Section A-Research paper

Risk Identification and Information System Management Control Techniques (The Implementation in Chemical Companies)

Salsabila[1] , Soraya Pramita[2] , Iskandar Muda[3]
[1,2,3] Universitas Sumater Utara, Medan, Indonesia
[1]Email: mithasoraya1730@gmail.com

Abstract :
The more sophisticated a technology, the more possible vulnerabilities that will arise during the use of that technology. Information systems require good management in order to run optimally. For each possible vulnerability, system managers must know how to prevent, reduce, avoid, or even accept the impacts that arise as a result of these vulnerabilities, so that system management is needed, which is often called risk management. Knowing the possible risks that arise in the implementation of this information system will make it easier for companies to form strategies and increase the success and sustainability of the organization's vision and mission.

Keywords

Information Systems, Information Systems Management, Risk, Risk management, Risk Identification

Introduction

The information system is a tool that is widely used and is growing in the current digital era. With increasingly complicated business activities, information systems are created with the aim of facilitating human work in achieving business goals (Betavia et al., 2022). In addition, with the implementation of information systems, organizations, companies and government agencies including educational institutions can process data and carry out their business processes accurately, effectively and efficiently, which were previously done manually and took a long time now can be done quickly and efficiently. with maximum results.

Conveying information and new ways for people to communicate along with technological developments has turned digital or is called economic digitalization. In producing, processing and disseminating information, initially the community used the face-to-face method as a means of conveying information (Hanum et al., 2021). Along with advances in technology, the mass media and other technological tools have emerged as a substitute for face-to-face methods to make it easier for people to disseminate information. With the existence of mass media and other technological equipment, the process of disseminating information develops and changes from analog format to digital format. The digital era encourages fundamental changes to patterns of communication, interaction and transactions (Mohammad Ikhsan Tualeka, CEO/Founder of IndoEast Network).

One of the negative impacts of misuse of information is cybercrime (Shulha et al., 2022a & 2022b). The existence of the potential for cybercrime is a threat that can create risks, so a Management Control System is needed to assist the Company in achieving the goals set by carrying out process improvements, strengthening the internal control system and increasing the effectiveness of risk management.

Security issues are one important aspect of an information system. It's a shame that this security problem often gets less attention from owners and managers of information systems. Information security is the activity of protecting information from all possible threats in an effort to ensure or guarantee business continuity, minimize business risks and maximize business opportunities (ISO 27001).Management of security can be seen from the side of risk management through control of management information systems in the company. Management information system is a system that provides information to support operational activities, management, and serves as material for decision making of an organization.

Information systems require good management in order to run optimally (Darmawan et al., 2021). Imagine if there were problems with one of the existing information systems resulting in delays in the work process being carried out. The more sophisticated a technology, the more possible vulnerabilities that will arise during the use of that technology. In the case of information systems, examples of vulnerabilities that must always be anticipated by system managers can be hardware, software, misuse by users, natural disasters, network security, and others. For each possible vulnerability, the system manager must know how to prevent, reduce, avoid, or even accept the impacts that arise as a result of these vulnerabilities, so that system management is needed which is often called risk management, which in this case is information system risk management.

Literature Review

a. Information Systems

The information system is a combination of the words system and information. The system (Jogiyanto, 2005, Mustika et al., 2021) is a network of procedures that are interconnected, gathered together to carry out an activity or to complete a certain goal. In addition, Jogiyanto concluded that the system is a collection of elements that interact to achieve a certain goal.

b. Management information System

The system is a set of elements that are interconnected and influence each other in a particular environment. The system is the parts that operate together to achieve some goals. In simple terms it can be said that an information system performs data processing, then converts it into information. According to O'Brien (2010), a management information system is an organized combination of people, hardware, software, communication networks, and data resources that collect, process, and disseminate information within the organization. Management Information System also has a definition, namely a system that provides information to be used in making decisions to solve problems for its users. problem solving consists of responding to things that are going well, as well as to things that are going badly by defining problems as conditions or events that are harmful or can harm the company, or that are beneficial or can provide benefits. In the process of solving problems, leaders in companies can use the management information system in decision making, namely the act of choosing among various alternative solutions to problem solving (Syahputra, et al., 2021). Decisions are defined as actions of choice and it is often necessary to make many decisions in the process of solving a single problem. Management information systems also have advantages, which can help companies improve operational efficiency, introduce innovation in business, and build strategic information sources.

c. Information Gathering Methods

There are several methods of gathering information that can be used to identify risks. There are three methods most often used, namely brainstorming (brainstorming) in this technique experts exchange ideas about the sources of risk that might occur; Risk Breakdown Structure (RBS) by compiling risks based on certain categories (Susilo & Kaho, 2014); SWOT analysis is used to determine possible risks, this stage can also be used in brainstorming sessions.

d. Risk

Risk is the potential harm that will arise if a threat exploits certain weaknesses causing damage to the organization's assets. In his book, Paul Hopkins explains several definitions of risk (Hopkin, 2018). Based on the Oxford English Dictionary risk is defined as the opportunity or possibility of harm, loss, injury or other adverse consequences. The Institute of Risk Management (IRM) defines risk as the combination of the likelihood of an event and its consequences. In ISO Guide 73, risk is defined as a result of unclear objectives. The impact or effect and the consequences that arise may be positive, negative or a deviation from what is expected.

e. Types of Risk

Risk may have positive or negative outcomes, or even provide uncertainty (Hopkin, 2017). Each risk has its own characteristics that require certain analysis or management.

Risks are divided into 3 categories, namely hazard risks, control risks and opportunity risks.

Hazard risks are risks that will only have a negative impact, for example theft. This type of risk will hinder the organization in achieving its mission. Especially risks or hazards that can be insured, including such as fire, storm, flood, accident and others. Control risks are risks that provide uncertainty about the outcome of a situation, usually often associated with project management. Usually organizations have an aversion to control risk. Uncertainty can be associated with the benefits that a project will generate, as well as uncertainty about project completion on time, on budget and within specifications. While opportunity risk is a risk that will be taken by the organization with speculation to get positive results. Many organizations are willing to invest in high-risk business strategies with the expectation of high returns.

f. Risk management

Risk management is, according to (Woody, C., 2006), “an iterative process that addresses the analysis, planning, implementation, control and supervision of security policy and implementation measures.” In fact, (Hubbard, 2009) the risk management process usually contains four steps: (1) risk identification, (2) risk assessment/measurement, (3) choice and implementation of risk mitigation options, (4) monitoring results (Burtonshaw-Gunn, 2009) share the same decomposition and assert that all descriptions follow a similar basic approach to identification, quantification, response and risk control.Although the denominations of the four phases may sometimes differ, this classification was adopted by several other authors.Likewise, (Thevendran & Mawdesley, 2004) outlines the risk management process into four phases: identification, analysis, response planning, and risk monitoring and control.In the same way, (Dikmen, et al. 2008) defines risk management as a procedure consisting of : (1) identification of risk; where sources of uncertainty are defined, (2) the analysis of risk; it is about assessing the consequences of uncertain events, (3) risk response: appropriate strategies based on stated expected results, and 4) analysis of results treatment and the associated risks lead to possible repetition of the first three stages. According to (Merna & Al-Thani, 2005), risk management has an iterative continuous cycle of identification, analysis, control and reporting. However, there are several works that propose a different grouping of risk management process activities. For example, (Smith, 2002) defines three processes for risk management: identification, analysis, and response. this grouping ignores the supervision and monitoring phase, which has the important effect of being an important activity in managing risk.

g. Risk Management Objectives

The purpose of risk management is to identify potential problems before these risks arise so that activities in dealing with these risks can be planned and reduce the impact of losses in the process of achieving organizational goals. Risk management provides a framework for organizations to overcome and to react to ambiguity (Hopkin, 2017). Risk management consists of procedures and stages for identifying, analyzing, evaluating, treating, monitoring and communicating risks (Neeti et al, 2015). Important phases in the risk management process are risk identification, risk analysis, and response to risk (DINU, 2012).

h. International Standardization Organization 27005 : 2018

The ISO 27005 standard, unlike other standards in risk management, makes it possible to build results that evolve with the organization. Any changes small or large can be incorporated into the risk management process. The ISO 27005 standard (ISO, 2011) provides an approach to setting up a risk management system but only in the context of information security. It proposes a methodology that complies with ISO / IEC 27001 and that implements the PDCA (Plan, Do, Check, Act) improvement cycle. The risk management process consists of six phases (Figure 6): (1) Setting the Context: Defining risk management areas, boundaries and environmental processes. During this phase, risk management criteria are established: treatment thresholds for evaluation, thresholds for considering risks in terms of their impact and acceptance thresholds, (2) risk assessment. risk: The first step of this phase is to define the context and elements that compose it such as the organization, information systems, critical elements to protect, entities that depend on them, and any boundaries that may arise. Then, it is necessary to reveal the security needs of the critical elements, to identify and characterize the threat opportunities that burden the information system. Finally, risk is determined by facing threats to security requirements. These risks are analyzed and evaluated to set priorities and schedule them according to the evaluation criteria, (3) Risk treatment: This is the process of selecting and implementing security measures. It starts with identifying the security objectives which are the specifications of the risk treatment process. Then, security requirements are defined to meet the security objectives and to describe how to address the risks. To determine the choice of treatment, the risk and cost of treatment must be adjusted, (4) risk acceptance: This is the accreditation of safety carried out by a designated testamentary authority for a certain period of time. This approval requires checking the security file whose contents must be determined. (5) Risk communication: This is the regular exchange and sharing of information about risks between risk managers, decision makers and all stakeholders. This risk communication helps to: (a) reduce misunderstandings with decision makers, (b) gain new knowledge about safety, (c) involve decision maker responsibilities. The final phase is: (6) risk monitoring and review to ensure that the process remains relevant and adjusted to safety objectives. It is also important to identify changes that require a reassessment of risks and new threats and vulnerabilities.

i. International Standardization Organization 31000

The ISO 31000 standard through its two components of the Framework: "principles" and "organizational framework", verifies the element of criterion 2. Indeed, the first two principles of risk management in this standard: "(1) risk management creates and sustains value" and (2) risk management risk integrated into organizational processes" ensures the first two objectives of this criterion. The organization's risk management framework allows risk management to be organized in such a way as to ensure consistent consistency. IT risk management can only be carried out within the framework of overall organizational risk management and in accordance with the organization's risk appetite. As for criterion 3, the generic aspect of the ISO 31000 risk management process allows it to be applied to all types of systems and especially IS as a work system with all its elements. The tool proposed by ISO 31000 also verifies criterion 4. Indeed, it incorporates the notions defined by (ISO, 2009-b) to standardize the vocabulary around risk. It is also based on the "AS/NZS 4360" standard, which is proven by industry realities (Sienou et al, 2009). However, for specific IS risks, it is important to consider the specificity of risk security processes and methods such as ISO 27005 and EBIOS.

j. NIST Guide (National Institute of Standards and Technology)

The NIST (National Institute of Standards and Technology) guidelines (Stoneburner, Goguen, & Feringa, 2002) provide the basis for developing an effective risk management program, which contains both the definitions and practical guidance needed to assess and mitigate the risks found in technology systems. information. In the NIST guidelines, risk assessment is carried out in 9 stages, namely system characterization, identifying threats, identifying vulnerabilities, conducting control analysis, determining likelihood, impact analysis, risk determination, control recommendations and documenting results.

1. System Characterization The first step in carrying out a risk assessment is to determine the scope of system characteristics. At this stage, the boundaries of the IT system and the resources and information related to the system are determined. By determining the scope of the characteristics of this system, the Risk assessment effort will be clearer and more focused, for example by determining hardware specifications, system authorization, system connectivity, software, and the responsibilities of each part will clarify the Risk assessment. According to NIST guidelines, for IT operational systems, the data collected pertains to IT systems in their production environment, including data on system configuration, connectivity, and documented and undocumented procedures and practices.

2. Threat Identification (Threat Identification) The risk assessment process must consider the threats that are expected to attack system weaknesses. Organizations need to compile a list of all possible threats. Threats can be seen from events, resources, actions taken or not carried out that can trigger losses or harm organizational assets (Haythorn, n.d.). A threat source can be defined as any event or situation with the potential to cause harm to IT systems. Common threats can come from nature, humans, or the environment. In considering the sources of threats, humans are the greatest potential threat due to their motivations and the actions they may take.

3. Identification of Vulnerability (Vulnerability Identification) Analysis of system threats must also include weaknesses in the system. By knowing the weakness of the system, it allows the organization to assess how much the threat will affect or harm the system. Weakness assessment can be more difficult than threat identification, because organizations must understand the specific weaknesses of their assets. It is important for companies to periodically document suspicious events that occur on their systems, so they can find out and have a list of weaknesses that may be attacked by several threat sources. The purpose of this stage is to develop a list of system weaknesses, which can be errors or vulnerabilities in the system that can be exploited by certain

threat sources. Errors or weaknesses in an organization can be considered from several aspects, namely system security procedures, system design, implementation, or internal controls carried out by companies that may accidentally or intentionally exploit causing system security policy violations.

4. Control Analysis (Control Analysis) This stage is carried out to analyze the controls that have been carried out or control plans designed by the organization to minimize or eliminate the possibility of a threat attacking system weaknesses. Control planning is an important aspect for organizations to reduce the possibility of threats that will occur. For example, a weakness in a system or procedure is unlikely to be attacked or the likelihood of an attack occurring is low when security controls are implemented effectively so as to eliminate or reduce the impact of a loss. This control analysis can be done in 3 ways, namely: a. Control Methods Security controls include the use of technical and non-technical methods. Technical controls are protections that are embedded in hardware, software, or firmware, such as access control mechanisms, identification and authentication mechanisms, encryption methods, intrusion detection software). Meanwhile, non-technical controls are operational and management controls such as security policies, control procedures, personnel, and the environment. b. Control Categories Control categories for the two control methods above can be classified into prevention and detection. prevention controls block attempts to violate the security policy, whereas detection controls alert when a security policy violation occurs. c. Analysis of Control Techniques In carrying out the analysis of control techniques, a list of security requirements is needed which is generated from the identification of weaknesses stage so that the organization can carry out control analyzes efficiently and systematically.

5. Determination of Likelihood The stages of determining the likelihood are carried out by analyzing and measuring how often a threat can appear and harm the system. Determining the likelihood can be done with two approaches, namely qualitative and quantitative for each threat. The results of this measurement can be used as a comparison between an incident and other events which will become a consideration for the organization regarding which threats must be immediately taken action against. The level of possible threat occurrence can be categorized into very low, low, moderate, high, and very high. Each level can also be determined based on a scale of 0-100.

6. Impact Analysis The next stage in the Risk assessment is to analyze the impact of the threats that will attack the system's vulnerabilities and their consequences for the company's operations or even organizational goals. At this stage the analysis is carried out by finding out what the mission of the system is, the value and importance of the system and data for the organization, and the sensitivity of the data. This information can be obtained from existing organizational documentation, such as important organizational asset appraisal reports, impact analysis reports, and others. However, if the above documentation is not owned by the organization or an assessment of the organization's assets has not been carried out, then important data and systems can be determined based on the level of security needed to maintain the availability, integrity

and confidentiality of data. This impact analysis will aim to prioritize information assets based on the results of a qualitative and quantitative assessment of these assets. Calculations with a quantitative approach can be made based on lost revenue, system repair costs, or the effort required to fix problems caused by successful threat actions. In addition to the impacts that can be calculated, the organization must also consider the impact of losses that cannot be calculated, such as loss of public trust, loss of credibility, and deterioration of the organization's image. Based on the possible impacts, an analytical assessment at this stage can also be carried out using two approaches, namely qualitative and quantitative based on categories or a Likert scale.

7. Risk Determination Stages of risk determination are carried out to assess the level of IT system risk. In order to measure Risk, a Risk scale and a Risk level matrix must be developed.

8. Control Recommendations Control is a security measure that can be carried out technically or non-technically. Non-technical security measures can take the form of administrative safeguards in the form of policies, regulations or procedures related to information system security. The purpose of carrying out control recommendations is to determine security measures both technically, administratively, preventive actions, or corrective actions against threats that may occur. Technically, security measures for the system can be in the form of preventive measures such as providing training on system security, installing a firewall, anti-virus on the system and/or applying IPS, and so on.

9. Documentation of Results way to do to provide document by using proof accurate record of sources information

Methods

The research design in this study is qualitative, namely data in the form of words, pictures, and not numbers (Danim, 2002). The research approach uses a phenomenological approach, which focuses on real experiences to describe experiences (Patton, 1990).

Result and Discussion

Risk Identification is efforts to find or know the risks that may arise in activities carried out by companies or individuals. Forms of threats for the risk of using information technology systems other than natural factors or natural factors/disasters (power failure, disaster, force majeure), namely threats arising from hackers or third parties who have the ability and skill to hack information technology systems, this hacker process has not up to the stage of damaging the information technology system, if it is damaged then it is called a cracker. There is also the threat of social engineering, the hacker first disturbs the user, such as committing fraud via SMS messages or fake telephone calls, e-mail (spoofing) on behalf of managers or leaders at the company. This attack is carried out by way of click-bait. The potential risk of hackers depends on the system, all information technology systems have the potential to be hacked depending on the benefits and advantages for the hacker. Hacking of financial information is crucial, financial information reflects whether an entity is healthy or not, and describes a transaction from various parties.

Risk Handling, The results of the risk assessment that has been carried out will be taken into consideration in making decisions on the control recommendations that must be carried out. From each risk, a recommendation will be given whether the risk is acceptable or risk mitigation must be carried out so that the impact of the risk can be reduced to an acceptable level. The decision to accept the risk is made based on the controls that have been implemented by the Company, so that the possibility of existing risks does not have a large impact on the organization.

Conclusion

In this paper, we present an overview of risk management (RM) information systems (IS). Some basic concepts and models are introduced to understand IS risk management. Since information systems are socio-technical systems, risk studies are needed to ensure the relevance of this paper. This study focuses on the concept of risk and risk management in general, then specifically on information systems. According to this state of the art, although the literature is quite rich in this field, there is still no consensus on risk management and the concept of IS risk management. This review introduces the most important risk management and risk management processes for information systems. Then, it shows a comparative analysis of these processes. This analysis shows the application of ISO 31000 to risk management of information systems as a socio-technical system, but also the need for integration of several RM process specifications when specific IS areas such as IS security and IS quality. Hence the importance of designing an adaptable IS RM system.

Recommendations for actions against threats that occur are divided into 2 (two) categories, namely accept and mitigate. An acceptable level of risk means that Pusdata has exercised adequate control over the system so that risks or threats that arise do not result in large losses. Meanwhile, a moderate to very high level of risk is recommended for risk mitigation so that the risk can be reduced or reduced to an acceptable level.

Reference

Betavia, A. E., Sanusi, A., (2022). General Ledger and Reporting System Cycle: Traditional Vs Digital Accounting Information System Era (Implementing In Pharmaceutical

Sector and Local Bank). *Journal of Pharmaceutical Negative Results*, 3533-3541. https://www.pnrjournal.com/index.php/home/article/view/5151

Burtonshaw-Gunn, S.A. (2009). Risk And financial Management In Construction‖ Gower, Burlington.

Danim, Sudarwan. (2002). Menjadi Peneliti Kualitatif, Bandung : Pustaka Setia.

Darmawan, R., Gumiwa, G. T., Sjuchro, D. W., & Atmanegara, A. W. (2021). Information Systems Audit Model Privacy and Confidentiality on Start Up the Go Food Business. In *Intelligent and Reliable Engineering Systems* (pp. 167-170). CRC Press. https://www.taylorfrancis.com/chapters/edit/10.1201/9781003208365-27/information-systems-audit-model-privacy-confidentiality-start-go-food-business-rizal-darmawan-gilang-trisna-gumiwa-iskandar-muda-dian-wardiana-sjuchro-agung-wahyudi-atmanegara-erlina

Dikmen, et al. 2008. Learning from risks: A tool for post-project risk assessment. Automation in Construction.

DINU, A.-M. (2012). Modern Methods of Risk Identification in Risk Management. International Journal of Academic Research in Economics and Management Sciences, 1(6), 5.

Hanum, Z., Muda, I., & Bukit, R. (2021). The Impact of Accounting Information System on Organizational Performance through Good University's Private Governance in Indonesia. *Webology*, 18(Special Issue). 1373–1388. https://www.webology.org/data-cms/articles/20211101040613pmWEB18204.pdf

Haythorn, M. (n.d.). Running Head: Information Security Risk Assessment Methods, Frameworks and Guidelines. 18.

Hopkin, P. (2017). Fundamentals of risk management: Understanding, evaluating and implementing effective risk management. Kogan Page Publishers.

Hopkin, P. (2018). Fundamentals of risk management: Understanding, evaluating and implementing effective risk management. Kogan Page Publishers.

Hubbard, D. W. 2009. The failure of risk management: Why it's broken and how to fix it: John Wiley & Sons.

Jogiyanto, H.M., (2005), Analisa dan Desain Sistem Informasi: Pendekatan Terstruktur Teori dan Praktik Aplikasi Bisnis, ANDI, Yogyakarta

Mustika, I (2021). Analysis of Accounting Information Systems in the Cash Flow Expenditure Cycle at UD. *Proceedings of the 1st International Conference on Social, Science, and Technology*, ICSST 2021, 25 November 2021, Tangerang, Indonesia. http://dx.doi.org/10.4108/eai.25-11-2021.2318829 or https://eudl.eu/pdf/10.4108/eai.25-11-2021.2318829

Neeti Mathur, Himanshu Mathur, & Trapti Pandya. (2015). Risk Management in Information System of Organisation: A Conceptual Framework. 2(1), 82– 88.

Neeti Mathur, Himanshu Mathur, & Trapti Pandya. (2015). Risk Management in Information System of Organisation: A Conceptual Framework. 2(1), 82–88.

O'Brien dan Marakas, 2010. Management System Information. McGraw Hill, New York.

Patton, M. Q. (1990). Qualitative evaluation and research methods (2nd ed.). Sage Publications

Shulha O, Yanenkova I, Kuzub M, Muda I, Nazarenko V. (2022). Banking Information Resource Cybersecurity System Modeling. *Journal of Open Innovation: Technology, Market, and Complexity*. 8(2):80. https://doi.org/10.3390/joitmc8020080

Shulha, O., Yanenkova, I., Kuzub, M., & Nazarenko, V. (2022). Modeling Regarding Detection of Cyber Threats Features In Banks Activities. *Journal of Management Information & Decision Sciences*, 25(25). 1-8. Print ISSN: 1524-7252; Online ISSN: 1532-5806).https://www.abacademies.org/articles/modeling-regarding-detection-of-cyber-threats-features-in-banks-activities-13697.html

Sienou, A., et al. 2007. Conceptual Model of Risk: Towards a Risk Modelling Language

Smith, P.G. and Merritt, G.M. (2002). Proactive Risk Management. Controlling Uncertainty in Product Development. Productivity Press, New York.

Stoneburner, G., Goguen, A., & Feringa, A. (2002). Risk management guide for information technology systems: Recommendations of the National Institute of Standards and Technology (No. NIST SP 800-30). https://doi.org/10.6028/NIST.SP.800-30

Susilo, Leo J dan Kaho, Victor R. 2011. Manajemen Risiko Berbasis ISO 31000 untuk Industri Nonperbankan. PP Manajemen : Jakarta

Syahputra, A., Ulina, P. T., Sjuchro, D. W., & Atmanegara, A. W. (2021). The Role of Information Systems Auditing and Control Association (ISACA) as an Institution for Information Systems Auditors, Establishing an Ethical Code for Auditors and Holder of ISACA Certificates. In *Intelligent and Reliable Engineering Systems* (pp. 188-192). CRC Press. https://www.taylorfrancis.com/chapters/edit/10.1201/9781003208365-31/role-information-systems-auditing-control-association-isaca-institution-information-systems-auditors-establishing-ethical-code-auditors-holder-isaca-certificates-audi-syahputra-pindi-try-ulina-iskandar-muda-dian-wardiana-sjuchro-agung-wahyudi-atmanegara-erlina

Thevendran, V., Mawdesley, M,J. 2004. Perception of human risk factors in construction projects: An exploratory study. International Journal of Project Management

Tony Merna, Faisal F. Al-Thani. John Wiley & Sons, 2005. Business & Economics.

Woody, Carol. (2006). Applying OCTAVE: Practitioners Report.