Robust

Research Business and Economics Studies

journal homepage: http://ejournal.iainkendari.ac.id/robust

Analysis Of Risk Management Implementation In The Internal Audit Unit (SPI) Politeknik Pelayaran Surabaya Using Iso 31000

Ita Masita [1]

[1] Faculty of Economics and Business, UPN Veteran Jawa Timur
Email :

ARTICLE INFO	A B S T R A C T
	The application of risk management aims to minimize the probability and or consequences of unfavorable events as well as increase awareness of risk in strategic and operational decision making in an effort to achieve organizational goals. The Internal Audit Unit (SPI) Politeknik Pelayaran Surabaya is a supervisory unit formed to assist the implementation of *Good University Governance* by carrying out inspections or audits of all work units in the non-academic field. Risk treatment is required as the implementation of the management function in risk management. The risk management process uses a standard risk management process 31000 which consists of a context setting process, risk identification, risk analysis, risk evaluation, risk management, monitoring and review, and communication and consultation. This study uses a descriptive qualitative method with a case study at Internal Audit Unit (SPI) Politeknik Pelayaran Surabaya which describes and analyzes risk management using interview and documentation techniques in data collection. Data were analyzed using an interactive model, including data collection, data reduction, data presentation, and conclusions or verification. The final result of the risk management analysis of the internal audit unit (SPI) Politeknik Pelayaran Surabaya is a form of handling strategy in the implementation of internal control.

1. **Introduction**

Developments in the field of education, especially universities, continue to change and develop following changes in the internal and external environment. Changes in the organization to adapt to this have the potential to create opportunities and risks for the organization. Opportunity can be an opportunity for the organization to be better at some level while risk becomes a potential loss and failure .

The importance of implementing risk management in universities, among others, is to maintain the pillars of Good University Governance to be maintained, because risk management is one of the pillars of the GUG in running the government's internal control system in a plenary manner, creating a new pattern of organization that makes risk as an *early warning system* tool in the implementation of organizational operations, the available resources are limited, therefore the risk-focused mitigation process is in dire need of countermeasures.

To ensure the implementation of Good University Governance, internal control has an important role for the sustainability of an entity. Therefore, the Internal Audit Unit (SPI) at universities is expected to be able to realize Good University Governance (GUG), which is in accordance with the mandate of Goverment Regulation No. 4 of 2014 that SPI has a non-academic supervisory function at higher education institutions. Furthermore, it was reaffirmed by Minister of Finance Regulation No. 200 of 2017 that SPI must create and maintain a control environment in order to be able to achieve the effectiveness and efficiency of BLU activities.

The Internal Audit Unit (SPI) Politeknik Pelayaran Surabaya carries out an inspection or audit process and evaluates the follow-up to the audit results aimed at assisting the implementation of supervision of the implementation of work unit tasks in non-academic fields within the Politeknik Pelayaran Surabaya Audit findings that are well presented in the internal audit report will inform management about weaknesses in internal control which if left unchecked can lead to fraud that is detrimental to the organization. These weaknesses can pose threats and risks that can cause losses so that risk management is one of the important elements in carrying out internal controls that have work complexity and all activities that can increase the level of risk faced by internal audit unit SPI Politeknik Pelayaran Surabaya.

The ISO 31000 method as a risk assessment method uses the term risk management which refers to the architecture to manage risk effectively ensuring complete and adequate risk information that is used as a basis for decision making. Therefore, the implementation of risk management is required SPI Pelayaran Surabaya to analyze the risks that exist I by using or referring to the ISO 31000 method.

2. **Literature Review**

2.1 Internal Audit Unit (SPI)

Internal Audit Unit (SPI) an auditor internally in a universities the duty and function to constantly evaluate the results of the performance of financial institutions is high, keep an eye on every policy management and reporting the results of the evaluation and supervision are the leaders. It the corresponding listedin Goverment Regulation No. 23 of 2005 chapter 35 paragraph 1 which states that the examination ofinternal Agency Services General or college high undertaken by the Internal Audit Unit which is a unit of work that is located directly under the leadership of General Services Agency.

According to Minister of Finance Regulation No. 200/PMK.05/2017 concerning the Internal Control System of Public Service Agencies chapter 1 BLU Internal Control Unit , here in after abbreviated as SPI, is a BLU work unit that carries out the Internal Control function . Supervision Internal is an activity giving assurance and consulting that bersift independently and objectively, withthe goal to increase value and improve operational BLU, through approaches that systematically, by evaluating and improving the   effectiveness of the management of risk, control, and process governance BLU. Meanwhile, according to Minister of Transportation'decision No. KM 144 2019 Unit Inspection Intern at Agency Services

General are hereinafter referred to as SPI BLU, a unit of work BLU who run the audit function internally that is formed by Leadership BLU

2.2 Risk and Risk Management

The definition of risk according to Hanafi (2006:1), risk is a hazard, consequence or consequence that can occur as a result of an ongoing process or future event. Meanwhile, according to The Institute of Risk Management (IRM) and The Association of Insurance and Risk Managers (AIRMIC) (2002), risk is the opportunity for something to happen, having an impact on goals. According to Griffiths (2005), risk is the threat that an adverse action or event will affect the organization's ability to achieve goals and implement successful strategies. Meanwhile, according to the Australian New Zealand International Standard (AS/NZS ISO 31000:2009) and Technical Guidelines for the Implementation of Control Systems Internal Government (SPIP) (2009), risk is the possibility of events that threaten the achievement of the goals and objectives of government agencies. Based on these definitions, it can be concluded that risk is a risk that can be defined as a state of uncertainty, where if an undesirable situation occurs, it can cause a loss that hinders the achievement of organizational goals.

IFC (2012) in R. Hidayah et al (2018:13) classifies risks into four, namely financial risk, operational risk, strategic risk, and hazard risk.
1. Financial risk, risk related to the entity's financial condition such as:
    a. credit (default, downgrade)
    b. price (commodity, interest rate, exchange rate)
    c. liquidity (cash flow)
2. Operational risk, namely all kinds of risks related to the entity's business operational processes, such as:
    a. Business operations (efficiency, supply chain, business cycles)
    b. information Technology
3. Strategic risk, is a risk related to the strategic entity such as:
    a. Reputational (ie, bad publicity)
    b. Demographic and social/cultural trends
    c. government policies and regulations
4. Hazard risk, is all kinds of risks that arise as a result of disasters or hazards such as:
    a. fire, property damage
    b. theft, crime
    c. disease epidemic

Risk is usually expressed in terms of: the source of the risk, the events that can occur, the impact/consequences of the event, and the likelihood of the event occurring. Susilo and Kaho (2018) describe the definition of each of these expressions;
a. A risk source is an element/element which alone or together with other elements has the potential to cause risk.
b. An event is an event or change in a certain condition that can be a source of risk.
c. Consequence is a result of an event that affects the target.
d. Likelihood is the chance of something happening.

The definition of strategic risk management according to Meilania (2014) includes all activities intended to identify risks, solve problems, adapt to changes, and successfully implement the plans that have been set. Meanwhile, according to Rilyani et al (2015) risk management aims to manage these risks so that we can obtain optimal results. Furthermore, YPIA (2015) states that risk management is the management of uncertainty which in summary can be said that risk assessment aims to provide assistance for organizations to manage the risks they may face. Then according to Minister of Finance Regulation Number 171/PMK.01/2016 concerning risk management within the Ministry of Finance, it explains that risk management is a systematic approach that includes culture, processes, and structures to determine the best actions related to risk. From these several

definitions, it can be concluded that risk management is an organizational activity that is directed and coordinated with risk management.

The purpose of risk management is to create and protect value. The purpose of risk management is to improve performance, encourage innovation and support the achievement of goals. Thus, risk management can improve the organization's capability to take advantage of existing and future opportunities to provide added value to the organization. In addition, risk management can anticipate risks that have a negative impact that can jeopardize the achievement of organizational goals to protect organizational values.(ISO 31000:2018)

2.3 Risk Management ISO 31000 Risk Management

ISO (International Organization for Standardization) is a non-governmental organization consisting of National Standardization Body from each country. ISO was founded in 1947 which is a combination of ISA (International Federation of the National Standadizing Associations) which was founded in New York in 1926 with UNSCC (United Nations Standards 34 Coordinating Committee), which was founded in London in 1944. ISO 31000:2009 Risk Management-Principles and Guidlines is one of the international standards in the field of management systems. After ISO 31000:2009 was published, many countries adopted it as their national risk management standard, including Indonesia which adopted SNI ISO 31000:2011 Risk Management – Principles and Guidelines in 2011. Then in 2018, the first revision of the ISO 31000 standard was carried out. since its publication in 2009 (Susilo and Kaho, 2018).

According to ISO 31000, risk management is a coordinated activity to direct and control an organization in dealing with risk. The purpose of risk management implementation is value creation and value protection which is achieved by managing risk in decision making, process setting and target achievement activities as well as performance improvement. ISO 31000 aims to provide principles, frameworks and processes for performing risk management. Although ISO 31000 provides general guidance, this standard does not aim to uniform risk management across organizations, but aims to provide supporting standards for the application of risk management in an effort to guarantee the achievement of organizational goals. This international standard can be used by any organization, regardless of size, activity or field of organization (Yap, 2017).

The advantages of ISO 31000 compared to other frameworks according to Susilo and Kaho (2010) are the ease of implementing it, the scope of application is more general. Meanwhile, according to Susanto (Pusdiklatwas BPK) ISO 31000 has keuanggulan essential in providing more detailed guidance and comprehensive and can be used in either organization with profi t and non-profit oriented.

In 2018, the international standards organization ISO published ISO 31000:2018 Risk Management Guidelines . This standard replaces ISO 31000:2009 Risk Management Principles and Guidelines published in November 2009. This revision is part of a systematic review process that applies to all ISO standards. ISOs. The implementation of risk management ISO 31000 consists of three elements: principles, frameworks, and processes. Risk management principles are the basis of risk management practice or philosophy. The framework is a structured and systematic arrangement of risk management systems throughout the organization. Processes are sequential and interrelated risk management activities.

According to ISO 31000:2018 the process of implementing risk management consists of several stages, including:
1. Communication and Consultation
2. Establish Scope, Context, and Criteria
3 . Risk Assessment
4. Risk Treatment
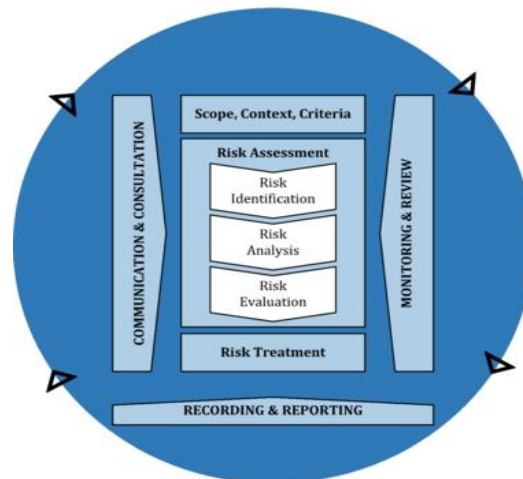5. Monitoring and Review
6. Recording and Reporting

Figure 1. ISO 31000:2018 Risk Management Process

1. Communication and Consultation

The purpose of communication and consultation is to assist relevant stakeholders in understanding the risks, the basis for decision making and the reasons why certain actions are needed. Communication seeks to increase awareness and understanding of risks, whereas consultation involves obtaining feedback and information to support decision making . (IEC 310100)

2. Establish Scope, Context, and Criteria (scope, context, and Criteria)

According to Susilo and Kaho (2018) the purpose of establishing the scope, context, and criteria is to design a unique risk management process according to the need to support effective risk assessment and appropriate risk treatment. Scope, context, and criteria include determining the scope, process, and understanding of the organization's internal and external context as well as criteria for assessing the level of risk.

3. Risk Assessment

Risk assessment refers to how various risks, both internal and external, will be identified, assessed and managed to ensure that unexpected events will harm the company's activities (Komalasari et al, 2018). According to BPKP Regulation No. 6 of 2018 risk assessment includes:

1) Risk identification

Identifying events that may occur and can interfere with the effectiveness of achieving organizational goals and objectives.

2) Risk analysis

Determine the magnitude of the likelihood and impact of risk based on the criteria that have been formulated in the context setting stage. Then calculate the risk value based on the product of the two so that it can calculate the level of risk.

3) Risk evaluation

Evaluating the previously calculated risk level, to determine how the risk management will be applied.

4. Risk Treatment

There are several options in risk treatment (Susilo and Kaho, 2018), including:

a. Risk avoidance, means not carrying out or continuing the activities that give rise to the risk.

b. Risk sharing / transfer, which is a measure to reduce the possibility of risk or the risk impact.

c. Risk mitigation, namely carrying out risk treatment to reduce the possibility of risk arising, or reducing the impact of risk if it occurs, or both, likelihood and impact. This treatment is actually part of the daily activities of the organization.

d. Risk acceptance, which means not treating or dealing with the risk .

5. Monitoring and Review

The purpose of monitoring and review is to ensure and improve the quality and effectiveness of process design, implementation and results. Ongoing monitoring and periodic review of the risk management process and its results should be a planned part of the risk management process, with clearly defined responsibilities. Monitoring and review should be carried out at all stages of the process. Monitoring and review includes planning, information gathering and analysis, recording of results, and providing feedback. Results of monitoring and review should be incorporated into all management activities, measurement, and reporting of the organization's performance. (IEC 31010)

6. Recording and Reporting

The risk management process and its results must be documented and reported through appropriate mechanisms. Recording and reporting aims to
a. communicating risk management activities and results across the organization;
b. provide information for decision making;
c. improve risk management activities
d. assisting interaction with stakeholders, including those with responsibility and accountability for risk management activities (IEC 31010)

2.4 Application of 31000 Risk Management in Government Agencies

In Indonesia, risk management was first implemented in 2008 at the Ministry of Finance in response to the mandate of Government Regulation No. 60 of 2008 concerning the Government's Internal Control System (SPIP), which stipulates that risk management must be implemented in all government agencies. Risk management according to Goverment Regulation No 60/2008 and its development takes the essence of three risk management frameworks from three major schools of international risk management standards, namely AS/NZS 4360:2004, COSO ERM-2004 and ISO 31000:2018 .(Yuli Ari, 2020:13)

BPKP encourages all government agencies to implement SPIP and risk management, one of which is the Ministry of Finance. The Ministry of Finance is one example of a government agency that has implemented SPIP, especially risk management in a structured and systematic way because it has used a risk management process framework that refers to ISO 31000: 2009 (Mukhlis & Supriydsi, 2018). The Ministry of Finance issues Minister of Finance Regulation Number 171/PMK.01/2016 concerning Risk Management in the Ministry of Finance. The Risk Management process consists of stages of communication and consultation, setting context, risk assessment which includes risk identification, risk analysis, and risk evaluation, risk management and monitoring and review.

Then it was also marked by the issuance of risk management ISO 31000 in 2009 which was adopted identically by BSN under the name SNI ISO 31000:2011 which is proof that the application of risk management in Indonesia has begun to be applied in several organizations as explained from the results of the CRMS Indonesia survey (Ahmad and Rosmiati, 2019). Meanwhile, in implementing risk management in Indonesia according to the National Committee on Governance Policy (KNKG), government agencies can refer to the guidelines issued by the KNKG in 2012 namely the Governance -based risk guidelines which mostly refer to ISO 31000:2018 Risk Management .

2.5 Relationship between ISO 31000 Risk Management and Government Internal Control System (SPIP) Goverment Regulation No. 60 Year 2008

Substantially, the implementation of SPIP as a whole, the implementation of the 5 elements is a form of the framework and process of implementing risk management as described in SNI ISO 31000. The framework and structure developed in the SPIP as stipulated in Goverment Regulation No. 60 of 2008, in line with SNI ISO 31000. The relationship between MR based on SNI ISO 31000 and SPIP based on PP 60 Year 2008 can be seen in the following diagram:
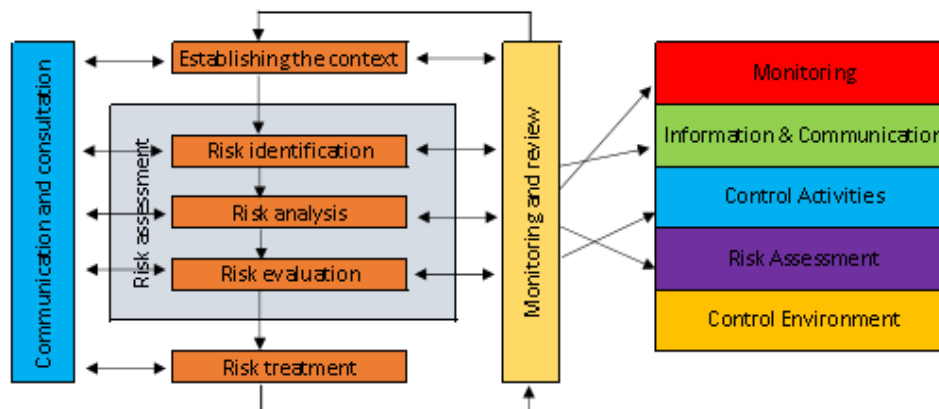
Figure 2. Relationship between ISO and SPIP
Source: BPKP Regulation No. 6 Year 2018

From the figure, it appears that the risk management process as referred to in ISO 31000 has been reflected in the elements of the implementation of SPIP. In addition, the risk management principles in ISO, one of which is to consider human and cultural factors, also reflects elements of the control environment in the implementation of SPIP.

2.6 Previous Research

Nadya Wiandhini (2019) conducted research on Risk Management Analysis at the University of Lampung Internal Control Unit (SPI) using the ISO 31000 Method . The study was conducted to determine how to identify, analyze, evaluate and treat risks in the SPI risk management analysis at the University of Lampung using the ISO 31000 method using a qualitative descriptive method. The results of this study indicate that risk management analysis using ISO 31000 can assist the decision-making process in improving audit management based on the results of the assessment carried out. The similarity between Nadya Wiandhini's research and this study is to use the same independent variable, namely the analysis of the application of risk management using ISO 31000, while the difference in previous studies in this study is in the risk management process and the object of research is the Internal Audit Unit (SPI) Politeknik Pelayaran Surabaya.

3.   Research Method

This study uses a qualitative method with a descriptive analytical approach to the Analysis of Application of Risk Management at the Internal Audit Unit (SPI) Politeknik Pelayaran Surabaa Using ISO 31000. Qualitative descriptive research can be interpreted as a problem-solving procedure that is studied by describing the subject and object based on the facts that occur in the field.

The location of the research was carried out at Politeknik Pelayaran Surabaya which is located at Jalan Gunung Anyar Boulevard No.1 Surabaya. The object of research in this study includes risk management that can be used to anticipate environmental changes, develop Good University Governance, optimize the preparation of strategic management in an effort to achieve organizational goals.

Meanwhile, the subject of this research is the Internal Audit Unit (SPI) Politeknik Pelayaran Surabaya for the period 2020. The type of data used in this study is qualitative data obtained from interviews and observations, while the data sources obtained consist of primary and secondary data. The primary data sources are the results of interview questions, while the

secondary data sources are books, journals, articles and risk management application standards using the ISO 31000 method.

4. Result

Implementation of ISO 31000 Risk Management at Internal Audit Unit (SPI)Politeknik Pelayaran Surabaya.

1. Communication and Consulting

    The implementation of communication and consultation is carried out at the initial stage of risk preparation which is carried out at the beginning of the year under the coordination of the Quality Assurance Unit by conducting risk management forums or socialization, periodic and incidental meetings as well as with Focus Group Discussions to units within Internal Audit Unit (SPI) Politeknik Pelayaran Surabaya is one of the units that also conducts communication and consultation related to risk management.

2. Context Determination

    Context determination is the stage of determining internal and external parameters, scope of work, and risk criteria. Setting the context is the basis for the subsequent risk management process. Obtaining a comprehensive picture of the basic parameters, scope, and framework, aiming to identify the environment for risk management implementation, identify and define the most interested parties (key stakeholders), define the scope, objectives, limiting conditions, and expected results and establish criteria for analyzing and evaluating risks
Overview of the Work Unit Scope in the internal external context

    Politeknik Pelayaran Surabaya is a university within the Ministry of Transportation, which is under and responsible to the Head of the Transportation Human Resources Development Agency which has the task of providing vocational education in the shipping sector . The purpose of the Surabaya Shipping Polytechnic is to produce graduates who have competence and knowledge in the field of shipping who are professional, excellent and ethical and able to follow the development of science and technology and have leadership and dedication to the Nation and State.
Internal Audit Unit (SPI) Politeknik Pelayaran Surabaya

    The Internal Audit Unit is an element of the examiner who carries out his duties in accordance with the provisions of the applicable laws and in carrying out his duties under and responsible to the Director of Politeknik Pelayaran Surabaya
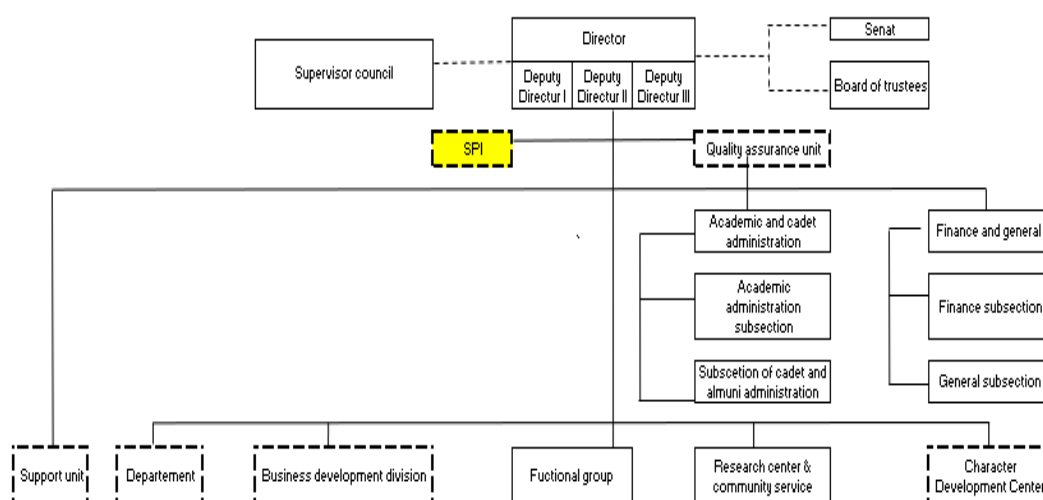

Figure 3 Organizational Structure of Politeknik Pelayaran Surabaya
Source: Politeknik Pelayaran Surabaya Strategic Plan 2020-2024

3. Risk Assessment

a. Risk Identification

The risk identification stage is the stage to identify all the entity's activities, both current and new ones. Risk identification is carried out with the aim of identifying risk factors that can hinder the achievement of the entity's objectives, cause losses, and even damage the reputation of the entity. This stage establishes what, where, when, why, and how something can happen, so that it can have a negative impact on goal achievement (4w + h). Thorough identification of risks that exist within the entity will produce a risk register .

Table 1. Risk Register

No	Risk Statement	In charge	Cause	Impact on Goal Achievement
1	2	3	4	5
1	Difficult to get data as audit material from the parts to be audited	Head of SPI	Auditee has busyness, data is not ready and auditee concern for the importance of operational audit is still lacking.	Implementation of operational audits not on schedule
2	The preparation of reports of operational audit results is less systematic	Head of SPI	Do not understand the rules on the preparation of audit results report	Reports of operational audit results are considered less credible
3	There is a misunderstanding between the auditor and the auditee in understanding the audit findings.	Head of SPI	There is a gap in understanding between auditors and auditees.	There is a conflict between the auditor and the auditee.
4	Operational Audit Results Report has not been followed up by auditee	Head of SPI	Auditee considers only internal audit findings	No improvements or improvements to the performance of Surabaya police
5	Auditors have conservative thinking in understanding auditee problems	Head of SPI	Limited auditor knowledge of auditee provisions	The scope of the audit becomes less broad and comprehensive.

The risk table above explains that the Internal Audit Unit (SPI) Politeknik Pelayaran Surabaya has 5 (five) risks in operational/performance audit activities that have the potential to become obstacles and will have an impact on achieving strategic goals and organizational goals.

b. Risk analysis

At the risk analysis stage, an analysis process is carried out to determine the magnitude of the likelihood and impact of the risk based on the criteria that have been formulated in the context setting stage. Then calculate the risk value based on the result of the multiplication between the two so that it can calculate the level of risk. Risk analysis aims to determine the profile and map of the risks that exist in the organization and will be used in the evaluation process and risk management strategies.

Table 2. Risk Analysis

No	Risk Statement	Opinions of group members on the Scale of Possibility								Average	Impact	Opinions of group members on impact scale								Average
		R1	R2	R3	R4	R5	R6	R7	R8			R1	R2	R3	R4	R5	R6	R7	R8	
1	Difficult to get data as audit material from the parts to be audited	3	3	3	3					3.00	Implementation of operational audits not on schedule	3	3	4	3					3.25
2	The preparation of reports of operational audit results is less systematic	1	1	1	1					1.00	Reports of operational audit results are considered less credible	3	3	3	3					3.00
3	There is a misunderstanding between the auditor and the auditee in understanding the audit findings.	2	2	2	2					2.00	There is a conflict between the auditor and the auditee.	3	3	2	2					2.50
4	Operational Audit Results Report has not been followed up by auditee	2	3	3	2					2.50	No improvements or improvements to the performance of Surabaya police	3	3	3	3					3.00
5	Auditors have conservative thinking in understanding auditee problems	1	2	1	1					1.25	The scope of the audit becomes less broad and comprehensive.	2	2	2	2					2.00

Based on the results of the risk analysis Internal Audit Unit (SPI) Politeknik Pelayaran Surabaya when viewed from the level of possibility and at the level of impact, there are 2 (two) main risks, including:
1. The risk of difficult to obtain data as audit material from the auditee
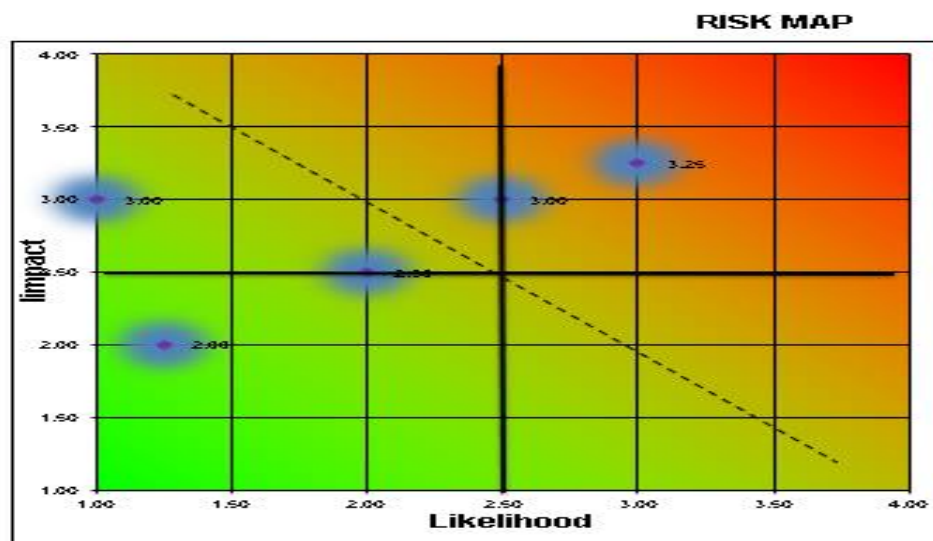2. Audit result report that has not been followed up by the audite

Figure 4. Risk Map

In the risk map above, there is a risk status map, which consists of 4 (four) levels, namely:
1. Level I is a very low risk status in the 5th (five) risk statement which hasa score of 2.00 on impact and a score of 1.25 on the impossibility of occurring.
2. Level II is a low risk status. there is a risk statement no. 2 (two) which has a score of 3.00 on impact and a score of 1.0 on the impereribility of occurring
3. Level III is a moderate risk statusin risk statement no. 3 (three) which has a score of 2.50 on impact and a score of 2.0 on the impereribility of occurring.
4. Level IV is the high risk status in risk statement no. 4 which has a score of 3.00 on impact and a score of 2.50 on the impereribility of occurring.
5. Level V is a very high risk status in the no. 1 risk statement which has a score of 3.25 on impact and a score of 3.00 on the impossibility ofoccurring.

c. Risk evaluation

Tabel 3. Risk Evaluation

No	Risk Statement	Impact on Goal Achievement	Likelihood Score	Impact Score	Total Score (4x5)	Rangking	Risk Level
1	2	3	4	5	6	7	8
1	Difficult to get data as audit material from the parts to be audited	Implementation of operational audits not on schedule	3.00	3.25	9.75	1	Very High
2	The preparation of reports of operational audit results is less systematic	Reports of operational audit results are considered less credible	1.00	3.00	3.00	4	Low
3	There is a misunderstanding between the auditor and the auditee in understanding the audit findings.	There is a conflict between the auditor and the auditee	2.00	2.50	5.00	3	Medium
4	Operational Audit Results Report has not been followed up by auditee	The scope of the audit becomes less broad and comprehensive.	2.50	3.00	7.50	2	High
5	Auditors have conservative thinking in understanding auditee problems	No improvements or improvements to the performance of Surabaya police	1.25	2.00	2.50	5	Very Low

Based on the results of the risk analysis, a risk evaluation was carried out at the Internal Audit Unit (SPI) Politeknik Pelayaran Surabaya which aims to determine which risks have the highest priority level to the lowest and determine which risks are followed up with treatment and which risks only need to be monitored. At this stage, each level of risk is assessed in order of risk priority, which will be the basis for risk management.

4. Risk Treatment

This stage is the stage of the risk management process aimed at determining the type of effective and efficient treatment for a risk

Table 4. Risk Treatment

No	Risk Statement	Risk Level	Risk Treatment	Control
1	2	3	4	5
1	Difficult to get data as audit material from the parts to be audited	Very High	Urgent action is needed to manage risk.	Further coordination to audits on audit data and internal socialization of legal foundations, guidelines by delivering ST and service notes and announcements at the time of apple morning
2	The preparation of reports of operational audit results is less systematic	Low	Action is taken if needed	Make the latest regulatory updates in accordance with standards in the preparation of audit results reports
3	There is a misunderstanding between the auditor and the auditee in understanding the audit findings.	Medium	Action is taken if resources are available	Conduct effective communication in carrying out audits
4	Operational Audit Results Report has not been followed up by auditee	High	Action is needed to manage risk.	Soasiization of draft audit guidelines especially about the deadline for completion of follow-up
5	Auditors have conservative thinking in understanding auditee problems	Very Low	No need for action	Transform understanding towards professional sketism with the development of auditor competence

From the results of risk management carried out based on the level of risk, risk management is carried out by identifying the various available options and deciding the best option. , 4) avoid Risk, 5) accept Risk

5. Monitoring and Review

Monitoring and review aims to anticipate sudden and persistent changes in risk, both in the level of risk and in the direction of risk, which have a negative impact on the risk profile. The monitoring and review process is carried out by monitoring the effectiveness of risk management plans, strategies, and risk management systems. Ongoing monitoring and periodic review of the risk management process and its results should be a planned part of the risk management process, with clearly defined responsibilities.

Table 5 Monitoring and Review

No	Key Risk Description	Monitoring carried out	Monitoring Results	Risks		Conclusion	Monitoring Improvements	Monitoring Time
				Likelihood	Impact			
1	2	3	4	5	6	7	8	9
1	Difficult to get data as audit material from the parts to be audited	Check list of completeness of auditee data	There are still some that need time.	3.00	3.25	Not yet effective	Communicating a lack of data at the time of the morning apple	Every month
2	The preparation of reports of operational audit results is less systematic	Ensure that the audit results report has been received and informed to the auditee	There are still auditors whose thinking is limited.	1.25	2.00	Not yet effective	Create an FGD schedule that is done every 1 time in 1 month, by completing it with a list of present and resume FGD results	Quarter
3	There is a misunderstanding between the auditor and the auditee in understanding the	Ensuring the completeness of the section representatives present in	There is no misunderstanding regarding the findings.	2.00	2.50	Effective	Add internal socialization activities to the SPI watch program list	Every semester
4	Operational Audit Results Report has not been followed up by auditee	Ensuring the readiness of draft operational audit guidelines	Audit findings have been more followed up	2.50	3.00	Effective	Ensuring management's willingness to discuss and certify operational audit implementation guidelines	Semester 1 2020
5	Auditors have conservative thinking in understanding auditee problems	Implementing FGD against new laws and regulations	The preparation of the report has been more systematic.	1.00	3.00	Efektive	Drafting and ensuring the time and budget of the implementation of socialization audit guidelines have been approved by management	Semester 1 2020

From the results of monitoring and evaluation, there are risks that have not been effective when ongoing monitoring is carried out, namely at risks no. 1 and 2. It is necessary to carry out continuous improvement monitoring to ensure that corrective actions have been effectively implemented.

6. Recording and Reporting

Report on the risk management process in the form of findings and suggestions from the results of research that has been carried out as a recommendation material for action by Internal Audit Unit (SPI) Politeknik Pelyaran Surabaya against the risks that occur. Preparation of report documentation in accordance with the format of reporting the results of the risk management analysis

5. Conclusion

Based on the analysis and discussion that has been described, it can be concluded that the implementation of risk management in the Internal Audit Unit using or referring to ISO 31000 has not been implemented thoroughly in accordance with the ISO 31000 standard ISO 31000, this is because Politeknik Pelayaran Surabaya in managing risk is still guided by the ISO standard. 90001 Quality Management that uses the principle of Risk Based Thinking (RBT) in achieving customer compliance and satisfaction, although it includes risk management but it is not in accordance with risk management standards so that it has not been able to meet the needs of stakeholders broadly, including evaluating the effectiveness of an organization in risk management . This can be seen from the implementation of the components of the risk management process at Internal Audit Unit (SPI) Politeknik Pelayaran Surabaya as follows:

a. The risk management communication and consultation process has not been implemented optimally
b. The context determination process has not been carried out thoroughly so that the criteria for risk management, risk appetite and risk tolerance have not been regulated
c. The results of risk identification have not yet identified all risks because there are only 5 (five) risks in operational/performance audit activities that have the potential to become obstacles and will have an impact on achieving strategic goals and organizational goals, it is known that 4 (four) of them come from internal risk sources.
d. The Risk Evaluation process has not been carried out optimally because there is no comparison between the results of the analysis and the
e. The risk management maturity level, which indicates the organization's maturity level in carrying out the risk management process, is still at the Risk Aware level , which is a condition that indicates that it already has an adequate control system but not all of it can be linked to risks that affect the organization's activities so that monitoring is unlikely to be carried out. appropriate for the relationship of risk to the existing control system in the organization

Suggestion

Based on the conclusions above, the authors provide suggestions that are expected to be useful in that the implementation of risk management at Internal Audit Unit (SPI) Politeknik Pelayaran Surabaya is to implement risk management in its entirety according to the risk management standard, namely ISO 31000 because ISO risk management if implemented, the purpose of risk management by value creation and protection, improving performance, encouraging innovation and supporting the achievement of organizational goals can be achieved. This can also be done by integrating the principles of Risk Based Thinking (RBT) in the ISO 91000 Quality Management System into the 31000 Risk Management System.

References

Ahmad and Rosmiati.2019. Risk Management Analysis in Realizing Good Governance in West Bandung Regency Government. Police. 10 th Industrial Research Workshop and National Seminar

BPKP Regulation Number 6 of 2018 concerning Guidelines for Risk-Based Internal Control.

Griffiths, Phil. (2005). Risk Based Auditing. Burlington, Gower Publishing Company

Government Regulation of the Republic of Indonesia. Number 60 of 2008. About. Government Internal Control System.

Government Regulation of the Republic of Indonesia.No. 23 of 2005. Concerning the Financial Management

Hanafi, M. 2006. Risk Management, Yogyakarta: Unit. Publisher and Printing College of Management. YKPN.

ISO 31000. 2009. Risk Management - Principles and Guidelines. ISO 31000. 2018. Risk management – Guidelines.

ISO 31000. 2018. Risk management – Guidelines

Meilania, T. 2014. Implementation of ISO 31000 in Risk Management in Rural Banks (Case Study of Rural Banks X). Journal of Business Administration, Vol. 10, No. 1, ISSN: 0216–1249.

Mukhlis and Supriyadi. 2018. Design of a Risk Management System at a Legal Entity State University (PTN BH) Case Study at Gadjah Mada University. Journal of Applied Accounting and Taxation, Vol. 3, No. 2, e-ISSN: 2548-9925.

Minister of Finance Regulation of the Republic of Indonesia Number 171/PMK.01/2016 concerning the Implementation of Risk Management in the Ministry of Finance.

Minister of Finance Regulation of the Republic Indonesia Number. 200/PMK.05/2017 concerning. Internal Control System in Public Service Agency.

Minister of Transportation Decree of the Republic of Indonesia Number KM 144 of 2019 concerning Internal Audit Units at Public Service Bodies.

Nadya Wiandhini (2019) Analysis of Risk Management at the University of Lampung Internal Control Unit (SPI) Using the ISO 31000 Method. University of Lampung Bandar Lampung

Rilyani, AN Firdaus, Y. and Jatmiko, DD 2015. Information Technology Risk Analysis Based on Risk Management Using ISO 31000 (Case Study: i-Gracias Telkom University). Journal of e-Proceeding of Engineering, Vol. 2 No.2, ISSN: 2355-9365.

Susilo, LJ and Kaho, VR 2010. ISO 31000-Based Risk Management for the Non-Banking Industry. Jakarta: PPM Publisher.

Susilo, LJ and Kaho, VR 2018. ISO 31000:2018-Based Risk Management – A Guide for Risk Leaders and Risk Practitioners. Jakarta: Publisher PT Grasindo.

The Institute of Risk Management (IRM) and The Association of Insurance and Risk Managers (AIRMIC). (2002). Risk Management Standards.

Yuli Ari. 2020. Implementation Of Risk Management In The Public Sector. Paris Review Edition 2020/no. 12ISSN 2088-2890