Cyber Supply Chain Risks in Cloud Computing – Bridging the Cloud Risk Assessment Gap

O. Akinrolabu, S. New, A. Martin

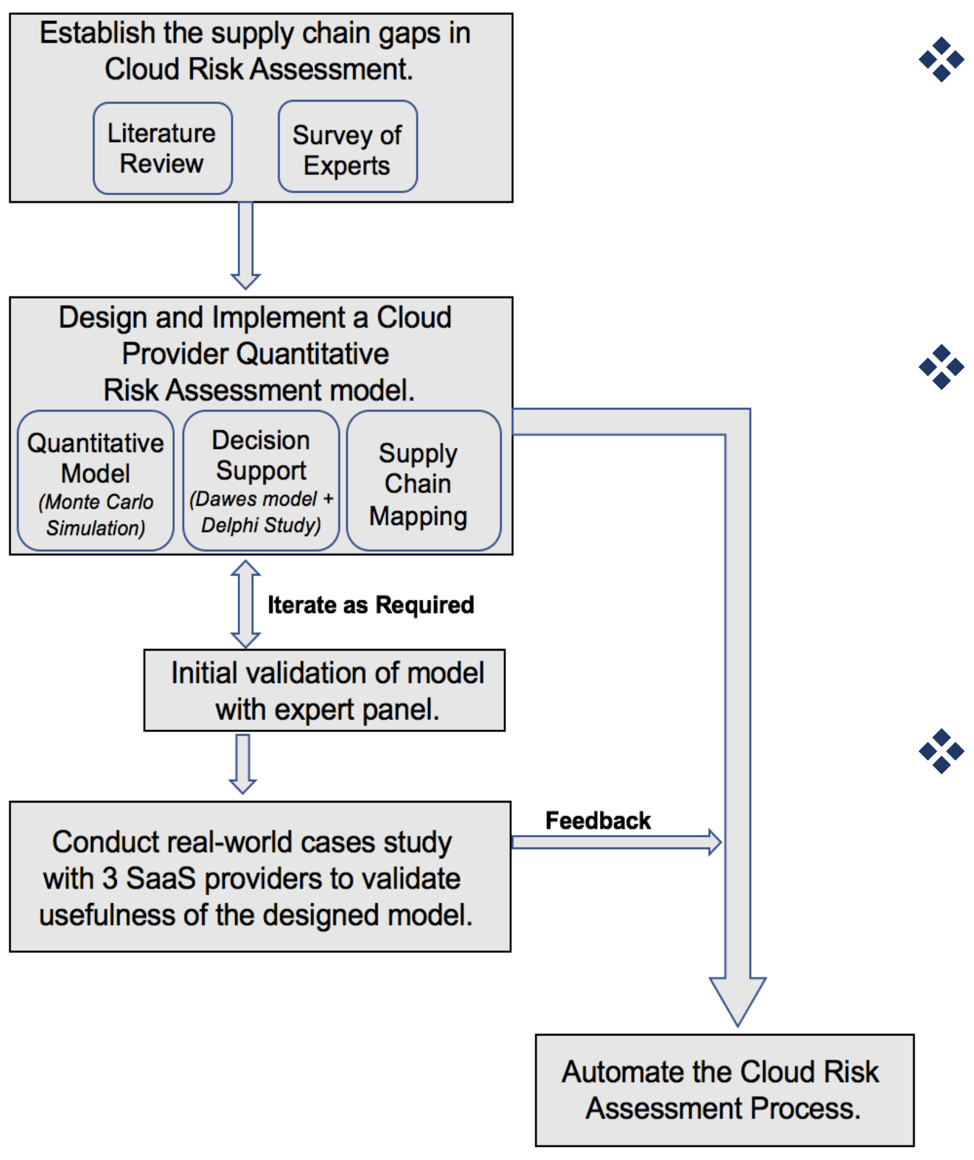
UNIVERSITY OF OXFORD

Cloud risk assessment gap

Security risks associated with the cloud's multi-tenancy, automation, vendor lock-in, and system complexity continues to be on the rise. Assessing and managing these risks can be a challenge due to the increased numbers of parties, devices and applications involved in cloud service delivery.

In a recent study conducted with cloud experts, we discovered how current risk assessment methods were unable to cope with the dynamic nature of the cloud, a gap linked to their failure to consider the inherent risk of the supply chain. This challenge is further exacerbated by the lack of cloud provider transparency and limited visibility of security controls.

Research Methodology & Progress

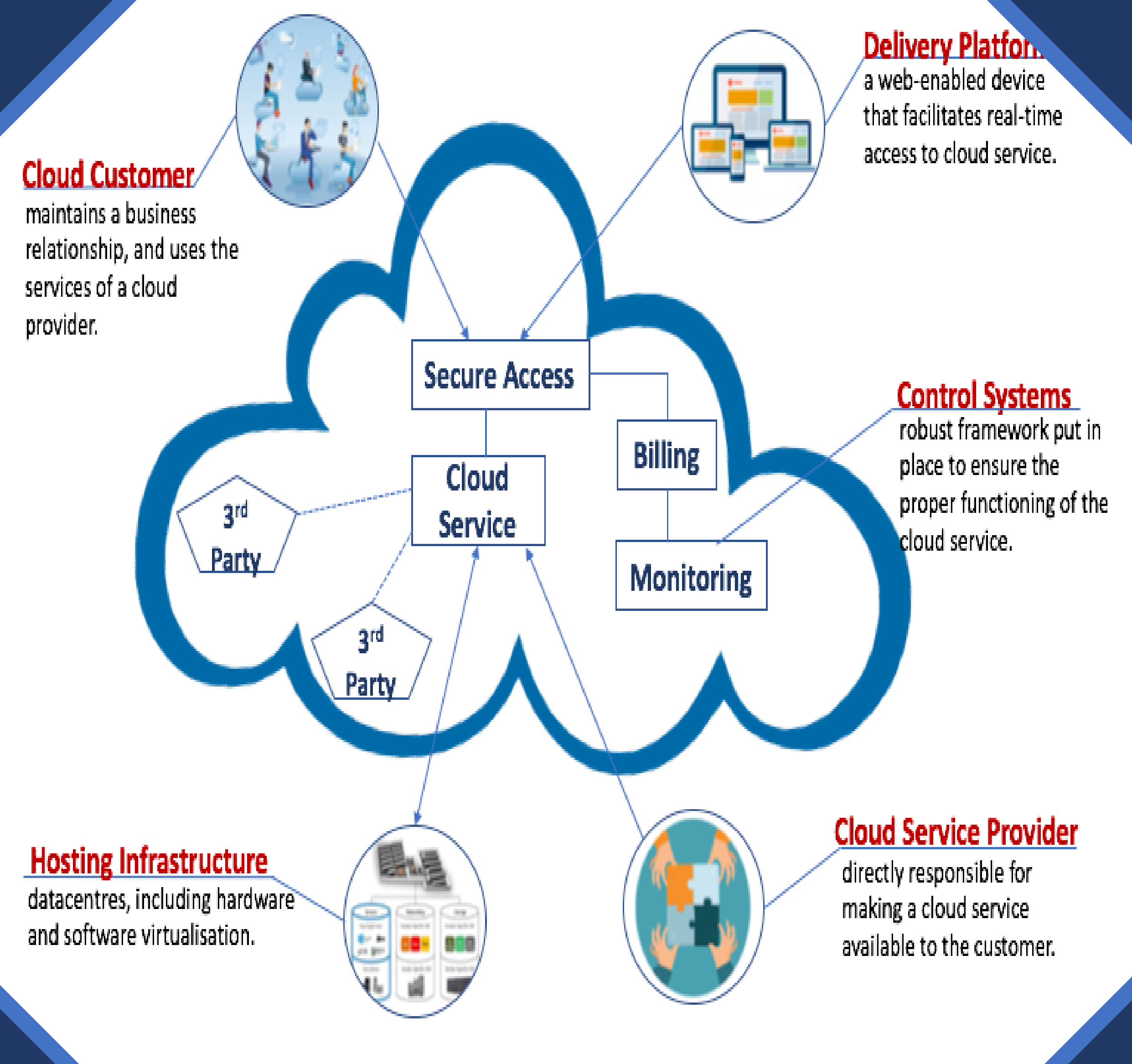

Establish the supply chain gaps in Cloud Risk Assessment.
Literature Review
Survey of Experts
Design and Implement a Cloud Provider Quantitative Risk Assessment model.
Quantitative Model (Monte Carlo Simulation)
Decision Support (Dawes model + Delphi Study)
Supply Chain Mapping
Iterate as Required
Initial validation of model with expert panel.
Conduct real-world cases study with 3 SaaS providers to validate usefulness of the designed model.
Feedback
Automate the Cloud Risk Assessment Process.

- ❖ We have developed a prototype quantitative cloud risk analysis model based on Monte Carlo simulation.
- ❖ We have just completed a Delphi study with cloud experts to identify security factors for our multi-criteria decision support system.
- ❖ We are in the process of completing the development of an automated supply chain mapping tool using a graph database platform.

CSCCRA: An Improved cloud risk assessment model

To address the above gap, we developed the Cloud Supply Chain Cyber Risk Assessment (CSCCRA) model, a quantitative risk assessment model which is supported by decision support analysis and supply chain mapping in the identification, analysis and evaluation of cloud risks.

The CSCCRA model is currently targeted at SaaS providers and follows a systematic approach to assessing cloud risks.


Cloud Customer
maintains a business relationship, and uses the services of a cloud provider.
Delivery Platform
a web-enabled device that facilitates real-time access to cloud service.
Secure Access
Cloud Service
Billing
Monitoring
3rd Party
3rd Party
Control Systems
robust framework put in place to ensure the proper functioning of the cloud service.
Hosting Infrastructure
datacentres, including hardware and software virtualisation.
Cloud Service Provider
directly responsible for making a cloud service available to the customer.

The five essential elements of a Cloud Supply Chain

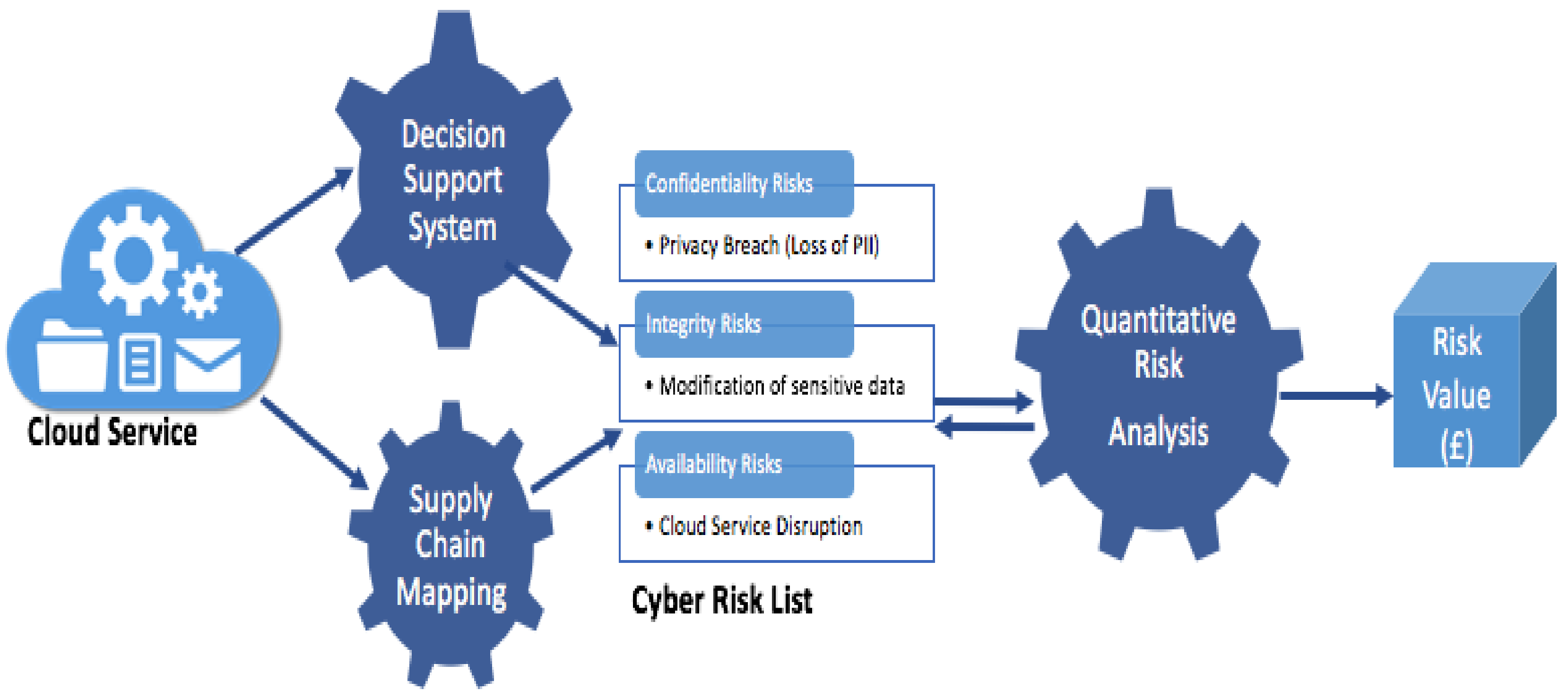
Delphi Study

A group of fifteen (15) experts were tasked with identifying security factors for cloud supplier assessment.

This group achieved consensus on nine (9) security target dimension, and they are:

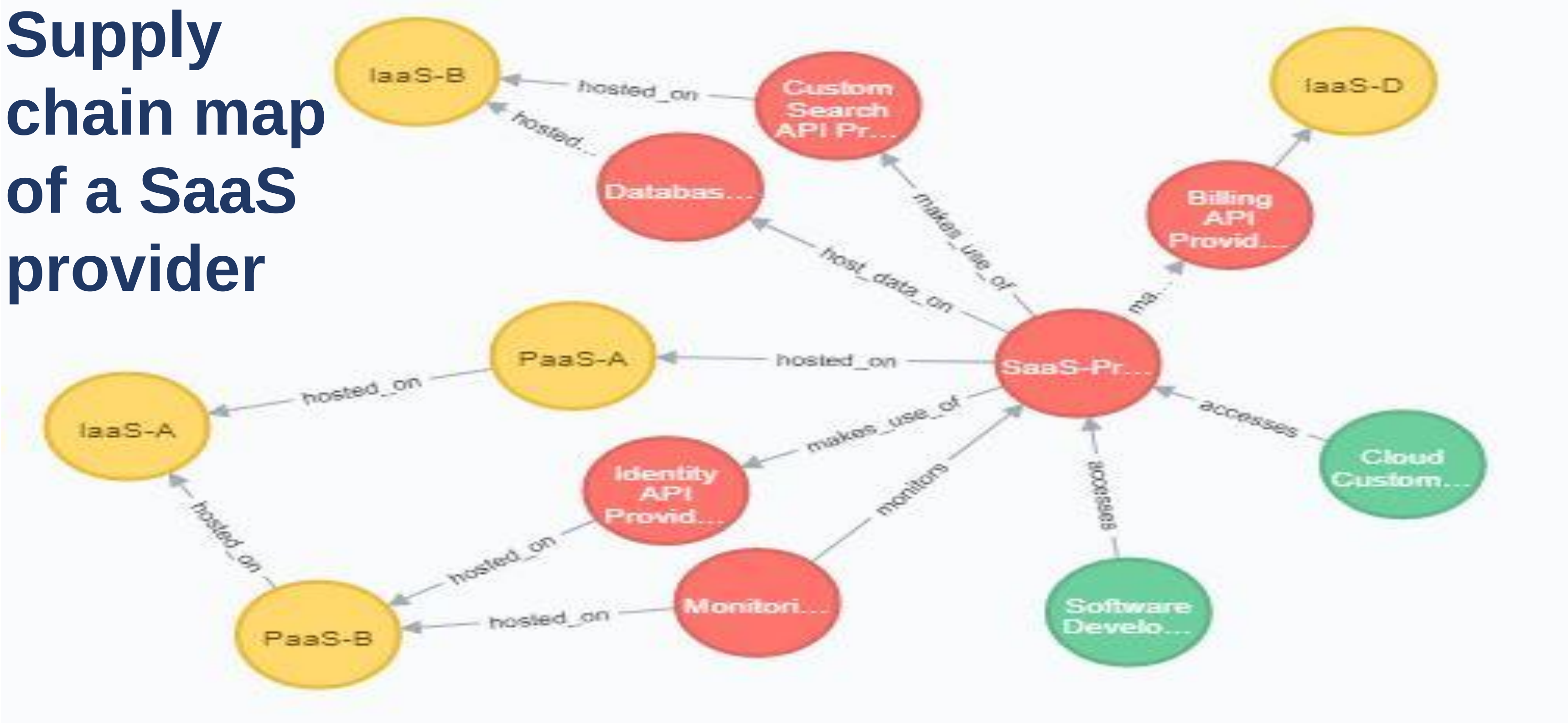
- Maturity of Operational Security
- Identity and Access Management
- Availability of Service
- Data security controls
- Application Security
- Encryption and Key Management
- Data & System hosting
- Data security controls
- Maturity of security assessment
- Security Governance & Compliance

How the CSCCRA Model works



- Decompose the cloud application into its component services and map out the supply chain.
- Assess the security of the supplier of each service component using a multi-criteria decision support system.
- Identify the weak link(s) within the chain and draw a comprehensive list of cloud security risks.
- Stakeholders make reasonable estimates of risk values.
- Input risk values to CSCCRA quantitative simulation tool, to arrive at the risk value in monetary terms.

Supply chain map of a SaaS provider



Open invitation for collaboration

The next phase of our research is to conduct at least 3 case Studies, where we will be using the CSCCRA model to analyse the risk of cloud providers.
We believe this exercise will provide SaaS providers with an opportunity to step back cognitively from their usual approach to risk assessment and fundamentally question and rethink their established interpretations of cloud risks.

For further discussions or enquiries, please contact Olu Akinrolabu (olusola.akinrolabu@kellogg.ox.ac.uk, +447875013532)

Recent Publications

- Olusola Akinrolabu and Steve New. Can Improved Transparency Reduce Supply Chain Risks in Cloud Computing? Operations and Supply Chain Management, 10(3):130{140, 2017.
- Olusola Akinrolabu, Steve New, and Andrew Martin. Cyber supply chain risks in cloud computing - bridging the risk assessment gap. Open Journal of Cloud Computing (OJCC), 5(1):1-19, 2018.

CENTRE FOR DOCTORAL TRAINING in CYBER SECURITY

EPSRC
Engineering and Physical Sciences Research Council