





Information Security Risk Assessment (ISRA): A Systematic Literature Review

Rias Kumalasari Devi^{1)*} , Dana Indra Sensuse²⁾ , Kautsarina³⁾ , Ryan Randy Suryono⁴⁾ 

¹⁾²⁾³⁾⁴⁾ Faculty of Computer Science, Universitas Indonesia, Indonesia
Depok 16424, West Java

¹⁾rias.kumalasari@ui.ac.id, ²⁾dana@cs.ui.ac.id, ³⁾kautsarina61@cs.ui.ac.id

⁴⁾ Faculty of Engineering and Computer Science, Universitas Teknokrat Indonesia, Indonesia
Bandar Lampung 35142, Lampung

⁴⁾ryan@teknokrat.ac.id

Abstract

Background: Information security is essential for organisations, hence the risk assessment. Information security risk assessment (ISRA) identifies, assesses, and prioritizes risks according to organisational goals. Previous studies have analysed and discussed information security risk assessment. Therefore, it is necessary to understand the models more systematically.

Objective: This study aims to determine types of ISRA and fill a gap in literature review research by categorizing existing frameworks, models, and methods.

Methods: The systematic literature review (SLR) approach developed by Kitchenham is applied in this research. A total of 25 studies were selected, classified, and analysed according to defined criteria.

Results: Most selected studies focus on implementing and developing new models for risk assessment. In addition, most are related to information systems in general.

Conclusion: The findings show that there is no single best framework or model because the best framework needs to be tailored according to organisational goals. Previous researchers have developed several new ISRA models, but empirical evaluation research is needed. Future research needs to develop more robust models for risk assessments for cloud computing systems.

Keywords: Information Security Risk Assessment, ISRA, Security Risk

Article history: Received 2 August 2022, first decision 16 August 2022, accepted 8 September 2022, available online 28 October 2022

I. INTRODUCTION

As the complexity of information systems grows over time, companies are faced with increasingly critical challenges. Evaluation and assessment of information security risks are crucial, which can be conducted through various frameworks and models. The aim is to assess the severity of a particular threat and its possible consequences. A hazard needs immediate precautionary measures because this poses the highest risk [1].

Information and communications technology (ICT) has created limitless business opportunities and has become inseparable from organisations. Besides its numerous benefits, ICT has drawbacks, i.e., cybersecurity threats, vulnerability, and a lack of effective control over administrative access that cybercriminals can exploit [2].

Information or data may be transferred and stored in digital and physical formats. As a result, information security encompasses the safeguarding of such data as well as the technological techniques of storage, transmission, and exchange. In several applications, information security concentrates on information and data confidentiality, integrity, and availability (CIA). Confidentiality denotes that information or data may only be viewed by parties with authority and is connected to the notion of the lowest privilege, where everyone has full permission. Data integrity implies that data are shielded from tampering or corruption throughout the storage and transmission process. Availability guarantees authorized users access to data if required [2].

Information security has become necessary for certain organisations since the transfer of information is vulnerable to threats. The need for information security in organisations is increasing since changes in information technology

* Corresponding author

potentially create risks, each of which has a different critical level, determined by the probability of occurrence and impact [3]. Improvements in information technology security do not imply more effective cyber threat mitigation. Humans are the weakest bond in the series due to recklessness, misinformation, and susceptibility to social engineering deceptions [4].

Information Security Risk Assessment (ISRA) is essential to an organisation's management procedures. It attempts to determine, assess, and prioritize risks depending on the specified requirements of risk as well as organisational goals. Risk management is the process of detecting, controlling, and eliminating or lowering the probability of an incident at an acceptable cost of protection in which an incident can harm information system resources. Risk management includes risk analysis, cost-effectiveness parameter analysis, selection, implementation, and testing. An information security audit also includes an evaluation of information security risks [1].

ISRA is essential in identifying and prioritizing information assets and identifying and monitoring specific threats an organisation poses, particularly the likelihood of threats occurring and their effects on business. Risk identification is locating and selecting an organisation's leading information and identifying vulnerabilities and threats associated with each asset. Upon identification and analysis, the organisation will value each detected risk. It subsequently assesses the threat's likelihood of occurrence and impact on information assets. The risk level is determined by integrating likelihood and effect. This effect and probability study might be quantitative, qualitative, or a hybrid of both. ISRA lists vulnerabilities, threats, risk levels, and control measures [3].

The information assets that are the subject of analysis are identified and assessed during the assessment process to protect them from prospective attackers. Consequently, it is essential to identify the appropriate information assets, and organisations choose their critical assets from a comprehensive list. If the assessment of information assets is incorrect, the most crucial information assets for the organisation's operations will remain unvalued [5].

This study conducted a literature review of papers related to ISRA. One of the papers is previous research conducted by Pan and Tomlinson; a search limited from 2004 to 2014 [6]. This research only shows a comparison of the number of papers based on research categories, followed by an explanation in the discussion section. The seven categories include risk identification, comparison of risk analysis, improvement of risk analysis, comparison of frameworks, improvement of frameworks, case study, and others. In addition, Pa et al. conducted similar research with a search range from 2005 to 2014 [7]. This research collected explicitly risk assessment papers related to IT governance. Subsequently, it compared the number of papers per year, empirical and theoretical studies, and data collection methods. The research identified three frameworks and model categories: COBIT, ISO 27002, and ITIL. This research has not presented the various frameworks, models, or methods that already exist. Moreover, this research has been obsolete for more than five years.

Therefore, this study was conducted because topics related to ISRA still have research opportunities, so it needs to be explored more deeply by looking for articles from 2016 to 2021. This study explains the aims and findings of each paper and categorizes them into different groups. The paper grouping was based on the type of model/framework, research object, research area, and risk analysis method. This study was carried out to provide academics with a better understanding of how much ISRA has evolved to determine ISRA's methods, models, and frameworks. The systematic literature review (SLR) approach developed by Kitchenham is applied in this research. Journal extraction and proceedings were carried out, followed by analysis and classification. This study concludes with an overview of the existing ISRA.

II. METHODS

Kitchenham's systematic literature review method, used by previous studies in computer science, was utilized in the paper selection [8], [9]. The search was conducted through Google Scholar, ScienceDirect, and Scopus databases. Each paper was examined, and the inclusion and exclusion criteria were considered, followed by categorizing selected papers [10].

The research question (RQ) in this study is as follows:

RQ1. What research focus on information security risk assessment did the researchers study?

RQ2. In what areas is this method applied?

A comprehensive search of available literature was performed by applying the search keywords:

("information security risk" OR "security risk") AND (assessment OR analysis) AND (framework OR model OR method).

A. Inclusion and Exclusion Criteria

This review focuses on research related to information security risk assessment. The search technique was limited to title, abstract, and key and restricted from 2016 to 2021. Journal articles and conference papers were included, while

other languages were eliminated from the search results favouring English. This systematic review included only full-text papers that were accessible online. Papers that did not meet this study's criteria were excluded, and duplicate papers were removed.

B. Selection of Papers

The paper selection process is presented in Fig. 1. In the first stage, a search was conducted on the selected database using search keywords for English-language papers, journal and conference articles published from 2016 to 2021. The search resulted in 1,641 potentially related papers consisting of 593 papers from ScienceDirect, 187 from Scopus, and 861 from Google Scholar. Subsequently, a selection was made based on title and abstract, resulting in 208 papers, consisting of 119 papers from ScienceDirect, 74 from Scopus, and 15 from Google Scholar. After filtering relevant papers for further review, 75 papers were obtained, consisting of 27 papers from ScienceDirect, 36 papers from Scopus, and 12 papers from Google Scholar. The selection was made by reading and conducting a full-text review. Papers that cannot be accessed in the full text were eliminated, with 52 papers remaining, consisting of 23 papers from ScienceDirect, 17 from Scopus, and 12 from Google Scholar. Data extraction and synthesis were then carried out. Papers with unclear research objectives, scopes, results, and conclusions not relevant to the aim of this research were eliminated. Thus, 25 final papers were eventually selected, consisting of ten papers from ScienceDirect, ten from Scopus, and five from Google Scholar.

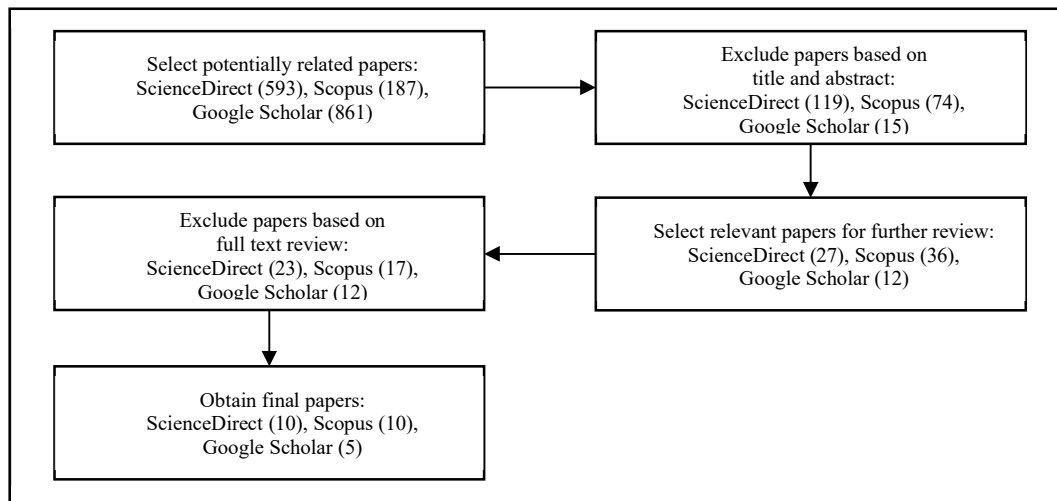


Fig. 1 Paper selection process

III. RESULTS

This section shows the search results for papers selected from journals and conference articles using Kitchenham's systematic literature review method.

A. Publications by year

Most papers are obtained from the ScienceDirect and Scopus database. Fig. 2 shows the number of papers by year of publication. Based on 25 papers, the most published in 2020 were nine papers.

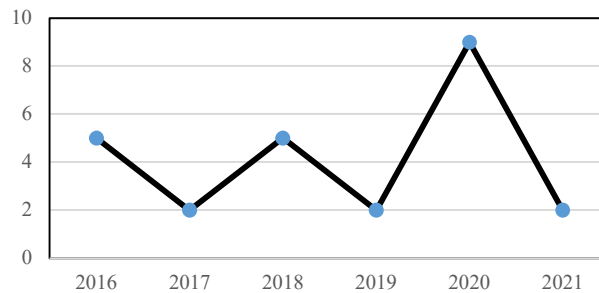


Fig. 2. Publications by year

Table 1 highlights that information security risk assessment is discussed in the 25 selected papers. It also presents the findings of the selected papers in the literature classification.

TABLE 1
LITERATURE PAPER

Author	Aim/Scope	Case Study	Method/ Model/ Framework	Finding
[11]	Analysis of four risk analysis methods using the classification scheme of Campbell et al.	N/A	CORAS, Conflicting Incentives Risk Analysis (CIRA), IS Risk Analysis Based on Business Model, Information Security Risk Analysis Method (ISRAM)	Ontology of CORAS, CIRA, and IS methods account for unique vulnerabilities, threats, assets, and countermeasures.
[12]	Proposal of a conceptual cloud computing security requirements model	Government	ISO/IEC 27002	A conceptual cloud computing security requirements model
[13]	Proposal of a risk analysis model	N/A	Event Tree Analysis (ETA) method, fuzzy decision theory.	A risk analysis model that discovers and analyses different sequences of events.
[14]	implementation of combined techniques for information security risk assessment	Government	ISO 27005, NIST SP 800-30 revision 1.	Combined techniques result in a comprehensive risk assessment.
[15]	Development of a framework for cybersecurity risk assessment in an organisation	N/A	PRISM framework	A novel PRISM framework.
[16]	Proposal of a model for ISRA. An integrated architecture-risk model would allow a complete risk evaluation at all organisational resource levels.	Education Institution	Risk relationship model, IT architecture model.	A conceptual integrated architecture-risk model
[17]	Proposal of a model that integrates fault tree analysis, decision theory, and fuzzy theory	Website, e-commerce, ERP	Fault Tree Analysis (FTA), Decision Theory, Fuzzy Theory.	A cybersecurity risk analysis model
[18]	Explanation of the connection between organisational performance and risk management	Corporation	Failure Mode and Effect Analysis (FMEA)	Demonstrated the existence of indirect and direct links between performance and risk management
[19]	Evaluation of cyber security risk	Government	The National Institute of Standards and Technology (NIST) Cyber Security Framework (CSF)	The NIST CSF assists in identifying particular people, processes, and technologies that require improvement.
[20]	Adoption of PRISM to improve the organisation's cyber policies	Education Institution	PRISM framework	PRISM can confirm that an organisation's performance and direction are as desired.
[21]	Proposal of a hierarchical time-dependent FMEA approach	N/A	Failure Mode and Effect Analysis (FMEA)	The time-dependent probabilistic loss model is a novel hierarchical risk evaluation model to minimize the weakness of the RPN approach used in FMEA
[22]	Comparison of a quantitative security risk model for cloud computing systems	N/A	SecAgreement: A Security Risk Assessment Model, The MFC Extension model (MFCE), The Mean Failure Cost Model (MFC), Multi-dimensional Mean Failure Cost Model (M2FC).	The comparison results assist decision-makers in selecting appropriate models to analyse security threats in the cloud computing environment and other information systems.
[23]	Risk assessment of digital library information security	Government	ISO/IEC 27002, The GB/T20984-2007 method (Chinese National Bureau of Standards).	Formulation of a digital library information security risk assessment scale.

TABLE 1 (cont.)
 LITERATURE PAPER

Author	Aim/Scope	Case Study	Method/ Model/ Framework	Finding
[24]	Development of a cyber risk management framework, discussion of the cyber risk assessment process	N/A	N/A	A cyber risk management framework
[25]	Proposal of a model for big data	N/A	Failure Mode and Effects Analysis (FMEA), Grey relational analysis Theory.	A risk model for big data. The most significant part of big data risk is data governance. Data governance awareness is essential in maintaining adequate controls.
[26]	Comparison of quantitative models resulting in a series of recommendations in selecting a quantitative model appropriate for security issues facing an organisation	N/A	Annual Loss Expectancy (ALE), Information Security Risk analysis method (ISRAM), Multi-dimension Mean Failure Cost (M2FC).	Suggestions for selecting the most effective quantitative model for businesses' security concerns
[27]	Assessment of a quantitative model with probability as a measure of the likelihood of an event occurring	N/A	Annualized Loss Expectancy (ALE)	Probability estimates used in quantitative models are subjective.
[28]	Measurement of the security capability of a system	State-Owned Enterprises (SOEs)	Control Objectives for Information and Related Technology (COBIT) 5	Measurement results can be used to recommend solutions in the decision-making process in an organisation.
[29]	Propose Theoretical Design of Information Security Risk Management	Government	ISO 27005: 2018, NIST SP 800-30 revision 1	The ISRM design outcomes, when combined with policy, can match organisational requirements for recognizing and controlling risks through operational activities.
[30]	Propose (Lightweight security risk assessment) LiSRA framework for information security decision assistance	SME	LiSRA framework, quantitative and qualitative analysis.	Framework for assessing overall risk and determining the most effective and cost-effective future security actions
[31]	Proposal of a novel information security risk assessment (ISRA)	Civil engineering company	Rich Description Method (RDM)	RDM is a detailed description technique that takes a formal and more comprehensive approach to the existing knowledge and information assets.
[32]	Investigation of the consistency of both improved FMEA and traditional FMEA in IT risk assessment	Government	Failure Mode and Effect Analysis (FMEA)	The consistency of enhanced FMEA was shown to be greater than that of traditional FMEA.
[33]	Information system risk management assessment	Education Institution	OCTAVE Allegro	A risk assessment can help reduce the hazards associated with an information system.
[34]	Improvement of information security risk analysis in the Magerit framework by incorporating threat-occurrence prediction models. Proposal of replacing historical threat frequency with future threat occurrence probability.	Government	Magerit (Spanish adaptation of ISO/IEC 27005)	A substitute prediction model for risk analysis techniques
[35]	Proposal of pISRA model	N/A	pISRA model	A privacy-considered information security risk assessment (pISRA) model

B. *Information Security Risk Assessment*

ISRA is the basis of a probability-based information security management system (ISMS). The objective of ISRA is to analyse a company's potential security risks and treat the risk to a tolerable or acceptable level while remaining within a reasonable budget [35]. Organisations use ISRA approaches to identify information assets and related security concerns wholly and systematically [31]. ISRA approach is established to analyse the mechanisms for securing data and how various possibilities can affect information guarantee [34].

TABLE 2
RESEARCH OBJECT

Type of framework	Framework	Research Object					Number of studies
		Evaluation	Comparison	Improvement	Implementation	Development	
International organisation	ISO/IEC 27002			[12]	[23]		2
	ISO/IEC 27005			[14]	[29]		2
	NIST SP 800-30			[14]	[19], [29]		3
Professional Organisation	COBIT 5				[28]		1
	CORAS (2003)		[11]				1
	OCTAVE Allegro				[33]		1
	Magerit (2006)			[34]			1
Framework derived from research projects	PRISM framework				[20]	[15]	2
	Lightweight security risk assessment (LiSRA) framework					[30]	1
	A cyber risk management framework					[24]	1
Models derived from research projects	privacy-considered Information Security Risk Assessment (pISRA) Model					[35]	1
	IS Risk Analysis Based on Business Model		[11]				1
	SecAgreement: A Security Risk Assessment Model		[22]				1
	The Mean Failure Cost (MFC) Model		[22]				1
	The MFC Extension (MFCE)		[22]				1
	Multi-dimensional Mean Failure Cost (M2FC) Model		[22], [26]				2
	Annual Loss Expectancy (ALE)	[27]	[26]				2
	Integrated architecture - risk model					[16]	1
Methods/ Analysis Technique	Information Security Risk Analysis Method (ISRAM)		[11], [26]				2
	Conflicting Incentives Risk Analysis (CIRA)		[11]				1
	Event Tree Analysis (ETA)					[13]	1
	Fault Tree Analysis (FTA)					[17]	1
	Failure Mode and Effect Analysis (FMEA)			[21], [25], [32]	[18]		4
	Rich Description Method (RDM)					[31]	1
	Fuzzy Decision Theory					[13], [17]	2
	Decision Theory					[17]	1
Grey Relational Analysis Theory			[25]			1	
Number of studies		1	3	6	7	8	25

Table 2 shows the classification of frameworks and models based on the focus of the research object. The most current research is to implement existing models and build new models. This shows that researchers are developing ISRA models enthusiastically. In addition to the frameworks and models provided in Table 2, there are professional organisation frameworks such as CRAMM (2001), Microsoft (2006), and Mehari (2007) [1] [3].

C. Research Areas

Several studies on ISRA have been conducted with various techniques and objectives. These studies aimed to assess the threats and risks that potentially harm organisational assets. Various studies have concentrated on specific situations [34]. Table 3 demonstrates several research areas that were the focus of the research. Seven articles focus on information security risk analysis in government, three on educational institutions, one on civil engineering companies, one on e-commerce in particular, two on cloud computing, and the others on information systems in general.

TABLE 3
RESEARCH AREAS

Research areas	Paper	Number of studies
Information Systems in general	[11], [13], [15], [18], [21], [24], [25], [26], [27], [30], [35]	11
Government	[14], [19], [23], [28], [29], [32], [34]	7
Education Institution	[16], [20], [33]	3
Civil engineering company	[31]	1
E-Commerce	[17]	1
Cloud computing	[12], [22]	2

D. Risk Analysis Method

Risk assessment appraisal techniques were further grouped into quantitative, qualitative, and hybrid types [16]. The quantitative method is an analysis that provides a value to assets and the costs of realized risks using a statistical method [36]. Qualitative or quantitative methodologies can be used to assess information security risks. The numerical value of risk is the output of a quantitative methodology's algorithm. In most cases, the assessment input data are utilized to acquire information concerning undesirable or unexpected occurrences that might threaten information security. Nevertheless, a common absence of sufficient statistics diminishes the relevance and precision of the outcome [1].

The qualitative technique is popular since it uses a simple scale with three risk assessment levels (low, medium, and high). Interviews with experts might be used for assessment [1]. Large companies and cities benefit the most from qualitative risk analysis using scenario models. It would be impractical to apply quantitative analysis to companies since they would have to declare all assets. Moreover, the list will contain hundreds or thousands of revisions, rendering it obsolete [36].

Not all selected papers for the study contain sufficient information to determine whether a qualitative or quantitative approach was used. Table 4 shows that researchers created and used qualitative methodologies such as CORAS and Failure Mode and Effect Analysis (FMEA).

Several well-known quantitative risk appraisal methods include Information Security Risk Analysis Method (ISRAM) [37], Annualized Loss Expectancy (ALE), Event Tree Analysis (ETA), and fuzzy theory. Examples of hybrid approaches that combine the best parts of qualitative and quantitative methods are ISO27005, NIST 800-30, and OCTAVE Allegro. There is one study that compares quantitative and qualitative methods [11].

TABLE 4
RISK ANALYSIS METHOD

Risk analysis Method	Paper	Number of studies
Qualitative	[11], [15], [18], [20], [21], [25], [28], [31], [32]	9
Quantitative	[11], [13], [16], [17], [22], [26], [27], [35]	8
Hybrid	[12], [14], [19], [23], [24], [29], [30], [33], [34]	9

IV. DISCUSSION

Research conducted by Pa et al. shows that the number of articles related to ISRA from 2005 to 2014 had decreased [7]. However, the results of this study represent that the number of related articles fluctuated. This systematic review shows that research related to ISRA is still in demand and presents opportunities for future research. The research of Pan and Tomlinson shows that, from 2004 to 2014, research related to ISRA included comparative and improvement research [6]. The improvement research used AHP (Analytic Hierarchy Process) analysis techniques or soft computing such as fuzzy theory. In the study, there were four papers in the field of cloud computing. Meanwhile, the results of this study indicated that only two papers are related to cloud computing [12], [22]. Ten years ago, researchers began to explore the field of cloud computing. However, the progress has not been too significant.

Based on the first research question of this study, the focus is on developing new analytical techniques, models, and frameworks (see Table 2). One research used a combination of analysis techniques, namely Event Tree Analysis (ETA) and Fuzzy Decision Theory [13]. Particular research also combined Fault Tree Analysis (FTA), Decision

Theory, and Fuzzy Decision Theory [17]. In addition, one study applied the Rich Description Method (RDM) technique [31]. The development of new models was also identified. A study by Wei et al. developed an ISRA model that considers privacy, named the privacy-considered Information Security Risk Assessment (pISRA) Model [35]. In addition, there were also studies using an integrated architecture-risk model [16]. The development of new frameworks resulted in the PRISM framework, the Lightweight security risk assessment (LiSRA) framework, and a cyber risk management framework [15], [24], [30].

On the other hand, based on the second research question, the most researched field is information systems in general (as shown in Table 3). For example, research that carried out a comparison of qualitative and quantitative methods. In addition, several improvements in the research of FMEA were initiated by adding a time-dependent probabilistic model and a grey relational analysis theory [21], [25]. There are opportunities to conduct case study research in a particular field. The second most researched area is the government sector. The number of research in this area has increased compared to previous systematic reviews. Research in the government sector is partly the implementation of international and professional organisational frameworks. In addition, several studies introduced improvements from ISO/IEC 27005 and Magerit [14], [34], as well as improvements to the Failure Mode and Effect Analysis (FMEA) analysis technique for governments [32].

The research objects of this study were classified into five types. The description of each type is discussed as follows.

A. *Evaluation Research*

Based on the paper selection process, one paper discusses the evaluation of the existing model. The paper tested the Annualized Loss Expectancy (ALE) model, a quantitative security assessment model with the probability of an event occurring. The results of this study indicate that probability estimates utilized in quantitative models are subjective. The study shows that quantitative evaluation is hardly realistic or practicable in the actual world. A scientific model must be empirically verifiable. ISRM applies empirical probabilities or predictors based on observations and experiences [27]. Future research can evaluate existing quantitative models with specific probabilities. Furthermore, an empirical evaluation of the new model developed from the research project is required.

B. *Comparison Research*

In this systematic review, it was discovered that three papers compare the models of ISRA. The first study compares two qualitative methods, namely CORAS and Conflicting Incentives Risk Analysis (CIRA), and two quantitative methods, namely Information Security Risk Analysis Method (ISRAM) and IS Risk analysis, based on the business model. This study compared risk analysis methodologies based on general characteristics such as methodology, inputs, outputs, objectives, scalability, effort, advantages, and disadvantages. CORAS is a business and asset-oriented risk analysis model. In contrast, CIRA is a risk analysis method focusing on non-technical security. The ISRAM method analyses information technology security risks by involving an organisation's internal participation with a survey-based approach. The IS model is an approach used to calculate the expected annual loss due to operating disturbances [11].

The second study compares quantitative security risk analysis models, including Information Security Risk Analysis Method (ISRAM), Annual Loss Expectancy (ALE), and Multi-dimension Mean Failure Cost (M2FC). The results of the study help decision-makers select the appropriate model to deal with the risk of security problems and reduce organisational security costs. The suitable models for assessing security risks related to cyber-attacks are ALE and ISRAM. The M2FC model can assess security risks related to virtualization technology and business continuity security issues such as human error. Meanwhile, to assess security risks related to data breaches, the M2FC and ISRAM models can be used [26].

The third study compares quantitative security risk models for cloud computing systems. This study compares the SecAgreement model, Mean Failure Cost (MFC), Mean Failure Cost Internal (MFCint), Mean Failure Cost External (MFCext), Multi-dimensional Mean Failure Cost Model (M2FC), and MFC Extension (MFCE) model. The comparison results help decision-makers choose the appropriate model to analyse security threats in the cloud computing environment. The SecAgreement model selects cloud providers based on their respective risk factor calculations. It does not estimate risks due to security breaches in the cloud computing environment. The MFC model is used to assess a system's security in financial terms or how much each stakeholder loses. The MFCext and MFCint models do not consider all the characteristics of threats and only consider one criterion that does not accurately describe the threat. Therefore, it does not provide an accurate value on the cost of security failure. The MFCE model does not represent costs according to security threat dimensions or perspectives. The M2FC model considers threats' perspectives and dimensions and identifies the critical dimensions that cause the highest costs [22].

In addition to comparing quantitative and qualitative-qualitative models, previous studies have been conducted to compare professional organisation frameworks [38]. In these comparative studies, researchers considered vulnerabilities, threats, assets, and countermeasures for security hazards [1]. For future research, qualitative models are the potential to be compared.

C. Improvement Research

There are six research papers related to improving the existing ISRA model. Several authors attempted to improve the model or framework by following current standards. Ali et al. proposed the ISRA model for cloud computing based on ISO/IEC 27002 [12]. On the other hand, Fikri et al. suggested an improvement with a combination of ISO/IEC 27005 and NIST [14]. Figueira et al. incorporated threat-occurrence predictive models to enhance information security risk analysis in magerit [34]. The other three studies improved the FMEA by adding time-dependent probabilities using grey relational analysis theory and performing a consistency analysis [21], [25], [32].

The improvement research framework provides a way to identify risks from different perspectives. Researchers focus on proposing methods or models that are more practical and calculate more objective risk levels, as well as models tailored to specific needs. This study provides more detailed steps in identifying information security risks, calculating risk values with particular methods, and establishing risk criteria. Improvement research aims to reduce the weaknesses of the existing model. Other current models can be improved for future research to be applied to cloud computing systems.

D. Implementation Research

Seven papers show the application of the ISRA model in several fields, such as organisations in general, governments, and educational institutions. The government sector is relatively attractive for researchers to conduct testing. Some studies applied international and professional organisational frameworks, which were subsequently adapted to governments. The frameworks used include The National Institute of Standards and Technology (NIST), COBIT 5, ISO/IEC 27002, and ISO/IEC 27005 framework [19], [23], [28], [29]. While the implementation in educational institutions includes PRISMA and OCTAVE Allegro [20], [33], and implementation in companies that utilize FMEA [18].

Several studies were conducted to ascertain the relationship between risk management and organisational performance. Implementation research aims to evaluate and control risks following the desired direction of organisations. This type of research can help identify people, processes, and technologies that require improvement. It can also provide recommendations for solutions and organisational decision-making processes.

E. Development Research

Eight papers discuss the development of new models. The development of new models was mostly focused on information systems in general. Some studies involved experts in the identification stage [13], [17], [30]. Wei et al. developed an ISRA model that considers the privacy [35]. The new model can determine the most effective and efficient actions related to security in the future [30]. The new models can combine two or more existing models or theories. An integrated approach can make a thorough risk assessment at all organisational asset levels [16].

The issue with qualitative evaluation is the lack of information in the measurement process, which limits the final assessment findings. Consequently, this influences the decision-making process. To address these shortcomings, creating new models combines the most exemplary aspects of existing models into a unique hybrid assessment.

There are three perspectives in analysing risk: asset-driven, business-driven, and service-driven [39]. Most studies perform asset-driven risk analysis. Only two studies developed the new model from a business-driven perspective [16], [31]. Previous research using a business-driven perspective through a process-oriented view can result in a much more complete inventory of information assets [5]. Future research can build a service-driven risk assessment model.

V. CONCLUSIONS

This literature study identified journal papers and proceedings between 2016 and 2021 that discuss information security risk assessments (ISRA). This literature reviewed and observed the direction of research during this period. Based on the classification, it can be stated that most of the papers concentrate on the implementation and development of new models for risk analysis. Most of these studies concern risk assessment in information systems in general. The selected papers rarely explain the methods of data collection and processing. Comparison research focuses on the advantages and disadvantages of existing methods or models. According to the findings, an organisation can choose an ISRA model that suits the goals and needs of the organisation. This research shows that there is no best model or framework since a good model or framework follows the needs and goals of a particular organisation.

The implementation research paper shows how ISRA is applied in various fields. Currently, research in the government sector tends to increase in number. Research in the government sector is partly the implementation of international and professional organisational frameworks. The absence of papers on developing new models in the government sector does not suggest that there have been no similar studies. However, it is due to the limitations of the database and the period applied in this literature study. Future research can develop new models to adequately assess information security risks in the government sector. In cloud computing systems, there are still opportunities. In addition, it is necessary to conduct empirical evaluation research of new assessment models derived from research projects.

Author Contributions: *Rias Kumalasari Devi:* Conceptualization, Methodology, Writing - Original Draft. *Dana Indra Sensuse:* Methodology, Writing - Review & Editing, Supervision. *Kautsarina:* Methodology, Writing - Review & Editing, Supervision. *Ryan Randy Suryono:* Methodology, Writing - Review & Editing, Supervision.

Funding: This research received no specific grant from any funding agency.

Conflicts of Interest: The authors declare no conflict of interest.

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] P. Shamala, R. Ahmad, and M. Yusoff, "A conceptual framework of info structure for information security risk assessment (ISRA)," *J. Inf. Secur. Appl.*, vol. 18, no. 1, pp. 45–52, 2013, doi: 10.1016/j.jisa.2013.07.002.
- [4] G. Strupczewski, "Defining cyber risk," *Saf. Sci.*, vol. 135, p. 105143, 2021, doi: <https://doi.org/10.1016/j.ssci.2020.105143>.
- [5] P. Shedden, W. Smith, and A. Ahmad, "Information security risk assessment: Towards a business practice perspective," *Proc. 8th Aust. Inf. Secur. Manag. Conf.*, no. November, pp. 119–130, 2010, doi: 10.4225/75/57b6769334787.
- [6] L. Pan and A. Tomlinson, "A systematic review of information security risk assessment," *Int. J. Saf. Secur. Eng.*, vol. 6, no. 2, pp. 270–281, 2016, doi: 10.2495/SAFE-V6-N2-270-281.
- [7] N. C. Pa, B. A. Jnr, R. N. Haizan Nor, and M. A. A. Murad, "Risk assessment of it governance: A systematic literature review," *J. Theor. Appl. Inf. Technol.*, vol. 71, no. 2, pp. 184–193, 2015.
- [8] P. Rahayu, D. I. Sensuse, B. Purwandari, I. Budi, F. Khalid, and N. Zulkarnaim, "A systematic review of recommender system for e-portfolio domain," in *ACM International Conference Proceeding Series*, 2017, pp. 21–26, doi: 10.1145/3029387.3029420.
- [9] R. R. Suryono, B. Purwandari, and I. Budi, "Peer to Peer (P2P) Lending Problems and Potential Solutions: A Systematic Literature Review," *Procedia Comput. Sci.*, vol. 161, pp. 204–214, 2019, doi: <https://doi.org/10.1016/j.procs.2019.11.116>.
- [10] B. Kitchenham and P. Brereton, "A systematic review of systematic review process research in software engineering," *Information and Software Technology*, vol. 55, no. 12, 2013, doi: 10.1016/j.infsof.2013.07.010.
- [11] V. Agrawal, "A Comparative Study on Information Security Risk Analysis Methods," *J. Comput.*, vol. 13, no. 1, pp. 57–67, 2017, doi: 10.17706/jcp.12.1.57-67.
- [12] O. Ali, A. Shrestha, A. Chatfield, and P. Murray, "Assessing information security risks in the cloud: A case study of Australian local government authorities," *Gov. Inf. Q.*, vol. 37, no. 1, 2020, doi: 10.1016/j.giq.2019.101419.
- [13] A. P. H. De Gusmão, L. C. E. Silva, M. M. Silva, T. Poletto, and A. P. C. S. Costa, "Information security risk analysis model using fuzzy decision theory," *Int. J. Inf. Manage.*, vol. 36, no. 1, pp. 25–34, 2016, doi: 10.1016/j.ijinfomgt.2015.09.003.
- [14] M. Al Fikri, F. A. Putra, Y. Suryanto, and K. Ramli, "Risk Assessment Using NIST SP 800-30 Revision 1 and ISO 27005 Combination Technique in Profit-Based Organisation: Case Study of ZZZ Information System Application in ABC Agency," *Procedia Comput. Sci.*, vol. 161, pp. 1206–1215, 2019, doi: <https://doi.org/10.1016/j.procs.2019.11.234>.
- [15] R. Goel, A. Kumar, and J. Haddow, "PRISM: a strategic decision framework for cybersecurity risk assessment," *Inf. Comput. Secur.*, vol. 28, no. 4, pp. 591–625, 2020, doi: 10.1108/ICS-11-2018-0131.
- [16] E. Hariyanti, A. Djunaidy, and D. O. Siahaan, "A Conceptual Model for Information Security Risk Considering Business Process Perspective," 2018, doi: 10.1109/ICSTC.2018.8528678.
- [17] A. P. Henriques de Gusmão, M. Mendonça Silva, T. Poletto, L. Camara e Silva, and A. P. Cabral Seixas Costa, "Cybersecurity risk analysis model using fault tree analysis and fuzzy decision theory," *Int. J. Inf. Manage.*, vol. 43, no. January, pp. 248–260, 2018, doi: 10.1016/j.ijinfomgt.2018.08.008.
- [18] L. Hezla, A. V.P, P. V.G, S. N.B, N. Hezla, and D. L., "The Role of Organisational Failure Mode, Effects & Analysis(FMEA) in Risk Management and Its Impact on the Company's Performance," in *Proceedings of the 2020 International Conference on Big Data in Management*, 2020, pp. 108–112, doi: 10.1145/3437075.3437082.

- [19] A. Ibrahim, C. Valli, I. McAteer, and J. Chaudhry, "A security review of local government using NIST CSF: a case study," *J. Supercomput.*, vol. 74, no. 10, pp. 5171–5186, 2018, doi: 10.1007/s11227-018-2479-2.
- [20] 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.
- [21] H. A. Jang and S. Min, "Time-dependent probabilistic model for hierarchical structure in failure mode and effect analysis," *Appl. Sci.*, vol. 9, no. 20, pp. 24–26, 2019, doi: 10.3390/app9204265.
- [22] M. Jouini and L. Ben Arfa Rabai, "Comparative Study of Information Security Risk Assessment Models for Cloud Computing systems," *Procedia Comput. Sci.*, vol. 83, no. Fams, pp. 1084–1089, 2016, doi: 10.1016/j.procs.2016.04.227.
- [23] Z. Han, S. Huang, H. Li, and N. Ren, "Risk assessment of digital library information security: A case study," *Electron. Libr.*, vol. 34, no. 3, pp. 471–487, 2016, doi: 10.1108/EL-09-2014-0158.
- [24] 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>.
- [25] M. Mendonça Silva, T. Poletto, L. C. E. Silva, A. P. Henriques De Gusmao, and A. P. Cabral Seixas Costa, "A grey theory based approach to big data risk management using FMEA," *Math. Probl. Eng.*, vol. 2016, 2016, doi: 10.1155/2016/9175418.
- [26] I. Meriah and L. B. A. Rabai, "A survey of quantitative security risk analysis models for computer systems," *ACM Int. Conf. Proceeding Ser.*, pp. 36–40, 2018, doi: 10.1145/3292448.3292456.
- [27] A. Munteanu, "Running the risk IT - More perception and less probabilities in uncertain systems," *Inf. Comput. Secur.*, vol. 25, no. 3, pp. 345–354, 2017, doi: 10.1108/ICS-07-2016-0055.
- [28] A. Pratiwi, D. R. Indah, J. Jauhari, and M. A. Firdaus, "Security Capability Assessment on Network Monitoring Information System Using COBIT 5 for Information Security," 2020, doi: 10.2991/aisr.k.200424.024.
- [29] I. M. M. Putra and K. Mutijarsa, "Designing Information Security Risk Management on Bali Regional Police Command Center Based on ISO 27005," 2021, doi: 10.1109/EIConCIT50028.2021.9431865.
- [30] C. Schmitz and S. Pape, "LiSRA: Lightweight Security Risk Assessment for decision support in information security," *Comput. Secur.*, vol. 90, p. 101656, 2020, doi: 10.1016/j.cose.2019.101656.
- [31] P. Shedden, A. Ahmad, W. Smith, H. Tscherning, and R. Scheepers, "Asset identification in information security risk assessment: A business practice approach," *Commun. Assoc. Inf. Syst.*, vol. 39, no. 1, 2016, doi: 10.17705/1cais.03915.
- [32] A. P. Subriadi and N. F. Najwa, "The consistency analysis of failure mode and effect analysis (FMEA) in information technology risk assessment," *Heliyon*, vol. 6, no. 1, 2020, doi: 10.1016/j.heliyon.2020.e03161.
- [33] J. S. Suroso and M. A. Fakhrozi, "Assessment of Information System Risk Management with Octave Allegro at Education Institution," in *Procedia Computer Science*, 2018, vol. 135, doi: 10.1016/j.procs.2018.08.167.
- [34] P. Tubío Figueira, C. López Bravo, and J. L. Rivas López, "Improving information security risk analysis by including threat-occurrence predictive models," *Comput. Secur.*, vol. 88, 2020, doi: 10.1016/j.cose.2019.101609.
- [35] Y. C. Wei, W. C. Wu, G. H. Lai, and Y. C. Chu, "pISRA: privacy considered information security risk assessment model," *J. Supercomput.*, vol. 76, no. 3, pp. 1468–1481, 2020, doi: 10.1007/s11227-018-2371-0.
- [36] M. Thangavel, D. K. S. Subamaa, P. Deepa, and E. S. Blessie, "A Review on Information Security Program Development and Management," 2018, doi: 10.1109/ICCIC.2018.8782304.
- [37] B. Karabacak and I. Sogukpinar, "ISRAM: Information security risk analysis method," *Comput. Secur.*, vol. 24, no. 2, pp. 147–159, 2005, doi: 10.1016/j.cose.2004.07.004.
- [38] A. Syalim, Y. Hori, and K. Sakurai, "Comparison of risk analysis methods: Mehari, magerit, NIST800-30 and microsoft's security management guide," *Proc. - Int. Conf. Availability, Reliab. Secur. ARES 2009*, pp. 726–731, 2009, doi: 10.1109/ARES.2009.75.
- [39] A. Shameli-Sendi, R. Aghababaei-Barzegar, and M. Cheriet, "Taxonomy of information security risk assessment (ISRA)," *Comput. Secur.*, vol. 57, pp. 14–30, 2016, doi: 10.1016/j.cose.2015.11.001.

Publisher's Note: Publisher stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.