P-ISSN: 2723-8202
E-ISSN: 2503-1171
Volume 9, No 2, Agustus 2024, Page: **154-162**

JURNAL TIKA
Fakultas Ilmu Komputer Universitas Almuslim
http://www.journal.umuslim.ac.id/index.php/tika/index

RISK MANAGEMENT IN INFORMATION SYSTEMS

Sigit Wijanarko
Informatics, Faculty of Communication and Information Technology, Universitas Nasional
e-mail: wijanarkosg@gmail.com

Abstract

Business is supported with information systems. Business process is expected to run normal and stable, and deliver outputs or service as expected. However in many systems, there are risks. Risks may be either supportive or disruptive. The occurrence of risk may influence the performance of the systems. Risk management is needed during the utilization of information systems. Risk Identification, Risk Assessment and Mitigation Strategy are example of Risk Management factors. Risk Management may varies in line with type of business being supported.

Keywords*:* risk identification, risk assessment, mitigation strategy

Abstrak

*[**Manajemen Risiko Dalam Sistem Informasi**] Bisnis didukung dengan sistem informasi. Proses bisnis diharapkan dapat berjalan normal dan stabil, serta memberikan output atau layanan sesuai dengan yang diharapkan. Namun di banyak sistem, terdapat risiko. Risiko dapat bersifat mendukung atau mengganggu. Terjadinya risiko dapat mempengaruhi kinerja sistem. Manajemen risiko diperlukan dalam pemanfaatan sistem informasi. Identifikasi Risiko, Penilaian Risiko dan Strategi Mitigasi adalah contoh faktor Manajemen Risiko. Manajemen Risiko dapat bervariasi sesuai dengan jenis bisnis yang didukung.*

Kata Kunci: *identifikasi risiko, penilaian risiko, strategi mitigasi*

1. Introduction

In line with organization dependence to its information systems or information technology operations, the existence and continuity of the systems need to be a focus for the organization. **Business continuity** depends on the stable operation of IT systems; thus, any risk to these systems becomes a risk to the entire organization.

When an information system operates, it is not without risks. These risks can originate from internal the organization itself, and from external sources. Risks can be internal, arising from within the organization, such as system vulnerabilities or weaknesses, outdated hardware/software, or inadequate policies. Risks can be external, arising from cyber-attacks, natural disasters, or regulatory changes. Internal weaknesses might include human error, technical failures, or policy flaws, while external threats include hacking, malware, or even economic shifts.

Risk refers to an event that can have an impact, whether supportive, disruptive, or causing uncertainty, on the effectiveness and efficiency of the organization's core business processes. Risks management has a relationship to the organization performance.

As written by Gibson (2011), Risk Management is the practice of identifying, assessing, controlling, and mitigating risks. Threats and weaknesses are the driving factors for risks. Identifying threats and weaknesses is

an important step for the organization. Once risks are identified, actions must be taken to address them. Risk Management can also be defined as managing risks. Risk management includes understanding threats and vulnerabilities. It also include knowledge of identifying ways to mitigate. An organization usually has mitigation plans. And as written by Hopkin (2017), Risk management is the set of activities within an organization undertaken to deliver the most favorable outcome and reduce the volatility or variability of that outcome.

2. Methods

The below is a literature review on journals related to risk management in information systems or information technology.

Rodriguez et all. (2017) on a research selecting an optimal risk management strategy for Information Technology (IT) projects, mentioned some key points e.g.:

1. Objective: The study addresses the challenge of selecting the most suitable risk management approach in IT projects, where project managers often face decisions under uncertain conditions. Traditional risk management methods may not effectively capture the subjective and ambiguous nature of risks.
2. Intuitionistic Fuzzy Logic: The research paper employs intuitionistic fuzzy logic (IFL), an advanced decision-making technique that enhances standard fuzzy logic by incorporating three degrees of assessment: membership (truth), non-membership (falsity), and hesitation (indecision). This allows decision-makers to handle uncertainty more effectively, which is crucial when managing IT risks where precise information is often unavailable.
3. Framework Development: The proposed method integrates risk assessment factors into a decision-making framework. This framework helps project managers evaluate potential risk management strategies by considering multiple criteria, such as project complexity, risk probability, and impact on project objectives.
4. Application in IT Projects: The method is tailored for IT project environments, where risks often stem from technological changes, budget constraints, schedule delays, and scope adjustments. The framework guides decision-makers in selecting a risk management approach that minimizes negative outcomes based on the specific risk profile of the project.
5. Risk Management Aspects:
    - Risk Identification: Identifying potential risks early in the project lifecycle, including technological, financial, and organizational risks.
    - Risk Analysis: Evaluating the probability and impact of identified risks using intuitionistic fuzzy logic, which accounts for uncertainty and hesitation.
    - Risk Prioritization: Ranking risks based on their significance and deciding which risks to mitigate or monitor closely.
    - Decision Support: Providing a structured method for choosing the most effective risk mitigation strategies, considering the subjective assessments of project stakeholders.
6. Practical Implications: The intuitionistic method offers a more flexible and comprehensive approach compared to traditional methods, allowing IT project managers to make better-informed decisions in uncertain and complex environments. By considering the uncertainty and hesitation factors in risk evaluation, the method improves the accuracy of risk management strategies.

The study provides an innovative and practical framework for risk management in IT projects, highlighting the importance of addressing uncertainty through intuitionistic fuzzy logic. The approach enhances decision-making in environments where risks are difficult to quantify, offering project managers a tool to mitigate potential project failures.

MacMahon et all. (2018) on a research on risk management of health information technology (IT) systems, mentioned some important things e.g.:

1. Scope of IEC 80001-1:
    - The original IEC 80001-1 standard provides guidelines for managing the risks associated with integrating medical devices into IT networks.
    - It focuses on ensuring safety, effectiveness, and data security in these systems, which is crucial as IT networks in healthcare become increasingly interconnected.

- The standard outlines roles and responsibilities for various stakeholders, including healthcare providers, manufacturers, and IT professionals.

2. Challenges in Implementation:
   - The research paper highlights challenges in applying the original standard, particularly regarding evolving healthcare technologies and systems that were not fully addressed.
   - The rapid advancement of technology, especially in cloud computing, mobile health, and wearable devices, demands a more flexible and adaptive approach to risk management.
   - Stakeholders also found the original guidance somewhat difficult to interpret, necessitating revisions to make it more user-friendly and applicable to current systems.
3. Revisions to IEC 80001-1:
   - The revisions focus on aligning the standard with modern healthcare IT practices, including the introduction of software as a medical device and networked systems that extend beyond hospital walls.
   - The revised version aims to incorporate new risk factors introduced by digital health platforms, like cybersecurity threats, data breaches, and system interoperability issues.
   - It also emphasizes a risk-based approach where stakeholders continuously assess potential risks as the network evolves, incorporating elements of dynamic risk management.
4. Risk Management Aspects:
   - Patient safety remains the top priority in the standard's risk management framework. This includes addressing risks that arise from system failures, data integrity issues, and unauthorized access to sensitive medical information.
   - Security risk is a growing concern, especially with the rise of networked devices and health data exchanges. The revised standard encourages proactive risk assessments and the use of cybersecurity tools to mitigate threats.
   - The standard promotes an iterative process for risk management, where systems are continuously monitored, and risks are reassessed as new technologies are integrated or system changes occur.
   - Interoperability risks are another focus, ensuring that systems from different manufacturers can work together without introducing new hazards or malfunctions.
5. Stakeholder Collaboration:
   - The revised IEC 80001-1 stresses the importance of cross-disciplinary collaboration between healthcare professionals, IT experts, and device manufacturers to manage risks effectively.
   - Clear communication and shared responsibility across different parties are necessary to ensure that all potential risks are identified and mitigated before they impact patients or operations.

The research highlights the ongoing evolution of the IEC 80001-1 standard to better address the complexities of modern healthcare IT systems. By revising the standard, the authors aim to create a more practical and adaptive framework for managing risks associated with health information technology. The revisions ensure that patient safety, cyber security, and system interoperability are consistently prioritized in an increasingly digital healthcare environment.

Ramalingam et. All (2018) on a research titled **"**Optimizing Governance, Risk management and compliance for Enterprise Information Security using DEMATEL and FoM", mentioned some important things e.g.:

1. Governance: The paper addresses governance structures that help organizations maintain control over their information security frameworks. It highlights how effective governance is crucial in setting policies and monitoring compliance.
2. Risk Management: The paper's core contribution is centered on risk management. The authors propose using the DEMATEL (Decision Making Trial and Evaluation Laboratory) method to analyze and optimize risk management processes in enterprise information security. DEMATEL is used to identify and visualize the complex interrelationships between various risk factors, helping organizations understand the cause-and-effect relationships among risks.
3. Compliance: Compliance is another critical component of GRC. The authors explore how compliance management frameworks can be optimized to meet regulatory standards and ensure information security measures align with legal and industry requirements.
4. DEMATEL: A technique used to structure and analyze the relationships between factors involved in decision-making. In this context, DEMATEL is employed to clarify the causal relationships between different security risks and identify the most influential factors.

5. FoM (Field of Management): A methodology for handling risk within a dynamic and complex information security environment. It provides a structured way of managing and mitigating risks by assessing how risks can be handled within the scope of enterprise management.
6. Risk Management Aspects:
   - The paper identifies key risk factors in information security and applies DEMATEL to understand their interdependencies. The risks analyzed include data breaches, cyber-attacks, compliance violations, and operational disruptions.
   - Mitigation: The DEMATEL approach enables organizations to prioritize risks and focus on mitigating the most critical ones by addressing their root causes.
   - Optimization: Using DEMATEL and FoM together allows for a more optimized risk management strategy, balancing governance and compliance while ensuring that security measures are effective and efficient.

This paper offers a novel framework for enhancing enterprise information security by integrating governance, risk management, and compliance (GRC). It demonstrates how DEMATEL and FoM can be used to optimize risk management processes by analyzing the relationships between different security risks and developing strategies to mitigate them. The proposed approach helps enterprises to efficiently manage complex risk scenarios while ensuring compliance and robust governance structures.

Suroso and Fakhrozi (2018) on a research titled "Assessment of Information System Risk Management with Octave Allegro at Education Institution", mentioned some key points, e.g.:

1. Objective: The research aims to evaluate information system risk management in educational institutions. Educational institutions rely heavily on information systems for operational effectiveness, and therefore, managing risks related to these systems is crucial to protect sensitive data, ensure system reliability, and mitigate potential disruptions.
2. Methodology: The authors employed the OCTAVE Allegro framework for assessing risks. OCTAVE Allegro is a streamlined risk assessment approach focusing on information assets and their security risks. It is specifically designed to identify risks in a structured manner and prioritize actions to mitigate those risks. This method involves a detailed understanding of the context in which the information assets operate.
3. Risk Factors: Several risk factors are considered in the study, including:
   - Human-related risks: These are risks due to human error or malicious actions, such as inadequate training, insider threats, and misuse of information.
   - Technical risks: Issues related to the technical infrastructure, such as system vulnerabilities, hardware failures, and network security gaps.
   - Operational risks: Risks associated with the day-to-day operations, including outdated procedures, insufficient backups, and lack of maintenance.
   - Compliance risks: Non-compliance with legal, regulatory, or institutional standards that can lead to penalties or data breaches.
4. Risk Management Process: The OCTAVE Allegro process involves eight steps:
   - Defining assets critical to the organization.
   - Identifying threats related to these assets.
   - Prioritizing risks based on their potential impact.
   - Developing mitigation strategies for the most critical risks.
   - The authors adapted this process to fit the specific context of educational institutions, considering factors such as student data protection, academic records security, and administrative system reliability.
5. Results and Recommendations:
   - The study highlights that educational institutions are vulnerable to a variety of risks, particularly in areas like unauthorized access to sensitive data and insufficient cybersecurity measures.
   - It recommends prioritizing training and awareness programs for staff and students, enhancing technical security measures (e.g., firewalls, encryption), and ensuring regular audits of the system to stay updated with new risks.
   - Continuous monitoring and evaluation of the risk management strategies are emphasized to adapt to changing technological landscapes and emerging threats.

The application of OCTAVE Allegro in educational institutions provides a structured way to manage information system risks. By identifying and addressing key risk factors, institutions can better protect their

systems, data, and operations. The paper underscores the importance of ongoing risk management and the role of both technology and human elements in mitigating risks.

Ki-Aries et all. (2022) on a research titled Assessing system of systems information security risk with OASoSIS, mentioned some important things e.g.:

OASoSIS (Organizational, Architectural, and System of Systems Information Security) is a framework designed to evaluate information security risks in SoS environments. The primary challenge in these environments is the complexity of identifying and managing security risks across multiple interdependent systems, each potentially governed by different organizations, policies, and technologies. The framework aims to:

1. Identify and model security risks across different layers, from the individual systems within the SoS to the organizational level.
2. Provide a structured approach to assess and mitigate security risks through a combination of organizational policies, architectural designs, and technical solutions.
3. Enable risk management decisions by mapping out potential security vulnerabilities, threats, and their cascading effects throughout the interconnected systems.

Key Risk Management Factors:

1. Interdependencies: In SoS, individual system vulnerabilities can have cascading effects, creating risks for the entire system network. Risk assessment must account for these interdependencies.
2. Lack of centralized control: SoS typically involves systems managed by different organizations. This decentralized control increases the complexity of managing risks, as security policies and risk management processes may vary.
3. Dynamic nature of systems: SoS environments are often fluid, with systems entering and leaving the environment. This dynamic nature requires adaptive risk management strategies that can evolve with the system landscape.
4. Organizational challenges: Different systems may belong to different organizations with varying risk tolerances, security policies, and objectives. Managing risk in such a context requires coordination and communication across organizational boundaries.
5. Information flow: The flow of information between interconnected systems poses risks related to data confidentiality, integrity, and availability. Mismanagement of data flow can expose the entire SoS to cyber threats.

Risk Assessment Process with OASoSIS:

The OASoSIS framework helps in risk assessment by breaking down the process into several stages:

1. System identification: Recognizing the individual systems and their roles within the SoS.
2. Risk identification: Identifying potential threats, vulnerabilities, and impact on the interconnected systems.
3. Risk modeling: Analyzing how risks in one system might propagate to others, taking into account system interdependencies and organizational policies.
4. Mitigation strategies: Proposing solutions that address identified risks, both at the system level and the broader SoS level.

The OASoSIS framework offers a structured approach to assess and manage information security risks in complex SoS environments, emphasizing the need for understanding system interdependencies and the broader organizational context. This framework is particularly valuable in environments where traditional risk management methods may not be sufficient due to the complexity and scale of interconnected systems.

Loft et all. (2022) on a research titled "CAESAR8: An Agile Enterprise Architecture Approach to Managing Information Security Risks", mentioned some key points e.g.:

1. Agile Enterprise Architecture: CAESAR8 integrates agile methodologies into enterprise architecture to provide flexibility and adaptability in managing information security. This agility is crucial for organizations that operate in fast-changing environments, where security risks evolve rapidly.
2. Information Security Risk Management: The framework specifically addresses how to identify, assess, and mitigate risks associated with information security. It emphasizes a structured approach that can

respond quickly to emerging threats while ensuring the alignment of security objectives with business goals.

3. Risk Management Factors:
    - Threat Identification: CAESAR8 facilitates early identification of potential security threats through continuous monitoring and evaluation of IT systems and business processes.
    - Risk Assessment: The methodology includes tools and techniques for assessing the likelihood and impact of various security risks on the organization.
    - Mitigation Strategies: CAESAR8 incorporates dynamic mitigation strategies that allow organizations to quickly adapt their risk controls and safeguards as new vulnerabilities or threats arise.
    - Stakeholder Involvement: One of the core principles of CAESAR8 is the involvement of diverse stakeholders, ensuring that risk management decisions are aligned with both IT and business objectives.
4. Agile Principles in Risk Management: CAESAR8's agile nature allows iterative improvements in security measures, making it possible to implement small, manageable changes in response to evolving security risks rather than relying on large, inflexible frameworks.

Risk Management Aspects:

1. Continuous Risk Monitoring: One of the strengths of CAESAR8 is its emphasis on continuous risk monitoring and feedback loops, ensuring that security measures remain effective over time.
2. Scalability: The framework is scalable, allowing it to be applied to various sizes of organizations, from small businesses to large enterprises, and adjust to the specific risk environments they face.
3. Alignment with Business Objectives: CAESAR8 stresses the importance of aligning security measures with broader business goals, which helps in making risk management decisions that do not hinder business operations but instead enhance the organization's resilience.

CAESAR8 offers a structured, agile approach to managing information security risks that is both flexible and robust, enabling organizations to quickly adapt to changing security landscapes while maintaining alignment with business objectives.

Razikin and Soewito (2022) on a research titled Cybersecurity decision support model to designing information technology security system based on risk analysis and cybersecurity framework, mentioned some important things e.g.:

1. Cybersecurity Framework: The authors utilize established cybersecurity frameworks (like NIST or ISO) as the foundation for developing security systems, ensuring compliance with international standards.
2. Risk Analysis: The model incorporates risk analysis techniques that assess vulnerabilities, threats, and potential impacts. The risk analysis helps prioritize security measures based on the likelihood and severity of potential cyber threats.
3. Decision Support System: The proposed model serves as a decision support system that guides IT managers and security professionals in making informed decisions about where and how to allocate resources for cybersecurity efforts.
4. Scalability and Flexibility: The model can be adapted to various organizational sizes and industries, making it versatile for different cybersecurity contexts.

Risk Management Factors:

1. Risk Identification: Identifying possible threats to the IT infrastructure is the first step, with a focus on potential cyberattacks, data breaches, and system vulnerabilities.
2. Risk Assessment and Evaluation: A thorough assessment of the probability of each risk and the potential consequences it might have on the organization is vital. This includes evaluating both financial and operational impacts.
3. Risk Mitigation Strategies: The model provides guidelines on designing and implementing security controls to reduce the likelihood of risks or to minimize their impact. These strategies involve technical defenses (firewalls, encryption) and organizational policies (employee training, incident response plans).
4. Continuous Monitoring and Improvement: The model encourages continuous monitoring of cybersecurity risks and system performance, allowing organizations to adapt to emerging threats and improve their security posture over time.

In conclusion, the paper by Razikin and Soewito contributes significantly to cybersecurity risk management by proposing a structured decision support model that balances risk analysis with practical implementation of

security frameworks. This helps organizations optimize their cybersecurity strategies while minimizing the risk of cyber threats.

Darwiesh et all. (2024) on a research titled Intelligent risk management system for enhancing performance of stock market applications, mentioned some important things e.g.:

1. Objective: The main objective of the study is to design and implement a smart system that enhances risk management strategies in stock market trading. The system leverages artificial intelligence (AI) and machine learning (ML) to predict market trends and manage risk proactively.
2. Methodology: The authors propose a hybrid approach combining various AI techniques, such as fuzzy logic, neural networks, and genetic algorithms, to create a predictive model that can assess and mitigate risks in real-time trading environments. The system evaluates factors like market volatility, financial indicators, and historical data to make informed predictions.
3. Risk Management Factors: The intelligent system identifies several risk factors critical to the stock market's performance, including:
    - Market Volatility: The system monitors fluctuations in market prices to predict potential risks and opportunities.
    - Liquidity Risk: It considers the ease with which assets can be traded without significantly affecting the stock price.
    - Systemic Risk: It accounts for risks that affect the entire financial system, such as economic downturns or geopolitical events.
    - Operational Risk: The system addresses internal failures, including technical malfunctions and algorithmic errors, that could lead to trading losses.
4. Performance: The proposed risk management system enhances trading strategies by providing real-time, data-driven insights. It aims to reduce exposure to high-risk trades, optimize decision-making processes, and ultimately improve the financial outcomes for stock market participants.
5. Results: Simulations and tests conducted by the authors indicate that the intelligent system significantly improves the prediction accuracy of market trends, reduces the likelihood of substantial losses, and supports more effective risk management strategies.

The integration of AI and ML techniques into risk management systems can transform stock market applications by providing more precise, timely, and reliable risk assessments. This leads to enhanced performance and better protection against unforeseen market disruptions.

3. Results and Discussion

From the above literature study, we could develop a table concerning Risk Management factors or aspects that the authors of journals have concluded. Please see the below table.

Table 1. Risk ManagementFactors

Written by	**Risk Management**
Rodriguez et all. (2017)	a. Risk Identification b. Risk Analysis c. Risk Prioritization d. Decision Support
MacMahon et all. (2018)	a. Patients or Clients safety b. Security risks c. Iterative process for risk management d. Interoperability risks
Ramalingam et. all (2018)	a. The risks analyzed include data breaches, cyber-attacks, compliance violations, and operational disruptions b. Mitigation c. Optimization

Suroso and Fakhrozi (2018)	a. Risk Factors: i. Human related risks ii. Technical Risks iii. Operational Risks iv. Compliance Risks b. Risk Management Process: i. Defining assets critical ii. Identifying threats iii. Prioritizing Risks iv. Mitigation Strategy
Ki-Aries et all. (2022)	Risk Assessment: a. System identification b. Risk identification c. Risk modeling d. Mitigation Strategies
Loft et all. (2022)	a. Risk Management Factors: i. Threat Identification ii. Risk Assessment iii. Mitigation Strategies iv. Stakeholder Involvement b. Risk Management Aspects: i. Continuous Risk Monitoring ii. Scalability iii. Alignment with Business Objectives
Razikin and Soewito (2022)	a. Risk Identification b. Risk Assessment and Evaluation c. Risk Mitigation Strategies d. Continuous Monitoring and Improvement:
Darwiesh et all. (2024)	Risk Management Factors: a. Market Volatility b. Liquidity Risk c. Systemic Risk d. Operational Risk

Based on the above table, we see that common factors of risk management are:
1. Risk Identification
2. Risk Assessment or Risk Analysis
3. Mitigation Strategy

Aside from the above factors, there some other accompanying factors e.g.:
1. Prioritize Risks
2. Optimization Strategy
3. Continuous Monitoring and Improvement

Further, from the above literature study, it is concluded that there are some factors that have influences to information systems risk management:
1. The business of the organizations and their business processes. Risk Management may varies between different businesses. At the above literature study, the cases were on different kinds of business such as on:
    a. Information Technology project
    b. Educational System
    c. Healthcare Information System
    d. Stock Market System
    e. Complex System of system or Multiple interdependent Systems, etc.

2. The methods that are being used in the Risk Management. There were some methods that have been used such as: IEC 80001-1, OCTAVE Allegro, Enterprise Architecture, NIST, etc.
    a. Fuzzy logic
    b. IEC 80001-1
    c. OCTAVE Allegro
    d. NIST

e. Enterprise Architecture

Smart System, based on Artificial Intelligence and Machine Learning

4. Conclusion

From the above literature study, we see there are some risk management factors on Information Systems, as well subjects that have influence on risk management. Further study need to be done to explore more on risk management on other field of business such as on Information Systems at industrial environment, at government affairs, etc

References

Darwiesh, A., El-Baz, A.H., Elhoseny, M., 2024, Intelligent risk management system for enhancing performance of stock market applications, Expert Systems with Applications.

Gibson, D, 2011, Managing Risk in Information Systems, Jones & Bartlett Learning

Hopkin, P., 2017, Fundamentals of Risk Management, 4th edition, KoganPage

Ki-Aries, D., Faily, S., Dogan, H., Williams, C., 2022, Assessing system of systems information security risk with OASoSIS, Computers & Security.

Loft, P., He, Y., Yevseyeva, I., Wagner, I., 2022, CAESAR8: An agile enterprise architecture approach to managing information security risks, Computers & Security.

MacMahon, S.T., Cooper, T., McCaffery, F., 2018, Revising IEC 80001-1: Risk management of health information technology systems, Computer Standards & Interfaces.

Ramalingam, D., Arun, S., Anbazhagan, N., 2018, A Novel Approach for Optimizing Governance, Risk management and compliance for Enterprise Information Security using DEMATEL and FoM, The 5th International Symposium on Emerging Inter-networks, Communication and Mobility (EICM 2018).

Razikin, K., Soewito, B., 2022, Cybersecurity decision support model to designing information technology security system based on risk analysis and cybersecurity framework, Egyptian informatics Journal.

Rodriguez, A, Ortega, F., Concepcion, R., 2017, An intuitionistic method for the selection of a risk management approach to information technology projects, Information Sciences.

Suroso, J.S., Fakhrozi, M.A., 2018, Assessment of Information System Risk Management with Octave Allegro at Education Institution, 3rd International Conference on Computer Science and Computational Intelligence 2018..