the scarcity of initiatives for the practical implementation of a quantitative cloud risk assessment, the development of the CSCCRA model aims to contribute towards improving the state-of-the-art in cloud risk assessment. It hopes to achieve this by showing how a holistic quantitative risk assessment and decision analysis model provides a unique capability for capturing the dynamic behaviour of risks within a cloud supply chain and measuring the overall risk behaviour. While numerous scholars have openly questioned the subjectivity of expert's estimate in quantitative analysis [12,18], our implementation of CSCCRA aims to prove that despite the lack of historical data,



cloud risk assessments can achieve increased objectivity through the use of controlled experimentation, clearly defined model, peer reviews and calibration of the expert judges [19,55].

The steps taken to assess cloud provisioning risks using the CSCCRA model are as shown in Figure 2 and are listed as follows [56]:

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.

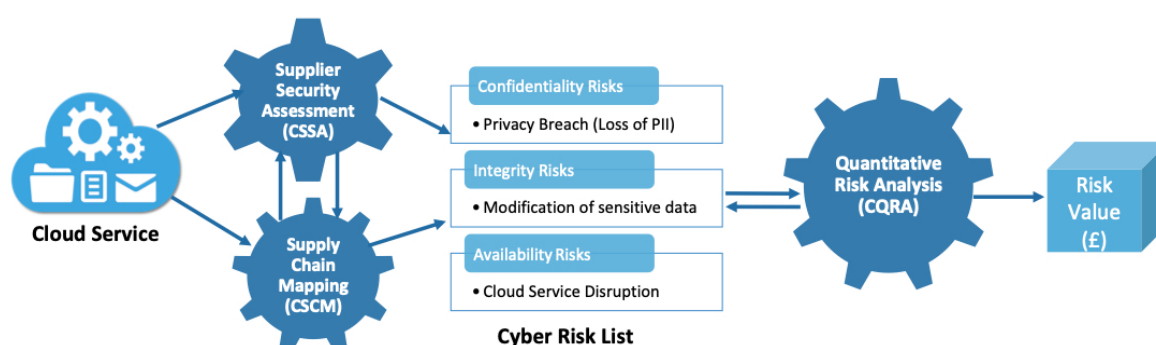


Figure 2. Overview of Cloud Supply Chain Cyber Risk Assessment (CSCCRA) model.

The three components of the CSCCRA model are [33]:

1. **Cloud Quantitative Risk Analysis (CQRA):** The CSCCRA model goes beyond the IT industry norm to apply a quantitative assessment method to cloud risks for at least three reasons. First, the ability to express risk as the combination of the probability of an event and its consequences as per ISO Guide 73:2009 [57]. Second, the rigorous process involved in the identification of supply chain risk factors [23], and third, the use of controlled experimentation [19]. With uncertainty being the primary factor in risk analysis, the CSCCRA model makes use of a probabilistic estimate of risk factors, for example, threat frequency, vulnerability and loss magnitude, representing the forecast as a distribution (e.g., PERT, Poisson). To avoid cloud risk assessment being classed as mere speculation or opinion of risk assessors, and moving it into the realm of knowledge, based on informed opinion, making up for the lack of empirical evidence, the CQRA makes use of calibrated assessors, who can make reasonable estimates. The tool is implemented using the @RISK Monte Carlo Simulation Engine by Palisade [58], which is an add-in to Microsoft Excel.
2. **Cloud Supplier Security Assessment (CSSA):** The CSSA module of the CSCCRA, is a novel addition to cloud risk assessment, and functions as a Security Rating Service (SRS) for the suppliers involved in the delivery of the cloud service. The CSCCRA model requires cloud providers to be aware of their supply chain and have sufficient information about the processes and capabilities of their vendors. The CSSA addresses the notion of a distorted and incomplete process involved in cloud supplier selection. Being a Multi-criteria decision making (MCDM) tool, its use in cloud risk assessment ensures that decision made around cloud risks follows a formal and rigorous form. Furthermore, Gartner also encourages organisations to adopt SRS as part of their ongoing program for third-party cyber risk management [59]. The CSSA process involves decomposing the cloud service into its component objects and using an improper linear model, rating all entities based on identified security criteria. This process results in the identification of weak suppliers readily susceptible to a cyber attack or those with a high risk

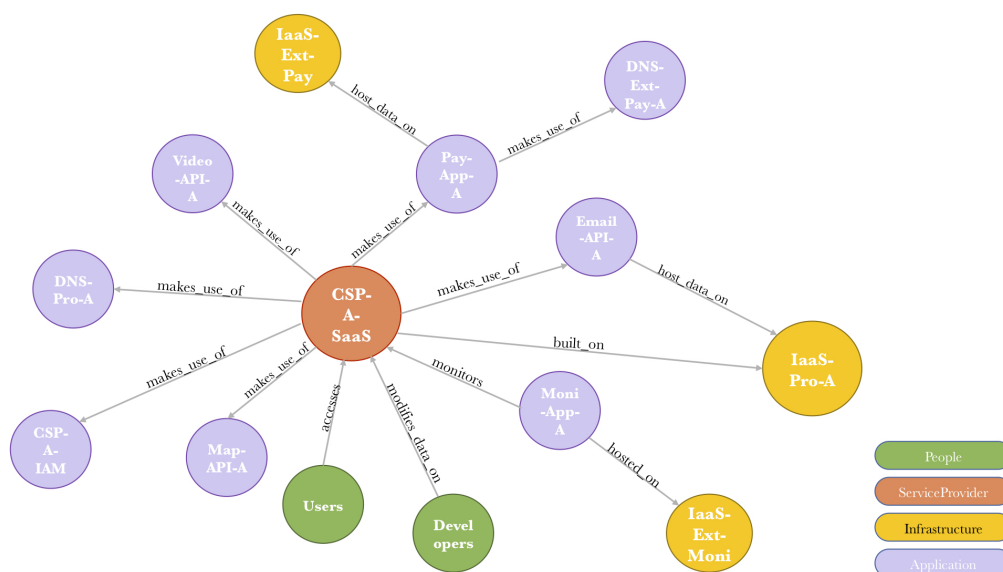


of failure. Ghadge et al. [53] supports this approach, arguing that the identification of potential weak spots in the supply chain through a dynamic model, captures its vulnerability and promote proactive mitigation of risks.

3. **Cloud Supply Chain Mapping (CSCM):** Providing end-to-end supply chain visualisation while assessing cloud risk makes it amenable to analyse and explore areas of weakness, strengths and the potential risks to a cloud service while also supporting collaboration and decision-making within the chain [60]. Visualising the information flow of a cloud service through the supply chain assists in identifying critical suppliers and single points of failures (SPOFs) within the chain. The benefit of a graphical representation of the inherent risk in the supply chain helps to counter any documented biases in risk estimation and decision-making and is thought to have an impact in reducing the cognitive load involved in the estimation of risk factors [61]. The CSCCRA model employs supply chain mapping during the pre-assessment stage, to allow for continuous monitoring and visibility of the current state of cloud risk, and enable a data-driven risk identification and estimation; not one based on assessor's instinct.

#### 4. Sample Risk Assessment with CSCCRA

To illustrate the steps of the CSCCRA model, we consider a cloud risk scenario where there is a loss of SaaS provider (CSP-A) assets, due to unauthorised access to the hosting platform by malicious actors. Here we assume that both the CSCM and CSSA Steps have been completed. In Figure 3, we present the supply chain mapping of the SaaS application. The use of a visual structural model illustrates the interdependencies between the components and accurately visualise the cloud information flow. Here we see that CSP-A-SaaS (focal SaaS) relies on IaaS-Pr-A not just for its hosting function, but there is also an indirect dependency on the provider for email services (Email-API-A).



**Figure 3.** Supply Chain mapping of CSP-A-SaaS using the Cloud Supply Chain Mapping (CSCM) tool.

Also, Table 2 shows the supplier security assessment. The cloud service is broken down into its components based on suppliers, and each supplier is scored on nine 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., assists CSPs in the identification of weak suppliers readily susceptible to cyber-attack or those with a high risk of failure. See Reference [62] for more information on the target dimensions. 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). After this, a Z-Score ( $Z_i$ ) is calculated for each

target dimension, and the Z-Scores are summed up in the last column. The Z-score is a statistical measurement of a score's relationship to the mean in a set of scores. It measures how many standard deviations ( $\sigma$ ), a score ( $y_i$ ) is above or below the population mean ( $y$ ) [63]. The use of colour and values are considered as suitable methods for communicating information in a visual framework [61]. The colour in each of the cells in the last column of Table 2, conveys the degree of risk that particular component has, compared to the rest of the chain. A green cell has the best risk score (least risky), followed by yellow and then red.

**Table 2.** Assessing CSP-A Supplier list using Cloud Supplier Security Assessment (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

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

$$PWC = PERT(5, 7, 10) \quad (2)$$

$$CE = PERT(2, 3, 4) \quad (3)$$

$$PC = PWC - CE \quad (4)$$

$$IC = PERT(50, 000, 250, 000, 700, 000) \quad (5)$$

$$Fr = Poisson(1) \quad (6)$$

$$IC_y = IC * Fr \quad (7)$$

$$ERV\_C = IC_y * PC \quad (8)$$

$$ERV\_WC = IC_y * PWC \quad (9)$$

The risk calculation shown in Table 3 and illustrated by the Equations (2)–(9), is based on a consensus of estimates by stakeholders within the CSP organisation based on their knowledge of the hosting provider. Each of the factors excluding the frequency of attack is represented by a PERT distribution, where the assessors are required to provide estimates to a 90% confidence interval, that is, lower bound (5%), most likely and upper bound (95%) estimate of the factors. A Poisson distribution represents the frequency of attack since it expresses the probability of a given number of events occurring within a fixed time. With the estimates provided, CQRA is then used to compute the risk value, both when controls are in place and when the controls are ineffective. The final risk value is presented in monetary terms (£) with three estimates (lower bound, mean value and upper bound). Moreover, the choice of which risk value is acceptable to the decision-makers depends on their risk appetite. Although from experience, when CSP's consider the threat and vulnerability of their application combined with their understanding of the controls in place, they arrive at a Most Likely (ML) risk value which sits around the 85% percentile of the distribution.

**Table 3.** Risk R1—Loss of CSP-A-SaaS assets due to unauthorised access to the hosting platform (IaaS-Pr-A).

Uncertain Inputs	Parameter of Distribution			
	Distribution	Lower Bound	Most Likely	Upper Bound
Probability of risk (without controls) (PWC)	PERT	5%	7%	10%
Control Efficiency (CE)	PERT	2%	3%	4%
Impact cost (IC)	PERT	£50,000	£250,000	£700,000
Average Rate				
Frequency of occurrence per year (Fr)	Poisson	1		
Estimated Risk Value (ERV)	Without Controls (ERV_WC)	With Controls (ERV_C)		
5% Percentile	£0	£0		
Mean	£20,768.90	£12,067.60		
95% Percentile	£68,667.13	£40,746.61		

In summary, the presentation of the risk value in monetary terms promotes cost-effective risk mitigation and optimal risk prioritisation. Also, the results of the model can be interpreted qualitatively to a lay audience using various formats including tables, graphs, heat maps, risk matrices and qualitative ratings, or to a learned audience using probability density functions (PDF) or cumulative density functions (CDF).

## 5. Completeness Comparison of the CSSCRA Model with Established Models and Standards

Having gone through the steps taken by the CSSCRA model to assess CSP cloud risks, we now compare the model with already established risk assessment standards and guidance documents based on their completeness. Here, completeness refers to an evaluation of whether the model considers all relevant inputs, includes all necessary tasks and whether the model outputs are linked to concepts of information systems (IS) risks [64]. While several frameworks could have been selected to conduct this comparison, we chose the Core Unified Risk Framework (CURF) [65]. The framework is proposed as an all-inclusive approach for comparing different risk assessment method [65]. All-inclusive, because the criteria for estimating the completeness of a risk assessment method, organically grow by adding new issues and tasks from every reviewed method. CURF allows for a detailed qualitative comparison of processes and activities in each RA method and provides a measure of completeness. It is scoped to compare the content of methods to a predefined set of criteria instead of evaluating process tasks or the issue the method is designed to address.

In their study, Wangen et al. [65] applied the framework to assessing 12 formal information system risk assessment (ISRA) methods and found the ISO/IEC 27005:2011 method to be the most complete approach overall, and both FAIR and ISO/IEC 27005:2011 to be the most complete for risk estimations. In this section, we will be assessing the CSSCRA based on the three main risk assessment processes: risk identification, risk estimation and risk evaluation, and scoring each task identified under the main process. As shown in Table 4, we evaluate if each task is **Addressed** (2), **Partially Addressed** (1) or **Not Addressed** (0).

**Table 4.** Scoring CSCCRA's Risk identification, estimation and evaluation process using the Core Unified Risk Framework (CURF). Scores: XX = 2, X = 1. XX Addressed, X Partially addressed, - Not addressed.

Risk Identification	Score	Risk Estimation	Score	Risk Evaluation	Score
Preliminary assessment	XX	Asset identification and evaluation	XX	Risk criteria assessment /revision (RCA)	X
Risk criteria determination	XX	Threat willingness/Motivation	X	Risk prioritisation/Evaluation (RPE)	XX
Cloud-specific risk considerations	XX	Threat capability (know how)	X	Risk treatment recommendation (RTR)	XX
Business objective Identification	XX	Threat capacity (Resources)	-		
Key risk indicators	XX	Threat attack duration	-		
Stakeholder identification	XX	Vulnerability assessment	XX		
Stakeholder analysis	XX	Control efficiency assessment	XX		
Asset identification	XX	Subjective Probability Estimate for event	-		
Mapping of personal data	X	Quantitative Probability Estimate for event	XX		
Asset evaluation	XX	Subjective impact estimation	-		
Asset owner and custodian	X	Quantitative impact estimation	XX		
Asset container	XX	Privacy risk estimation	X		
Business process identification	X	Utility and incentive calculation	XX		
Vulnerability identification	XX	Cloud vendor assessment	-		
Vulnerability assessment	X	Opportunity cost	XX		
Threat identification	XX	Level of risk determination	X		
Threat assessment	X	Risk aggregation	XX		
Control identification	XX	<i>Event,</i>	XX		
Control assessment	X	<i>Consequence,</i>	XX		
Outcome identification	XX	<i>Uncertainty,</i>	XX		
Outcome assessment	X	<i>Probability,</i>	XX		
<i>Asset,</i>	XX	<i>Model sensitivity,</i>	XX		
<i>Vulnerability,</i>	XX	<i>Knowledge about risk</i>	X		
<i>Threat,</i>	XX				
<i>Outcome</i>	XX				
<b>Completeness (Total)</b>	<b>43/50</b>		<b>31/46</b>		<b>5/6</b>

According to Wangen et al. [65], a baseline level of security can be achieved through compliance with standards, legislation and regulations, but to align with industry best practice (cloud in our case) is highly dependent on having a tailored and functional information security risk management (ISRM) processes. Our model helps CSPs to complete two of the most common risk identification activities, that is, asset identification and evaluation. The unique addition of the CSSA and CSCM pre-assessment steps tailors the model to assess the risk of composite systems. Furthermore, to improve the completeness of our proposed model, we accompanied it with a software toolkit, available to CSPs who are interested in using the model in assessing their cloud service.

1. **Risk Identification:** CSCCRA's risk identification process follows a risk scenario approach, which accounts for the major risk factors that play a part in the risk event. It identifies the asset (cloud service), vulnerability, threat, impact, consequence, and existing controls. Its pre-assessment activity leads to risk identification and risk scenario development. This helps with identifying situations where an asset could be vulnerable without being threatened or threatened without being vulnerable, or where a vulnerable asset is not critical to the organisation.
2. **Risk Estimation:** The CSCCRA is a quantitative risk assessment model that defines risk as a function of events, consequences, frequency, probability and their associated uncertainties. It uses the Monte Carlo simulation for the calculation of risk value, accounting for the expert's uncertainty about their estimation and representing risk value as a probability distribution. The model incorporates a control efficiency assessment into the probability of risk event estimations, to provide stakeholders with the strength of their existing controls.
3. **Risk Evaluation:** The final phase of the CSCCRA model is the risk evaluation, where the analysed risks are evaluated and prioritised according to their risk values. Also, during this phase, the risk assessor makes a recommendation to the CSP about the treatment of their top ten risks using security best practices as a guide. This provides the decision-makers with the information they need to prioritise and mitigate their risk according to the available resources.

In Table 5, we place our self-evaluated CSCCRA scores alongside other established models. In this evaluation, the CSCCRA model had a completeness score of 79 out of a possible total of 102. The evaluation of the other models was completed in Wangen et al. [65] where more information on the scoring can be found.

Critically looking into the CSCCRA framework and comparing its completeness with other well-established models like ISO/IEC 27005, NIST 800-30, FAIR and ISACA's RiskIT, we see that the CSCCRA has made functional improvements on the existing models. Applying the criteria outlined in the CURF framework shows the CSCCRA model met most of the requirements for each stage of the risk assessment process and can be judged to be a more complete method. Nevertheless, this result must be interpreted with caution because our scoring of the CSCCRA was based on a self-appraisal, and the complete objectivity of the evaluation completed by Wangen et al. [65] cannot be ascertained.

While the performance of the CSCCRA model can be attributed to the fact that the model builds on existing risk assessment standards and guidance documents, we argue that the novelty to expand its functional scope to include the supply chain also plays an integral part in its success. The completeness test also shows the extent of the model's granularity as a risk assessment framework and its adaptability to assessing the risks of any other composite system.

**Table 5.** Comparing CSCCRA's Risk identification, estimation and evaluation process with other established models.

	CSCCRA	CRAMM	FAIR	OCTAVE Allegro	ISO 27005	NIST 800-30	RISK IT	Max Score
Risk Identification	43	29	26	32	38	24	29	50
Risk Estimation	31	10	30	14	27	26	22	46
Risk Evaluation	5	4	2	5	3	2	4	6
<b>Completeness Total</b>	<b>79</b>	<b>43</b>	<b>58</b>	<b>51</b>	<b>68</b>	<b>52</b>	<b>55</b>	<b>102</b>

## 6. Conclusions and Future Work

This study set out to identify the supply chain gap in cloud risk assessment and propose the CSCCRA model as a way of bridging this gap. In describing the model, we listed its principal components and presented a cloud provider scenario where the model is valuable. We examined the effect of supply chain transparency on cloud risks, by applying an iterative, incremental and inclusive approach to cloud risk assessment. Using our proposed model, we showed how the

decomposition of risk items into its various risk factors, allows decision-makers to investigate cloud risks, avoiding extreme subjectivity in their evaluation.

Although targeted only at CSPs and not cloud customers, a distinctive contribution of this study is that it caters for the complexities involved in cloud delivery 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. This rigorous and dynamic risk assessment model, combines aspects of various disciplines, ranging from cybersecurity, supplier assessment, systems thinking, decision support systems, transparency, modelling, supply chain mapping and risk assessment, applying them in a multi-staged approach to the problem area.

While not ignorant of the counter-argument against quantitative models, particularly around their complexity of computation and cost, we argue that the CSCCRA, being a well-defined model, simplifies the process of cloud risk assessment. Also, the rigour involved in the process, allows decision-makers to investigate each aspect of the risk, avoiding extreme subjectivity in their evaluation. The model's completeness score also emphasises its functional improvement on existing risk assessment methods.

Future work will see us conduct more real-world case studies with SaaS cloud providers to validate the applicability of our model to multicloud systems. After which, we plan to develop the CSCCRA model into a web-based application that can be accessed by CSPs over the internet.

Collectively, we anticipate that the implementation of the CSCCRA model will reveal that the structured and systematic approach to cloud risk assessment can deliver objective risk results, saving the CSP time and effort as they mature into the use of the model.

**Author Contributions:** Conceptualization, O.A., S.N., and A.M.; Investigation, O.A.; Methodology, O.A.; Writing—original draft, O.A.; Writing—review and editing, O.A. and S.N.; Supervision, S.N. and A.M.

**Funding:** 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. The article is an extended version of the paper presented at the 15th European, Mediterranean and Middle Eastern Conference on Information Systems (EMCIS) in 2018.

**Conflicts of Interest:** The author declares no conflict of interest.

## References

1. Ruparelia, N.B.; Ruparelia, N. *Cloud Computing*; MIT Press: Cambridge, MA, USA, 2016.
2. Mell, P.; Grance, T. The NIST Definition of Cloud Computing Recommendations of the National Institute of Standards and Technology. *Nist Spec. Publ.* **2011**, *145*, 7. [\[CrossRef\]](#)
3. Jansen, W.; Grance, T. Guidelines on Security and Privacy in Public Cloud Computing. *Director* **2011**, *144*. [\[CrossRef\]](#)
4. Bleikertz, S.; Mastelić, T.; Pieters, W.; Pape, S.; Dimkov, T. Defining the Cloud Battlefield: Supporting Security Assessments by Cloud Customers. In Proceedings of the IEEE International Conference on Cloud Engineering (IC2E 2013), Redwood City, CA, USA, 25–27 March 2013; pp. 78–87. [\[CrossRef\]](#)
5. Pearson, S. Data Protection in the Cloud. *Cloud Secur. Alliance Online* **2016**, 10–13.
6. Sherman, M. Risks in the Software Supply Chain. In Proceedings of the Software Solution Symposium, Alexandria, VA, USA, 20–23 March 2017; pp. 1–36.
7. Cayirci, E.; Garaga, A.; De Oliveira, A.S.; Roudier, Y. A Cloud Adoption Risk Assessment Model. In Proceedings of the 2014 IEEE/ACM 7th International Conference on Utility and Cloud Computing, London, UK, 8–11 December 2014; pp. 908–913. [\[CrossRef\]](#)
8. Islam, S.; Fenz, S.; Weippl, E.; Mouratidis, H. A Risk Management Framework for Cloud Migration Decision Support. *J. Risk Financ. Manag.* **2017**, *10*, 10. [\[CrossRef\]](#)
9. Sendi, A.S.; Cheriet, M. Cloud Computing: A Risk Assessment Model. In Proceedings of the 2014 IEEE International Conference on Cloud Engineering, London, UK, 8–11 December 2014; pp. 147–152. [\[CrossRef\]](#)
10. Sivasubramanian, Y.; Ahmed, S.Z.; Mishra, V.P. Risk Assessment for Cloud Computing. *Int. Res. J. Electron. Comput. Eng.* **2017**, *3*, 2412–4370. [\[CrossRef\]](#)



11. SECCRIT. Secure Cloud Computing for Critical Infrastructure IT, “Methodology for Risk Assessment and Management”. 2014. Available online: <https://cordis.europa.eu/project/rcn/106660/reporting/en> (accessed on 8 September 2019).
12. Theoharidou, M.; Tsalis, N.; Gritzalis, D. In Cloud We Trust: Risk-Assessment-as-a-Service. *Trust Manag.* **VII** **2013**, *401*, 100–110. [[CrossRef](#)]
13. Drissi, S.; Benhadou, S.; Medromi, H. Evaluation of Risk Assessment Methods Regarding Cloud Computing. In Proceedings of the 5th Conference on Multidisciplinary Design Optimization and Application, Shenzhen, China, 26–30 June 2016.
14. Ellison, R.J.; Goodenough, J.B.; Weinstock, C.B.; Woody, C. *Evaluating and Mitigating Software Supply Chain Security Risks*; Technical Report; Carnegie-mellon University, Pittsburgh PA software Eng, Institute: Pittsburgh, PA, USA, 2010.
15. Akinrolabu, O.; New, S.; Martin, A. CSCCRA: A Novel Quantitative Risk Assessment Model for Cloud Service Providers. In Proceedings of the European, Mediterranean, and Middle Eastern Conference on Information Systems, Limassol, Cyprus, 4–5 October 2018; pp. 177–184.
16. ISO 27005. *BS ISO/IEC 27005: 2011 BSI Standards Publication Information Technology—Security Techniques—Information Security Risk Management*; ISO: Geneva, Switzerland, 2011.
17. International Standards Organisation. *ISO 31000—Risk Management*; ISO: Geneva, Switzerland, 2009. [[CrossRef](#)]
18. Ross, R.S. *Guide for Conducting Risk Assessments*; Special Publication (NIST SP)—800-30 Rev 1; NIST: Gaithersburg, MD, USA, 2012; p. 95.
19. Freund, J.; Jones, J. *Measuring and Managing Information Risk*; Butterworth-Heinemann: Oxford, UK, 2015; pp. 293–333.
20. Kaliski, B.S., Jr.; Pauley, W. Toward Risk Assessment as a Service in Cloud Environments. In Proceedings of the 2nd USENIX Conference on Hot Topics in Cloud Computing, Boston, MA, USA, 22–25 June 2010; pp. 1–7.
21. Groubauer, B.; Walloschek, T.; Stöcker, E. Understanding Cloud Computing Vulnerabilities. *Softw. Reuse Emerg. Cloud Comput. Era* **2011**, 204–227. [[CrossRef](#)]
22. Vohradsky, D. Cloud Risk—10 Principles and a Framework for Assessment. *ISACA J.* **2012**, *5*, 1–11.
23. Hubbard, D. *The Failure of Risk Management: Why It's Broken and How to Fix It*; John Wiley & Sons: New York, NY, USA, 2009; pp. 134–143.
24. Tang, H.; Yang, J.; Wang, X.; Zhou, Q. A Research for Cloud Computing Security Risk Assessment. *Open Cybern. Syst. J.* **2016**, *10*, 210–217. [[CrossRef](#)]
25. Samani, R.; Honan, B.; Reavis, J. *CSA Guide to Cloud Computing*; Number November 1996; Elsevier, Inc.: Philadelphia, PA, USA, 2015; pp. 1–216.
26. Alturkistani, F.M.; Emam, A.Z. A Review of Security Risk Assessment Methods in Cloud Computing. In *New Perspectives in Information Systems and Technologies, Volume 1*; Rocha, Á.; Correia, A.M., Tan, F.B., Stroetmann, K.A., Eds.; Springer International Publishing: Cham, Switzerland, 2014; pp. 443–453.
27. Albakri, S.H.; Shanmugam, B.; Samy, G.N.; Idris, N.B.; Ahmed, A. Security risk assessment framework for cloud computing environments. *Secur. Commun. Netw.* **2014**, *7*, 2114–2124. [[CrossRef](#)]
28. Djemame, K.; Armstrong, D.J.; Kiran, M. A Risk Assessment Framework and Software Toolkit for Cloud Service Ecosystems. In Proceedings of the Second International Conference on Cloud Computing, GRIDs, and Virtualization, Rome, Italy, 25–30 September 2011; pp. 119–126.
29. Fito, J.; Macias, M.; Guitart, J. Toward Business-Driven Risk Management for Cloud Computing. In Proceedings of the 2010 International Conference on Network and Service Management, Niagara Falls, ON, Canada, 25–29 October 2010; pp. 238–241. [[CrossRef](#)]
30. Liu, P.; Liu, D. The new risk assessment model for information system in Cloud Computing Environment. *Procedia Eng.* **2011**, *15*, 3200–3204. [[CrossRef](#)]
31. Saripalli, P.; Walters, B. QUIRC: A Quantitative Impact and Risk Assessment Framework for Cloud Security. In Proceedings of the 2010 IEEE 3rd International Conference on Cloud Computing, Miami, FL, USA, 5–10 July 2010; pp. 280–288. [[CrossRef](#)]
32. Zhang, L.J.; Zhang, J.; Fiaidhi, J.; Chang, J.M. Hot Topics in Cloud Computing. *IT Prof.* **2010**, *12*, 17–19. [[CrossRef](#)]



33. Akinrolabu, O.; New, S.; Martin, A. Cyber Supply Chain Risks in Cloud Computing—Bridging the Risk Assessment Gap. *Open J. Cloud Comput.* **2018**, *5*, 1–19.
34. Boyens, J.; Paulsen, C.; Moorthy, R.; Bartol, N. Supply Chain Risk Management Practices for Federal Information Systems and Organizations. *NIST Spec. Publ.* **2015**. [CrossRef]
35. Lindner, M.; Chapman, C.; Clayman, S.; Henriksson, D.; Elmorh, E. The Cloud Supply Chain: A Framework for Information , Monitoring , Accounting and Billing. In Proceedings of the 2nd International Conference on Cloud Computing, Barcelona, Spain, 25–28 October 2010.
36. Jenks, M. Critical Infrastructure Protection Supply Chain Risk Management. 2016. pp. 1–6. Available online: <https://www.ferc.gov/CalendarFiles/20160127144710-Jenks,%20KCPL.pdf> (accessed on 17 July 2017).
37. Motta, G.; You, L.; Sfondrini, N.; Sacco, D.; Ma, T. Service Level Management ( SLM ) in Cloud Computing Third party SLM framework. In Proceedings of the 2014 IEEE 23rd International WETICE Conference, Parma, Italy, 23–25 June 2014.
38. Luna, J.; Suri, N.; Iorga, M.; Karmel, A. Leveraging the Potential of Cloud Security Service-Level Agreements through Standards. *IEEE Cloud Comput.* **2015**, *2*, 32–40. [CrossRef]
39. Hofstede, G.J. *Supply Chain Management*; IGI Global: Hershey, PA, USA, 2007.
40. Conley, R. *Three Levels of Trust—Where Do Your Relationships Stand?* Blanchard LeaderChat on WordPress.com; 2012. Available online: <https://leaderchat.org/2012/10/25/three-levels-of-trust-where-do-your-relationships-stand/> (accessed on 26 July 2017).
41. Charney, S.; Werner, E.T. *Cyber Supply Chain Risk Management: Toward a Global Vision of Transparency and Trust*; Microsoft Corporation: Redmond, WA, USA, 2011; p. 19.
42. New, S.; Brown, D. The Four Challenges of Supply Chain Transparency. *Eur. Bus. Rev.* **2012**, 1–7. Available online: <https://www.europeanbusinessreview.com/challenges-supply-chain-transparency/> (accessed on 24 July 2017).
43. Pearson, S.; Labs, H.P. Towards Accountability in cloud.pdf. *HP Labs Tech. Rep.* **2011**, *15*, 64–69.
44. Bruce Schneier. Should Companies Do Most of Their Computing in the Cloud? (Part 1)—Schneier on Security. 2015. Available online: [https://www.schneier.com/blog/archives/2015/06/should\\_companie.html](https://www.schneier.com/blog/archives/2015/06/should_companie.html) (accessed on 21 March 2017).
45. Ismail, U.M.; Islam, S.; Ouedraogo, M.; Weippl, E. A framework for security transparency in Cloud Computing. *Future Internet* **2016**, *8*. [CrossRef]
46. Werff, L.V.D.; Lynn, T.; Xiaong, H. Building Trust in the Cloud Environment: Towards a Consumer Cloud Trust Label. In Proceedings of the Eighth International Conference on Digital Society (ICDS 2014), Barcelona, Spain, 23–27 March 2014.
47. Sako, M. *Price, Quality and Trust: Inter-Firm Relations in Britain and JAPAN*; Number 18; Cambridge University Press: Cambridge, UK, 1992.
48. Sung, S.; Kang, S. The Trust Levels, Trust Determinants, and Spatial Dimensions in Inter-Firm Relationships: A Warehousing Firm’s Perspective in the City of Busan, South Korea. *iBusiness* **2012**, *4*, 371. [CrossRef]
49. Grzybowska, K.; Kovács, G.; Lénárt, B. The supply chain in cloud computing. *Res. Logist. Prod.* **2014**, *4*, 33–44.
50. CPNI. *Security for Industrial Control Systems—Manage Third Party Risks*; CPNI: London, UK, 2015; Volume 1, pp. 1–16.
51. Power. The risk management of everything. *J. Risk Financ.* **2004**, *5*, 58–65. [CrossRef]
52. Ko, R.; Lee, S.; Rajan, V. *Cloud Computing Vulnerability Incidents: A Statistical Overview*; Cloud Security Alliance: Palo Alto, CA, USA, 2013; p. 21.
53. Ghadge, A.; Dani, S.; Chester, M.; Kalawsky, R. A systems approach for modelling supply chain risks. *Supply Chain Manag. Int. J.* **2013**, *18*, 523–538. [CrossRef]
54. Sterman, J.D. *Business Dynamics: System Thinking and Modeling for a Complex World*; MIT-Engineering Systems Division Working Paper Series; McGraw-Hill Education: Berkshire, UK, 2002; p. 982.
55. Hubbard, D.; SEIERSEN, R. *How to Measure Anything in Cybersecurity Risk*; John Wiley & Sons: New York, NY, USA, 2016; pp. 1–247.
56. Akinrolabu, O.; Nurse, J.R.; Martin, A.; New, S. Cyber risk assessment in cloud provider environments: Current models and future needs. *Comput. Secur.* **2019**, *87*, 101600. [CrossRef]
57. Burtescu, E. Decision Assistance in Risk Assessment—Monte Carlo Simulations. *Inform. Econ.* **2012**, *16*, 86–93.

58. Palisade. *Monte Carlo Simulation: What Is It and How Does It Work?* Palisade: New York, NY, USA, 2017.
59. Olcott, J. Input to the Commission on Enhancing National Cybersecurity: The Impact of Security Ratings on National Cybersecurity. 2016. Available online: [https://www.nist.gov/sites/default/files/documents/2016/09/15/bitsight\\_rfi\\_response.pdf](https://www.nist.gov/sites/default/files/documents/2016/09/15/bitsight_rfi_response.pdf) (accessed on 20 March 2018).
60. Sourcemap. *Sub-Supplier Mapping: Tracing Products to the Source with a Supply Chain Social Network*; Sourcemap: Lower Manhattan, NY, USA, 2011; p. 5.
61. Gresh, D.; Deleris, L.A.; Gasparini, L.; Evans, D. Visualizing Risk. In Proceedings of the IEEE Information Visualization Conference, Las Vegas, NV, USA, 26–28 September 2011.
62. Akinrolabu, O.; New, S.; Martin, A. Cloud Service Supplier Assessment: A Delphi Study. In Proceedings of the Eighth International Conference on Innovative Computing Technology (INTECH), Luton, UK, 15–17 August 2018; pp. 142–150.
63. Hogan, R. Introduction to Statistics for Uncertainty Analysis. 2016. Available online: <http://www.isobudgets.com/introduction-statistics-uncertainty-analysis/> (accessed on 26 September 2018).
64. Miles, S.B. Participatory model assessment of earthquake-induced landslide hazard models. *Nat. Hazards* **2011**, *56*, 749–766. [CrossRef]
65. Wangen, G.; Hallstensen, C.; Snekkenes, E. A framework for estimating information security risk assessment method completeness. *Int. J. Inf. Secur.* **2018**, *17*, 681–699. [CrossRef]



© 2019 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<http://creativecommons.org/licenses/by/4.0/>).