Risk Assessment Model for Cloud-Connected Networks with Case Study on an Academic Institution

نموذج تقييم المخاطر لشبكات الحاسوب الموصولة مع الخدمات السحابية للمؤسسات الاكاديمية

Islam Younis Amro
Associate Professor/ Al-Quds Open University / Palestine
iamro@qou.edu

اسلام يونس عمرو
أستاذ مشارك / جامعة القدس المفتوحة / فلسطين

Received: 07/09/2021, Accepted: 27/09/2021
DOI: https://doi.org/10.33977/2106-000-005-004
https://journals.qou.edu/index.php/PJTAS

تاريخ الاستلام: 2021/09/07، تاريخ القبول: 2021/09/27
E-ISSN: 2521-411X
P-ISSN: 2520-7431

Abstract

The reliance on cloud services has increased recently, resulting in an abundance of networks connected to these services partially or fully. However, several risks emerge from this action that imposes new challenges. Organizations often maintain a range of services managed in its own local or expanded networks as well as services that could exist on the cloud services sites partially or totally. Organizations have to deal with two types of risks: The first relates to the internal information systems risk of the organization, and the second relates to risks that come with working with cloud services providers. Furthermore, organizations lack benchmarking and references on assessing information systems risks. Most organizations work with vulnerability management concepts rather than risk assessment and mitigation. In this paper, we reformulate strategic e-services in an educational institution as it works between local networks and cloud services at the same time to study the risks associated with them in a hybrid manner. These services are distributed over local network nodes and relevant cloud components. The local network components and nodes; represent hosts with known vulnerability values generated from commercial tools. These vulnerabilities are gathered into vectors with expected impacts and estimate assets value related to these services. Probabilities or risks are identified accordingly. The other component of the research considers analyzing the risk of the cloud services with the computational approach, but it deals with cloud standard components such as data management policies, internal cloud provider management, and internet security. Vulnerability in cloud providers is identified as the compromise of these components and their impact on business continuity. Using vulnerability concepts for both local network and cloud, we introduce a risk probability model for educational organization (e.g.: QOU) services where risks are estimated over Borda Count generated weights for both local network and cloud. Moreover, the overall risk is estimated independently for each component; local network and two clouds. The final step is to investigate the overall risk for the organization. It will be done by prioritizing these risks mutually and analyzing the value of each risk in terms of other risks. For this purpose, we use the analytic hierarchy process (AHP).

***Keywords**: Cloud Computing Risk Assessment, Vulnerability Management, Business Continuity, Borda Count., Analytic hierarchy process (AHP).*

الملخص

يزداد الاعتماد مؤخرا على الخدمات (السحابية) بحيث يتصل كثيرا من الشبكات بهذه الخدمات بشكل جزئي أو كلي. يصاحب هذه التغيرات جملة جديدة من المخاطر والتحديات تضاف إلى المخاطر القائمة في الشبكة. ففي كثير من الأحيان تحتفظ المنظمة بمجموعة من الخدمات التي تدار في الشبكات المحلية أو الموسعة الخاصة بها إلى جانب الخدمات التي يمكن أن تتواجد كليا أو جزئيا على مواقع الخدمات (السحابية). يضاف إلى هذه الإشكالية الضعف العام في المنظومات الإدارية للمخاطر في كثير من المنظمات بحيث تُغيب وثائق أساسية في التعامل مع المخاطر، مثل: استراتيجية نظم المعلومات، واستراتيجية أمن المعلومات، والأوراق المرجعية لمحددات أمن المعلومات، والمخاطر ذات العلاقة في المنظمات. أمّا ما يتم العمل عليه في المنظمات وبشكل يومي هو إدارة نقاط الضعف بحيث يتم التعامل مع نقاط الضعف الفنية في الشبكات المحلية والموسعة من خلال التقييم الدائم للتغيرات الدائمة على تقنيات البنى التحتية والتطبيقات، واقتراح الحلول الأمنية على مستوى العقدة في الشبكة، وحلها وبشكل آلي في بعض الأحيان وذلك بالاعتماد على تقنيات صناعية معدة لهذا الغرض، دون المرور على مفهوم المخاطر والتعامل معه. في هذا البحث نعمل على إعادة صياغة الخدمات الالكترونية الاستراتيجية في منظمة تعليمية والتي تعمل بشكل (هجين) بين الشبكات المحلية، والخدمات (السحابية) في الوقت نفسه؛ لدراسة المخاطر المرتبطة بها. وتم تقسيم الخدمات الاستراتيجية إلى مجموعات عمل تضم العقد المشاركة في بناء هذه الخدمة سواء كانت في الشبكة المحلية أو في المواقع (السحابية)، ثم تمّ احتساب الضعف لكل عقدة من العقد المشكلة للخدمة باستخدام أدوات تجارية متخصصة بهذا الشأن، وتم رسم مسار للعقد التي تشكل هذه الخدمة في الشبكة المحلية والتعبير عنه بمتجه يعرف بمتجه نقاط الضعف لخدمة استراتيجية معينة، وتم تقدير قيمة الأصول واحتمالية وقوع الخطأ، ودرجة تأثير الخطأ حين حدوثه. والخطوة التالية كانت اسناد أوزان هذه الخاطر، واحتساب قيمتها لكل خدمة استراتيجية، ومن ثم احتساب المخاطر الكلية للخدمات الاستراتيجية التي تعمل في المنظمة على شبكاتها المحلية. ومن ثم تمّ احتساب المخاطر المصاحبة للعمل مع الخدمات (السحابية) وهي ذات نوع وتأثير مختلف من حيث تسريب المعلومات أو فقدانها أو تعرضها للسرقة أو أي خلل يتسبب به مزود

الخدمة (السحابية). وهنا أودّ الإشارة إلى أن المخاطر المستخدمة في هذه الورقة هي ضمن المخاطر المعيارية، والمنصوص عليها في الأدبيات ذات العلاقة. وتمّ اتباع المنهجية ذاتها في احتساب مخاطر الخدمات (السحابية) ومن ثمَّ تمّ احتساب المخاطر الكلية حسب شدة الخطورة؛ وذلك حسب خوارزمية عملية التحليل الهرمي. بحيث تم الخروج برقم موحد لمخاطر المنظمة اعتمادا على الخوارزمية سالفة الذكر.وتمّ الاستناد إلى بيئة جامعة القدس المفتوحة في إعداد بيانات هذا البحث.

الكلمات المفتاحية: الشبكات السحابية، تقييم المخاطر، إدارة نقاط الضعف، استمرارية الاعمال، عداد بوردا، عملية التحليل الهرمي.

INTRODUCTION

General Prospect on Information Systems Risk Assessment

In the modern age of the fourth information systems revolution, an extensive dependency on information systems has become noticeable. One of the key issues related to the presence of information systems is the need for information systems security risk assessment. The key problem affecting information systems risk assessment arises from the lack of organizational benchmarks and references to assess an overall prospect for information systems risk. This leads to more contingency approaches in managing vulnerabilities-they can be assessed more easily than systems risk-as a substitute for system risk but not a replacement. Information system risk has a very broad concept that alludes to generic business risk and forms an essential compound of business risk matrices. This explains how organizations usually have very good knowledge, skills, and plans to manage vulnerability on an information systems level. However, they still have a less mature explanation and methodologies on transforming vulnerabilities management into information systems risk assessment and part of business risk over an organization. Information systems risk is concerned with issues of vulnerabilities but exceeds those concepts to risk identification, analysis, prioritization in terms of impact, probabilities, dependencies, time, and other avalanches. The outcome of this process is subjected to risk mitigation plans and so on (Metzenger et al., 2007). Based on ISO/IEX IS13335X and ISO 27001 families, some are actively modified and updated while some are withdrawn since a key common concept of information systems seems timeless. These concepts are assets, threats, and vulnerabilities. An asset is defined as anything tangible or intangible within an organization and has value. Each asset presence, absence, or malfunction has a certain impact on an organization which is very important to understand when risk is being assessed. The process of tracking the impact is defined as the impact assessment. Another key concept is threat. Threats are a set of actions and/or events that may cause harm. The last concept is vulnerability, which refers to the weakness in protecting this asset. The combination of these three elements forms the foundation of information security risk management. Risk management entails two main phases; the first is to identify the risk, and the second is to manage it. Risk identification entails the process of assessing assets and their values, their impact on the system cycle, and their vulnerabilities. Managing risk is related to defining and implementing mitigation plans that would avoid risks or define operational alternatives then adopting them if the risk is being actualized. The International Organization for Standardization ISO developed a wide set of procedures and concepts in this regard under the ISO 2700(1:5) family (ISO 2018). However, the problem arises from several standards, approaches, concepts, and even understanding of the risk assessment, as in Lonita et al. (2014). Moreover, the strengths and weaknesses of each approach are difficult to track. From the researcher's point of view, the key problem of all approaches comes from answering two questions: 1- How to integrate the information security risks as a business risk for non-technical people and 2- How to calculate the framework parameters regardless of the type of the framework. The inner details of each approach and standards are different; therefore, the comparison between the approaches can be fascinating. We should take into account the purpose of information risk assessment as a part of the organizational risk assessment. Regarding the first problem on the integration of technical terms into business terms, the techniques of calculating the risk assessment parameters may vary from simple questionnaires to Heuristic calculation methodologies, as in Andersen (2014). These parameters include threats, impacts, and even vulnerabilities. The need for Heuristic methods arises from the lack of

benchmarks, references, and clear organizational assessment. The importance of Andersen's work arises from combining business and technical risks on one computational model, which reflects the tight relationship between technical risks and business risks on the computational level. This has presented sufficient information to non-technical people, according to Andersen. Business risk assessment for cloud computing was addressed (Bernardo, 2013), where a computational model was developed to assess information systems risks over the cloud for non-technical people. Khidzir (2010) pointed out that the investigation worked with the outsourced services and risks related to them, namely, risk identification, analysis, treatment plans, implementations, monitoring, and control. Moreover, regarding technical issues, the research suggested business Service Levels Agreements (SLA) rather than infrastructures problems. Extensive work on parameters calculations found in reference (Amin et al., 2013) considers the impact of organizational structure combined with information security tools and technology-based security systems in fault-tolerant control on risk calculations. The analysis considers the service-oriented architecture (SOA) as a reference. Amin (2013) also suggested that the risk assessment might also depend on the technical architecture and showed good incorporation between business and technical terms. Maule et al. (2009) presented in a study a specific risk model for SOA. Furthermore, the research found that this model is very similar to the traditional risk model based on risk probability and asset value. From our perspective, the real value of this research is that it focuses on the business components of SOA. Xiaojun et al. (2011) introduced another risk assessment of a Web service case based on SOA of multiple applications. Asosheh et al. (2009) found a very clear incorporation between technical and business terms. This research represents a new quantitative method for assessing the overall information security risk in a real business environment. The new method is based on Microsoft and Callio Secura methods, which are common and practical methods. The advantage of this approach is that the organization can determine its business risks and return on security investments. Kassou (2012) introduced a maturity model of SOA risk assessment. In contrast, this research introduces the principles of a new tool that supports the organization's SOA security maturity assessment called SOASMM (SOA Security Maturity Model). This model is defined by combining information security best practice methods into a service-oriented architecture paradigm using controversial methods and mapping models. Saleem et al. (2015) considered integration between business risk analysis and IT Security Risk. He showed the classification between services according to strategic importance and considered these issues accordingly in assessing the organization's risk. In reference to the second point: How to calculate the framework parameters regardless of the type of the framework, we can conclude the following. All of the preceding techniques, such as ISO/IEC 13335-2, ISO/IEC IS 17799, and ISO 270001, would still require a method for quantitative risk assessment, estimating the values of assessing values, risk impact, with a series of questionnaires included in security plans for organizations. Unfortunately, a wide range of organizations lacks detailed information security strategies and sometimes mitigate on purpose. These strategies are usually acquired from broader strategies such as information systems strategy, which in its turn reflects the broader organizational strategy. Butting all of these cascaded strategic documents is exploited to calculate the overall organizational risks, technical and non-technical. A wide range of methodologies is used to project the organizational strategies. Most of these methods are computational, but some are empirical. For an organization that has not developed these concepts maturely, the systems' risk is minimized into technical vulnerability management. These vulnerabilities are quantified and obtained from specific systems that analyze the security status of these assets. Other problems have appeared, such as specifying the asset's value, risk probability, and risk impact. Then sorting out these values and how these values are going to be expressed in business terms. Furthermore, several approaches have been developed addressing the exploitation of vulnerability value, asset value, risk impact, and the probability of the occurrence of the risk. To translate these calculations into business terms, Andersen (2010) of IBM and Asosheh et al. (2009) used probabilistic approaches. These two interrelated works subjected the parameters to a probabilistic model and projected the overall risk

within an organization based on technical information. The researcher used a multistage approach in analyzing the systems and then expected the overall risk based on a specific estimation model. The weights produced from an adaptive hierarchical process were optimized using a heuristic neural network method made by Xi et al. (2010). This issue entailed substantial calculations for the weights of risk assets. However, we do not believe risk assessment should go through due to the dynamic nature of risks. Xi et al. (2010) had the same concerns with large calculations as in Xiao et al. (2010). Another approach exploited fuzzy logic and inference systems to identify the risk parameters and protect them from given vulnerability systems, as in Jinxing et al. (2020) study. Another exploitation of fuzzy logic and Bayesian networks for estimating the overall risk was based on known vulnerability values found in the study of Zang et al. (2018). Relatively simpler approaches were found in Riaz et al. (2019) study; it exploited simpler fishbone methods in investigating business risks on software development. The weights produced from an adaptive hierarchical process were optimized using a heuristic neural network method made by Xi et al. (2010). This issue entailed substantial calculations for the weights of risk assets; still, we do not believe risk assessment should go through due to the dynamic nature of risks. Xi et al. (2010) have the same concerns with large calculations as in Xiao et al. (2010) study. Furthermore, other approaches exploited fuzzy logic and inference system to identify the risk parameters and protect them from given vulnerability systems, as in Jinxing et al.'s (2020) work. Another exploitation of fuzzy logic and Bayesian networks for estimating the overall risk based on known vulnerability values was found in the study of Zang et al. (2018). Relatively simpler approaches were found in Riaz et al.'s (2019) study since it exploited simpler fishbone methods in investigating business risks on software development. Another approach based on calculating Risk and Borda Calculations was exhibited in Amro's (2015) study.

From the previous literature review, we can conclude that some issues need to be dealt with. First, scientists have to do extensive work relating to business information systems risk methodologically, where technical terms do not consume business terms. In addition, there are several models identified to quantify business risk related to system architecture and software services type. Furthermore, several numerical methods vary in complication to estimate the business risk value based on given technical information. Regardless of any organization's situation, there are three documents -Business Strategy, IT Strategy, and Security Strategy- which should be referenced to build a proper risk assessment and containment plan, as in known frameworks or Information Security Management System (ISMS). These documents are essential to assess the risks related to business assets, Assets Values, and related impacts on business. Unfortunately, many businesses lack either an IT strategy or a security strategy and sometimes both. We still need organizational references to figure out how much our assets are worth. Even though technical knowledge about vulnerabilities is available, the risk model's calculation must be quantified on business. Unfortunately, many organizations do not have an IT strategy or security strategy, or both. We still need organizational references to assess the values of our assets.

Information Security Risk Identification for Cloud Services

The core issues of IT sourcing services were addressed by Moona et al. (2018). The core of the information security risk for the outsourced managed services running on clouds is related to the nature of the service provider company. Theoretically, the information of the served company will be processed by the serving company. There is a potential of exposure of sensitive information for the served company by the serving company. Unauthorized access to sensitive information and leaked information to a third party can be possible. The information security risk is divided into subjective risk and objective risk. The subjective occurs when the contractor takes advantage of services running on his cloud to achieve certain benefits and uses the client's data for other risks. However, the objective risk occurs under the condition when someone leak the information and the contractor lacks experience and level, even though he has realized the importance of security and taken certain measures. This can be addressed using a

powerful information security system. Key security risks form for managed services contains the following issues:

Data Protection Protocol

The clients in these cases should establish a very clear data protocol where clients define all the types of the implemented process. In transfer, processing, transmitting, storing, etc., this protocol has a contractual value and should be very controlling to the service provider. This is an essential step to reduce the information security risks. Moreover, this would include defining very clear security technologies, communication technologies, how to move and store data, the kind of protocols, levels of security, conditions on future subcontracts, and the cause of breaking the contract.

Network Security

Network security contains the subsequent contents: the hardware and software of the network system. The data within the system should be protected against damage, modification, and leakage for infrequent or vicious reasons: The system can normally operate constantly and reliably, and the network service will not be interrupted. Network security means the data security on the network in essence. Hackers aim to illegally obtain, peep, modify or damage sensitive information by using various technologies. The contractor should utilize the foremost advanced technology to extend firewall and antivirus systems in the network, such as invasion detection and vulnerability scanning to the network as well as set storage limits to guarantee the safety of the network, host machine system, and application system. Moreover, contractors should make a powerful disaster recovery plan and data backup to guarantee the client's information security.

Internal Management

An early survey on information security affairs by Gartner-collective information technology marketing research company-found that over 70% of faults are caused within corporate. The survey and research made in two departments by Abdulwahes et al. (2014) verified that almost all affairs related to security occur within the organization. These security risks/violations include using the organization's resources for other purposes, such as sharing the password with colleagues and external persons and plugging incorrect or forged information in the system and computer procedure. Moreover, the organization should implement information security education and career training for its staff, improving their knowledge of the significance of security knowledge and ensuring the client's info security. Second, each confidential staff passes security authentication, signs the safety and confidentiality agreement, and understands concrete security measures. Third, the organization should perfect the principles and regulations and ensure that the division of labor is explicit and the responsibilities are clear yet strictly controlling the confidential scope. Fourth, the organization should perfect the network supervision and management mechanism and forestall any security accidents caused by internal employees, particularly confidential staff and external interference, to maintain the client's information security. Fifth, organizations should provide clear administrative management measures such as door access, internal and external monitoring systems, and server protection.

Regulations

The information security protection does not depend on the contractor alone, but it requires the government's provision of a decent information security environment such as legal support towards dispute in outsourcing managed services and explicit specification for the defense of property. Furthermore, enhancing the public knowledge awareness of security and perfecting belongings protection and interrelated law. China's legislation of information security protection is comparatively backward; there was no law protecting the individual and organizations' information security until 2010. In this year, DOC, Industrialization and Informationization Department issued several regulations about Information Protection of Outsourcing Managed Service Contracted by domestic companies, to complete relative law as soon as possible. Moreover, the protection executive strength for holding is weak. Chinese people have weak awareness of private information protection and belongings protection because China lacks laws within the field for an extended time. Although a

series of rules and regulations have been made in recent years, changing people's concepts requires a process, which also causes information security risk towards clients. Therefore, education, publicity, and execution efforts should be enhanced. Third, the industry entry threshold should be set positively to guide the contracting enterprises to attain ISO27001 Information Security Management System (ISMS) authentication. The full information security condition of the corporate should pass the assessment of some institutions. The safety and reputation of the contractor company should be assessed to confirm the grade. Targeted protection measures should be applied maximally to reduce the data security risk for the client.

Supervision Mechanism

Enhancing supervision and management is an essential means for effectively finishing the enterprise's execution. During the execution of the contract, the contractor should establish a regularly formal communication system, find information security risk in time, and establish corresponding preventive measures to reduce information security risk and guarantee the client's information security via control. The client must participate in planning and processing and consider his role as a supervisor. The corporate might form the supervision and management team internally or consider hiring a third-party supervising institution to search out the matter in time, take measures and reduce risk. The corporate should realize visualization of its internal operation and might respond quickly when the client monitors the qualitative process, and thus the objectivity of assessment will further improve.

Determination of Danger Elements

Based on the International Information Security Management Practice Norms ISO/IEC 17799 and Information Security Technology and Knowledge Security Risk Assessment Standards GB/T20984-2007\. Five risks exist within the IT Outsourcing Managed Service Security, which concluded betting on three fundamental elements: assets, threat, and vulnerability. By taking the knowledge safety features of IT Outsourcing Managed Service into consideration, the concrete content of every risk is demonstrated in Table 1.

Table 1 Risk Concerns of IT Outsourcing Managed Cloud Service

The data protection agreement	methods, scope, degree, intellectual property ownership, liability for breach of contract, safety measures, etc., of data protection
Internal management	System construction, educational training, information Access control and maintenance, prevention of the malicious staff to tamper with the information emergency measures.
Internet security	Including data protection of the internet, the host system and application system, and antivirus measures
Supervising Mechanism	Communicate and exchange ideas, clients participate in the supervision, establish supervision institution, and visualize the internal operation.
Law and policy	The construction of laws and regulations, intellectual property protection, set industry entry threshold, and evaluate the information security Protection level of the contractors.

This paper addresses building a risk assessment model for a network that has a series running locally and other services and services components running over clouds. The Local Network has vulnerability values only, without referencing documents essential for calculating risk values and impacts. The following section explains our problem, relates it to the literature review and discusses the research problem and methodology. After that, we discuss the proposed Network Service-Based Risk Assessment Model, which combines the local area network and cloud service. It explains the roadmap for building the model components through several steps. First, we build the testing environment, which is the network we based our simulation on, then we work on the Vulnerability Calculation Model for local networks and clouds. After that, we explain our method- Risk Probability and Risk Impact Estimation- then we work on the Determination of the Risk Rank Reference. Later, we determine the risk rank and then calculate the Risk Weight Estimation, which will be used in the Overall Risk Calculation. Finally, we write a final flow chart summary for all the steps on how to exploit this approach for similar networks. In section 4, we implement our model into a testing environment as a case study, go over the steps in section 3 and generate the risk of an educational organization.

Then we conclude our research with a finalization of the results.

RESEARCH PROBLEM AND SOLUTION METHODOLOGY

Three documents: Business Strategy, IT Strategy, and Security Strategy should be referenced to build a risk assessment and containment plan, as in known frameworks or Information Security Management System (ISMS). These documents are essential to assess the values related to risk: the Business Assists, Asset Values, and the related impacts on business. Unfortunately, many businesses lack either an IT strategy or a security strategy, or both. Although technical knowledge about vulnerabilities is available, we still need organizational references to figure out how much our assets are worth. In addition, the risk model's calculation must be quantified.

1. Without an IT or security strategy, how can you construct a network services risk assessment model?
2. How to put together a composition that provides strategic services by combining business strategies, information system components, Cloud services, and infrastructure components.
3. Introduce a more user-friendly adaptive approach to calculating risk doe both locally hosted and managed services.
4. How to build a risk assessment model that is aware of cloud-based services.
5. In light of the preceding circumstances, how can risk be assessed for both cloud and network risks?

We adapted these concepts in expressing business strategies in terms of information systems services and infrastructure services, which is not an SOA. Instead, we used a combination of infrastructure components and information systems resources to measure its vulnerability in expressing them as services and then reflecting these services on business strategies. In addition, we took into consideration the risk problems that appear in services running over clouds. This research extends the works conducted by Amro (2015) to include services running on cloud connected to the network topology. This is conducted by computing the risk values for the local network then the risk for each cloud. A final resultant risk is obtained from the three elements local network, Cloud A, Cloud B, using the AHP method explained in Moona et al. (2018). Several multi-criteria of decision-making methods can be used in resultant risk assessment, as in Maček et al. (2020). However, we used AHP for its relevant simplicity.

Network Service-Based Risk Assessment Model Testing environment

Suppose we have a computer network for an organization, as represented in Figure 1. This figure suggests a topology-based representation for the network, with one broadcasting domain around its central switch and protected behind a firewall. The network can be accessed through two router ports; internal and external. These routers represent a separation point between the routing and broadcasting domains. The organization's network is connected to two clouds, cloud A and cloud B.

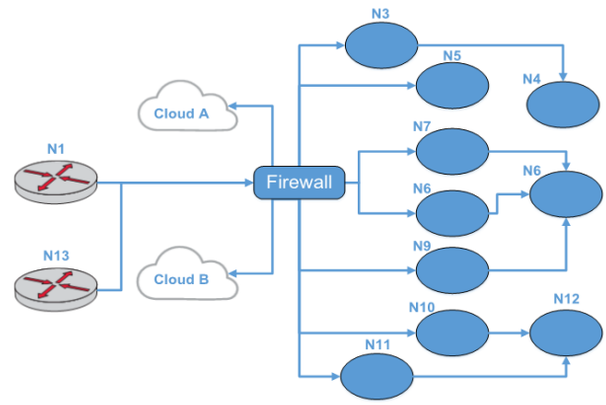

Figure 1 Computer network for Testing Organization

The network has several hosted services running on or through the Nodes (N); these are the insourced network services. Each node represents the hosting machine(s) for the provided services over the network. Each node N is associated with a vulnerability vector V which is calculated using standard tools and quantized from 0 to 5. In this research, Qualys Vulnerability Assessment Tool is used. The vulnerability number for each node represents the average of vulnerabilities for this host. The problem with this number is that it comes with a high-dimensional vector that varies in its norm after each scan. The rating of each vulnerability is given according to Qualys Standard, which is beyond the scope of this paper. However, for the nodes 1 - 12 in Figure 1, the vulnerabilities were 2, 3, 4, 1, 3, 4, 3, 2, 4, 3, 4, and 3, respectively. On the other hand, the risks

incorporated with clouds A and B are different in nature since they are outsourced services. Both circumstances and conditions are different. The sources of risk in IT outsourced managed services are listed in Table 1. The resultant risk for the organization is a summation of both internal and external risks. Suppose that we have the following strategic elements, and we would like to investigate and assess their risk. These strategic services are running on the mentioned network in Figure 1. Table 2 shows these services. Table 2 maps service elements with corresponding nodes, i.e., service path scenarios based on the network predefined access plan. In Addition, for elements, we clarify that CA stands for Cloud A and CB for Cloud B.

Table 2 Service Path Access Scenarios

Element	Service Elements	Related Nodes
1	E-learning	N1,N12,N2,N3,N4,CA
2	MAIL	N1,N12,N2,N5,CA
3	Registration and Student portal	N1,N2,N12N7,N6,CA
4	HR portal	N1,N12,N2,N8,N6,CA
5	Financial system	N1,N2,N9,N6,CB
6	Journals portal	N1,N2,N10,N12,CB
7	Library portal	N1,N12N2,N11,N12,CB
8	Infrastructure	All Nodes

We need to incorporate Tables 2 and 3 by mapping service elements into a higher level for business-related purposes since risks are addressed on a higher level of the servers and other connectivity issues. Table 3 maps the major risk items that we have identified in this study S1 to S6 with the service elements. It is worth mentioning that this issue is network-scenario specific, and it might vary from one network to another.

Table 3 Service Elements Incorporation with Risk Element

Risk Item	Service Elements
Student electronic Services (S1)	Mail, e-Learning, registration and student portal, Library portal
Academic Systems (S2)	Mail, e-learning, registration and student portal, Library portal, Journal System
Human Resource Systems(S3)	Mail, HR Portal.
Financial Systems (S4)	Financial system, HR Portal
Research Systems(S5)	Library portal, Journal System
Infrastructure Components(S6)	All Service Elements in table 1.

Vulnerability Estimation Model

Vulnerability Assessment software works on the network node level, which does not express the business risk level. Figure 1 shows If N is a node in a network configuration. If we rewrite services running on the network nodes as shown in Table 2 in terms of network nodes in Figure 1, the services are classified into service elements E and are expressed in Table 2. The vulnerability for the network node N, expressed as, is the weighted average of all vulnerabilities of node N. Accordingly, each node is expressed by the vulnerability value and expresses the number of nodes' participation in the constitution of service element E expressed in Table 2. The resultant value for the vulnerability service element E expressed as and calculated by taking the maximum vulnerability value obtained from the above process for the nodes N1 to Ni constituting the element E, formally can be expressed as:

$$V_E = Max\,(V_{N_1}, V_{N_2}, ..., V_{N_i}) \quad (1)$$

The use of the maximum in Equation 1 is justified by the need to obtain the extreme value for the risk. Other approaches may use weighted averages, but we do not prefer to use them since they might only drop the vulnerability value for calculation. The next step is to incorporate node risks with risk elements that are forming the services to obtain the service vulnerability. The element vulnerability is mapped to the total risk items vulnerability Vs using the same logic in building Equation 1. Formally, is written as:

$$V_S = Max\,(V_{E_1}, V_{E_2}, ..., V_{E_j}) \quad (2)$$

where *j* represents the service element of component *E*, which forms risk item S. Equations 1 and 2 make it possible to write vulnerabilities on an organizational level in our work. The values calculated for V_S were 3, 4, 4, 4, 3, and 4, respectively.

The Estimation of Risk Probability and Risk Impact

We suggest that the risk probability P and risk impact I are ranked in 5 levels: very low, low, medium, high, very high, which express the frequency of vulnerabilities encountered and the risk probability. The value for the service reflects

the impact of risk. Probability and Impact are then expressed in 2D matrices exploited in the retrieval of the quantified value of P and I value. The risk probability P is then quantified by threats encountered for T times. In addition, it is expressed in Equations 3.

$$P = f_1(V, T) \tag{3}$$

$$T = (t_1, t_2, \dots\dots, t_i, \dots t_m) \quad , \quad 1 \leq i \leq m$$

$$f_1 = \alpha t + \beta v_S$$

$$\alpha = \begin{cases} 2, t \leq 3 \\ 3, 3 < t < 5 \\ 4, t = 5 \end{cases}$$

$$\beta = \begin{cases} 1, v \leq 3 \\ 2, 3 < v < 5 \\ 3, v = 5 \end{cases} \tag{4}$$

Alpha (α) and beta (β) are important to quantify P over the interval assumed. We selected the values of α and β so the higher the vulnerability, the higher the values for *P*. The impact *I* expresses the impact of the risk in accordance of asset value, these terms are expressed in Equations 5 and Equations 6:

$$I = f_2(V, A) \tag{5}$$

$$f_2 = \varphi a + \phi v$$

$$\phi = \begin{cases} 1, a \leq 2 \\ 2.5, 2 < a < 5 \\ 3, a = 5 \end{cases}$$

$$\varphi = \begin{cases} 2, v \leq 2 \\ 3, 2 < v < 5 \\ 4, v = 5 \end{cases} \tag{6}$$

$$V = (v_{S1}, v_{S2}, \dots\dots, vj, \dots . v_m), 1 \leq j \leq n$$

Estimation of the Reference of the Risk Rank

Table 4 below expresses the risk quantification by combining numerical and description levels; the first column presents the risk probability level. The impact has several levels and may vary from very low (-L) to medium (M) for the first row and from medium (M) to very high (+H) in the fifth row. Table 4 demonstrates a fine resolution between risk probability levels and risk impact levels.

Table 4 Relationship Between Risk Probability and Risk Impact Levels

Risk probability	**Risk Impact levels**				
levels	1	2	3	4	5
1	0.5 –L	1 -L	1.5 L	2.5 M	3 M
2	1 –L	1.5 -L	2 -L	2.5 M	3.5 H
3	1.5 L	1.5	3 M	3 M	4 H
4	2.5 M	3 M	3 M	3.5 H	4.5 +H
5	3 M	3.5 H	4 H	4.5 + H	5 + H

Risk Weight Estimation

In order to translate values from qualitative to quantitative, we need to define and determine risk weights; we exploited Borda count to achieve that. If total risk factors set of *N*, and *i* is a specific risk of set *N* with a criterion of k, then the value for risk in *N* can be expressed as:

$$b_i = \sum_{k=1}^{n} (\mathrm{N} - r_{ik}) \tag{7}$$

With total risk value expressed as:

$$B = \sum_{i=1}^{N} b_i \tag{8}$$

The weight for given risk RW_i expressed as:

$$RW_i = b_i / B \tag{9}$$

Overall Risk Calculation

Upon completion of the resultant risk-judging matrix, the overall security risk rank is expressed in equation 10, as:

$$RRT = \sum_{i=1}^{k} (\mathrm{RR}_i \, \mathrm{x} \mathrm{RW}_i) \tag{10}$$

CASE Implantation

The implementation goes through the steps as seen in Figure 2.

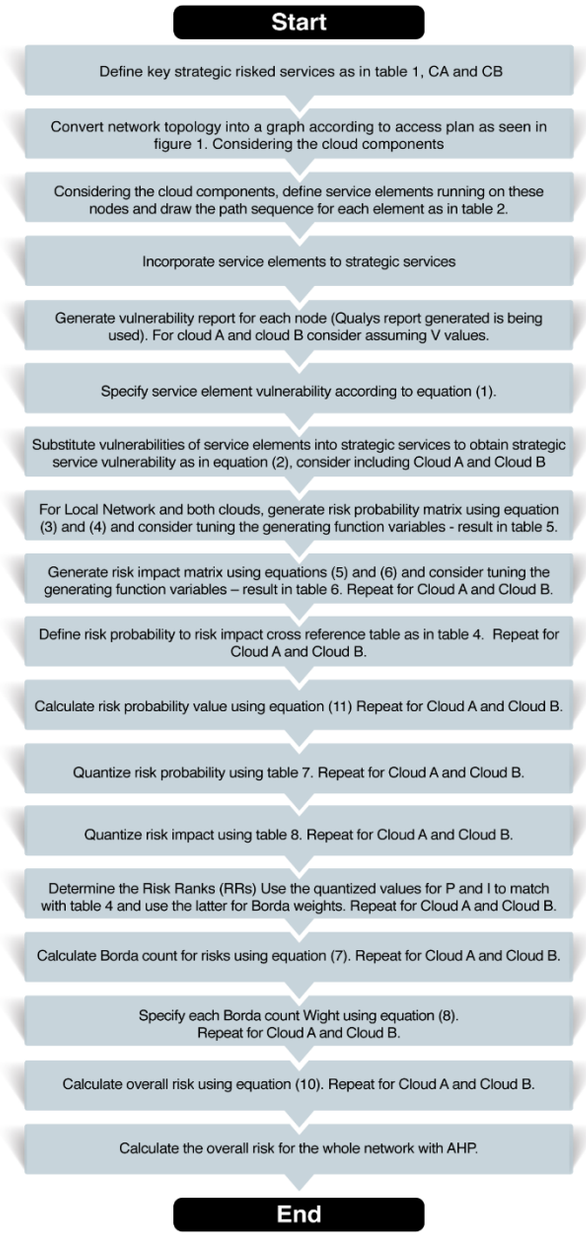

Figure 2 Experiment Case Implementation

As seen in Figure 2, we have implemented the previously mentioned steps to construct the general risk matrix seen in Table 9 for the local network, Table 10 for cloud A, and Table 11 for Cloud B. The steps from 1 to 6 have been previously implanted and explained. The resulting risk for six strategic services is 3, 4, 4, 4, 3, and 4, respectively. Then we implement step 7 to generate the risk probability and step 9 to generate the risk impact matrix. The matrices are shown in Tables 5 and 6, respectively. For Table 5 representing P, we assume the T values to be 5, 2, 2, 1, 3, and 4, respectively. For Table 6 representing I, we assume A to be 3, 3, 5, 2, 2, and 5, respectively. We assume the resulting risk for 6 strategic services running on a local network to be 4, 3, 4, 4, 4, and 4, respectively. For Cloud A V values are 3, 3, 2, 1, 1 and for cloud B 2, 2, 3, 1, 1. Note that the value for both clouds are obtained from Table 3. Then we implement step 7 to generate the risk probability and step 9 to generate the risk impact matrix. The matrices are shown in Tables 5 and 6, respectively. For Table 5 representing P; we assume the T values for the local network to be 5, 2, 2, 1, 4, and 4. And for the T value for Cloud A 2, 2, 3, 1, 3 and for Cloud B 2, 1, 1, 2, 1 For Table 6 represents I for services running on the local network; we assume A to be 3, 3, 5, 2, 2, and 5. And for cloud A 1, 3, 2, 1, 2 and for cloud B 1, 2, 2, 1, 3.

Table 5 Risk Probability Matrix

$P = f1(V,T)$	V				
	1	2	3	4	5
T	1	3	4	5	10	12
	2	5	6	7	12	14
	3	7	8	9	14	16
	4	13	14	15	20	22
	5	16	17	18	23	25

Table 6 Risk Impact Matrix

$I = f2(V,A)$	V				
	1	2	3	4	5
A	1	3	5	10	13	16
	2	4	6	11	14	17
	3	9.5	11.5	16.5	19.5	22.5
	4	12	14	19	22	25
	5	14.5	16.5	21.5	24.5	27.5

Using table 5; the risk probability for given values for V and T were 23, 7, 12, 20, and 20, and for cloud A, the risk probability is Cloud A 7, 7, 8, 3, 7 Cloud B6, 4, 7, 5, 3. The impact of these vulnerabilities were 19.5, 16.5, 24.5, 14, 11, and 27.5. I for cloud A was 3, 16.5, 6, 3, 4. I for cloud B 5, 6, 11, 3, 3. For step 10 we need to specify the risk probability value; this was achieved in equation 11:

$$r = \frac{Risk \quad Probability}{TotalRisk} \tag{11}$$

Total risks are 25 from Table 5, and thus the value of *r* becomes 23/25 and so on. These values were the local network 0.92, 0.28, 0.48, 0.8, 0.36, and 0.84. The total risk for cloud A 0.28, 0.28, 0.32, 0.12, 0.25 and for cloud B 0.24, 0.16, 0.28, 0.2, 0.12. In steps 12 and 13, we quantize *R* values, and *I* values using Tables 7 and 8. The quantization

in both tables is done by finding the interval *P* and *I*, the quantization values for *P*are 5, 2, 3, 4, 2, and 4. For *I*, the quantization values are 4, 4, 5, 4, 3, and 5

Table 7 Risk Probability Quantization

Probability P	1—5	6—11	12—16	17—21	22—25
P Level	**1**	2	3	4	5

Table 8 Risk Impact Level Quantization

Impact I	**1-5.5**	**6—11**	**12—15.5**	**16—22.5**	**23—27.5**
Impact level	**1**	**2**	**3**	**4**	**5**

In step 14, we use the quantized values of *P* and *I* to refine the risk rank. This was done by substituting *P* and *I* into Table 4. The values of risk rank (RR) were 4.5H, 3M, 4H, 3.5H, 1.5L, and 3.5H, as seen in Table 9. The implementation of steps seen in case implantation shows the result for the Local Network with an overall Risk of Value of 3.445 and the overall risk for Cloud as seen in Table 10 with a value of 1.8. For cloud B, the overall risk was 1.53.

Table 9 General Risk Matrix for The Local Network

Service (Risk)	P%	Quantized I	Quantized P	RISK RANK R	Quantized value Rank	Borda P criterion r_{11}	Borda I criterion r_{12}	b_i	risk Wight RW	Overall risk
S1	92	4	5	4.5	H	0	0	9	0.26	0.9
S2	28	4	3	3	M	1	1	4	0.13	1.29
S3	48	5	2	4	H	0	0	8	0.23	0.29
S4	80	4	2	3.5	H	0	1	6	0.17	0.6
S5	36	3	4	1.5	L	1	1	1	0.03	0.045
S6	84	5	5	3.5	H	1	0	6	0.17	0.6
Total								34		3.445

Table 10 General Risk Matrix for Cloud A

Service (Risk)	P%	Quantized I	Quantized P	RR	Quantized value Rank	Borda P criterion r_{11}	Borda I criterion r_{12}	b_i	b_i Wight	0verall risk
CA1	28	1	2	1	L	1	0	1	0.03	0.03
CA2	28	3	2	2	L	1	1	2	0.16	0.32
CA3	32	1	2	2	L	1	0	3	0.25	0.5
CA4	12	1	1	2	L	1	0	3	0.25	0.5
CA5	25	1	2	2	L	0	1	3	0.25	0.5
Total								12		1.8

Table 11 GENERAL RISK MATRIX FOR CLOUD B

Service (Risk)	P%	Quantized I	Quantized P	RR	Quantized value Rank	Borda P criterion r_{11}	Borda I criterion r_{12}	b_i	b_i Wight	Risk Wight RW
CB1	0.24	1	2	1.5	L	0	1	2	2/11=0.18	0.27
CB2	0.16	2	1	1.5	L	1	0	2	0.18	0.27
CB3	0.28	3	2	2	L	1	0	3	0.27	0.54
CB4	0.20	1	2	1.5	L	1	0	2	0.18	0.27
CB5	0.12	1	1	1	L	0	1	2	0.18	0.18
Total								11		1.53

Table 10 and 11, concerning the cloud value CA1 and CB1, represent the values acquired from Table 1 and the data protection agreement. CA2 and CB2 represent internal management risks, while CA3 and CB3 represent internet security. The fourth row of the two tables represents the supervision mechanisms, and the fifth row represents the law and policy. The first column of Tables 9, 10, and 11 represent the strategic element of service we are analyzing. The second column P% represented the risk probability value obtained from equation 10. The Quantized Impact I is the third column and is obtained from Quantizing impact vector using Table 8, while the fourth column Quantized P is obtained from Quantizing probability vector using Table 7. The Quantized Risk value is obtained from Table 4. Table 4 also plays an important role in quantizing both risk impact and probability. The fifth and sixth columns are dedicated to Borda P criterion r_{11} concerning the probability of risk and Borda I criterion r_{12} concerning the impact of risk. Since we are working with two Borda parameters, the impact and the probability has two criteria. These values are set to maximize or minimize the effect of either impact or probability in the final stages of assessment. Column b_i is the Borda count for that element obtained from equation 7. The following column is b_i Wight and is obtained from equation 9. The last column is the calculated completion of the resultant risk-judging matrix. The overall security risk rank is expressed in equation 10. We have the result for the Local Network with an overall Risk of Value of 3.445 and the overall risk for Cloud A seen in Table 10 with a value of 1.8. For Cloud B, the overall risk was 1.53.

Estimating Resultant Risk Using AHP

From the previous section, we find that the overall local network risk is 3.445, where cloud A is 1.8 and Cloud B is 1.53. Let us assume the following:

- Local Network with a value of 3.445 is two times riskier than Cloud A with a 1.8 value; accordingly, Cloud A is 1/3 risky from the local network.
- Local Network with a value of 3.445 is three times riskier than Cloud B with a 1.53 value; accordingly, Cloud A is 1/2 risky from the local network.
- Cloud A and Cloud B are within the same risk margin; therefore, their risk has equal impact and is set to 1.

Based on this assumption, we generate the AHP matrix in Table 11.

Table 12 AHP Priority Matrix

	Local Net.	Cloud A	Cloud B	Operta Criteria	Result	Wight
Local Net.	1	1/2	1/3	$(1 \times 1/2 \times 1/3)^{1/3}$	=0.5505	0.1692
Cloud A	2	1	1	$(2 \times 1/2 \times 1)^{1/3}$	=1.2599	0.3874
Cloud B	3	1	1	$(3 \times 1 \times 1)^{1/3}$	=1.4423	0.4434
				Sum =	3.2525	

We have the following risks with the following weights:

Table 13 AHP Result at Organizational Risk

	Network Risk	Wight	$RRT = \sum_{i=1}^{k} (\mathrm{RR}_i \mathrm{xRW}_i)$
Local Net.	3.445	0.1692	2.067
Cloud A	1.8	0.3874	0.57
Cloud B	1.53	0.4434	0.79
			3.429

The resultant risk for the whole network in terms of cloud services is equal to 3.429.

CONCLUSION

Recently, networks have considered partial or total migration of their services to clouds. This move, which produces new obstacles, presents several risks. Many of the networks run on multiple network connections or wide-area networks of organizational ownership. An organization has two sorts of risks to cope with; firstly, the risk of the organization's internal information systems, and secondly, the risk involved in dealing with cloud service provider companies. Another issue is the lack of benchmarking and references in the information system of risk assessment for enterprises.

Most organizations, rather than risk assessments and mitigation, are working with vulnerability management ideas. In this study, we conceive strategic services for information systems that function simultaneously and hybrid through local network and cloud services spread through local network nodes and cloud components. Regarding local network components and nodes that represent hosts, known vulnerability values created by commercial tools are identified. These vulnerabilities are collected in vectors with anticipated effects and an evaluation of the value of assets associated with such services. Probabilities or risks are therefore recognized.

The other part of the research investigates the computer approach to analyze the potential of cloud services. It addresses common cloud components such as data management policies, internal cloud provider administration, and internet security. The vulnerability of these components and their influence on business continuity in cloud providers is determined. We have presented a risk probability model for an educational organization, using vulnerability ideas for both local and cloud networks. Risks are calculated for both local and cloud-created weights via Borda Count, and the overall risk has been evaluated separately for each component; local network and two clouds. Finally, the organization's entire risk should be assessed jointly by priorities, and each risk should be analyzed in relation to other risks. For this aim, we employ analytical hierarchy (AHP).

References

- *Amin Saurabh, Galina A., Schwartz, & Alefiya Hussain (2013). In quest of benchmarking security risks to cyber-physical systems. IEEE Network Transaction. 27(1)19 - 24*
- *Amro I. (2015). A Network Service-Based Risk Assessment Model with Case Study on an Educational Organization. Palestinian Journal for Open Learning and e-Learning. Volume 15*
- *Andersen A. (2010). Firm objectives, IT alignment, and information securit. IBM Journal of Research and Development.54(3):5.1-5.7*

- *Asosheh A., & Dehmoubed A., & Khani A. (2009). A new quantitative approach for information security risk assessment. Presented in 2nd IEEE International Conference on Computer Science and Information Technology pp. 222-227. China*
- *Bernardo D. (2013). Utilizing Security Risk Approach in Managing Cloud Computing Services. Presented in IEEE 16th International Conference on Network-Based Information Systems. South Korea*
- *George R. (2014). Systems Engineering Guide. The MITRE Corporation. Produced by MITRE Corporate Communications and Public Affairs. USA*
- *International Organization for Standardization ISO (20018) The ISO 27001 standard on information security matters, http:// www.27000.org/*
- *Jianxing Y. , C. Haicheng, W. Shibo & F. Haizhao (2020).A Novel Risk Matrix Approach Based on Cloud Model for Risk Assessment Under Uncertainty. in IEEE Access, vol. 9, pp. 27884-27896, 2021.*
- *Kassou M., & Kjiri L. (2012). SOASMM: A novel service-oriented architecture Security Maturity Model. Presented in IEEE International Conference on Multimedia Computing and Systems, 2012, pp. 912-918. Morroco*
- *Khidzir Nik Zulkarnaen, & Azlinah Mohamed, & Noor Habibah Hj Arshad (2010). Information Security Risk Management: An Empirical Study on the Difficulties and Practices in ICT Outsourcing. Presented in IEEE Second International Conference on Network Applications, Protocols and Services. Malysia.*
- *Lonita D., & Hertel P., & Pieters W., & Wieringa R. (2014). Current Established Risk Assessment Methodologies and Tools. ICT Section, Delft University of Technology. Netherlands*
- *Mačekl Davor, & Magdalenić1 Ivan, & Nina Begičević Ređep1 (2020). A Systematic Literature Review on the Application of Multicriteria Decision Making Methods for Information Security Risk Assessment.International Journal of Safety and Security Engineering Vol. 10, No. 2, pp. 161-174*
- *Maule R. W., & Lewis W. C. (2009). Risk Management Framework for Service-Oriented Architecture. Presented 2009 IEEE International Conference on Web Services. Proceeding pages: 1000-1005. USA*
- *Metzger Louis, & Bender Lisa (2007). MITRE Systems Engineering (SE) Competency Model Version 1.13. The MITRE Corporation. Bedford, MA 01730*
- *Moona Jewook, & Chanwoo Lee, & Sangho Park, & Yanghoon Kimc (2018). Mathematical model-based security management framework for future ICT outsourcing project.Discrete Applied Mathematics The Journal of Combinatorial Algorithms, Informatics, and Computational Sciences.Volume 241: 67-77*
- *Riaz M. T., M. Shah Jahan, K. S. Arif and W. Haider Butt (2019). Risk Assessment on Software Development using Fishbone Analysis. 2019 International Conference on Data and Software Engineering (ICoDSE), 2019, pp. 1-6,*
- *Saleem M, & Jaafar J., & Hassan F.Model Driven Security framework for definition of security requirements for SOA based applications. Presented in IEEE International Conference on Computer Applications and Industrial Electronics, 2010, pp. 266-270, Malasya.*
- *Xi G., H. Ruimin, P. Yongjun, B. Hao and L. Haitao (2010). The Comprehensive Assessment Method for Community Risk Based on AHP and Neural Network Presented in 2010 Second International Conference on Networks Security, Wireless Communications and Trusted Computing, 2010, pp. 410-413, doi: 10.1109/NSWCTC.2010.230.*
- *Xiao B. and J. Ran. (2010). Risk Evaluation of Network Security Based on NLPCA-RBF Neural Network," in Multimedia Information Networking and Security, International Conference on, Nanjing, Jiangsu China, 2010 pp. 398-402.*
- *Xiaojun Wu and Cong Li (2011). Research and design of one security model for service-oriented multi-application architecture. Presented in IEEE International Conference on Computer Science and Service System (CSSS), pp. 3990-3993. China*
- *Zhang, Q. C. Zhou, Y. Tian, N. Xiong, Y. Qin and B. Hu (2018). A Fuzzy Probability Bayesian Network Approach for Dynamic Cybersecurity Risk Assessment in Industrial Control Systems. in IEEE Transactions on Industrial Informatics, vol. 14, no. 6, pp. 2497-2506*