iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 11 **Issue:** V **Month of publication:** May 2023

DOI: https://doi.org/10.22214/ijraset.2023.53379

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue V May 2023- Available at www.ijraset.com

Qualitative and Quantitative Risk Assessment through IISRA Framework

Keerti Dixit[1], Dr. Umesh Kumar Singh[2], Dr. Bhupendra Kumar Pandya[3]
[1, 2, 3]*Institute of Computer Science Vikram University, Ujjain*

Abstract: ***Information and communications technology (ICT) has expanded commercial potential beyond comprehension and has merged completely with organizations. In addition to its many advantages, ICT has disadvantages, such as cybersecurity risks, vulnerabilities, and a lack of adequate administrative access control that cybercriminals might take advantage of. Organizations are becoming more dependent on information security as a result of potential hazards brought on by advances in information technology, each of which has a different critical level based on its likelihood of happening and potential consequences. Methodologies for evaluating information security threats can be either quantitative or qualitative, depending on the*** Information ***outcome of their assessment. It is clear that both of the aforementioned choices have a number of fundamental flaws. In order to overcome them, this research paper focused on developing an Integrated Information Security Risk Assessment (IISRA) Framework that would be both more accurate and adaptable because existing approaches are frequently inappropriate and ineffectual due to the ongoing appearance of new sources of risks.***
Keywords: Security Risk Assessment, Risk, Threat, Vulnerability.

I. INTRODUCTION

Organizations are placing more and more emphasis on information security. Organizations rely substantially on information technology as digitalization progresses and new technologies are adopted quickly [1]. Many organizations now place a high priority on protecting themselves against information security risks [2]. Assessments of the threats to information security are crucial in preventing and reducing those risks.

Organizations are becoming more and more dependent on technology, which increases the need to secure digital environments. Information security breaches can have a variety of negative effects on a company's operations, finances, reputation, and legal standing [3-5]. Every day, organizations that have experienced data breaches, disruptions, cybercrime, and hacking make the news. Threats and strong opponents are multiplying more quickly than we can devise and employ effective defenses [6, 7].

A vital ingredient of enterprise' risk assessment plan, ISRA assistance in recognizing, measuring, and prioritizing risk in relation to objectives relevant to the organization and basis for risk acquiring [8-10]. The word "risk assessment" refers to a procedure that includes the identification, elimination, or reduction of the probability of incident that can negatively influence the welths of the information structure, subject to an acceptable cost of defense compute that accommodate a risk Assessment, analysis of "cost-effectiveness" parameter, and selection, construction, and testing of the computation of security [11, 12].

In essence, an information risk assessment approach looks at the information risks connected to the organization assets, including an application & infrastructure that supports it. We discover risks and vulnerabilities that are relevant to information asset within the technique. Appropriate controls are chosen based on the likelihood of occurrences and their potential impact. Controls are employed to stop incidents from happening or lessen their impact on the organization [13-15].

Figure 1: Information Security Risk Assessment

1) Something that has worth to an organization is considered an asset.
2) A threat is a possible catalyst for an unwelcome event that could affect a system or organization.
3) A flaw is something that one maybe more threats can use to access an asset without authorization.
4) Impact refers to how serious the effects of an occasion or incident are. Information availability, integrity, and secrecy are all negatively impacted.
5) The probability that a threat may materialize is called likelihood.
6) Risk is the outcome of the possibility that a danger may manifest through vulnerability and the consequences of that occurrence.
7) Control is a risk management and mitigation tool.

II. INFORMATION SECURITY RISK ASSESSMENT APPROACHES

There are various methods that support the process of risk assessment. Approaches to Risk Assessment can be categorised as qualitative or quantitative.

A. *Qualitative Information Security Risk Assessment*

Qualitative ISRA is an approach to evaluating security risks that focuses on identifying, analyzing, and prioritizing risks based on subjective judgments rather than on quantitative measurements.

This approach typically involves a subjective assessment of the probability and potential impact of security threats to an organization's assets. It involves assessing risks based on their probability of occurrence and the potential impact they could have on an organization.

1) *Advantages of Qualitative ISRA*

These are several advantages of qualitative information security risk assessment, including:

a) Cost-Effective: Qualitative risk assessment is often less expensive and less time-consuming than quantitative risk assessment since it does not require the collection and analysis of large amounts of data.
b) Flexibility: Qualitative risk assessment can be easily adapted to different types of organizations and situations since it relies on expert judgment and does not require a specific methodology or tool.
c) Subjective Evaluation: Qualitative risk assessment allows for a subjective evaluation of risks, taking into account the knowledge and experience of the individuals involved in the assessment process.
d) Effective Communication: Qualitative risk assessment can help communicate the risks to stakeholders who may not have a technical background, allowing them to understand the risks and their potential impact more easily.
e) Early Identification of Risks: Qualitative risk assessment can help identify potential risks early on, allowing organizations to implement risk management strategies before the risks become a significant threat.
f) Risk Prioritization: Qualitative risk assessment enables organizations to prioritize risks based on their potential impact, which can help in the allocation of resources to mitigate the risks more effectively.

2) *Disadvantages of Qualitative ISRA*

While qualitative ISRA has its advantages, it also has some potential disadvantages, including:

a) Subjectivity: Since qualitative risk assessment relies on expert judgment and subjective evaluations, it can be prone to biases and inconsistencies, which may lead to inaccurate or incomplete risk assessments.
b) Lack of Quantitative Data: Qualitative risk assessment does not rely on quantitative data, so it may not provide a comprehensive understanding of the actual likelihood and impact of risks.
c) Limited Scope: Qualitative risk assessment may not be suitable for complex or large-scale projects, as it may not cover all potential risks and may not provide a detailed analysis of each risk.
d) Limited Comparability: Qualitative risk assessment may not be easily comparable across different projects, organizations, or contexts, as the evaluation criteria may vary depending on the specific circumstances.
e) Lack of Transparency: The qualitative risk assessment process may not be transparent or easily explainable to stakeholders, which may result in reduced trust in the assessment process.

B. Quantitative Information Security Risk Assessment

Quantitative ISRA is a method to evaluating security risks that relies on data and mathematical analysis to determine the likelihood and potential impact of security threats to an organization's assets. Quantitative risk assessment can provide a more objective and data-driven approach to risk management, as it is based on quantifiable data rather than expert judgment alone. It can also provide a more thorough understanding of the potential impact of each risk and help organizations make more informed decisions about risk mitigation strategies.

1) Advantages of Quantitative ISRA

There are several advantages to using quantitative risk assessment in information security risk management, including:

a) Objectivity: Quantitative risk assessment uses data-driven analysis and mathematical models, providing a more objective approach to risk management.

b) Detailed Analysis: Quantitative risk assessment provides a more detailed analysis of risks, taking into account the probability and potential impact of each risk.

c) Better Prioritization: Quantitative risk assessment enables organizations to prioritize risks based on their probability and impact, allowing them to efforts on the risks that pose the greatest threat.

d) Improved Decision-Making: Quantitative risk assessment provides a more informed basis for decision-making, enabling organizations to make more accurate and effective risk management decisions.

e) Improved Communication: Quantitative risk assessment can help improve communication with stakeholders, allowing them to better understand the risks and their potential impact.

f) Increased Credibility: Quantitative risk assessment can provide increased credibility with regulators, auditors, and other stakeholders, who may require a more rigorous and data-driven approach to risk management.

2) Disadvantages of Quantitative ISRA

While quantitative information security risk assessment has its advantages, it also has some potential disadvantages, including:

a) Data Availability: Quantitative risk assessment relies on accurate and reliable data to be effective, which may not always be available or may be difficult to obtain.

b) Complexity: Quantitative risk assessment can be complex and time-consuming, requiring specialized skills and knowledge to conduct effectively.

c) Cost: Quantitative risk assessment may be more costly than qualitative risk assessment due to the need for data collection, analysis, and modeling.

d) Subjectivity: Even with quantitative data, risk assessment still involves some level of subjectivity, such as assumptions made during data analysis or modeling.

e) Lack of Realism: Quantitative risk assessment may not always reflect the real-world complexities and uncertainties of the organization's environment.

f) Limited Scope: Quantitative risk assessment may not cover all potential risks, as some risks may be difficult to quantify or may not have sufficient data available.

III. INTEGRATED INFORMATION SECURITY RISK ASSESSMENT (IISRA) FRAMEWORK

We have developed an Integrated Information Security Risk Assessment Framework to identify and analyze security risk of organizations. We construct the risk matrix for information security during which we identify both qualitative and quantitative risks.

Figure 2: Integrated Information Security Risk Assessment Framework

IISRA Framework involves the following steps:

1) Qualitative assessment: We evaluate each identified risk using a qualitative method (risk matrix) which assigns a rating based on likelihood and impact.
2) Quantitative assessment: We assess each risk numerically by calculating its expected value to estimate its impact.
3) Combine results: We have combine the results of the qualitative and quantitative assessments and adjusted the ratings if necessary.
4) Develop Risk Matrix: The result of an event's significance and probability is risk. Depending on the threat's probability and effect, the hazard level is determined for known threats and recorded on the risk matrix. The "dark red" sections represent the major risk areas, which are determined by the critical impact degree and likelihood of occurrence. Red is used to indicate high danger areas. Areas with a medium danger are indicated in yellow, while regions with a low risk are underlined in green.

Table 1: Severity Rating

Severity Rating	
Critical	A critical risk vulnerability has a high likelihood of having an adverse effect on business operations, causing disruption or downtime, and giving an attacker privileged access, leading to a severe outage. If misused, it directly affects CIA.
High	A high risk vulnerability is one where the CIA accessible application or even backend resources like databases, operating systems, etc., could be significantly impacted by successful exploitation.
Medium	When combined with another vulnerability, a medium risk vulnerability exposes details about the programme and its underlying infrastructure that an attacker can use to take over the application or the operating system that supports it.
Low	Low risk vulnerability that could expose system information and allow unauthorized users to get access, potentially compromising the system. The work required to take advantage of this kind of vulnerability would be greater.

To capture the risk rating, following risk assessment matrix is used considering Impact and probability of risk in terms of ease of exploitation.

Table 2: Risk Matrix

Risk Assessment Matrix				
Impact of Vulnerability – Consequence	Major	High	Critical	Critical
	Moderate	Medium	Medium	High
	Minor	Low	Medium	Medium
Risk Severity = Impact x Probability		Low	Moderate	High
		Probability of Risk occurrence		

5) Remediation Plan: To keep the risk assessment and management strategy current and efficient, evaluate it frequently.
6) Regular review: To keep the risk assessment and management strategy current and efficient, evaluate it frequently.

IV. RESULT AND DISCUSSION

In order to evaluate an organization's effectiveness, the created Integrated Information Security Risk Assessment (IISRA) Methodology was put into practice. We have chosen an organization where vulnerability assessment is a continuous process for the methodology's adoption.

The objective of this study was to identify any conceptual or operational weaknesses in the publicly exposed assets and to provide recommendations for lowering potential risks in the event that these weaknesses were effectively exploited. The purpose of this testing was to determine whether an attacker could exploit security issues in the applications and underlying infrastructure.

A. *Results of the Network Vulnerability Risk Assessment*

1) *Network Devices*

Table 3: Risk Assessment result of Network Devices

Domain	Critical	High	Medium	Low	Total
Vulnerability Assessment	0	2	5	1	8

2) *Servers*

Table 4: Risk Assessment result of Servers

Domain	Critical	High	Medium	Low	Total
Vulnerability Assessment	4	2	7	1	14

3) *Workstations*

Table 5: Risk Assessment result of Workstations

Domain	Critical	High	Medium	Low	Total
Vulnerability Assessment	3	4	9	2	18

4) *WIFI Controller*

Table 6: Risk Assessment result of WIFI Controller

Domain	Critical	High	Medium	Low	Total
Vulnerability Assessment	1	1	4	2	8

B. *Results of the Web Vulnerability Risk Assessment*

Table 7: Risk Assessment result of Web Application

Domain	Critical	High	Medium	Low	Total
Vulnerability Assessment	0	1	1	7	9

Using the IISRA framework, we evaluated the organization's network and online vulnerabilities. Assets have been divided into four groups for the network vulnerability assessment: network devices, servers, workstations, and WiFi controller. We have found that these devices are currently susceptible to a number of network-related security problems. These devices have eight critical, nine high, twenty-five medium, and six low network risk vulnerabilities, according to our research.

The organization's web application has then been evaluated against the majority of application security-related concerns. We discovered nine security flaws on this website during the application security testing conducted to date. One high, one medium, and seven low vulnerabilities were found that required action.

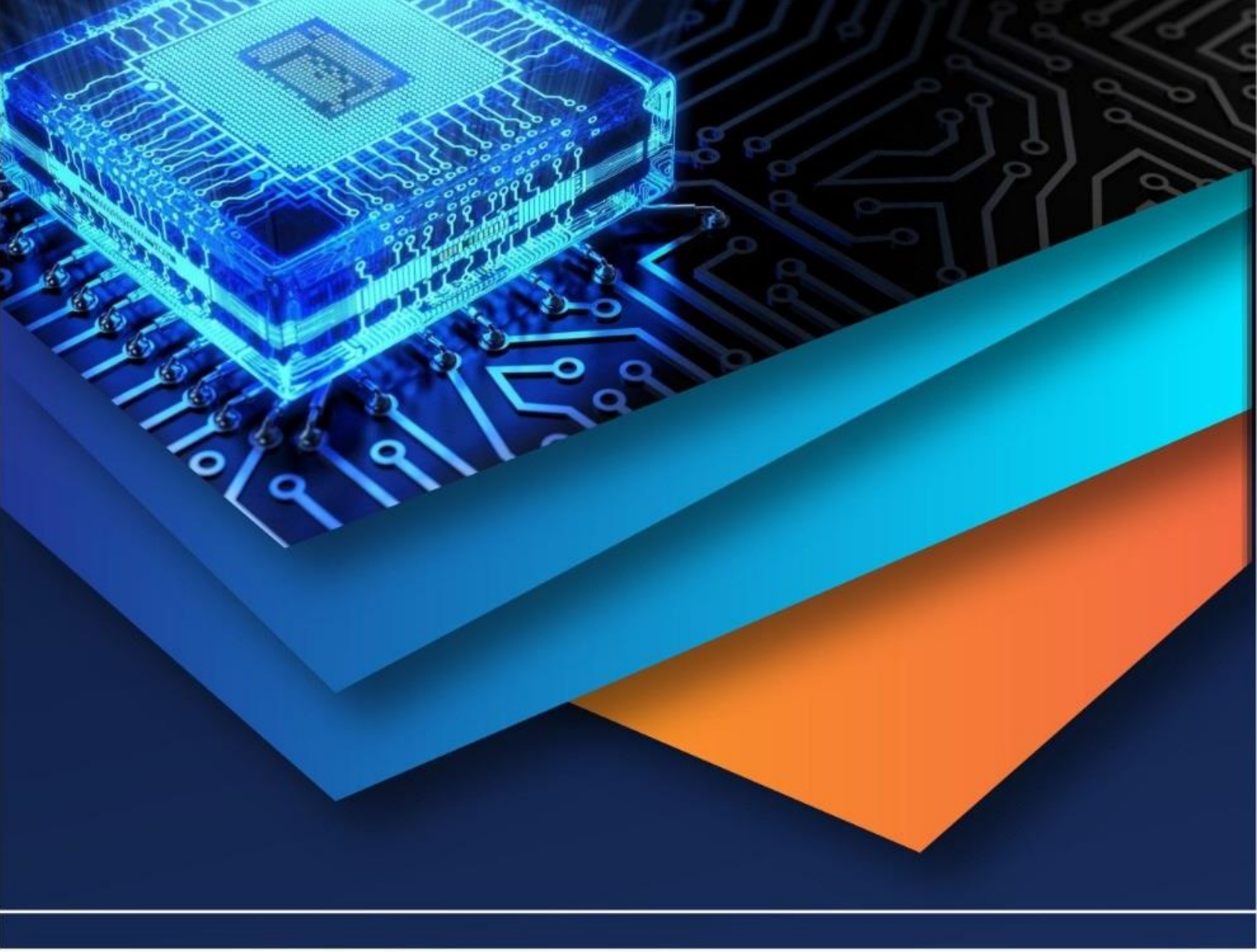
V. CONCLUSION

In this research paper, we have developed an Integrated Information Security Risk Assessment (IISRA) Framework. In order to demonstrate the effectiveness of the suggested IISRA framework, we implemented it in a real computer environment and examined the results. The weaknesses of the organization are described in detail. The measuring of the risk magnitude of discovered vulnerabilities in the organization's computing network setup is made possible by combining qualitative & quantitative risk assessment to maintain the security level of the organizations. Our research has significantly aided in the identification of flaws that ensure the security of an organization's overall system and the most important data.

Overall, this research project has provided an integrated method for tackling the intricate problem of information security risk, which today's majority of organizations must deal with.

REFERENCES

[1] L. Kuzminykh, B. Ghita, V. Sokolov, and T. Bakhshi, "Information security risk assessment," Encyclopedia, 2021, doi: 10.3390/encyclopedia1030050.
[2] R. Hoffmann, J. Napiórkowski, T. Protasowicki, and J. Stanik, "Risk based approach in scope of cybersecurity threats and requirements," Procedia Manuf., vol. 44, pp. 655–662, 2020, doi: https://doi.org/10.1016/j.promfg.2020.02.243.
[3] G. Strupczewski, "Defining cyber risk," Saf. Sci., vol. 135, p. 105143, 2021, doi: https://doi.org/10.1016/j.ssci.2020.105143.
[4] Keerti Dixit, Dr. Umesh Kumar Singh, Dr. Bhupendra Kumar Pandya, An Information Security Risk Assessment Framework for Cyber-Physical System, International Journal of Computer Applications (0975 – 8887) Volume 183 – No. 53, February 2022
[5] Ms. Keerti Dixit, Dr. Umesh Kumar Singh, Dr. Bhupendra Kumar, Attack Taxonomy for Cyber-Physical System, International Journal for Research in Applied Science & Engineering Technology (IJRASET) ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538 Volume 10 Issue I Jan 2022- Available at www.ijraset.com
[6] B. Irvin Lamarca, "Cybersecurity Risk Assessment of the University of Northern Philippines using PRISM Approach," in IOP Conference Series: Materials Science and Engineering, 2020, vol. 769, no. 1, doi: 10.1088/1757-899X/769/1/012066.
[7] I. Lee, "Cybersecurity: Risk management framework and investment cost analysis," Bus. Horiz., vol. 64, no. 5, pp. 659–671, 2021, doi: https://doi.org/10.1016/j.bushor.2021.02.022.
[8] H. Lallie et al., "Cyber security in the age of covid-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic," Computers & Security, vol. 105, June 2021.
[9] Keerti Dixit, "Information Security Risk Assessment in Higher Educational Institutions-Issues and Challenges" presented in 36th M.P. Young Scientist Congress, March 23 - 26, 2021
[10] K. Dixit, U. K. Singh, B. K. Pandya, "Comparative Framework for Information Security Risk Assessment Model", ICCIDS-2022 International Conference on Computational and Intelligent Data Science(Elsevier) 21 May 2022
[11] K. Dixit, U. K. Singh, B. K. Pandya, "Threat and Asset Identification through IISRA Framework", International Journal of Creative Research Thought (IJCRT), Vol. 11, Issue 4, Apr. 2023.
[12] K. Dixit, U. K. Singh, B. K. Pandya, "Identification of Web Vulnerabilities through IISRA Framework", International Journal of Novel Research and Development (IJNRD), Vol. 8, Issue 5, May 2023.
[13] K. Dixit, U. K. Singh, B. K. Pandya, "Comparative study of Information Security Risk Assessment Model", International Journal of Computer Application (IJCA), Vol. 185, No. 7, May 2023.
[14] K. Dixit, U. K. Singh, B. K. Pandya, "An Integrated Information Security Risk Assessment (IISRA) Approach" presented in 2nd International Conference on Data Science and Artificial Intelligence ICDSAI 2023, California State University USA and Lendi Institute of Engineering and Technology, Apr. 24-25, 2023
[15] K. Dixit, U. K. Singh, B. K. Pandya, "Identification of Network Vulnerabilities through IISRA Framework", International Journal of Research in Applied Science and Engineering Technology (IJRASET), Vol. 11, Issue 5, May 2023



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY