Information Security Risk Assessment and Management: A Comprehensive Approach

Ishitha Saravan[1], Raiyan Mustafa Mulla[1], Lilibeth Reales[1#] and Vikas Rao Naidu[1#]

[1]Middle East College, Muscat, Oman
[#]Advisor

ABSTRACT

A highly important methodology used by organizations to safeguard their electronic assets from several risks and weaknesses is information security risk assessment and management. Apart from taking into account all of the different kinds of security threats, this study seeks to present a comprehensive approach to risk assessment and management of information security. This holistic strategy's elements include identifying specific risks and vulnerabilities, assessing the possibility and magnitude of attacks and choosing the the most suitable countermeasures. A review of the literature pertaining to research on the comprehensive approach will be a crucial aspect of this study. In order to investigate the security threats that an established company experiences and to recommend the best way for minimizing them, a case-study approach is going to be utilized to gain insight on the practical use of the suggested solution in the real-world setting. This study will project a thorough comprehension of the various information security risk parameters, the discovery of numerous practices followed for risk evaluation and management, and finally the formulation of an appropriate approach for dealing with security-related risks that can be used by businesses of every kind. The findings of the research will contribute to the formulation of strategies and recommendations for the management of information security risk. The recommended approach is expected to assist businesses in determining their information security risks and prioritizing them, setting up the appropriate mechanisms to minimize those hazards, and monitoring how effectively these measures are functioning. The primary objective of the study is to give businesses an approach to manage the security of their data risks, which is essential for preserving their priceless assets and brand.

Introduction

Information Security Risk Assessment and Management is an essential step that firms must implement for protecting their information assets from possible threats. Hence, among the most efficient techniques for dealing with privacy and security concerns in the business environment is by employing an approach based on risks. Any risk mitigation plan needs to involve risk analysis, which is the method that evaluates the weaknesses of a system and the threats it faces.

A general discussion of information security risk assessment and management is the primary objective of this study's work. The comprehension of hazards starts out by comprehending the concepts of assets, risks, and vulnerabilities. Furthermore, this paper will examine and compare all the approaches that are currently employed to evaluate the risk to information security and highlight their shared characteristics.

The risk management process can be described as the methodical implementation of managerial guidelines, processes, and techniques to the duties of interacting, consulting, providing information, and recognizing, evaluating, assessing, addressing, observing, and evaluating risk. Risk Assessment is the result of identifying the risk, evaluation, and review procedures. Risk management enhances productivity within an organization while reducing the probability of undesirable repercussions (Ayo et al., 2018).

An information security audit's fundamental objective is to ensure that the record of a business meets the CIA triad security model (C- confidentiality, I- integrity, and A- available). An audit of information security additionally comprises a risk assessment for information security.

Methodologies for assessing threats to information security may include quantitative or qualitative analysis according to the outcome of their review. The value of risk, as a number, is determined by the algorithm of a quantitative approach. Information regarding undesirable or unanticipated circumstances in the information security framework which may threaten the confidentiality of is frequently collected by making use of the input data for analysis. However, the outcomes are less precise and timely since there is often insufficient statistical data (Kuzminykh et al., 2021).

Whereas A system security assessment approach centered around knowledge and decision-making technology serves as a qualitative, subjective analysis technique, and the level of expertise of the reviewer has an important influence on the preciseness of the findings from the assessment. As an outcome, there are certain extremely high standards for the evaluator's technical skill and excellence. Thus, new risk assessment approaches and techniques have been developed immediately for enhancing the protection of information system functioning and to guarantee the preciseness and dependability of information security risk assessment findings (Cai & Yao, 2021).

The paper will present the comparison of different types of Risk Assessment and Management in different scenarios with their framework. To name a few, Risk Assessment uses a 7-Step, 8-step, and 9-step and includes the Information security Risk Assessment using Fuzzy Rule Set and providing a comprehensive framework based on the understanding of the findings. The approaches of information security risk assessment that are currently now in use are reviewed and contrasted in this article, highlighting their similarities, benefits, and limitations. The paper will wrap up with an argument on the value of information security risk assessment and management in the modern digital era, in addition to the need for businesses to adopt a risk-based method for information security.

Literature Review

Ayo and the others specified five fundamental organizational resources: workers, RMS programs, digital information, and IT infrastructure. The greatest information security risks in a company are caused by human mistakes committed by workers, SQL injections, breaches of data, scams, cross-site scripting, stolen data, social engineering, and interruptions in power. The misuse of vulnerabilities discovered with the resources has been avoided, identified, mitigated, and minimized using relevant industry-standard administrative duties, technical, and physical security measures. The purpose of carrying out a risk assessment serves to systematically identify the primary risks as well as shortcomings that could prevent the company from attaining its business goal. With the objective of bringing down identified levels of risk to the ultimate minimum, essential mitigation techniques are going to be created utilizing the findings from the risk assessment (Ayo et al., 2018).

According to this study, risk management is referred to as the method of identifying, regulating, and reducing or eliminating security hazards that could impact information systems, at a feasible cost. Risk assessment is the Evaluation of threats to, effects on, and vulnerabilities of data and facilities where the data is being processed and the probability of their occurrence. Alternatively, it is also the identification of the risk, assessment of the risk in the context of efficiency, expenditure, and other key aspects, and classification of the risks based on exposure and leveraging.

Assessment of risks, mitigation of risks, evaluation, and assessment are the four phases that constitute risk management. The process of assessing risks entails identification, assessment, and suggestion of risk-reduction approaches. The expression "risk mitigation" pertains to the prioritization, execution, and upkeep of the relevant measures that reduce the risk, suggested by the risk assessment process. Concerns associated with an IT system need to be assessed in conjunction with other variables to assess the risk of a potentially undesirable event. The first step in the procedure for the risk management approach is risk assessment. Throughout the SDLC of a computerized system, companies make use of risk assessment to evaluate the magnitude of any potential threats and the potential hazards

involved. As part of the risk mitigation process, the outcome of this method aids in determining appropriate measures for minimizing or eliminating risk.

The risk assessment process comprises nine key elements,

Step 1 is to define the system. Followed by identifying the threat, identification, analysis of the control, probability determination, assessment of impact, determining the risk, suggestions for control, at last documenting the results (Mandal et al., 2018).

(Kuzminykh et al., 2021) says that there are plenty of software applications are being created in line with the developed techniques for tackling the challenge of information security risk assessment, and these applications are now utilized by enterprises and auditors. IT security risk assessment can be accomplished with over thirty approaches and models. One of the most common alternatives for risk management has to be the Central Computer and Telecommunications Agency (CCTA) Risk Analysis and Management Method (CRAMM). Combining estimations of assets and vulnerabilities, the qualitative risk evaluation and management tool CRAMM assists in estimating risk. The risks of the system are identified and assessed in the initial phases, while recommendations for risk management are put forward in the next phase. Implementing the recommended processes and performing a process assessment for risk management are the final two steps. Every element of risk management is dealt with by the CRAMM technique, from the real determination of risks to the execution of countermeasures. All the information necessary for the CRAMM technique is provided by evaluations by experts and staff replies to questionnaires about how they make use of different resources, which will generate an immense quantity of data. This brings us to the system's flaw, which is that it would take a lot of time and effort to collect this data. Additionally, CRAMM is that its application cannot be reused since it is incapable to make use of previous findings into consideration when calculating the risk factor.

The Facilitated Risk Analysis Process (FRAP) is a strategy for locating the precautionary measures required by companies to minimize risk. It involves assembling a threat list that includes potential risks developed earlier by specialists, reviewing statistics, and participating in staff brainstorming. A professional then compares the compiled list of threats to the possibility of their occurrence, following which an assessment of the negative impact that the threat caused, and its level is determined using the outcomes. The documentation is involved in the final phase. Comprehensive documentation of the assessment's findings will be made once it has been completed to make it possible for additional use or deeper examination.

The approach known as Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) was developed for the administration of data contained within an organization. It entails the establishment of a joint team of leaders and experts to evaluate potential safety concerns and the monetary implications of implementing countermeasures. Three levels of analysis are provided by OCTAVE:

• Creation of a threat profile relevant to the resource; • vulnerabilities identification; • Creation of security objectives and approaches. The OCTAVE technique uses a tree structure, with a separate tree structure for each significant asset. Risk assessment is supplied with a qualitative high/medium/low scale, having an emphasis on anticipated damage instead of chance.

Additionally, to assess the value of various restrictions for assets of the company, the risk assessment approach uses a matrix that integrates resources, vulnerabilities, risks, and restrictions. It consists of three distinct but connected matrix: a threat matrix, a vulnerability matrix, and a control matrix. The threat matrix investigates the interactions between threats and vulnerabilities, and the control matrix analyzes the connections between controls and threats. The vulnerability matrix comprises the connections between resources and vulnerabilities. The typical qualitative low/medium/high system of rating is applied for assessing the effects of the data (where "0" indicates no impact, "1" indicates a weak effect, "3" implies a moderate impact, and "9" denotes a great impact). This approach offers accessible matrix frameworks for analytics and may be used with nearly any organization (Kuzminykh et al., 2021).

In this research, Yalcin & Kılıç suggest the techniques and resources used for the ENISA (European Union Agency for Network and Information Security) Threat and Risk Management research on Risk Management and Risk Assessment are reviewed. The seventeen approaches and 31 tools that EISA is studying for its collection of work are explained in the research at the most basic level. The techniques and tools will be compared with regard to a variety

of variables such as the kind of risk categorization, the level of reference, the scope of practicality, the lifecycle, and the licensing process of their use. Explaining all the tools will be out of the scope of the research but a relevant figure has been mentioned below to get a better understanding of the techniques and their features.

				Risk Assessment Method			Risk Management Method			
Tools	Origin	Coverage	Support	Identification	Analysis	Evaluation	Assessment	Treatment	Acceptance	Communication
Callio	Canada	1	X		X		X		X	X
Casis	Belgium	1								
CCS Risk Manager	USA	2	X	X	X	X	X	X	X	X
CloudeAssurance	USA	2	X	X	X					X
Cobra	United Kingdom	1	X		X		X		X	X
Countermeasures	USA	2	X	X	X		X	X	X	X
Cramm	United Kingdom	1	X	X	X		X			X
EAR / PILAR	Spain	1	X	X	X	X	X	X	X	X
Ebios	France	1	X	X	X		X	X	X	X
GSTool	Germany	1	X	X	X		X	X	X	X
KRiO	Spain	1, 2, 3	X	X	X	X	X	X	X	X
ISAMM	Belgium	2								
Mehari Expert (2010) RM tool	France - Canada	2	X	X	X	X	X		X	X
MIGRA Tool	Italy	1	X	X	X	X	X	X	X	X
Modulo Risk Manager	Brazil	2	X	X	X	X	X	X	X	X
Octave	USA	3	X	X	X		X	X		X
Proteus	United Kingdom	2	X	X	X	X	X	X	X	X
Ra2	Germany	1	X	X			X		X	X
REAL ISMS	USA	2								
Resolver Ballot	Canada	2								
Resolver Risk	Canada	2								
Risicare	France	2	X	X	X	X	X		X	X
Riskwatch	USA	1	X	X	X		X	X		X
RM Studio	Iceland	1,2, 3	X	X	X	X	X	X	X	X
SISMS	Turkey	2	X	X	X	X	X	X	X	X

Figure 1. Types of Risk Assessment tools (Yalcin & Kılıç, 2019).

Additionally, this study shows the most common strategies that can be used in the management of security are,

1. To minimize the development of threats,
2. 2. Reduction in the probability of the threat,
3. 3. Limiting the consequences of threats when they occur (Yalcin & Kılıç, 2019).

Cai and Yao propose unique risk assessment approaches and models based on fuzzy rule sets with the aim of strengthening information security. A fuzzy system of experts that evaluates the risk to information security has been developed using fuzzy rule sets. The proposed approach employs fuzzy logic and a stacked model to assess the risk associated with information security. The suggested approaches and frameworks aim to boost the accuracy of risks

associated with information security assessment findings and assure the secure functioning of information systems. The three distinct components that include security organization, management of security, and security technology collaborate to establish the information system security system. An associated model framework that confirms the system's functionality through experimental study has been constructed using fuzzy sets of rules (Cai & Yao, 2021).

Methods

There are two distinct types of methodology: qualitative and quantitative. Inputs for qualitative research arise from interactions with individuals and identify factors, areas, and various types of risks. Numerous kinds of quantitative evaluation can be carried out, but risk management assessment is carried out in a qualitative approach instead of a quantitative way. A qualitative risk assessment is an excellent tool for taking into consideration how various parts of a company are related to each other and evaluating not merely technical factors but also problems created by people and processes. This study uses a qualitative analysis that will be used for this project, which entails gathering data via conversations and evaluating documents. The intention of the research is to gain a greater awareness of the techniques that are currently in effect and the challenges companies face whilst assessing and handling risks related to information security.

Analysis of content is primarily utilized as the source for data collection and findings for this study. The study will additionally investigate documents that are significant to the assessment and management of information security risks in businesses, such as risk evaluation reports, regulations, and suggestions.

Data were examined by the convergence of data. By analyzing the commonalities found with the paper's evaluation, the study will apply the technique of data convergence. This will assist ensure the reliability of the results. For the comprehensive approach, we will choose the 9-step Risk Assessment framework to produce the desired outcome.

Results/Findings

After analyzing various information security risk assessment types, we have found the following types relevant to the scope of the project.

To begin with, we have the 7-stage risk assessment method.

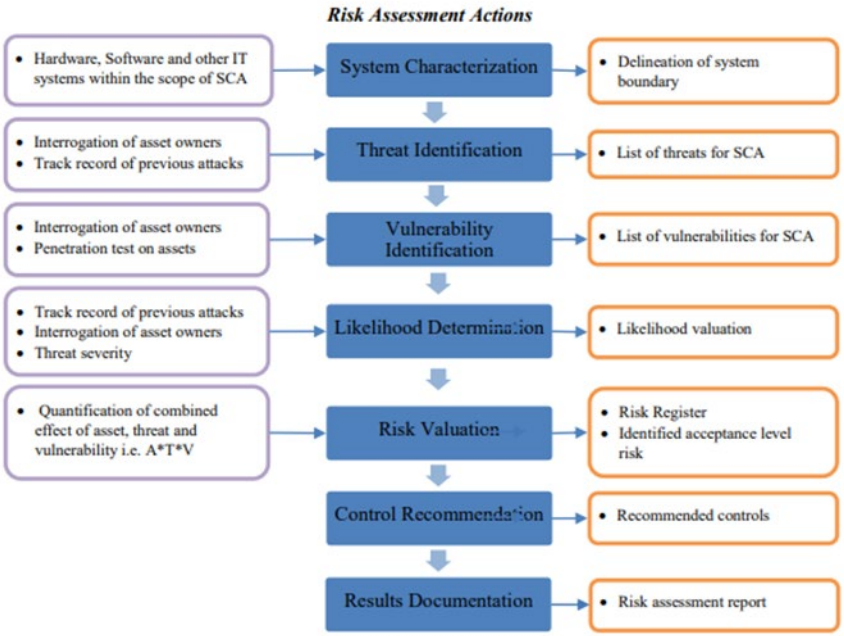

Figure 2. 7-Stage Risk Assessment (Ayo et al., 2018)

The flowchart for the risk assessment approach is shown in Fig. 2 above. It illustrates the phases required for performing the risk assessment for a company in a planned, step-by-step manner. That includes,

1. Defining the system based on its features, which include hardware, software, and other technologies under the scope.
2. Identifying any potential threat to the system by keeping a record of attacks that took place previously and doing regular audits.
3. Identifying the vulnerability of the system by monitoring the activities of the users regularly and having vulnerability scans.
4. Determining the probability of risk again involves keeping tabs on attacks that took place earlier and on the users.
5. Valuation of Risk can involve the numbering of the combined consequences of resources, vulnerability, and threat.
6. Control Recommendations- Involves any recommendations on the restrictions on the system.
7. Final Documentation – This provides the documented report of the risk assessment.

Even though the steps mentioned seem to be feasible for an organization it does have a few shortcomings on its own to not be a comprehensive approach as, it can be perhaps excessively restrictive and impractical for all businesses or sectors and might require more time for completion compared to other risk assessment techniques, which could delay the execution of key security measures according to this research.

Secondly, we discuss the 6-stage framework of risk assessment,

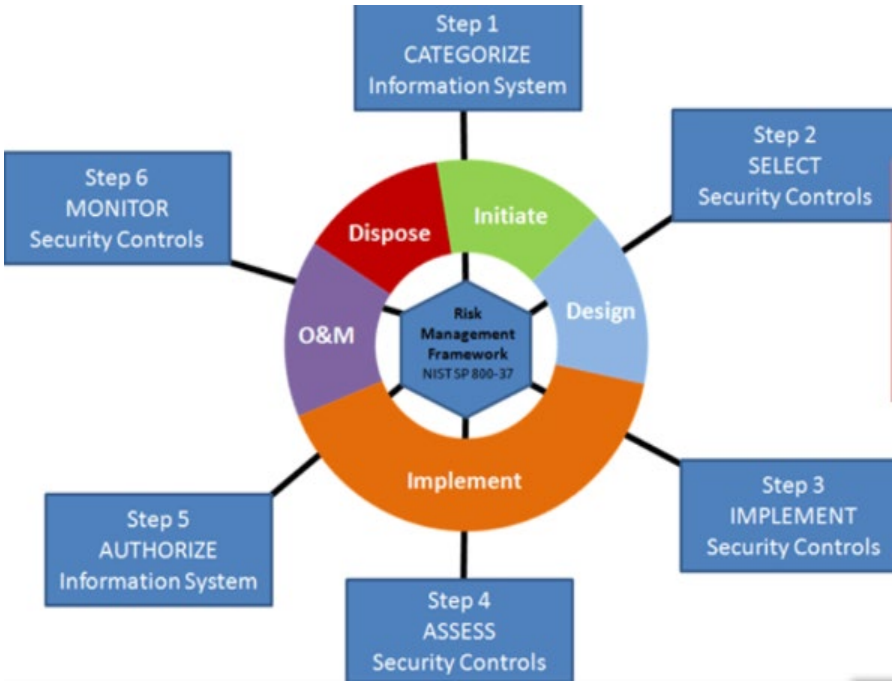

Figure 2. 6- stage (Information Security Risk Assessment Integrates Risk Management & SDLC, 2020)

Fig.3 above clearly shows the different steps and the functionality of Risk Assessment that requires only 6 stages that includes, including Classifying the system based on identifying the risks, Selecting the controls required to maintain the security level, Executing that particular control, analyzing them, Providing the ability for the system to authorize themselves to verify the users and at last monitor the appropriate working of the security measure on the system. Apart from its simple function, it might not prove to be a better option over others as it might not address every necessary element of risk assessment, leaving certain vulnerabilities open to possible attack, and could fail to provide adequate depth or information in the research, leading to a less accurate assessment of risks and possible consequences.

Figure 3. 8-step approach (Drain, 2022)

The above figure points out the tasks in each of the steps to identify the risk and mitigate them through this assessment plan.

Stage	Input	Risk Assessment Stages	Output
1	Hardware, software, system interfaces, data and information, personnel, system mission	Determining the characteristics of the information system	System boundaries System functions Criticality of the system and data System and data sensitivity
2	Preliminary risk assessment reports Auditors' comments Security requirements Security test results	Identification of vulnerabilities	List of potential vulnerabilities
3	History of attacks on the system Information from response teams, media, law enforcement	Threat identification	List of potential threats
4	Available security regulators Planned security regulators	Analysis of security regulators	List of available and planned security regulators
5	Motivation of the source of threats Threat source resources The nature of the vulnerability Existing countermeasures	Determining the probability of threat realization	Probability rating
6	Analysis of the impact on the mission of the organization Assessment of asset criticality Data criticality Data Vulnerability	Definition of impact Loss: confidentiality, availability, integrity	Impact rating
7	Probability of threat realization Level of influence Adequacy of existing and planned countermeasures	Risk identification	Risks and their levels
8	Risk levels	Countermeasures	List of countermeasures
9	Risk levels	Resulting documentation Risk analysis report	Reports

Figure 4. 9-step Process working (Kuzminykh et al., 2021)

Fig.5 defines each stage along with the input and the output of the stage. The steps of risk assessment typically appear in Table 1 above for the majority of the approaches used. The risk can be prevented, eliminated, decreased, transmitted, or permitted based on the requirements of the company and the leadership's evaluation of the asset's value. By deciding not to use the resource, you can eliminate the at last, by creating a plan of action and setting the requirements in place, the risk will likely be accepted.

The number of phases is the primary distinction between an 8-step and a 9-step information security risk assessment technique. The 9-step approach adds an additional phase for periodically evaluating and revising the risk assessment, while the 8-step procedure consists of only eight clearly stated steps.

As the organization's technological advances, infrastructure, and activities evolve, the nine-step risk assessment process offers an extra procedure for periodically examining and revising the risk assessment. This will make sure that the assessment is precise and appropriate.

The 8-step method may be simpler and easier to carry out than the 9-step procedure regarding pros and cons. The nine-step method, however, could provide better prospects for ongoing growth and risk management, this enables a comprehensive approach to the management of risks.

Discussion

Based on the finding above, it will aid in the development of strategies and recommendations for the evaluation and handling of information security risk. Organizations will be able to implement the suggested strategy to identify and categorize their information security risks, put into effect the appropriate precautions to reduce those risks and assess the extent to which those measures are working. As the research implies a comprehensive approach which means, we should provide a platform that includes nearly all the aspects of the process.

Our reliance on IT continues to rise constantly as numerous firms employ computer systems and networking architectures on an immense scale. The most crucial concern for stability and the setting up of these systems is Security. Therefore, a significant number of companies make investments in this area as they set up Information Security Management Systems (ISMS). The ISMS process comprises the Information Security Risk Assessment (ISRA), which is essential to identify risks and mitigate them in the organization.

There are various types of information security risks and as the usage of computer systems increases, the risks increase as well. Some of the risks are Database security threats (SQL Injection, Denial of Service, Weak Authentication, etc.), Web Threats (Cross-Site Scripting, DDoS Attacks, Vulnerable Plug-Ins, etc.), and some of the major threats like intrusion, spoofing, malware, etc.

After comparing the shortcomings and their ability to be comprehensive for an organization of various other approaches mentioned in the literature review and findings section, we decided to choose the 9- step Risk Assessment for providing a level of comprehensiveness.

Therefore, to overcome various threats in the system, it is necessary to follow a comprehensive Information Security Risk Assessment and Management Plan. A plan that meets the requirements of this study is the 9-step Risk Assessment Process.

Figure 6. Recommended Risk Assessment Process

The Diagram above lists the following tasks,

1. Establish the guidelines of the risk assessment- Specify what falls in the assessment's area of responsibility, which could include a division of the company, an area, or a particular aspect of the enterprise.

2. List the resources- Determine what kind of resources, such as intellectual property, financial details, or information about consumers, are required to be adequately safeguarded.

3. Determine the threats- Determine any possible risks to the data, such as viruses, social engineering, or hackers.

4. Evaluate the weak point (Vulnerability)- Determine the areas where the data assets are unsecured or vulnerable so that opponents can take advantage of them.

5. Estimate the probability of the threats - Determine the possibility that the threats are serious according to past events, market patterns, or professionals' opinions.

6. Analyze the effects of risks - Calculate the likelihood of loss of revenue, damage to reputation, or legal accountability that the risks identified could have on the information assets.

7. Identify the degree of the risk- Based on the probability and effect analyses, establish the risk level associated with every recognized risk.

8. Establish and execute security controls and the required countermeasures- Establish and execute controls and countermeasures, including access control lists, firewalls, data encryption, etc. to minimize the risks or any security-related problems.

9. observe and review- Continuously evaluate and review the efficiency of the controls, making necessary modifications.

Taking these steps is essential to guarantee all possible vulnerabilities and threats are acknowledged and dealt with rapidly and successfully. As part of the approach, resources are located, vulnerabilities and threats to security have been identified, risks are prioritized and identified, security controls are evaluated and constructed, results are documented, a strategy for countermeasure is made, suggestions are put into action, and the risk assessment procedure is continually tracked and reviewed. The final phase is to create a report that clearly and concisely outlines all the assessment's findings. Management at all levels will receive an electronic copy of this report, which should also include departmental assessment and recommendations. The outcomes of a risk assessment for IT should be documented in a report that goes out to all necessary parties.

Conclusion

This study report emphasizes the significance of a holistic approach to regulating risks related to information security within businesses. The management of possible threats to the company's essential resources and minimizing the impact of identified risks depends primarily on the execution of effective security controls.

This study highlights different methods of Risk Assessment used in various scenarios, their features, and shortcomings. After comparing various approaches, this paper recommends a Nine-step risk assessment approach that provides a structured and methodical approach to identifying, assessing, and categorizing information security risks.

Overall the results of this study suggest that in order to protect their most valuable resources and keep users' confidence, businesses need to establish an active and comprehensive strategy for information security risk assessment and management.

Limitation

One of the limitations of this project was the time and resource constraint, which limited the broad-based findings of this research. This paper was limited to qualitative analysis of various research that has taken place over the years and expert opinions. The capacity to draw general inferences and provide the findings was thus constrained. The results and findings of the research might not be the regular approach of the full target audience due to numerous contexts. The research was hence unable to use tools and quantitative measure like matrix, statistical and mathematical tools. The results of this study could be seen as a basis for further study and validation with larger and further varied categories.

Acknowledgment

Completing this research paper would not have been possible without the contribution and support of many individuals to whom I would like to express my deepest appreciation. I would like to thank the co- authors Raiyan Mustafa, Ms.

Lilibeth Reales, and Dr. Vikas Rao Naidu for their invaluable contribution and guidance throughout the research process. Their expertise and suggestions were instrumental in shaping this project in the right direction.
In addition, I would also like to extend my sincere thanks to all the participants in our study, who shared their valuable insights, experiences, and time with me. Their willingness towards the project was essential in the smooth completion of this project and its success, and I am deeply grateful for their participation.

References

Ayo, S., Ngala, B., & Amzat, O. (2018). *Information Security Risks Assessment: A Case Study*. University of East London. https://www.researchgate.net/publication/329608166_Information_Security_Risks_Assessment_A_Case_Study

Cai, W., & Yao, H. (2021). Research on Information Security Risk Assessment Method Based on Fuzzy Rule Set. *Hindawi*, 9663520. https://doi.org/10.1155/9663520

Drain, H. (2022, February 22). *An 8-Step Risk Assessment for Your Facility's Security - Facilities Management Advisor*. Facilities Management Advisor. https://facilitiesmanagementadvisor.blr.com/security/8-step-risk-assessment-facilitys-security/

information security risk assessment integrates risk management & SDLC. (2020, October 21). Enterprise Architects. https://enterprisearchitects.eu/services/assessments/information-security-risk-assessment/

Kuzminykh, I., Ghita, B., Sokolov, V., & Bakhshi, T. (2021). Information Security Risk Assessment. *Encyclopedia*, *1*, 602–617. https://doi.org/10.3390/1030050

Mandal, T., Jana, B., Mitra, S., & Poray, J. (2018). A Study on Risk Assessment in Information Security. *SSRN*, 1–9. https://doi.org/10.2139/3261593

Yalcin, N., & Kılıç, B. (2019). Information Security Risk Management and Risk Assessment Methodology and Tools. *International Conference on Cyber Security and Computer Science*. https://www.researchgate.net/publication/330170264_Information_Security_Risk_Management_and_Risk_Assessment_Methodology_and_Tools