Implementation of ISO 31000 for Information Technology Risk Management in the Government Environment

Ucu Nugraha[a], **Rozahi Istambul**[b], [a,b]Engineering Faculty, Widyatama University, Indonesia, Email: ucu.nugraha@widyatama.ac.id

Information technology in government and private agencies is used to support the quality of services. Information technology is an important component in carrying out government affairs which include information security and information security services. However, the use of information technology is not always in line with expectations. The emergence of various possible threats and risks that hinder and disrupt the business processes are undeniable and operating across several fields. These threats and risks need to be overcome by implementing risk management strategies that are expected to reduce the threats and risks that occur. To determine the extent to which potential threats and risks are related to information technology and how to handle them, an analysis of risk management using ISO 31000 is needed. The process of risk management analysis is, setting context, risk identification, risk analysis, risk evaluation and risk mitigation. The expected results are in the form of risk values, based on identification and analysis of risks. The final results of this activity are in the form of recommendations to reduce and prevent risks that occur.

Key words: *Technology Information, Risk Management, ISO 31000.*

Introduction

Some units of government have a role in carrying out strategic plans for government information security and digital resource security management systems. The existence of these units is of importance due to the rapid use of information technology (computers, the internet, smart phones, etc.) which have several social phenomena that serve as clues or indicators of a serious social problem. These phenomena include misusing files for ransomware, circulation of coding products such as secure VPN, selling software for password analysis online, and leaking government classified data into the internet.

In carrying out its duties and functions, the field of Coding and Information Security has never been separated from the use of information technology where there are various possibilities of threats and risks that arise and can disrupt or even paralyze activities in the system, so that the system cannot run optimally. Possible threats from these risks can come from various factors that can be caused by the nature of business, structure and culture. Based on these factors, it can lead to impacts on finances, declining in reputation, cessation of business operations, failure of assets that can be assessed, and delays in the decision-making process.

Therefore, it is necessary to carry out a risk management analysis to determine the extent of the potential threats from the risks that occur and how to handle them so that units within the government can carry out risk management as a whole. Risk management is a process with the aim of getting a balance between efficiency and realizing opportunities to benefit and minimize vulnerability and loss. Risk management must be a non-stop and repetitive process that consists of several phases, that when properly implemented allows continuous improvement in decision making and improvements in performance.

Literature Review

Risk

Risk is a danger, a consequence that can occur as a result of an ongoing process or future event, or, it can be interpreted as a state of uncertainty, where if an unwanted situation occurs a loss can result. Risk is a combination of the possibility of an event and the consequences of the event by not addressing the possibility that there is more than one consequence which might occur due to one particular event (Dali, 2012). Own risk, when seen in general, can be divided into 4 types of risks, namely:

1. Operational Risk, which is the risk associated with the organization's operations, among others. For example, risks that cover organizational systems, work processes, technology and human resources.
2. Financial Risk, namely risk that impacts on the financial performance of the organization such as the occurrence of risk due to currency fluctuations, and interest rates including the risk of credit, liquidity and market conditions.
3. Disaster risk, namely the risk associated with physical accidents such as damage due to fire, earthquake, physical threat.
4. Strategic risk, namely risk that has to do with corporate strategy, politics, economics, and law. This risk is also related to the reputation of the organization's leadership and changes in customer tastes.

Risk Management

Risk management is a structured/methodological approach to managing uncertainties related to the threat of a series of human activities including: risk assessment, developing strategies to manage them and mitigating risks using empowerment / resource management. Strategies that can be taken include moving risk to other parties, avoiding risks, reducing the negative effects of risk, or accommodating some or all of the consequences of certain risks (CRMS Indonesia, 2018). Traditional risk management focuses on risks that arise from physical or legal causes (such as natural disasters or fires, deaths, and lawsuits).

The goal of implementing risk management is to reduce the different risks associated with the chosen field to a level acceptable by the community. This can be in the form of various types of threats caused by environment, technology, people, organizations and politics. On the other hand, the implementation of risk management involves all means available to humans, especially for risk management entities (human, staff, and organization). The objectives of risk management are as follows (Gibson, 2011):

1. Protect the company
   Providing protection for companies from a significant level of risk that can hinder the process of achieving company goals.
2. Helps create a framework
   Assist in the process of creating a risk management framework that is consistent with the risks present in business processes and functions within a company.
3. Encourage management to be proactive
   Encourage management to act proactively in reducing risk potential, and make risk management a source of competitive advantage and company performance.
4. As a warning to be careful
   Encourage all individuals in the company to act cautiously in facing company risks in order to achieve the desired goals together.
5. Improve company performance
   Helps improve company performance by providing information on the level of risk mentioned in the risk map. This is also useful in developing strategies and improving the risk management process on an ongoing basis.

Threats

Threats in an organization can be divided based on the source. The source of the threat is divided into two groups, namely threats originating from internal and threats originating from external (Hanafi, 2009). Sources of threats originating from within (internal) of an organization include:

1. Management
2. Employees
3. Unreliable systems

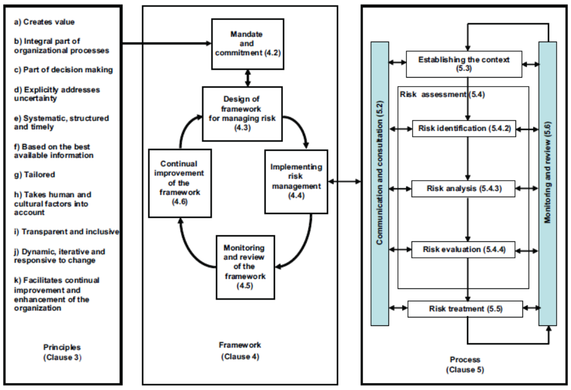
Sources of threats that come from outside (external) of an organization include:

1. Nature/Acts of God
2. Hardware suppliers
3. Software suppliers
4. Contractors
5. Other resource suppliers
6. Competitors
7. Debt and equity holders
8. Unions
9. Governments
10. Environmentalist
11. Criminals/hackers

ISO 31000

The International Organization for Standardization (ISO) 31000: 2009 Risk Management - Principles and Guidelines is an international standard prepared with the aim of providing generic principles and guidelines for the application of risk management. International standards issued on November 13, 2009 can be used by all types of organizations in the face of various risks inherent in their activities (Indrajit, 2000). Although ISO 31000: 2009 provides a generic guide, this standard is not intended to homogenize risk management across organizations, but is intended to provide a supporting standard for the application of risk management in an effort to guarantee the achievement of organizational goals. ISO 31000: 2009 provides risk management principles, frameworks and processes that can be used as an architecture of risk management in an effort to guarantee the application of effective risk management. This standard does not only focus on information security risks but can also be used for all types of risks including business continuity, market, currency, credit, operations, and others. Basically this ISO also uses a general framework including the PDCA cycle (Plan, Do, Check, Act).

Figure 1. Relationships between the risk management principles, framework and process (Weber, 1999).


a) Creates value
b) Integral part of organizational processes
c) Part of decision making
d) Explicitly addresses uncertainty
e) Systematic, structured and timely
f) Based on the best available information
g) Tailored
h) Takes human and cultural factors into account
i) Transparent and inclusive
j) Dynamic, iterative and responsive to change
k) Facilitates continual improvement and enhancement of the organization
Principles (Clause 3)
Mandate and commitment (4.2)
Design of framework for managing risk (4.3)
Implementing risk management (4.4)
Monitoring and review of the framework (4.5)
Continual improvement of the framework (4.6)
Framework (Clause 4)
Communication and consultation (5.2)
Establishing the context (5.3)
Risk assessment (5.4)
Risk identification (5.4.2)
Risk analysis (5.4.3)
Risk evaluation (5.4.4)
Risk treatment (5.5)
Monitoring and review (5.6)
Process (Clause 5)

1. Principles of Risk Management

   ISO 31000: 2009 Risk Management - Principles and Guidelines determine eleven principles that need to be understood and applied to the risk management framework and process to ensure their effectiveness. The eleven principles are:

   a. Provide added value and protect the value of the organization
   b. Integrated part of the entire organization process
   c. Part of decision making
   d. Specifically dealing with uncertainty
   e. Systematic, structured, and timely
   f. Based on the best information available
   g. Adapted to the needs of the organization
   h. Consider cultural and human factors
   i. Transparent and inclusive
   j. Dynamic, repetitive, and responsive to changes
   k. Facilitating continuous improvement and organizational improvement.

2. Risk Management Framework

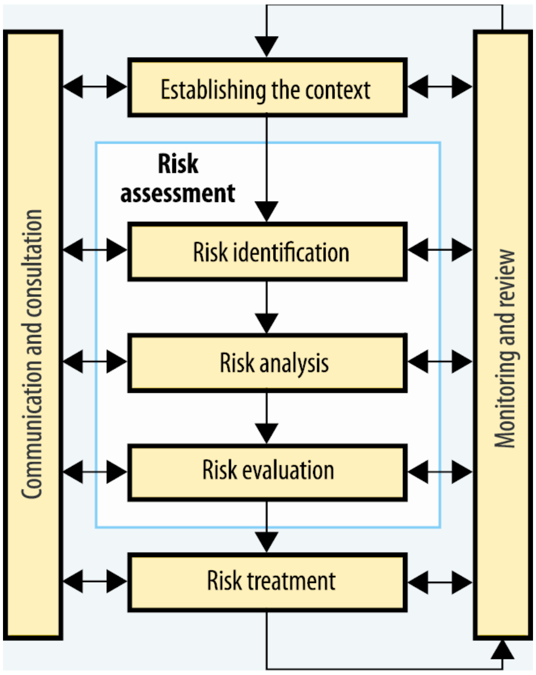
   ISO 31000: 2009 risk management framework Risk Management - Principles and Guidelines begin with the provision of mandates and commitments. Providing mandates and commitments is very important because it determines the accountability, authority and capability of the risk management actors. After provision of the mandates and commitments, the ISO 31000: 2009 framework continues with the implementation framework of Plan, Do, Check, Act. Planning a risk management framework includes understanding of the organization and its context, establishing risk management policies, establishing accountability for risk management, integrating risk management into the organization's business processes, allocating risk management resources, and establishing internal and external communication mechanisms. After planning the framework, the risk management process is implemented. In implementing the risk management process, it is necessary to monitor and review the risk management framework. After that, the risk management framework needs to be improved on an ongoing basis to facilitate changes that occur in the internal and external context of the organization. These processes are then repeated to ensure the existence of a risk management framework that undergoes continuous improvement and can result in the application of reliable risk management.

3. Risk Management Process

The process of risk management is a critical activity in risk management, because it is an application of the principles and frameworks that have been built (Oehmen et al., 2010).

In the risk management process a very important first step is Establishing the Context or setting the context. Establishing this context includes setting goals, strategies, scope, and other parameters related to the risk management process of an organization. In the risk management process a very important first step is Establishing the Context or setting the context. Establishing this context includes setting goals, strategies, scope and other parameters related to the risk management process of an organization. The third process is Risk Analysis or analysis of risks, namely the process of determining how much impact (impact or consequences) and how possible (frequency or likelihood) it is that the risks will occur. Risk analysis can be carried out with various levels of detail depending on the risk, purpose of the analysis, information, data, and available resources. The fourth process is Risk Evaluation or comparing the risks that have been calculated above with standardized Risk Criteria (placing risk positions on the risk criteria image), and then considering if those risks acceptable/acceptable, are becoming an issue/watch out, or are unacceptable/not accepted, then prioritizing mitigation or handling them. The fifth process is Risk Treatment or mitigation of risks. Mitigation of risks must be planned as well as possible with consideration given to all alternative solutions, before implementing the mitigation, in order to get the expected results effectively and efficiently. The sixth process is Monitor & Review. Monitoring & Review is carried out on the entire risk management process including the context (environment, process, organization, strategy, stakeholders etc).

Figure 2. Risk management process (Leo and R, 2010)



Checklist

Checklist is an observation tool that is intended to obtain data in the form of a list containing the factors and subjects to be observed. Observers, in carrying out observations in the field, can only give a check (check, or usually checked) on the list of factors according to behaviors that appear on the observation sheet. This allows the observer to perform their task quickly and objectively because the observer has limited themselves to the presence or absence of aspects of the subject's actions as listed in the checklist (Hanafi, 2007).

Methodology

The methodology used in the execution of this paper were:

5. Early Stage
   This is the stage of determining the research topic, then determining the object of research. From here the authors identify and formulate a problem which then directs a literature study as a reference in solving the problems to be studied.

6. Data Collection Phase
   This stage is carried out to collect the necessary data that is relevant to the objective of the research. The steps taken are observation and interview. Make direct observations and ask questions to define problems.
7. Stage of Risk Management Preparation and Planning

Form of preparation and risk management planning stage by determining the framework that will be used in managing risk.

8. Risk Identification Phase
   Is a stage to identify possible risks that occur and the impacts that occur.
9. Preparation and Processing Phase Checklist
   Checklist is done to simplify the risk identification process. Using a checklist can be done early identification of possible risks and impacts.

10. Stage of Risk Analysis
    The stage which determines the likelihood and magnitude of the risk impact
11. Evaluation and Recommendation Phase
    The stage of obtaining the risk level then provides recommendations to minimize and prevent the risk of re-occurring.

Result and Discussion

Risk Identification

Identify risks in the field of Information Security and Coding aims to determine what, how and why a condition can occur that has an impact on the institution. The process of identifying this risk is grouped based on every possible risk that occurs. In conducting this risk identification stage, the method used is the checklist and interview method. The use of these two methods aims to obtain all information that is relevant, comprehensive and valid from the possible risks that occur. Checklist methods and interviews are also used at the risk analysis stage. The following is the identification of risks in the field of Coding and Information Security.

1. Identification of Assets
   In identifying assets, the steps taken are identifying assets owned by the Information Security and Coding field. These assets are grouped according to the Information Technology (IT) component. The approach used in identifying these assets uses the method of observation and interviews with those directly involved.

2. Identify Possible Risks
   This stage of identifying possible risks is steps to identify various possible risks that arise based on the origin of occurrence. ID is the coding given to explain the factors/threats of each risk.

3. Identification of the Impact of Risk

The last stage of risk identification is the identification of the impact of risk based on the results of the possible risks that occur. The impact referred to here are things that become a result if the possibility of the risk occurs.

Risk Analysis

Risk analysis is the process of determining how much impact and possible risks will occur. The results of this risk analysis will be an input for risk evaluation and a decision-making process regarding risk mitigation. In the risk analysis process an assessment of the risks that arise in the relevant field is carried out. This includes assessing the possibility of risks and impacts if a risk occurs. By carrying out a checklist and interviewing the parties directly involved with the assets in the field, then the value of the possibility and impact of a risk is obtained.

Table 1: Results of Risk Analysis

ID	Risk	Possibility	Impact
R1	Hardware theft	3	3
R2	Lack of number of human resources	5	5
R3	Human error	4	3
R4	Hardware damage	2	2

Risk Evaluation

The risk evaluation phase is to compare the risks that have been calculated at the risk analysis stage with the standardized risk criteria (placing the risk positions) whether those risks are acceptable, being an issue/being watched out, or not being accepted. Based on the description of the risk matrix adopted from ISO 31000, the plots are arranged to facilitate the placing of each risk into the values that belong to the matrix. The value used is the value of the possibility and impact of risk.

Table 2: Risk Evaluation Matrix

LIKELIHOOD						
	Almost Certain (5)	Moderate	Moderate	High	High	High
	Likely (4)	Low	Moderate	High	High	High
	Possible (3)	Low	Low	Moderate	High	High
	Unlikely (2)	Low	Low	Moderate	Moderate	High
	Rare (1)	Low	Low	Low	Moderate	Moderate
		Insignificant (1)	Minor (2)	Moderate (3)	Major (4)	Catastrophic (5)
		IMPACT				

Table 3: Matrix of Risk Evaluation Results

LIKELIHOOD						
	Almost Certain (5)	🟨	🟨	🟥	🟥	🟥 **R2**
	Likely (4)	🟩	🟨	🟥 **R3**	🟥	🟥
	Possible (3)	🟩	🟩	🟨 **R1**	🟥	🟥

	Unlikely (2)	🟩	**R4**	🟨	🟨	🟥
	Rare (1)	🟩	🟩	🟩	🟨	🟨
		In-significant (1)	Mi-nor (2)	Mo-derate (3)	Major (4)	Catas-trophic (5)
		IMPACT				

The following is a table that describes the risk rating/level of risk at each risk that exists, ranking is based on the risk evaluation matrix.

Tabel 4: Level of Risk

ID	Possibility	Impact	Level of Risk
R1	3	3	*Moderate*
R2	5	5	*High*
R3	4	3	*High*
R4	2	2	*Low*

Treatment (Mitigation) Risk

Risk mitigation is an action or approach that needs to be performed to overcome and deal with any risks identified in that field in order to get effective and efficient results. Services provided such as Electronic Certificate Services (SE), Jamming Services, Information Security Audit Services, Penetration Testing Services, and Counter Surveillance Services can be carried out optimally without having to interfere with the risks identified. When the regional device sends a service request, it can quickly provide response and assistance. Therefore, it is important to determine risk mitigation strategies that are appropriate in overcoming each problem with careful planning. The proposed risk mitigation is given to minimize, prevent and reduce any risks.

From the results of analysis and mitigation of risks, it is known that 1 is a low risk category, 1 is a moderate risk category, and 2 are a high-risk category. As high-categorized risks are a dangerous risk and must be dealt with as soon as possible, it has an impact on business processes that can stop completely. Besides this, these risks also have an impact on material and non-material losses. At medium risk, there is a need for ongoing monitoring and handling because the possibility that this risk has a negative impact on the sustainability of the business process has not been rules out, so the main tasks and functions of the field are constrained and cannot run properly. At low category risk, even though it does not have a big effect, there needs to be a policy so that this risk does not occur.

Conclusion

Based on the results of the risk analysis carried out in the field, it can be concluded that the information technology risk analysis process in the relevant field using ISO 31000 is carried out in several stages, namely setting context, risk identification, risk analysis, risk evaluation and risk treatment. By carrying out a series of risk management processes based on ISO 31000, the risk level results that have a value of 1 are low risk categories, 1 is a moderate risk category, and 2 are a high risk category. Almost every risk is considered to interfere with the business process of the field. After assessing the magnitude of the likelihood and impact of the risks that occur, the proposal given is to minimize the existing risks by treating (mitigating) the risks that have been suggested.

REFERENCES

A. Dali, “ISO 31000 Risk Management,” The Golden Standard, vol. 45, no. 5, 2012.

A. Kadir dan T. Triwahyuni, Pengantar Teknologi Informasi, Yogyakarta: ANDI, 2013.

CRMS Indonesia, “Membedah Anatomi ISO 31000:2009 Risk Management Principles and Guidelines,” http://crmsindonesia.org/ (Accessed 11 June 2018).

Darmawi, Herman, Manajemen Risiko. Jakarta: Bumi Aksara, 2006.

G. Joyce, “ISO Risk Management,” *Guidelines and Principles*, 2009.

Gibson, Darril, Managing Risk in Information Systems. Sudbury: Jones Learning, 2011.

Hanafi, Mamduh M, Manajemen Risiko. Yogyakarta: UUPSTIMYUKPN, 2009.

Indrajit, Richardus Eko, Manajemen Organisasi dan Tata Kelola Teknologi Informasi. Jakarta: Elex Media Komputindo, 2000.

International Standard ISO 31000, “Risk management - Principles and guidelines”, 2009.

Oehmen, J., Ben-Daya, M., Seering, W., Al-Salamah, M.: Risk Management in Product Design: Current State, Conceptual Model and Future Research. DETC2010-28539. Proceedings of the ASME 2010 International Design Engineering Technical Conference & Computers and Information in Engineering Conference IDETC/CIE 2010. August 15-18, 2010, Montreal,Canada. ISBN 978-0-7918-3881-5.

P. Hopkin, Fundamental of Risk Management: Understanding, Evaluating and Implementing Effective Risk Management, London: Kogen Page, 2010.

R. Weber, Information Systems Control and Audit, New Jersey: Prentice-Hall, Inc., 1999.

S. Leo J dan R. K. Victor, Manajemen Risiko Berbasis ISO 31000 Untuk Industri Non Perbankan, Jakarta: PPM, 2010.