Assessment Framework for Defining the Maturity of Information Technology within Enterprise Risk Management (ERM)

Rokhman Fauzi, Muharman Lubis
Department of Information System, Telkom University, Bandung, Indonesia

***Abstract*—The process of reviewing, assessing and improving the organization's IT risk management requires some basic information summarized in a process maturity profile. In general, IT risk management standards or frameworks do not include a mechanism for assessing the maturity level of process implementations. This study was conducted to develop a framework, which can be applied to assess the maturity level of IT risk management under ISO / IEC 27005. A standards-based management system implementation can be represented as a model cycle of planning, implementation, validation and also action plan. The proposed evaluation framework consists of templates, methods, and working papers. Therefore, the template focus on the evaluation areas, which are planning, execution, validation, and execution, then evaluation area details (8 domains, 35 subdomains, 82 items), and evaluation metrics and criteria. Meanwhile, a working paper has been created to assist in conducting the evaluation. Actually, by using this evaluation framework, it can provide a representation of the maturity level from the entire process in managing IT risk, based on the provisions of ISO/IEC 27005. This framework complements the existing model with the representation of (1) providing a single-cycle planning, establishment, validation, and execution, (2) evaluation tools, (3) more comprehensive data collection methods, and (4) priority list of elements to be reformed and/or improved.**

***Keywords*—Risk management; assessment framework; maturity level; PDCA cycles; ISO/IEC 27005**

I. Introduction

In the process of forecasting, minimizing, monitoring, and controlling the likelihood or impact of unfortunate events, also in maximizing the realization of opportunities; organizations utilize enterprise risk management (ERM) frameworks in particular to manage every potential loss, problem or damage towards company. This framework needs to provide a structured process that integrates risk management activities into the systems development life cycle (SDLC) or agile management project to enable risk managers in making the informed decisions. In general, this process should involve determining the accuracy of risk decisions and the possible accepted risks. On the other hand, good prescriptions for making risk decisions include a mixture of objective data, pass or fail test results, mitigation measures, qualitative analysis, subjective data, and a healthy bit of intuition [1]. In actual, a description of the enterprise's risk management maturity level should provide the benefit of identifying the actual strengths and weaknesses of risk management in the enterprise. Then get measurement results that will help organization to increase its maturity level and ladder. It also integrates organizational risk management documents to enhance its contribution to be more effective organizational governance and to improve the quality of risk management and risk mitigation processes. Thus, the company's leadership must define expectations for the company's risk management programs on how to measure them, especially the security assessment stage of the risk management framework. Asking the right questions is important for auditors to discover how risk management software works and the true state of program integration. Moreover, audit teams need to focus and concentrate on a more in-depth review of a broader set of systems and integrity testing.

Each year, the public sector provides indicators and metrics to support government compliance and reporting requirements. Some of these many metrics include the number of systems that company operates in their viability to execute and risk of acceptability. Therefore, the accuracy in measuring the effectiveness of risk management programs depends on whether safety controls are regularly tested as well retested, and whether there is a record of test results related to five primary sources of risk namely production, marketing, financial, legal and human [2]. Risk is a necessary part of doing business and in a world where massive amounts of data are processed at an ever-increasing rate, identifying and mitigating risks is a challenge for any company. Actually, little wonder that many contracts and insurance policies require strong evidence of good risk management practices [3]. In addition, it is imperative that the framework provides guidance for companies to integrate risk-based decision-making into organizational governance, planning, management, reporting, policies, values and culture. It is an open principles-based system that allows organizations to apply standard principles in their context.

Every International Standard Organization (ISO) are reviewed every five years and revised as needed. This allows them to remain a useful and relevant tool in the market. Therefore, in this case, the study focuses on old versions and emphasize about ownership that many organizations face obstacles and barriers directly to further modernizing technology and infrastructure, while at the same time needing the guidance to be as simple as possible so the older versions provide benefit in term of contextual more compare to the latest version developed. In particular, this framework helps provide the basis for a comprehensive risk management methodology for assessing and improving program risk management practices. The risk management framework can be applied to all stages of the system development life cycle, including acquisition, development and operations. In addition, the framework can be used to guide the management of various types of risks, including acquisition program risks, software development risks, operational risks, and information security risks [4]. In short, risks are of paramount importance to organizations that need to identify, assess, manage and the process to report many types of risks for the company is extremely important to improve external and internal decision-making. Interestingly, risks can be viewed as threats or called as a negative event to the organization. Managing risk in this context means using management techniques to reduce the likelihood and impact of adverse events without incurring excessive costs. On the other hand, risk also can be defined as uncertainty as the danger related to the distribution of all possible outcomes, positive and negative. Thus, managing risk means minimizing the difference between expected and actual results. Finally, risk can be described contextually as an opportunity that can be viewed as a source of business opportunities [5], [6]. Thus, it is recommended to utilize the popular and older version of ISO/IEC 27005 with the modified version to bring simplification to the organization that have been used in certain period of time without the burden in the transition process or adopting the new method regularly every five year while at same time creating flexibility and improvement to the business process as a whole, which, this study want to offer the ERM template.

II. Literature Review

Processes in risk management besides functioning to reduce negative impacts can also be used to identify and optimizing the positive and potential aspect of the organization. Meanwhile, ISO/IEC Guide 73 defines risk as a combination of an opportunity (likelihood) and its impact (implication). Information Technology (IT) Risk is a business risk related to the use, ownership, operation, involvement, influence, and application of IT in a company [7], [8]. It is also defined as something that is wrong with IT and has a negative impact on business [9], [10]. The types of risks that affect and/or become a direct result of IT activities have a broad scope. In short, risks can be grouped into several categories that help providing an overview of the organization's risk profile. The IT risk portfolio is one approach in identifying and grouping IT risks, which can be grouped into 7 (seven) categories, namely: projects, continuity of IT services, information assets, service providers, applications, infrastructure, and strategic matters [11], [12]. The IT risk portfolio provides an overview of things that should be the main concern of the organization in managing the risks associated with IT, which Symantec [13] classifies IT risk into 4 categories, namely: security risk, availability risk, performance risk, and compliance risk. In addition, the common threads that serve as for the various IT risk rating models are confidentiality, integrity, and availability [14].

In general, PDCA (Plan, Do, Check, Act) is included in an endless cycle of risk management where all executed and implemented solutions can be seen as indicators of further improvement activities. This knowledge is used as a basis and fundamental organizational resource that provides an ongoing competitive advantage in a relevant and dynamic environment and market by identifying gap between strategic planning and potential knowledge [12]. National Institute of Standards and Technology [15] defines IT Risk Management as a process that allows IT managers to balance operational and economic costs from the protection of IT and benefit from such protection. This definition compromises between classical definitions in business and definitions in the context of the organization's IT operations. Risk management also must be carried out continuously and have sustainability to be developed in order to overcome the risks of the organization at present and in the future. Thus, every manager and staff must understand their roles and responsibilities in risk management. In addition, risk management must also be integrated with organizational culture through policies and programs led directly by senior management [16]. In fact, IT Risk Management is the foundation of the implementation of the Information Security Management System [17]. ISO/IEC 27001 stipulates that the controls implemented within the scope, limits, and context of the Information Security Management System (ISMS) must be risk-based. The PDCA has been engaged as an impressive and essential tool for quality and continuous improvement with both simple and powerful to implement the strategy and policy in the organization. The application of the PDCA cycle has been found more effective than adopting “the right first time” approach. By using of the PDCA cycle means continuously looking for better methods of improvement and enhancement [18].

Implementing a risk management process is not always easy, and some organizations give up without achieving the desired results. This may be due to the inability to implement the risk management process in a consistent and predictable manner in the long term. On the other hand, a maturity model is a tool that represents the pathway to an increasingly structured and systematic way of doing business, usually involving people, organizations, and processes. Over the past few years, these tools have become very popular, using models of maturity in many areas, such as data management, information security, and project management. In a maturity model, the evolutionary path is described through separate stages. To reach the next level, the organization must achieve the objectives of the required level and all previous levels [19], [20]. To enable the measurement of maturity levels and identify gaps between current levels and follow-up to enable planning efforts; priorities and objectives should be formulated to achieve proposed goals. It allows the assessment process run smoothly and building the achievement compliance. Ultimately, this approach provides organizations with an understanding of strengths, weaknesses, and opportunities that can support audits, benchmarks, and progress assessments against goals, strategic decisions, and project portfolio management [21], [22].

The difference between organizations whose systems are more or less mature is not only related to the results of the indicators used, but also to the fact that dominantly mature organizations measure differently using various indicators when compared to immature organizations. The concept of maturity is related to one or more of the elements identified as being related but the concept of function is only appropriate for each of these elements [23], [24]. It appears very important for non-financial companies to promote and discuss on how to implement and manage risk management efforts. One of the key issues is how to effectively evaluate the quality of a company's risk management performance. The most important factor is the growth of a consistent risk culture and the independence of the board of director in determining the decision for integration process within the organization [25], [26], [27]. Therefore, it is also important to understand the role of individual, institutional and environmental within the organization as the primary prerequisites for improvement in raising awareness of the strategies used in each business process within the framework of a particular project or service [28].

III. Framework Design

This study was conducted using several phases: literature review, framework design, and case studies (see Fig. 1). The evaluation framework, on the other hand, consists of evaluation forms, methods, and a worksheet of descriptive structure (see Fig. 3). Evaluation forms are a key component of this framework, which this model consists of 8 domains, 35 subdomains, and 4 evaluation domains (PDCA) detailing 82 items with the detail area is a set of provisions of the ISO / IEC 27005 standard. The domains are taken from the main blocks in the standard process model. Meanwhile, subdomains and elements refer to clauses of the standard in each domain. Interestingly, the presence of a Chief Risk Officer (CRO) does not clarify the level of support and leadership from the CEO and the Board of Directors in relation to the creation and distribution of risk information throughout the organization, which dedicated to mitigate and manage major risks [29], [30]. Most importantly, create a portfolio of company risks and opportunity events: finance, strategy, compliance, operations, and reputation can influence the achievement of strategic goals.

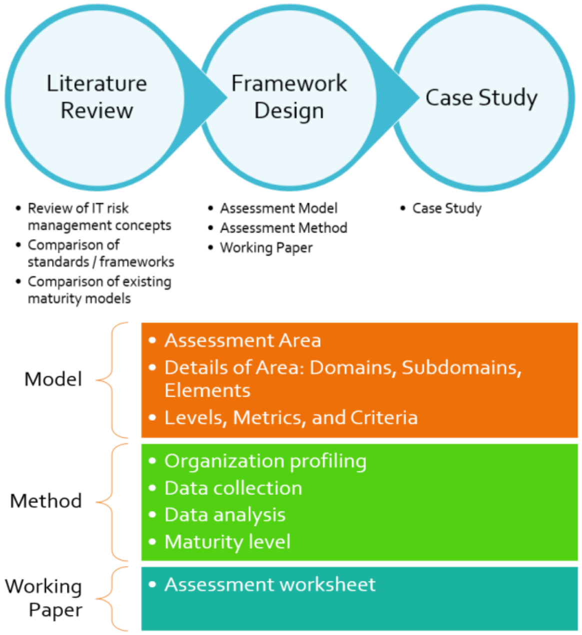


Fig. 1. Methodology and Assessment Framework.

IV. Assessment Area

In fact, this study divided the process into five groups related to the plan in implementing ERM: full implementation, partial execution, implementation planning process, feasibility study or evaluation, and level of ERM implementation. On the other hand, traditional risk management approaches utilize segmented methods to face different risks across different organizations. In contrast, ERM is a relatively new paradigm that enhances a company's ability to predict the set of risks it faces [31], [32], [33]. ERM is a top-down approach that includes identifying, assessing and addressing strategic, operational and financial risks to achieve the following four objectives: (1) high-level strategic objectives aligned with the corporate mission, (2) effective and efficient use of resources, (3) reliability of reporting, and (4) compliance - enforcement of legal and regulatory compliance [34]. As can be seen in Fig. 2, the process is started and ended with context establishment to risk identification, estimation and evaluation, the once again context become the consideration to determine risk treatment as well risk acceptance.

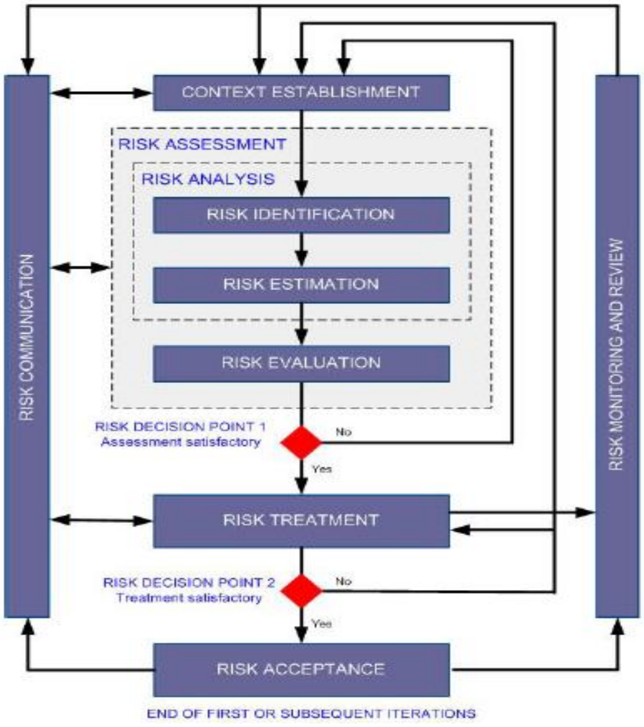


Fig. 2. Process Model of ISO/IEC 270005.

The main purpose of placing this evaluation form is to provide a structured description of the improvement stages of the PDCA cycle process. The following table defines levels using the Business Risk Management Maturity Model and the Business Process Maturity Model. Providing metrics is essential because the lack of process measurement affects the determination of performance levels and further disrupts the organization's business and activity improvement processes. Measurements are an approach of the evaluation process and organizational performance, and in this model the standard is defined as a metric of the elements score level and a list of conditions that indicate the determination of requirements. In addition, referring to the standard paragraph, each domain is divided into several subdomains and elements. The result was 35 subdomains and 82 items (Table I). In addition, PDCA code elements are assigned to classify needs based on several specifications to increase the sustainability of the activity process (Table II).

TABLE I. SUBDOMAINS AND ELEMENTS

Domains	**Number of subdomains**	**Number of elements**
Context Establishment	6	16
Risk Communication	4	13
Risk Identification	5	15
Risk Estimation	4	6
Risk Evaluation	3	4
Risk Treatment	7	7
Risk Acceptance	2	2
Risk Monitoring and Review	4	19
	35	82

TABLE II. MAPPING OF AREA: PLAN, DO, CHECK AND ACT

Area	**Code of elements**
PLAN	1.1.1, 1.2.1, 1.3.1, 1.4.1, 1.4.2, 1.4.3, 1.4.4, 1.4.5, 1.4.6, 1.4.7, 1.4.8, 1.4.9, 1.4.10, 1.4.11, 1.5.1, 1.6.1
	2.1.1, 2.2.2, 2.3.1, 2.3.2, 2.3.3, 2.3.7, 2.3.8, 2.3.9
	3.1.1, 3.1.2, 3.1.3, 3.1.4, 3.2.1, 3.2.2, 3.2.3, 3.3.1, 3.3.2, 3.4.1, 3.4.2, 3.4.3, 3.5.1, 3.5.2, 3.5.3
	4.1.1, 4.1.2, 4.2.1, 4.2.2, 4.3.1, 4.4.1
	5.1.1, 5.2.1, 5.2.2, 5.3.1
	6.1.1, 6.2.1, 6.7.1
	7.1.1, 7.1.2
DO	2.4.1
	6.3.1, 6.4.1, 6.5.1
CHECK	2.2.1, 2.3.5
	6.6.1
	8.1.1, 8.1.2, 8.1.3, 8.1.4, 8.1.5, 8.1.6, 8.1.7, 8.2.1
ACT	2.3.4, 2.3.6
	8.3.1, 8.3.2, 8.3.3, 8.3.4, 8.3.5, 8.3.6, 8.3.7, 8.3.8, 8.3.9, 8.4.1, 8.4.2

The life cycle of an innovation project is a series of interrelated processes and stages of novelty. Innovation projects generally include the following life cycle rule with well-defined stages: innovation development, production readiness, market entry, growth, maturity, recovery, or decline. In order to maintain the competitiveness of innovation projects at all stages, it is necessary to develop and implement specific type of innovations (incremental, responsive, disruptive or radical) that are included in the portfolio of innovation projects and which are implemented in a specific order with different levels of innovation content and research intensity [35]. Entirety was used then to map the component into each Assessment Area, in which each element is also mapped into them respectively (Fig. 3-7). The level and criteria should be defined to set the indicators that can be looked at and matching for the purpose of improvement in the process (Table III). Meanwhile, the metrics is also essential to simplify the process maturity to be recognized in every type of risk domain respectively (Table IV). Risks are localized in implementing innovation projects in the process of analyzing and modeling a set of innovations. Choosing the best combination of risk management techniques as part of a particular innovation project requires assessing a range of factors, such as the complexity and specificity of innovation activities and the level of profitability of the innovation at a given time. Time periods, insurance service costs, likelihood of risk, size and quality, predictability of risk, legal limits and provisions, and project implementation phases are several aspects that become primary considerations [36].

TABLE III. LEVEL AND CRITERIA

Level	**Criteria**
Level 5	Organizational focus is the ongoing improvement process. The whole process was in accordance with the reference standard.
Level 4	Organizational focus is the evaluation and optimization of existing resources. Much of the process followed a reference standard.
Level 3	Organizational focus is to build a standard managerial processes to achieve organizational goals. A small part of the process followed the reference standard.
Level 2	Organizational focus is to build managerial foundation in every program or project. Some processes are standardized, without a reference standard.
Level 1	No specific targets. Achievement of the organization depends on the competence and hard work of a handful of personnel. There is no standard process.

TABLE IV. METRIC COMPONENTS

Domain	**M1**	**M2**	**M3**	**M4**	**M5**	**M6**
Context Establishment	P	P	P	P		
Risk Communication	P		P	P		P
Risk Identification	P		P	P	P	P
Risk Estimation	P		P	P	P	P
Risk Evaluation	P		P	P	P	P
Risk Treatment	P		P	P	P	P
Risk Acceptance	P		P	P		
Risk Monitoring and Review	P		P	P	P	P

*P: Primary related; metric component used in the domain assessment

Metrics and Assessment Criteria are determined per domain because each has its input, process and output characteristics. In this case, it used various assessments namely [M1] policy, plans and procedures, [M2] goals and success measurements, [M3] roles and responsibilities, [M4] communications, [M5] skills and trainings, as well as [M6] tools. Furthermore, the metric components used in the domain context of establishment; the assessment are [M1], [M2], [M3] and [M4] communications. On the other hand, the metric components used in the domain of risk communication; the assessment are [M1], [M3], [M4] and [M6]. Nonetheless, the metric components used in the domain risk identification; the assessment are [M1], [M3], [M4], [M5] and [M6]. Then, the metric components used in the domain of risk estimation; the assessment are [M1], [M3], [M4], [M5] and [M6].

The ERM template can be seen in Table V is designed for use as a self-assessment for the tool to be effective; it must be conducted in such a way that the process is as objective as possible to avoid bias or group thinking. From experience using the model, the self-evaluation discussion includes the following important considerations such as project duration and role responsibility. According to the government comments, it could take hours to a day or more, depending on the amount of preparation before the group discussion and the level of detail of the discussion itself take place. Ideally, there should be a diverse group of employees responsible for managing ERM involved in the self-assessment across the ranks. Thus, caring must be taken to ensure that the conversation is open and transparent, which people should be encouraged to express their opinions. It may be helpful to ask someone outside of the management chain to manage ERM to facilitate discussion. That person should read specific note and understand on how to handle the self-evaluation of the form [37]. In addition to facilitating discussions, a person should be able to challenge the opinions of the self-assessment group, including looking for supporting evidence as needed. The metric components used in the domain risk evaluation, the assessment are [M1], [M3], [M4], [M5] and [M6]. Meanwhile, the metric components used in the domain risk treatment; the assessment are [M1], [M3], [M4], [M5] and [M6]. Nevertheless, the metric components used in the domain risk acceptance; the assessment are [M1], [M3] and [M4]. At last, the metric components used in the domain risk monitoring and review; the assessments are [M1], [M3], [M4], [M5] and [M6]. All of them can be seen in Table VI, respectively based on each separated criteria level.

TABLE V. LEVELS, METRICS AND CRITERIA FOR DOMAIN CONTEXT ESTABLISHMENT, RISK COMMUNICATION, RISK IDENTIFICATION AND RISK ESTIMATION

Level	**Criteria**	**Criteria**	**Criteria**	**Criteria**
Domain	**Context Establishment**	**Risk Communication**	**Risk Identification**	**Risk Estimation**
Level 5	All items in this clause already exist in the Policy, Planning and/or Procedure documents. Defining goals and measures of success is clearly given. All roles and responsibilities are clearly described and there is no overlap. Socialization is carried out on all stakeholders.	Senior management and all stakeholders understand and care about key aspects of IT risk management; IT risk is part of the main consideration of decision making. All roles and responsibilities are clearly described and there is no overlap. There are procedures for all forms of risk communication needed. There are communication aids that support normal and emergency conditions.	Risk identification activities are regulated in Policies, Planning and/or Procedures. Risk identification details are in accordance with all clauses in the Standard. All roles and responsibilities are clearly described and there is no overlap. Risk identification involves all parties involved. Implementing risk identification is an internal team of organizations (who have received special training) and experts from outside the organization. Risk identification is carried out with tools that are in accordance with the Standards and conditions of the Organization.	Risk estimation activities are regulated in Policies, Planning and/or Procedures. Details of risk estimates are in accordance with all clauses in the Standard. All roles and responsibilities are clearly described and there is no overlap. Risk estimates involve all parties involved. The executor of risk estimation is the internal team of the organization (who has received special training) and experts from outside the organization. Risk estimates are carried out with tools that are in accordance with the Standards and conditions of the Organization.
Level 4	All items in this clause already exist in the Policy, Planning and/or Procedure documents. Defining goals and measures of success is clearly given. All roles and responsibilities are clearly described and there is no overlap. The socialization was carried out for some stakeholders.	Senior management and all stakeholders understand and care for key aspects of IT risk management. All roles and responsibilities are clearly described and there is no overlap. There are procedures for all forms of risk communication needed. There are communication aids that support normal and emergency conditions.	Risk identification activities are regulated in Policies, Planning and/or Procedures. Risk identification details are in accordance with all clauses in the Standard. All roles and responsibilities are clearly described and there is no overlap. Risk identification involves all parties involved. Implementers of risk identification are internal organization teams (who have received special training) or experts from outside the organization. Risk identification is carried out with tools that are in accordance with the Standards and conditions of the Organization.	Risk estimation activities are regulated in Policies, Planning and/or Procedures. Details of risk estimates are in accordance with all clauses in the Standard. All roles and responsibilities are clearly described and there is no overlap. Risk estimates involve all parties involved. Implementers of risk estimation are internal organization teams (who have received special training) or experts from outside the organization. Risk estimates are carried out with tools that are in accordance with the Standards and conditions of the Organization.
Level 3	All items in this clause already exist in the Policy, Planning and/or Procedure documents. Defining goals and measures of success is clearly given. All roles and responsibilities are clearly described, but	IT and Management staff related to IT understand and care for key aspects of IT risk management. All roles and responsibilities are clearly described, but there are still overlaps. There are procedures for some form of risk communication that is needed.	Risk identification activities are regulated in Policies, Planning and/or Procedures. Risk identification details are in accordance with some clauses in the Standard. All roles and responsibilities are clearly described, but there are still overlaps. Risk identification involves all parties involved. Implementers of risk identification are	Risk estimation activities are regulated in Policies, Planning and/or Procedures. Details of risk estimates are in accordance with some clauses in the Standard. All roles and responsibilities are clearly described, but there are overlaps. Risk estimates involve all parties involved. The executor of risk estimation is an

	there are still overlaps.	There are communication aids that support normal conditions.	internal organization teams (who have not received special training) or experts from outside the organization. Risk identification is carried out with tools that are in accordance with the Standards and conditions of the Organization.	internal team of organizations (who have not received special training) or experts from outside the organization. Risk estimates are carried out with tools that are in accordance with the Standards and conditions of the Organization.
Level 2	Some items in this clause already exist in the Policy, Planning and/or Procedure documents. Defining goals and measures of success is not clearly stated. All roles and responsibilities have been described, but are still unclear and there are overlaps.	IT and Management staff related to IT understand and care for key aspects of IT risk management. All roles and responsibilities are described, but still unclear and there are overlaps. There is no procedure; risk communication is carried out informally.	Risk identification activities are regulated in Policies, Planning and/or Procedures. Risk identification details are in accordance with some clauses in the Standard. All roles and responsibilities are described, but still unclear and there are overlaps. Risk identification does not involve all parties involved. Implementing risk identification is an internal team of organizations (who have not received special training)	Risk estimation activities are regulated in Policies, Planning and/or Procedures. Details of risk estimates are in accordance with some clauses in the Standard. All roles and responsibilities are described, but still unclear and there are overlaps. Risk estimates do not involve all parties involved. Implementing risk estimates is an internal team of organizations (who have not received special training)
Level 1	This clause does not yet exist in the Policy, Planning and/or Procedure document. Defining goals and measures of success is not clear.	There is still IT staff who do not understand and care for the key aspects of IT risk management.	Risk identification activities are not regulated in Policies, Planning and/or Procedures. Risk identification does not involve all parties involved. Implementing risk identification is an internal team of organizations (who have not received special training).	Risk estimation activities are not regulated in Policies, Planning and/or Procedures. Risk estimates do not involve all parties involved. Implementing risk estimates is an internal team of organizations (who have not received special training).

TABLE VI. LEVELS, METRICS AND CRITERIA FOR DOMAIN RISK EVALUATION, RISK TREATMENT, RISK ACCEPTANCE AND RISK MONITORING & REVIEW

Level	**Criteria**	**Criteria**	**Criteria**	**Criteria**
Domain	**Risk Evaluation**	**Risk Treatment**	**Risk Acceptance**	**Risk Monitoring and Review**
Level 5	Risk evaluation activities are regulated in Policies, Planning and/or Procedures. Details of risk evaluation are in accordance with all clauses in the Standard. All roles and responsibilities are clearly described and there is no overlap by involving all parties involved. Risk evaluation implementers are internal organizational teams (who have received special training) and experts from outside the organization. Risk evaluation is carried out with tools that are in accordance with the Standards and conditions of the Organization.	Risk handling activities are regulated in Policies, Planning and / or Procedures. Risk handling details are in accordance with all clauses in the Standard. All roles and responsibilities are clearly described and there is no overlap. Risk management involves all parties involved. Risk management executors are internal organization teams (who have received special training) and experts from outside the organization. ERM is carried out with tools that are in accordance with the Standards and conditions of the Organization.	Risk acceptance activities are regulated in Policies, Planning and/or Procedures. Roles and responsibilities are clearly defined. Acceptance of risk in accordance with all risk acceptance criteria. Justification, communication and monitoring of risk acceptance are carried out in accordance with the clause in the Standard	Monitoring and risk checking activities are regulated in Policies, Planning and / or Procedures. Details of monitoring and risk checking are in accordance with all clauses in the Standard. All roles and responsibilities are clearly described and there is no overlap. Risk monitoring and inspection involves all parties involved. Implementers of risk monitoring and inspection are internal organization teams (who have received special training) and experts from outside the organization. Risk monitoring and inspection is carried out with tools that are in accordance with the Organization's Standards and conditions.
Level 4	Risk evaluation activities are regulated in Policies, Planning and/or Procedures. Details of risk evaluation are in accordance with all clauses in the Standard. All roles and responsibilities are clearly described and there is no overlap. Risk evaluation involves all parties involved. Risk evaluation implementers are internal organization teams (who have received special training) or experts from outside the organization. Risk evaluation is carried out with tools that are in accordance with the	Risk handling activities are regulated in Policies, Planning and/or Procedures. Risk handling details are in accordance with all clauses in the Standard. All roles and responsibilities are clearly described and there is no overlap. Risk management involves all parties involved. Risk management executors are internal organization teams (who have received special training) or experts from outside the organization. Risk management is carried out with tools that are in accordance with the	Risk acceptance activities are regulated in Policies, Planning and / or Procedures. Roles and responsibilities are clearly defined. Acceptance of risk is in accordance with some risk acceptance criteria. Justification, communication and monitoring are carried out on the entire list of risk acceptance that does not meet the criteria.	Monitoring and risk checking activities are regulated in Policies, Planning and / or Procedures. Details of monitoring and risk checking are in accordance with all clauses in the Standard. All roles and responsibilities are clearly described and there is no overlap. Risk monitoring and inspection involves all parties involved. Implementers of monitoring and risk checking are internal organization teams (who have received special training) or experts from outside the organization. Risk monitoring and inspection is carried out with tools that are in accordance with the Organization's Standards and conditions.

	Standards and conditions of the Organization.	Standards and conditions of the Organization		
Level 3	Risk evaluation activities are regulated in Policies, Planning and/or Procedures. Details of risk evaluation are in accordance with some clauses in the Standard. All roles and responsibilities are clearly described, but there are overlaps. Risk evaluation involves all parties involved. The risk evaluation implementer is an internal team of organizations (who have not received special training) or experts from outside the organization. Risk evaluation is carried out with tools that are in accordance with the Standards and conditions of the Organization.	Risk handling activities are regulated in Policies, Planning and/or Procedures. Risk handling details are in accordance with some clauses in the Standard. All roles and responsibilities are clearly described, but there are still overlaps. Risk management involves all parties involved. Risk management implementers are internal organization teams (who have not received special training) or experts from outside the organization. Risk management is carried out with tools that are in accordance with the Standards and conditions of the Organization.	Risk acceptance activities are regulated in Policies, Planning and/or Procedures. Roles and responsibilities are clearly defined. Acceptance of risk is in accordance with some risk acceptance criteria. Justification, communication and monitoring are carried out on part of the risk acceptance list that does not meet the criteria.	Monitoring and risk checking activities are regulated in Policies, Planning and / or Procedures. Details of monitoring and risk checking are in accordance with some clauses in the Standard. All roles and responsibilities are clearly described, but there are overlaps. Risk monitoring and inspection involves all parties involved. Implementers of monitoring and risk checking are internal organization teams (who have not received special training) or experts from outside the organization. Risk monitoring and inspection is carried out with tools that are in accordance with the Organization's Standards and conditions.
Level 2	Risk evaluation activities are regulated in Policies, Planning and/or Procedures. Details of risk evaluation are in accordance with some clauses in the Standard. All roles and responsibilities are described, but still unclear and there are overlaps. Risk evaluation does not involve all parties involved. Risk evaluation implementers are internal organization teams (who have not received special training)	Risk handling activities are regulated in Policies, Planning and/or Procedures. Risk handling details are in accordance with some clauses in the Standard. All roles and responsibilities are described, but still unclear and there are overlaps. Risk management does not involve all parties involved. Risk management executors are internal organization teams (who have not received special training)	Risk acceptance activities are regulated in Policies, Planning and / or Procedures. Roles and responsibilities are not clearly defined.	Monitoring and risk checking activities are regulated in Policies, Planning and / or Procedures. Details of monitoring and risk checking are in accordance with some clauses in the Standard. All roles and responsibilities are described, but still unclear and there are overlaps. Risk monitoring and inspection do not involve all parties involved. Implementers of risk monitoring and inspection are internal organizational teams (who have not received special training)
Level 1	Risk evaluation activities are not regulated in Policies, Planning and/or Procedures. Risk evaluation does not involve all parties involved. The risk evaluator is an internal team of organizations (who have not received special training).	Risk handling activities are not regulated in the Policy, Planning and/or Procedure. Risk management does not involve all parties involved. Risk management implementers are internal organization teams (who have not received special training).	Risk acceptance activities are not regulated in the Policy, Planning and / or Procedure.	Monitoring and risk checking activities are not regulated in Policies, Planning and / or Procedures. Risk monitoring and inspection do not involve all parties involved. Implementers of risk monitoring and inspection are internal organization teams (who have not received special training).

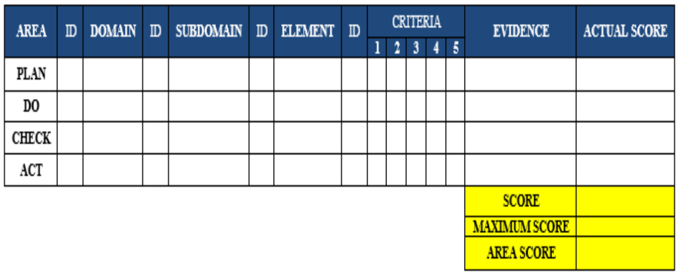
In general, the framework evaluation process consists of four steps, starting with the definition of an organizational profile, the collection and analysis of data, and finally the maturity profile of the presentation. In the early stages of defining an organization's profile, it helps determine the most suitable data collection method for targeted application. The next step is data collection, which the methods are: (1) Document analysis, (2) Interview, (3) Questionnaire, or (4) Material review [19, 20]. Methods (1) and (2) are the two main data collection methods for obtaining evidence. Methods (3) and (4) are necessary when the organization is highly complex and high risks are expected in the IT arena. The resulting data is processed into a worksheet that contains the results of data evaluation, data manipulation and data processing in the basic form as shown graphically in the Fig. 3.

$$\text{Maturity Level} = (\sum \text{Area Score}) \text{ x } 1.25 \qquad (1)$$

$$\text{Area Score} = (\sum \text{Actual Score}) / (\text{Maximum Score})$$

$$\text{Maximum Score} = (\sum \text{Elements}) \text{ x } 5$$

The result at this phase is related to the maturity of the PDCA cycle. These values also indicate the plane position (1-5) and its properties. In addition to the PDCA cycle maturity model, data processing can also explain the status of each component in each region. These results form the basis of the merit assessment of each component. The final step is to prepare a PDCA cycle maturity profile for the organization. This profile consists of at least: (1) Maturity model, (2) Maturity evaluation of each component, (3) Evaluation of conclusions and recommendations.



AREA	ID	DOMAIN	ID	SUBDOMAIN	ID	ELEMENT	ID	CRITERIA					EVIDENCE	ACTUAL SCORE
								1	2	3	4	5		
PLAN														
DO														
CHECK														
ACT														
													SCORE	
													MAXIMUM SCORE	
													AREA SCORE	

Fig. 3. Working Paper.

V. Case Study

The organization's overview involves services with offices in multiple cities with more than 1000 employees, information technology (IT) helps supporting basic business and IT departments with the employees at around 30 to 60 people. The data was collected using interviews and document analysis, which is obtained through storage process using the analytical methods described in the previous section. The interview was conducted with an IT risk manager with the material used was the material described in the worksheet and clarified with the reference document for evaluation. The analysis performed on the referenced document was directly related to IT risk management as they are complementary methods. A list of included documents can be stated such as MRTI/20xx policy, MRTI/20xx appendix policy, asset registration software, hardware asset registration, movable property registration, asset data or information record. The evaluation results consist of (a) PDCA cycle maturity, (2) maturity evaluation of each component, and (3) conclusions and recommendations. Organizational policies are forward-looking policies, based on strong evidence of what the organization can achieve, and that promote a consistent approach to health and safety at all levels of the organization. Therefore, organizational leaders promote a consistent approach to health and safety and setting the transition or transmiting the clear directives that shape daily activities. It also works continuously at all levels of the organization, promotes the values, ethics and culture needed to achieve the goals of the organization, and transforms the leadership style for the entire organization rather than transactional [38]. The result for case study can be seen in Table VII for the maturity assessment.

ERM should be viewed as an evolutionary process within an organization. This is often considered a compliance driven exercise that is achieved, documented and presented while it is doubtful at certain situation whether much value can be extracted from this type of effort [39]. Solving cost and skill problems in the evaluation process also motivates the organization to provide correct answers, and to show robust results in all real-world ways [40]. Aligning the IT investments with ever-changing business goals and priorities remains a major challenge for IT managers. Despite management's efforts to improve project success, an unacceptable number of IT initiatives cannot reach specific goals and target, or simply do not reach the objective in full. There is no end to the various factors that can contribute to the failure of the project. As a result, IT organizations have invested significantly in improving output predictability, productivity, and quality. Techniques such as estimation, risk assessment, process management, delivery management, and project management improve project implementation, but they cannot address the more important issues of investment selection and improving IT performance [41].

As can be seen in Fig. 4 to 7, each code of element and heatmap are distributed to plan, do, check and act realm. The resulting heat map can also be used to inform senior management, audit committees and councils of risk assessment. By having iterative design and management methods used in the business, it can support for continuous control and improvement of processes and products. Basically, the two frameworks in this study cannot be compared with the difference in maturity model for reference. However, the framework proposed in this study includes several aspects that may complement the missing aspects of the current model such as the representation, measurement, method, and presentation of evaluation results as the conclusion. It is important to keep the results anonymous in certain timeframe to ensure that community or governments are not influenced by the use of the maturity model due to concerns about outside perceptions, and its primary purpose as a self-assessment tool to inform the future strategies as well as to promote the attempt to assess the process quality within the organization [37]. Historically, organizations have sought to improve project visibility by compiling schedules, budgets, progress, and spending information from detail-oriented project management tools or enterprise risk management systems.

TABLE VII. Maturity Profile of IT Risk Management Process

AREA	**AREA SCORE**
PLAN	0.65926
DO	0.45
CHECK	0.52727
ACT	0.6
MATURITY OF THE PDCA CYCLE	2.79566

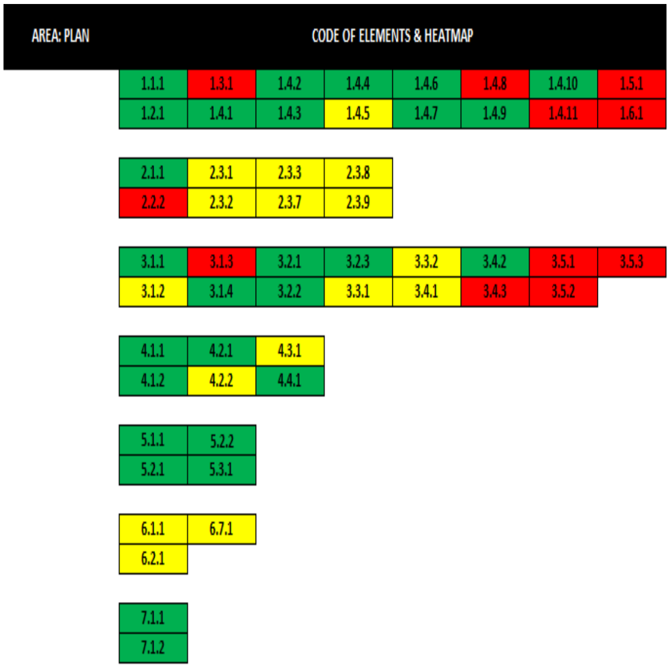


Fig. 4. Case Study: Area PLAN Evaluation.

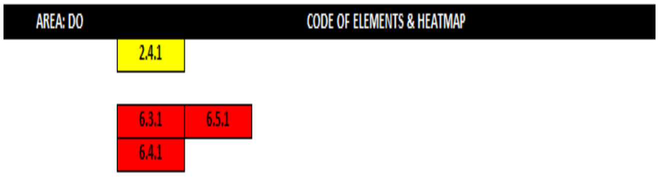


Fig. 5. Case Study: Area DO Evaluation.

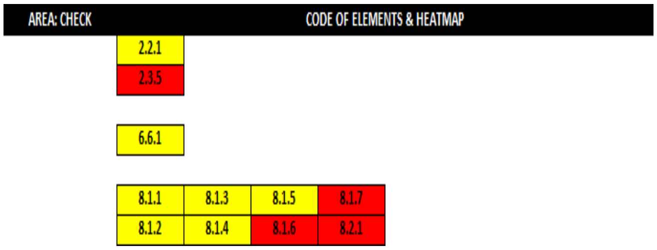


Fig. 6. Case Study: Area CHECK Evaluation.

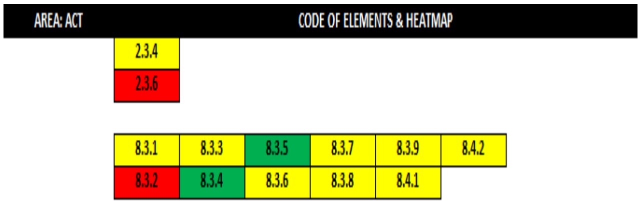


Fig. 7. Case Study: Area ACT Evaluation.

To be successful, all projects must be planned in detail and updated in a consistent and reliable manner. This is a rare case, and the resulting collected data is often inaccurate, outdated and misleading [41]. It should be noted that PDCA cycle in IT Risk Management (ISO/IEC 27005) could not be separated from the company's overall risk management [42]. In addition, clients and organizations often misunderstand responsibilities and rights in business functions, processes, and levels. Thus, it is necessary for professionals to think about how to formulate the rules governing the collection and distribution of information; also, information system specifications and requirements for developers and administrators. Therefore, to improve the effectiveness of stakeholder interactions and communication, many related factors such as human beings, environment, culture, language, literacy, and organization have to be taken into account [43], [44], [45]. Interestingly, by leveraging the creativity and entrepreneurial spirit of employees and managers, it should depend on the ability of the organization to create favorable conditions for potential entrepreneurial to emerge in the proper way that align with context and trend within the environment [46], [47], [48]. In the end, the most effective risk functions have gained strategic influence within the organization and are empowered to invest in the overall development of task and role responsibilities [49], [50].

VI. Conclusion

The unexpected framework recommends establishing the appropriate alignment between the ERM design parameters called ERM Mix or Modified with contingent variables in order to achieve organizational effectiveness. These type of ERM includes specific roles for risk identification processes, frequency of risk meetings, risk tools, risk functions, then, contingent variables as the types of risks that refer to preventable organizational and industry variables, parameters, strategy or external domain. Finally, it must also be understood that it is impractical to expect an ERM process to develop into this mature state in a relatively short period of time. Interestingly, it can be implemented shortly if the organization want to concentrate or focusing in assessing certain aspects only such as risk treatment and risk acceptance by utilizing context establishment. Several sample companies have integrated ERM software for some time and the process still ongoing especially to improve the quality. On the other hand, the ERM process should continually update existing risk inventories and reviewing probability and impact assessments to ensure that significant and potentially catastrophic risks are not overlooked. To ensure that this ERM approach becomes dominant within the company, both the Board of Directors and the CEO explicitly agree on the ERM efforts, and elements of the mature ERM process described by the framework reported with the ERM staff as it is also essential to have sufficient resources available to fully achieve the implementation. As this modified framework has been used in case study, it is expected to be evaluated further in different context and perspective of diverse case study to strengthen and advance the proposed framework.

References

[1] L. Dubsky. Assessing Security Controls: Keystone of the Risk Management Framework. *ISACA Journal* 6, 2016.

[2] L. Grane, G. Gantz, S. Isaacs, D. Jose and R. Sharp. *Introduction to Risk Management: Understanding Agricultural Risk*. 2nd Edition, Extension Risk Management Education and Risk Management Agency, 2013.

[3] ISO. *Risk Management ISO 31000*. International Organization for Standardization, February 2018.

[4] C.J. Alberts and A.J. Dorofee. *Risk Management Framework*. Software Engineering Institute, Technical Report, August 2010.

[5] J. Harvey. *Introduction to managing risk. Topic Gateway series no. 28*. The Chartered Institute of Management Accountant, 2007.

[6] P.M. Collier and S. Agyei-Ampomah. *Management accounting: risk and control strategy*. Oxford: Elsevier. (CIMA Official Study System), 2006.

[7] ITGI. *IG Measurement Tools*. Information Technology Governance Institute, 2005.

[8] ITGI. *Information Risks: Whose Business Are They?* IT Governance Institute, 2005.

[9] ITGI. *COBIT 4.0/COBIT 4.1*. Information Technology Governance Institute, 2005/2007.

[10] ITGI. *Enterprise Risk: Identify, Govern and Manage IT Risk*. The Risk IT Framework Exposure Draft. 2009.

[11] M. Jagusiak-Kocik. PDCA Cycle as a Part of Continuous Improvement in the Production Company – A Case Study. *Production Engineering Archives 14*, pp. 19-22, 2017.

[12] E. Jordan and L. Silcock. *Beating IT Risks*. John Wiley & Sons, England., 2005.

[13] Symantec. *IT Risk Management Report Volume 2*. White Paper 2008.

[14] T. Abram. The Hidden Values of IT Risk Management. *ISACA Journal, 2*, 2009.

[15] NIST. *Risk Management Guide for Information Technology Systems – Recommendations of the NIST*. SP 800-30, USA, 2002.

[16] AIRMIC - ALARM - IRM. *Risk Management Standard*. 2002.

[17] ISO/IEC. 27001:2005 – 27002:2005 – 27005:2008.

[18] M. Sokovic, D. Pavletic, K.K. Pipan. Quality Improvement Methodologies – PDCA Cycle, RADAR Matrix, DMAIC and DFSS. *Journal of Achievement in Materials and Manufacturing Engineering, vol. 43(1)*, pp. 476-483, 2010.

[19] D. Proenca, J. Estevens, R. Vieira and J. Borbinha. Risk Management: A Maturity Model Based on ISO 31000. *IEEE 19th Conf. on Business Informatics* 2017.

[20] D. Proenca, R. Vieira and J. Borbinha. *A Maturity Model for Information Governance*. In book: Research and Advanced Technology for Digital Libraries. Springer International Publishing, September 2016.

[21] D. Proenca and J. Borbinha. Maturity Assessment of TOGAF ADM using Enterprise Architecture Model Analysis and Description Logics. In book: Advances in Enteprise Engineering XIII, 2020.

[22] D. Proenca and J. Borbinha. Maturity Models for Information Systems – A State of the Art. *Procedia Computer Science* 100, 1042-1049, 2016.

[23] T. Cooke-Davies and A. Arzymanowc. The maturity of project management in different industries: An investigation into variations between project management models. *International Journal of Project Management*, Vol. 21, No 6, pp. 471-478. 2003.

[24] M. Koshgoftar and O. Osman. Comparison between maturity models. *2nd IEEE International Conference on Computer Science and Information Technology*, Vol. 5, pp. 297-301. 2009.

[25] M. Wieczorek-Kosmala. Risk Management Practices from Risk Maturity Models Perspective. *J. for East European Management Studies* 19(2), 133-159, 2014.

[26] H.Y. Ching and T.M. Colombo. Enterprise Risk Management Good Practices and Proposal of Conceptual Framework. *J. of Management Research* 6(6/3), 69-85, 2015.

[27] E. Kerraous. A literature review of the factors that influence the adoption of an Enterprise Risk Management's process. *Revue Internationale des Sciences de Gestion* 6(3/1), 774-798, 2020.

[28] A.R. Ahlan, M. Lubis, A.R. Lubis. Information Security Awareness at the Knowledge-based Institution: Its Antecedennts and Measures. *Procedia Computer Science*. 72: 361-373, 2015.

[29] Y. Aleisa. Factors affecting implementation of enterprise risk management: an exploratory study among Saudi organizations. *J. of Economics, Business and Management* 6(1), 2018.

[30] A. Mikes and R. S. Kaplan. Towards a contingency theory of enterprise risk. *Working Paper* 13-063, Harvard Business School, 2014.

[31] S. Soltanizadeh, S.Z.A. Rasid, N. Golshan, F. Quoquab and R. Basiruddin. Enterprise Risk Management Practices Among Malaysian Firms. *Procedia – Social and Behavioral Sciences* 164, 2015.

[32] A.P. Liebenberg, and R.E. Hoyt. The determinants of enterprise risk management: Evidence from the appointment of chief risk officers. *Risk Management and Insurance Review*, 6(1), 37-52, 2003.

[33] M.S. Beasley, R. Clune and D.R. Hermanson. Enterprise risk management: An empirical analysis of factors associated with the extent of implementation. *Journal of Accounting and Public Policy*, 24(6), 521-531, 2005.

[34] M.M. Harner. *Barriers to effective risk management*. Seton Hall L. Rev., 40, 1323, 2010.

[35] M. Aleksandrova, N. Sergeeva, L. Zakharova, E. Okolelova and M. Shibaeva. Formation of a portfolio of innovation projects based on management of their life cycle parameters. *MATEC Web of Conf.* 265(80-1), 07033, 2019.

[36] S.M.S. Danish, M. Ahmadi, M.S.S. Danish, P. Mandal, A. Yona and T. Senjyu. A Coherent Strategy for Peak Load Shaving using Energy Storage Systems. *Journal of Energy Storage* 32, 101823, 2020.

[37] OECD. *Enterprise Risk Management Maturity Model*. Forum on Tax Administration, Model Series, 2021.

[38] N. Anderson. Risk Management Maturity Model. *White Paper*, Strategic Risk and Competence Team, 2017.

[39] CGMA. How to evaluate enterprise risk management maturity: case study. *White Paper*, 2012.

[40] B. Monda and M. Giorgino. An Enterprise Risk Management Maturity Model. *Munich Personal RePEc Archive* 45421, 2013.

[41] J. Miller. *A proven project portfolio management process*. Project Management Institute Annual Seminars & Symposium, 2002.

[42] R. Fauzi, S.H. Supangkat and M. Lubis. *The PDCA Cycle of ISO/IEC 27005:2008 Maturity Assessment Framework*. In book: User Science and Engineering, Springer, 2018.

[43] Rosmaini, E., Kusumasari, T.F., Lubis, M., Lubis, A.R.: Insights to develop privacy policyfor organization in Indonesia. J. Phys.: Conf. Ser.978(1), 012042, 2018.

[44] M. Lubis and A.H. Azizah. *Towards Achieving the Efficiency in Zakat Management System: Interaction Design for Optimization in Indonesia*. In book: User Science and Engineering, Springer, 2018.

[45] G. Elia and A. Margherita. Assessing the maturity of crowventuring for corporate entrepreneurship. Business Horizons 61(2), 271-283, 2018.

[46] M. Sokovic, D. Pavletic, K.K. Pipan. Quality Improvement Methodologies – PDCA Cycle, RADAR Matrix, DMAIC and DFSS. *Journal of Achievement in Materials and Manufacturing Engineering, vol. 43(1)*, pp. 476-483, 2010.

[47] The IACCM. Organizational Maturity in Business Risk Management. RM Working Group, 2003.

[48] R. Fauzi, S.H. Supangkat and M. Lubis. The PDCA Cycle of ISO/IEC 27005:2008 Maturity Assessment Framework. *Communications in Computer and Information Science*, 2018.

[49] T. Abram. The Hidden Values of IT Risk Management. *ISACA Journal, 2*, 2009.

[50] A.R. Ahlan, M. Lubis, A.R. Lubis. Information Security Awareness at the Knowledge-based Institution: Its Antecedennts and Measures. *Procedia Computer* Science. 72: 361-373, 2015.