IMPLEMENTATION OF RISK CONTROL SELF ASSESSMENTS USING RAPID APPLICATION DEVELOPMENT MODEL IN BANK OPERATIONAL RISK MANAGEMENT PROCESS

[1]AWAN SETIAWAN, [2]ERWIN YULIANTO

[1]Langlangbuana University, Department of Informatics, Bandung, Indonesia

[2]Langlangbuana University, Department of Informatics, Bandung, Indonesia

E-mail: [1]awans2425@gmail.com, [2]rwinyulianto@yahoo.com

ABSTRACT

Risk management is an important factor to run a bank business because of business growth and the increasing complexity of bank activities which of course is accompanied by the risk level faced by the bank. POJK no 18/POJK.03/2016 concerning about Application of Risk Management for Commercial Banks states "Banks must implement an internal control system effectively for the implementation of operational activities at all levels of the Bank's organization". In particular, the Basel II Capital Accord defines operational risk as the risk of losses arising from the failure or inadequate internal processes, human resources, systems, and external events that affect the bank's operations. In carrying out its business, banks offer financial services to the Bank will receive and manage various types of risks to be controlled effectively so they can avoid large losses. The Financial Services Authority Regulation (POJK) describes the definition of risk management as a series of methodologies and procedures used to identify, measure, monitor and control risks arising from all bank business activities. One important issue in the context of operational risk management is the need for assessment data carried out by the risk owner in managing daily banking operational risk, to facilitate data management related to risk mitigation so that similar events do not recur in the future. To achieve this, it is necessary to develop a system that manages assessment data sourced from the risk owner using tools called Risk Control Self Assessment. The Rapid Application Development (RAD) model is used to refer to adaptive software development approaches. RAD is very suitable to be used to develop software that is driven by the requirements of Graphical User Interface and a short time period.

Keywords: *Operational Risk Management, Risk Control Self Assessment, Rapid Application Development*

1. INTRODUCTION

The external and internal banking environment is currently facing stiff competition challenges, coupled with increasingly complex operational risks for business activities and bank services. The complexity of operational risk will automatically improve good corporate governance practices and risk management functions in the bank so that potential losses will not exceed the bank's ability and will not interfere with the bank's business continuity.

The Financial Services Authority Regulation No. 18/POJK.03/2016 concerning about Application of Risk Management for Commercial Banks states "Banks are required to implement an internal control system effectively for the implementation of business activities and operations at all levels of the Bank's organization". The application of risk management is needed because the Bank enters into a high-risk business. In carrying out its business, the Bank offers financial services to the Bank will receive and manage various types of risks to be controlled effectively so they can avoid large losses.

Some banking cases that have become phenomena from operational risk events include:

1. Melinda Dee was sentenced to eight years in prison for embezzling City Bank customer funds [2]
2. ATM "Skimming" crime and involvement of foreign nationals [10]
3. Collapse Rp. 75 billion, the red plate Islamic bank employee jailed for 8.5 years old [5]
4. The police assigned three employees of the UOB Bank as the burglary suspect of Rp. 21.6 billion [1]
5. BII ATMs are broken into tens of billions of rupiahs [3]

6. The story of rich customers instantly due to Bank mistakes [12]
7. Australia's largest bank is forced to reveal the loss a dozen millions of customer data [6]

One of the important issues in managing operational risk is the need for assessment data carried out by the risk owner in managing daily banking operational risk. The purpose of facilitating data management related to risk mitigation is that similar events do not recur in the future.

Management of each bank's functional activities must be integrated into an information system that is able to carry out an accurate and comprehensive risk management process. To achieve this, it is necessary to develop a system that manages assessment data sourced from the risk owner. Risk Management Division accommodates and facilitates using tools called Risk Control Self Assessment (RCSA) using Rapid Application Development (RAD) as a guide to the software development model.

Development of Risk Control Self Assessment tools is expected to minimize the risk events that occur with the presence of strong and effective risk mitigation from the risk owner in each working unit.

2. LITERATURE REVIEW

2.1 Theoretical Basis

The foundation of the theory is a set of concepts and definitions that have been systematically arranged including explaining variables and dimensions in research. The foundation of this theory will be a strong basis for supporting research.

2.1.1. Operational risk management

Risk Management is a series of methodologies and procedures used to identify, measure, monitor, and control risks arising from all business activities of the Bank. In general, banks in Indonesia have eight types of risks, namely credit risk, market risk, liquidity risk, operational risk, compliance risk, reputation risk, strategic risk, and legal risk. In this study, the discussion will focus on bank operational risk management[7].

Operational Risk is one of the risks that must be managed by the bank that occurs due to lack of and/or malfunctioning of human errors, internal processes, system failures, and/or the existence of external events that affect the Bank's operational activities and/or have an operational loss. Factors that cause operational risk can be seen in Figure 1 below.

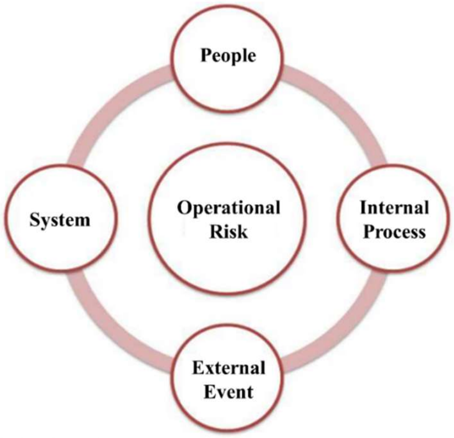


Figure 1: Factors Causing Operational Risk [16]

Banks are required to implement operational risk management effectively which includes at least the availability of operational risk management standard policies and procedures, setting operational risk limits, availability of identification, measurement, monitoring, and operational risk control processes, implementation of operational risk management information systems and comprehensive internal control systems. The implementation of operational risk management must be adjusted to the bank's vision and mission, bank's objectives, annual directors' general policies, the size and complexity of the business, and the Bank's capabilities.

According to Basel II, there are seven types of operational risk events at the first level as shown in figure 2.

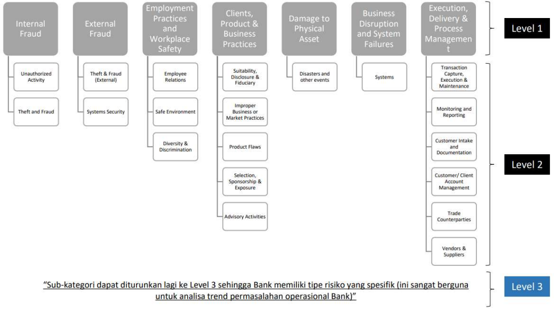

Internal Fraud
External Fraud
Employment Practices and Workplace Safety
Clients, Product & Business Practices
Damage to Physical Asset
Business Disruption and System Failures
Execution, Delivery & Process Managemen t
Level 1
Unauthorized Activity
Theft and Fraud
Theft & Fraud (External)
Systems Security
Employee Relations
Safe Environment
Diversity & Discrimination
Suitability, Disclosure & Fiduciary
Improper Business or Market Practices
Product Flaws
Selection, Sponsorship & Exposure
Advisory Activities
Disasters and other events
Systems
Transaction Capture, Execution & Maintenance
Monitoring and Reporting
Customer Intake and Documentation
Customer/ Client Account Management
Trade Counterparties
Vendors & Suppliers
Level 2
"Sub-kategori dapat diturunkan lagi ke Level 3 sehingga Bank memiliki tipe risiko yang spesifik (ini sangat berguna untuk analisa trend permasalahan operasional Bank)"
Level 3

Figure 2: Operational Risk Event Types [16]

Figure 1 and figure 2 taken from the white paper made by Prospero Consulting & Training explain four causes of bank operational risk. Furthermore, the seven types of operational risk management made by Prospero Consulting & Training are also grey literature related to and in line with the provisions of the regulator (in this case the Financial Services Authority / OJK).

The process of identifying, measuring, monitoring and controlling operational risk management must be supported by a timely operational risk management information system for policies and procedures including accurate and informative reports regarding financial conditions, performance of functional activities and bank risk exposures as well as realization of implementation of operational risk management compared to the target set [7].

The operational risk management framework and information system that will be developed can refer to figure 3 below.

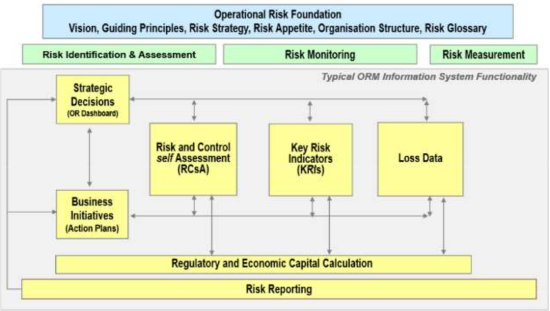

Operational Risk Foundation
Vision, Guiding Principles, Risk Strategy, Risk Appetite, Organisation Structure, Risk Glossary
Risk Identification & Assessment
Risk Monitoring
Risk Measurement
Typical ORM Information System Functionality
Strategic Decisions (OR Dashboard)
Risk and Control self Assessment (RCsA)
Key Risk Indicators (KRIs)
Loss Data
Business Initiatives (Action Plans)
Regulatory and Economic Capital Calculation
Risk Reporting

Figure 3: ORM Framework & Information System [16]

The figure 3 is a framework taken from the Prospero Consulting & Training working paper in developing Risk Control Self Assessment (RCSA) as a tool in identifying, measure, monitor, and control risks.

2.1.2. Risk control self-assessment

Risk Control Self Assessment (RCSA) is a qualitative and predictive operational risk management tool and is used to identify and measure operational risk by using the dimensions of impact and frequency of events. RCSA can be done through mapping processes, brainstorming sessions, surveys, and assessments from Special Matter Expertise (SME) or interviews. There is no best approach to implementing self-assessment. This depends on the circumstances and availability of resources in choosing the right approach. [16]

The risk assessment process is carried out by using a list of questions (checklist) of:

1. Evaluation of risk levels;
2. Events possibility;
3. The magnitude of the impact;
4. Control effectiveness level.

Some objectives with the application of RCSA include:

1. Become a helpful tool to understand risks that must be managed and controlled at all times in carrying out products / processes / business and operations activities.
2. Identify and detect operational risk sources which are the causes of irregularities/failures in carrying out functional activities and the adequacy of controls to prevent and detect irregularities/failures that occurred.
3. Measuring operational risk with a dimension of the possibility of occurrence frequency and magnitude of impact.
4. Implement operational risk controls to remain within acceptable levels of operational risk tolerance.
5. Improve risk awareness culture.
6. Monitor the risk control effectiveness level that has been carried out and determine the priority scale of corrective actions.
7. Become a communication media to improve the effectiveness of internal control functions and the continuity of business and operational effectiveness.
8. Provide input for management in making decisions and for internal audit in preparing audit plans.

The RCSA preparation method can be seen in the chart as shown in figure 4 below [16]:

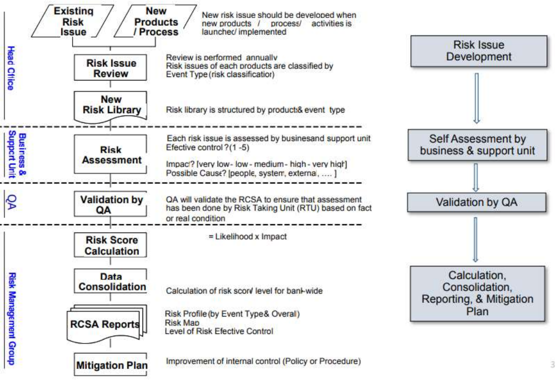

Existing Risk Issue
New Products / Process
New risk issue should be developed when new products / process/ activities is launched/ implemented
Head Office
Risk Issue Review
Review is performed annually
Risk issues of each products are classified by Event Type (risk classification)
New Risk Library
Risk library is structured by product& event type
Business & Support Unit
Risk Assessment
Each risk issue is assessed by businesand support unit
Efective control ?(1 -5)
Impact? [very low - low - medium - high - very high]
Possible Cause? [people, system, external, ...]
QA
Validation by QA
QA will validate the RCSA to ensure that assessment has been done by Risk Taking Unit (RTU) based on fact or real condition
Risk Management Group
Risk Score Calculation
= Likelihood x Impact
Data Consolidation
Calculation of risk score level for bank-wide
RCSA Reports
Risk Profile (by Event Type& Overall)
Risk Map
Level of Risk Efective Control
Mitigation Plan
Improvement of internal control (Policy or Procedure)
Risk Issue Development
Self Assessment by business & support unit
Validation by QA
Calculation, Consolidation, Reporting, & Mitigation Plan
3

Figure 4: Methodology of RCSA Compilation [16]

Based on the methodology above, we need to identify and measure the adequacy of operational controls. The operational risk control framework can be seen in table 1 below.

Table 1 Operational Control Framework [16]

Control Category	Control Nature	Control Type
a. Application System b. Policy & Procedure c. Physical Security d. Segregation of Duties e. Verification & Reconciliation f. Independent Review g. Insurance h. Human Resource i. Archives Management j. Communication k. Outsourcing & Vendor Management l. Monitoring, Reporting, & Escalation	a. Manual b. Semi-Automatic c. Automatic	a. Preventive b. Detective c. Corrective

A list of operational inherent risk issues is mapped into the risk library and operational risk control through control adequacy matrix to produce residual risk. Furthermore, the bank will make decisions related to the list of existing residual risk whether it will be accepted (risk acceptance), avoided (risk avoidance), transfer to other parties (risk transfer), or mitigate risk through improving control quality as a form of risk management.

The person in charge of risk is the highest working unit leader who evaluates RCSA and manages the risk exposures directly. The leader of the highest working unit must report the results of RCSA filling if the results of RCSA produce a moderate, moderate to high or high-risk issue/risk profile along with the action plan to the Risk Management Division of the Bank concerned.

Our literature gap is based on the provisions of the regulator and the working paper / White Paper compiled by Prospero Consulting & Training, namely :

1. Regulatory provisions (POJK) explain operational risk management and the factors that cause operational risk
2. Prospero Consulting & Training working paper / White Pape explains in more detail the types of operational risk events, Operationa Risk Management Framework & Information System, RCSA Compilation Methodology, and Operational Control Framework.

2.2 Research Gap

Phenomena that occur in banks in Indonesia such as City Bank, UOB Bank, BII, Red Plate Bank, and other banks such as embezzling customer funds, skimming, burglary suspect, ATM theft, bank mistakes, customer data loss, and so on occur due to lack of process identification, measurement, monitoring and risk control which is a challenge for banks in Indonesia. The proposed solution to answer this challenge is supported by several previous studies. To support this research, we have conducted a literature study of several scientific works as follows:

1. Martias (2016), revealed that the Risk Control Self Assessment can be applied and is useful for identifying risks and improving the business process of the company's management assisted by the role of internal auditors as a third line defense unit. The causes of operational risk were in addition to the negligence of Person in Charge (PIC) related to the implementation of duties but also due to the weak of dual control from other related parties. A large number of risk mitigation controls causes difficulties in testing all controls by internal parties and external audits so the RCSA tools become a good solution [13].
2. CRMS (2017), Risk and Control Self Assessment (RCSA) is a framework that can be used by banks to analyze bank individual risk profiles, especially those that are closely related to bank operations. RCSA can help provide a broad view of bank operational risks and help keep banks focused on achieving goals. Every risk owner must understand in depth about the Risk Control Assessment process and have the ability to be directly involved in the lower level business units/functional units[4].
3. Putro & Perdana (2013), information security management is closely related to digital data protection because the process of digital data preservation is applied by the company that has a clause of physical and environmental contained in ISO/IEC 27001 standards. The company has a high target in achieving the maturity level of information security management. Gap Analysis conducted on the information security management in the company found several findings that are still not in accordance with ISO/IEC 27001 standards, including

building security that has not been fully resistant to fire and vibration, and findings on the composition of cabling in companies that are still not neat, resulting in risk high against damage caused by users and other possibilities such as animals. This can increase the likelihood of losing data and information [17].

4. Institute of Operational Risk (2010), explains that individual findings from RCSA testing are very informative to help identify some areas that require control enhancement, risk concentration, controls duplication or other forms of excessive control and increase cross-functional risk awareness, through comparison of results across various functions [8].
5. Khan, et al (2014), said that apart from the internal losses event database, banks are encouraged to use other risk identification/monitoring tools such as Risk Control Self Assessment (RCSA). These tools not only add dimensions to the future but also help to capture risky causal relationships. RCSA is a process where potential material risk is identified and recorded together with controls related to inherent risk to produce residual risk with optimal risk mitigation. RCSA simulation aims to support banks in assessing the adequacy of bank operational risk management and the effectiveness of the risk control process. RCSA provides a better understanding of the bank about the business environment and internal controls[9].

2.3 Hypothesis

Based on the literature review and research gap discussed earlier, we formulated several hypotheses as follows:

1. Is the Risk Control Self Assessment (RCSA) application function as a tool in understanding the risks that must be measured, managed and controlled at all times in carrying out business processes and bank operations?
2. Can the users of the Risk Control Self Assessment (RCSA) be able to identify and detect sources of operational risk which are the causes of irregularities / failures in carrying out functional activities and ensure the adequacy of controls to prevent and detect irregularities that occur?
3. Is the application of Risk Control Self Assessment (RCSA) able to measure operational risk with the possibility of frequency dimensions and the magnitude of the impact that might occur while implementing operational risk controls to remain within the acceptable operational risk tolerance level?
4. Can the application of the Risk Control Self Assessment (RCSA) improve the risk awareness culture through monitoring the level of effectiveness of the risk controls that have been carried out and determining the priority scale of corrective actions?
5. Can the reports generated from the application of the Risk Control Self Assessment (RCSA) provide input for management to make audit planning decisions?

3. METHODOLOGY

3.1. Descriptive Method

According to Nazir (2013), a descriptive method is a method that aims to examine the status of an object, a group of people, a condition, a system of thought or a class of events in the present. The purpose of this descriptive research is to make illustrations systematically, descriptions visual, accurate facts, and characteristics and relationships between the phenomena investigated. The main characteristics of the descriptive method, among others[14] :

1. Focus on the problems that exist at the time the research is carried out or actual problems.
2. Describe the facts about the problem that was being investigated, accompanied by a balanced rational interpretation.
3. Provide an overview of phenomena including explain relationships, hypotheses testing, making predictions, and get the meaning and implications of a problem

Some of the activities carried out in this study are based on the techniques and tools used, as well as place and time, among others. [14]:

1. Survey research is an investigation that is held to obtain facts from existing symptoms and looks for information in fact, all about political, economic, social, technology, environment or from a group or a region.

2. Case study research is a study of research subject status that is pleasing to a specific or typical phase of the overall personality.
3. Library research is an activity to observing various literature that relates to the subject matter raised both in the form of books, papers or writings that are helpful so that they can serve as guidelines in the research process.
4. Work analysis and activity research is a study aimed at investigating in activities detail, humans work, and the research results can provide recommendations for the needs of the future.
5. Action research is research that focuses on the application of actions with the aim of improving the quality or solving problems in a group of subjects that studied and observed for the success level or the impact of actions.

Descriptive method stages in the research can be seen in the following figure 5.

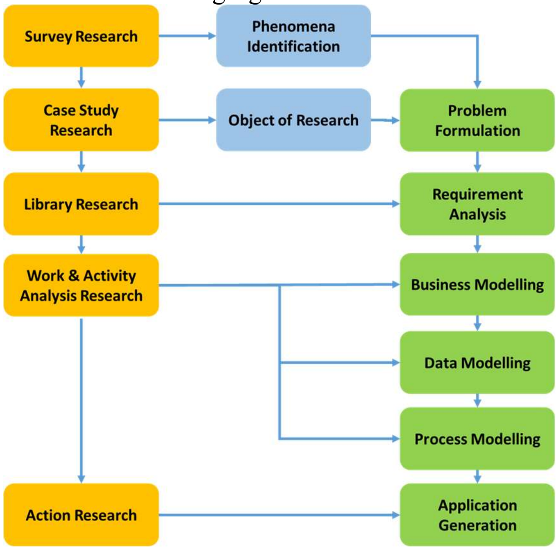


Figure 5: Stages of Descriptive Methods

This research emphasizes more on how to implement the basic concepts and frameworks that have been previously defined through software development as a tool. Research conducted focuses on the application of Risk Control Self Assessment through software development using Rapid Application Development method.

3.2. Rapid Application Development Model

The Rapid Application Development (RAD) model is a fast software development model wherein each component or function is developed in parallel as if they were a mini project. The development of each component and function is in a time box, sent and then assembled into a prototype that works well. This can quickly give customers something to see, to use and to provide feedback on user needs and requirements.

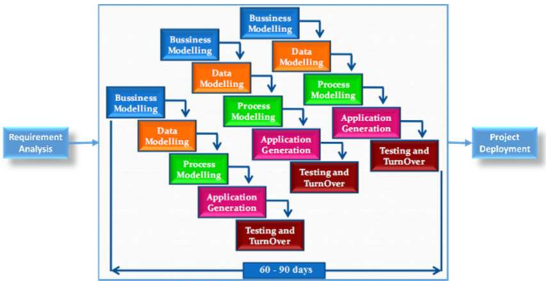


Figure 6: Rapid Application Development Model [15]

Rapid Application Development (RAD) model as seen in Figure 6 above has several phases, namely:

1. Business Modeling: Information flow is identified among various business functions.
2. Data Modeling: Information collected from business modeling is used to define data objects needed for business.
3. Process Modeling: Data objects defined in data modeling are converted to achieve business information flow to achieve certain business objectives. Descriptions are identified and CRUD is created for each data object.
4. Application Generation: An automatic tool that used to change a process model into a code in system/application.
5. Testing & Turnover: Testing new components and all interfaces.

Advantages of the RAD model:
1. Reducing development time.
2. Optimizing component reuse
3. Initial reviews can occur quickly
4. Encourage customer feedback
5. Integration carried out from the beginning solves many problems of integration.

Disadvantages of the RAD model:
1. Depends on the performance of the team and strong individuals to identify business requirements.
2. Only modular systems that can be made that can be built using the RAD model.
3. Requires highly skilled developers/designers.
4. High dependence on modeling skills.

5. It cannot be applied to cheaper projects because the cost of modeling and automated coding is very high.

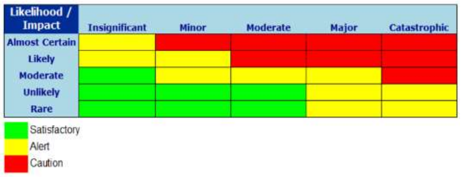
The RAD model can be used when there is a need to create a system that can be developed modularly within two to three months. The Software Development Life Cycle (SDLC) RAD model must be chosen only if resources with high business knowledge are available and there is a need to produce the system in a short span of time.

4. RESULT AND DISCUSSION

4.1. Business Modelling

Steps that must be taken in making a Risk Control Self Assessment (RCSA) modeling, namely:

1. Build an operational risk assessment matrix (frequency and impact), as shown in figure 7 below:



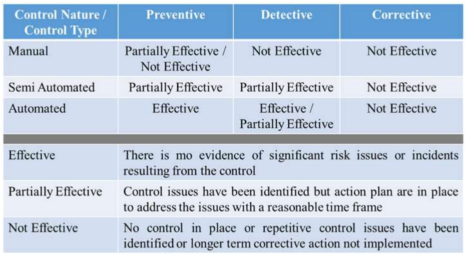
Likelihood / Impact	Insignificant	Minor	Moderate	Major	Catastrophic
Almost Certain	🟨	🟥	🟥	🟥	🟥
Likely	🟨	🟨	🟥	🟥	🟥
Moderate	🟩	🟨	🟨	🟨	🟥
Unlikely	🟩	🟩	🟩	🟨	🟨
Rare	🟩	🟩	🟩	🟨	🟨

🟩 Satisfactory
🟨 Alert
🟥 Caution

Likelihood	Description
Almost Certain	Likelihood of happening is more than once a week
Likely	Likelihood of happening is more than once a month
Moderate	Likelihood of happening is more than once a year
Unlikely	Likelihood of happening is one every one to five years
Rare	Likelihood of happening is one in more than five years

Figure 7: Preparation of Assessment Mapping

2. Assess the Inherent Risk through the Control Adequacy Matrix and Control Implementation Matrix as shown in Figure 8 below.



Control Nature / Control Type	Preventive	Detective	Corrective
Manual	Partially Effective / Not Effective	Not Effective	Not Effective
Semi Automated	Partially Effective	Partially Effective	Not Effective
Automated	Effective	Effective / Partially Effective	Not Effective

Effective	There is mo evidence of significant risk issues or incidents resulting from the control
Partially Effective	Control issues have been identified but action plan are in place to address the issues with a reasonable time frame
Not Effective	No control in place or repetitive control issues have been identified or longer term corrective action not implemented

Figure 8: Control Adequacy Matrix

3. Determine the control testing method in each working unit, as follows

   a. Testing controls for inherent risks with Moderate, Moderate to High, and High-rank level.
   b. Using a sampling method for a maximum of 10% or a maximum of 30 data samples from a total data population that has been determined scattered throughout the month.
   c. The same data sample can be used to test different controls.
   d. Perform the control testing steps in a simple, precise, and easy to follow, where if >= 10% of the selected data sample is found to be an error (for example 3 out of 30), then the control is considered a failure and needs to be evaluated.
   e. Make an action plan for each failed control as a control improvements evaluation.

The final results that are expected with the implementation of the Risk Control Self Assessment (RCSA), which is the improvement of risk consolidation after risk mitigation as shown in the following figure 9.

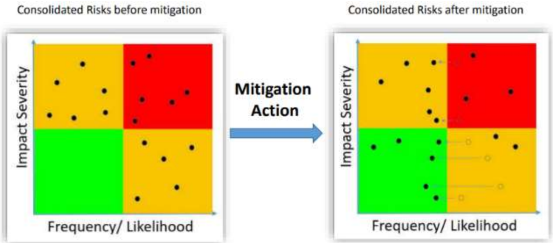


Figure 9: Consolidation Risk

Monitoring is carried out through a review of the trend rating per risk statement "High", "Medium to High" or "Moderate". Priority in improving the control is carried out on the risk statement which tends to deteriorate. Control is carried out by grouping risk statements that tend to deteriorate from the inherent risk rating group "High", "Medium to High", and "Moderate" then facilitating the Working Unit in developing an Action Plan to improve the control quality, determine the responsible party for the action plan, and set the implementation targets time.

In terms of reporting, each working unit needs to develop an operational risk profile approved by the Working Unit Leader and the person in charge of implementing RCSA. RCSA reports from each working unit are processed and used as data sources to understand the overall operational risk profile.

4.2. Data Modelling

In general, the data modeling architecture that will be implemented in the Integrated ORM Tools can be seen in Figure 10 below:

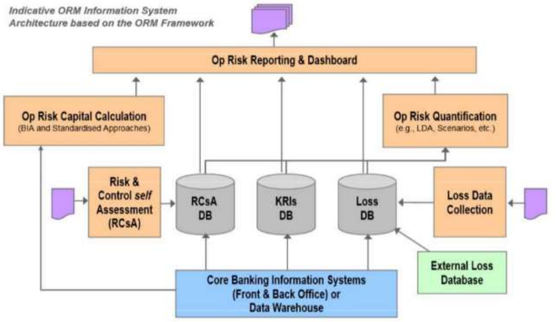

Indicative ORM Information System
Architecture based on the ORM Framework
Op Risk Reporting & Dashboard
Op Risk Capital Calculation
(BIA and Standardised Approaches)
Op Risk Quantification
(e.g., LDA, Scenarios, etc.)
Risk & Control self Assessment (RCsA)
RCsA DB
KRIs DB
Loss DB
Loss Data Collection
External Loss Database
Core Banking Information Systems
(Front & Back Office) or
Data Warehouse

Figure 10: ORM Information System Data Modeling Architecture

The explanation of Figure 10 above can be described as follows :

1. Loss Database records all loss data both from internal and external into loss data sets.
2. Every financial loss data is integrated with the core banking information system.

3. The Key Risk Indicator (KRI) database contains the parameters that cause the risk in the loss data set.
4. The Risk Control Self Assessment (RCSA) Database recaps all data from Loss Database and KRI Database related to the frequency and impact of operational risks.
5. Based on the RCSA database, self-assessment will be made regarding risk control over inherent risks that occurred (root cause) so the risk mitigation applied will be more optimal and resulting in a residual risk that can be accepted by the risk owner.
6. Each database generates operational risk reporting and dashboard as reporting to executive management, supervision, and evaluation at the internal risk owner, and centralizing measurement of inherent risk and risk control in the Bank's Risk Management Working Unit.

4.3. Process Modelling

Based on survey result of several banks in Indonesia, obtained results of a process modeling design consisting of the business process analysis results, use case diagram modeling and sitemaps design from the Risk Control Self Assessment application which will be implemented as tools of operational risk management on the Bank.

4.3.1. Business process analysis

The business processes flow in implementing RCSA can be seen in figure 11 below:

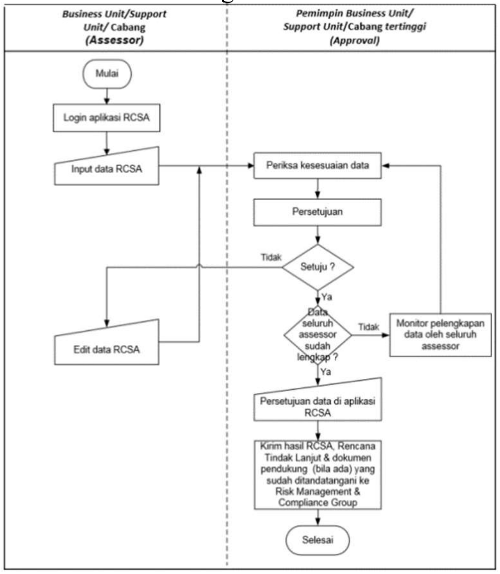

Business Unit/Support Unit/ Cabang (Assessor)
Pemimpin Business Unit/ Support Unit/Cabang tertinggi (Approval)
Mulai
Login aplikasi RCSA
Input data RCSA
Periksa kesesuaian data
Persetujuan
Tidak
Setuju ?
Ya
Edit data RCSA
Data seluruh assessor sudah lengkap ?
Tidak
Monitor pelengkapan data oleh seluruh assessor
Ya
Persetujuan data di aplikasi RCSA
Kirim hasil RCSA, Rencana Tindak Lanjut & dokumen pendukung (bila ada) yang sudah ditandatangani ke Risk Management & Compliance Group
Selesai

Figure 11: RCSA Implementation Process Business

4.3.2. Use case diagram

Mapping of business process analysis results and user requirement for the implementation of the Risk Control Self Assessment (RCSA) as a Bank operational risk management tool can be seen in the use case diagram as shown in figure 12 below.

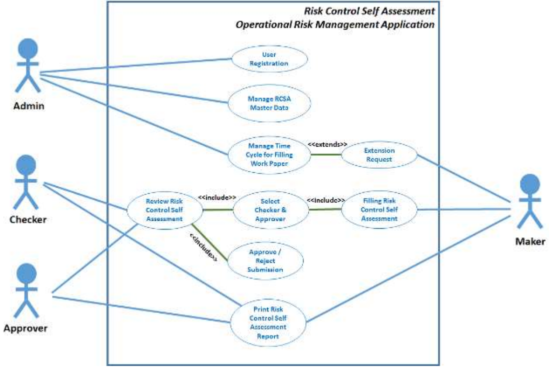

Risk Control Self Assessment
Operational Risk Management Application
Admin
Checker
Approver
Maker
User Registration
Manage RCSA Master Data
Manage Time Cycle for Filling Work Paper
<<extends>>
Extension Request
Review Risk Control Self Assessment
<<include>>
Select Checker & Approver
<<include>>
Filling Risk Control Self Assessment
<<include>>
Approve / Reject Submission
Print Risk Control Self Assessment Report

Figure 12 : Risk Control Self Assessment Use Case Diagram

4.3.3. Sitemap

The site map of the Risk Control Self Assessment (RCSA) Application that will be developed consists of two main modules, namely a special module for admin which in this case is a

Person In Charge (PIC) from the Risk Management Working Unit and a module for each Risk Owner. The module used by risk owner is managed by three PICs with the level of user: maker, checker, and approver. Following figure 13 is the site map design for two main modules referred to above along with the menus and sub-menus that are managed by them.

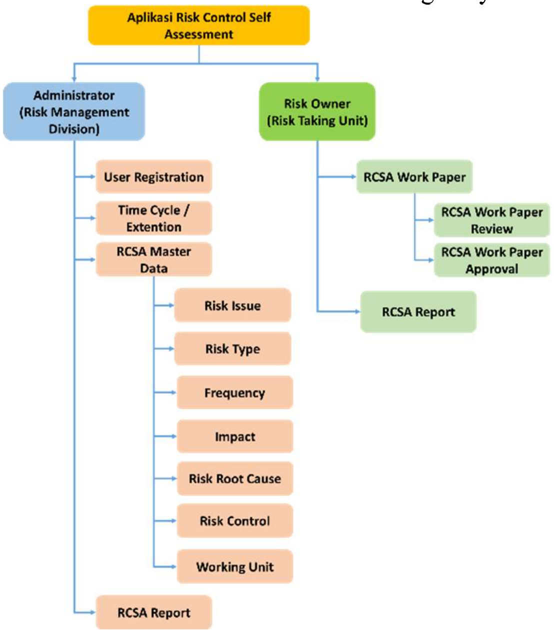


Figure 13 : Risk Control Self Assessment Application Sitemap

4.4. Application Generation

The Risk Control Self Assessment (RCSA) application is a web-based application system that becomes an operational risk measurement tool. Data contained in RCSA is used by banks to learn every event that results in operational losses in a bank so that the same event can be mitigated and is expected to not occur again at other times. In addition, with these data, the bank can measure how much the probability of an event can occur (risk event) and how much the effect of the losses incurred from the event (risk impact).

4.4.1. Database design

Database design that will be applied to the implementation of the Risk Control Self Assessment (RCSA) application can be seen in table 2 below.

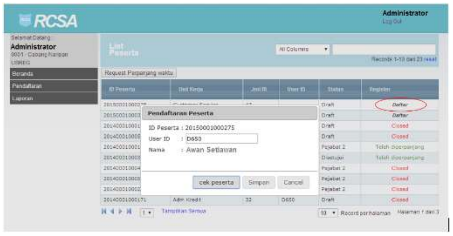
Table 2: RCSA Database Design

Table Name	Fields
TUser	**ID_User**, Username, ID_User_Type, Status
TUserType	**ID_UserType,** User_Type, Description, Status
TRiskIssue	**Risk_Code,** Risk_Issue, RiskType_Code, Risk_Owner, Status
TRiskType	**RiskType_Code,** Risk_Type, Description, Status
TImpact	**Impact_ID,** Impact_Parameter, Description, Value, Status
TImpactCriteria	**ImpactCri_ID,** ImpactCri_Parameter, Description, Impact_ID, Status
TFrequency	**Frequency_ID,** Freq_Parameter, Description, Value, Status
TFrequency Criteria	**FrequencyCri_ID,** FrequencyCri_Parameter, Description, Frequency_ID, Status
TRiskRootCause	**RiskCause_ID,** Description, Status
TRiskCause	**Risk_ID,** Description, RiskCause_ID, Status
TRiskControl	**Control_ID**, Description, Status
TRiskSolution	**Solution_ID,** Description, Control_ID, Status
TWorkingUnit	**Unit_ID**, Name, Description, Status
TTimeCycle	**Cycle_ID**, Start_Date, End_Date, Description, Status

4.4.2. Interface design

User Interface Design is a design for software applications, websites, simulation, and other forms of software that focus on user experience and interaction between users. Following is the interface design of the Risk Control Self Assessment (RCSA) Application and the explanation can be seen as follows:

1. Special module for Administrator
   a. User Registration Menu, a menu that serves to appoint users who will fill in self-assessments at the level of a maker, checker, or approver. This menu can be seen in Figure 14 below.



ID Peserta : 20150001000275
User ID : D650
Nama : Awan Setiawan

Figure 14: User Registration Menu Interface

b. Time Cycle/Extention Menu, the menu that functions to determines the period/time cycle of filling that has been determined by the Bank including providing an extension of time to the risk owner if there are special cases that require additional time. This menu can be seen in Figure 15 below.

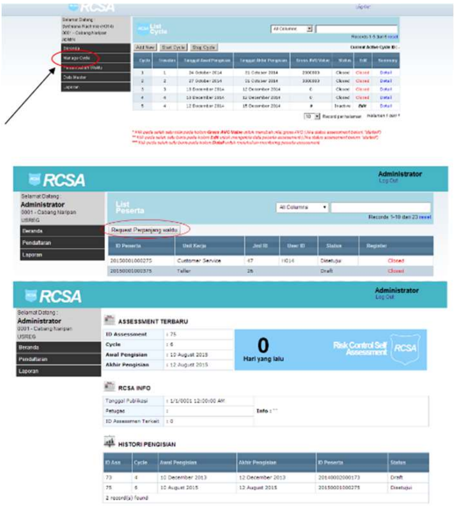


Figure 15: Time Cycle/Extention Menu Interface

c. RCSA Master Data Menu, a menu that functions specifically to manage parameters used in the Risk Control Self Assessment application developed. This menu can be seen in Figure 16 below.

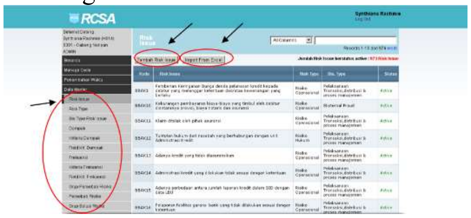


Figure 16: RCSA Master Data Menu Interface

In addition, to manage RCSA master data can be done manually, it can also be filled through the import from Excel feature, as shown in Figure 17 below.

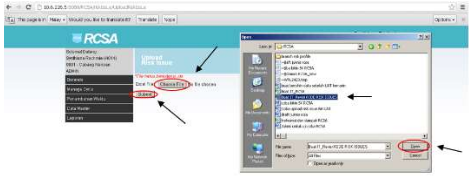
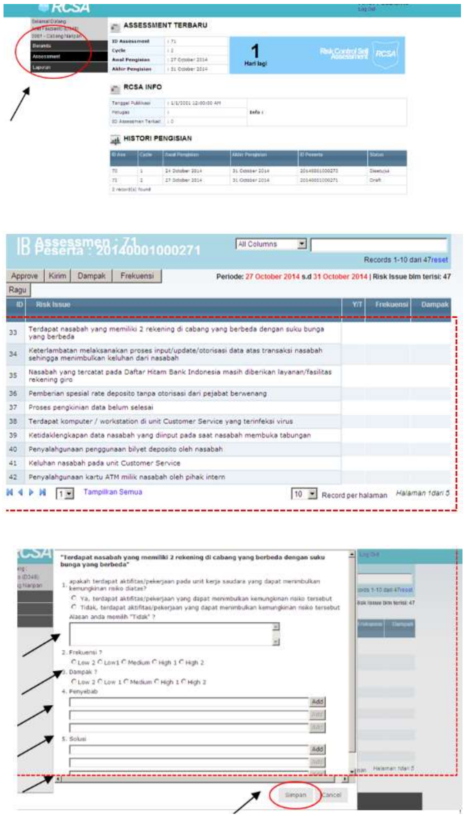


Figure 17: RCSA Master Data – Import From Excel Menu Interface

2. Module for Risk Owner

a. RCSA Work Paper Menu, the menu for fill up RCSA web worksheet while viewing information about the filling period and historical filling of the previous period. This menu can be seen in figure 18 below.



ID Assessmen : 71
ID Peserta : 20140001000271

Records 1-10 dari 47reset

Periode: 27 October 2014 s.d 31 October 2014 | Risk Issue blm terisi: 47

ID	Risk Issue	Y/T	Frekuensi	Dampak
33	Terdapat nasabah yang memiliki 2 rekening di cabang yang berbeda dengan suku bunga yang berbeda			
34	Keterlambatan melaksanakan proses input/update/otorisasi data atas transaksi nasabah sehingga menimbulkan keluhan dari nasabah			
35	Nasabah yang tercatat pada Daftar Hitam Bank Indonesia masih diberikan layanan/fasilitas rekening giro			
36	Pemberian spesial rate deposito tanpa otorisasi dari pejabat berwenang			
37	Proses pengkinian data belum selesai			
38	Terdapat komputer / workstation di unit Customer Service yang terinfeksi virus			
39	Ketidaklengkapan data nasabah yang diinput pada saat nasabah membuka tabungan			
40	Penyalahgunaan penggunaan bilyet deposito oleh nasabah			
41	Keluhan nasabah pada unit Customer Service			
42	Penyalahgunaan kartu ATM milik nasabah oleh pihak intern			

Halaman 1dari 5

"Terdapat nasabah yang memiliki 2 rekening di cabang yang berbeda dengan suku bunga yang berbeda"

1. apakah terdapat aktifitas/pekerjaan pada unit kerja saudara yang dapat menimbulkan kemungkinan risiko diatas?
○ Ya, terdapat aktifitas/pekerjaan yang dapat menimbulkan kemungkinan risiko tersebut
○ Tidak, terdapat aktifitas/pekerjaan yang dapat menimbulkan kemungkinan risiko tersebut
Alasan anda memilih "Tidak" ?

Figure 18: RCSA Work Paper Menu Interface

b. RCSA Maker Checker Approver Menu is an end to end process flow that starts when the maker performs the filling process, then checks by the checker, they are approved by the approver. This menu can be seen in figure 19 below.

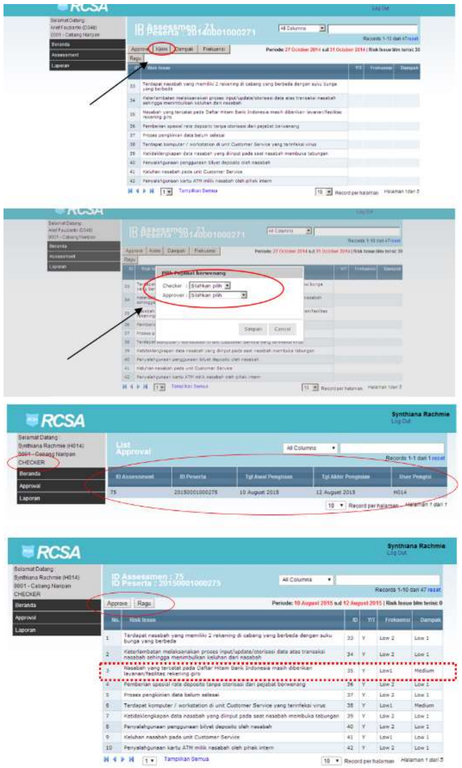


Figure 19: RCSA Maker Checker Approver Menu Interface

c. RCSA Report Menu, menu to see all assessments from Risk Owners during a particular filling period. This menu can be seen in figure 20 below.

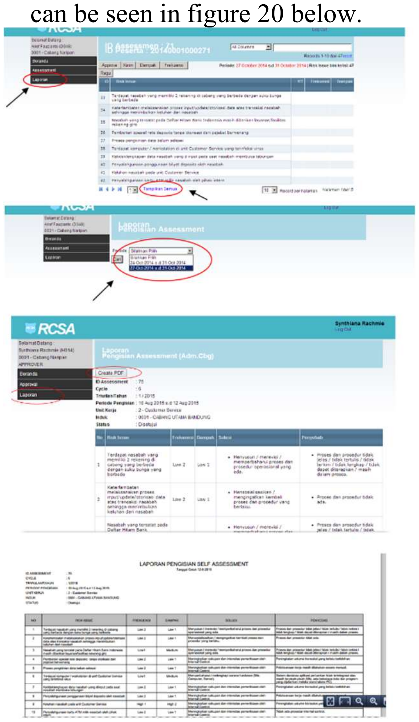


Figure 20: RCSA Report Menu Interface

d. RCSA Contingency Plan menu, this menu can be used if a system failure occurred such as a network that is not connected. Risk Owner can input RCSA using a manual method where the working paper can be downloaded from the application. The RCSA Contingency Plan menu display can be seen in the following picture 21.

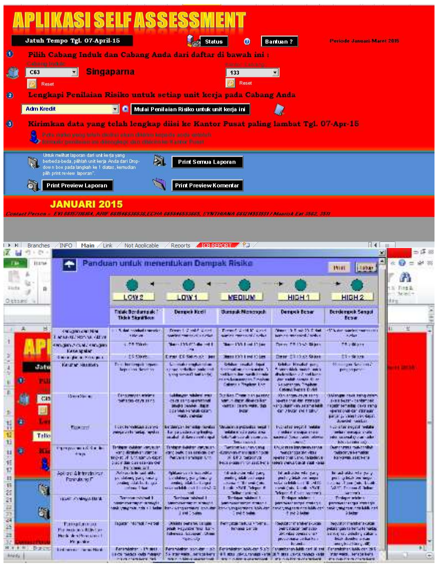


Figure 21: Contingency Plan Menu Interface

5. CONCLUSIONS AND SUGGESTIONS

5.1. Conclusions

Based on the results of the research conducted, the development of the Risk Control Self Assessment (RCSA) application was able to answer all the initial hypotheses as tools in the implementation of operational risk management in banking. The implementation by using Risk Control Self Assessment (RCSA) application as a tool in measuring risk control, conclusions obtained in the research include:

1. Implementation of Risk Control Self Assessment (RCSA) application can function as a helpful tool to understand risks that must be managed and controlled at all times in carrying out products/processes/business and operational activities.
2. Risk Control Self Assessment (RCSA) users can identify and detect the sources of operational risk which are the causes of irregularities/failures in carrying out functional activities and ensure the adequacy of controls to prevent and detect irregularities/failures that occur.

3. Risk Control Self Assessment (RCSA) can measure operational risk with dimensions of possible occurrence frequency and magnitude of impact while implementing operational risk controls to remain within acceptable levels of operational risk tolerance.
4. Improving the risk awareness culture through monitoring the level of risk control effectiveness that has been done and determining the priority scale of corrective actions.
5. Reporting that produced from the Risk Control Self Assessment (RCSA) application can provide input for management to making audit planning decisions.

5.2. Suggestions

Suggestions recommended in this research include:

1. Add other tools to identify, measure, monitor and control operational risks such as Loss Event Database and Key Risk Indicators.
2. Implementation of Risk Profile that includes eight types of risks managed by the bank, namely credit risk, market risk, liquidity risk, operational risk, compliance risk, reputation risk, legal risk, and strategic risk.

REFERENCES:

[1] Antara News, 2017, “Polisi Tetapkan Tiga Karyawan Bank UOB Tersangka Pembobolan Rp21,6 Miliar”, https://www.antaranews.com/berita/669661/polisi-tetapkan-tiga-karyawan-bank-uob-tersangka-pembobolan-rp216-miliar, 21/02/2019 16:35

[2] BBC News Indonesia, 2012, “Malinda Dee Divonis Delapan Tahun Penjara”, https://www.bbc.com/indonesia/berita_indonesia/2012/03/120307_vonismalinda, 21/02/2019 14:27

[3] Bisnis, 2014, “ATM BII Dibobol Puluhan Miliar Rupiah”, https://finansial.bisnis.com/read/20140510/90/226848/atm-bii-dibobol-puluhan-miliar-rupiah, 21/02/2019 16:37

[4] CRMS Indonesia, 2017, “RCSA (Risk Control Self Assessment)”, http://www2.crmsindonesia.org/programs/rcsa-risk-control-self-assessment, 25/02/2019 13:01

[5] Detik, 2017, “Bobol Rp 75 M, Pegawai Bank Syariah Pelat Merah Dibui 8,5 Tahun”, https://news.detik.com/berita/d-3643089/bobol-rp-75-m-pegawai-bank-syariah-pelat-merah-dibui-85-tahun, 21/02/2019 14:40

[6] Epoch Times Indonesia, 2018, “Bank Terbesar Australia Dipaksa Mengungkap Hilangnya Belasan Juta Data Nasabah”, https://epochtimes.id/2018/05/03/bank-terbesar-australia-dipaksa-mengungkap-hilangnya-belasan-juta-data-nasabah/, 21/02/2019 16:31

[7] Hadad, Muliawan D, 2016, “Peraturan Otoritas Jasa Keuangan Nomor 18/POJK.03/16 Tentang Penerapan Manajemen Risiko Bagi Bank Umum”, Otoritas Jasa Keuangan, Jakarta, Indonesia

[8] Institute of Operational Risk, 2010, “Operational Risk Sound Practice Guidance: Risk Control Self Assessment”, United Kingdom

[9] Khan, Muhammad A, et all, 2014, “Implementation of Operational Risk Management Framework”, State Bank of Pakistan

[10] Kompas, 2018, “Kejahatan "Skimming" ATM dan Keterlibatan Warga Negara Asing”, https://megapolitan.kompas.com/read/2018/03/20/10055211/kejahatan-skimming-atm-dan-keterlibatan-warga-negara-asing, 21/02/2019 14:34

[12] Liputan6, 2018, “Kisah Nasabah Kaya Sekejap Gara-Gara Kesalahan Bank”, https://www.liputan6.com/bisnis/read/2456547/kisah-nasabah-kaya-sekejap-gara-gara-kesalahan-bank, 21/02/2019, 16:39

[13] Martias, Andi, 2016, “Analisa Penerapan Control Self Assessment Sebagai Aplikasi Pengendalian Intern Pada PT. ABC Insurance”, Moneter, Vol. III, No. 1, pp. 1 – 13

[14] Nazir, Moh., 2013, “Metode Penelitian”, Ghalia Indonesia, Bogor

[15] Pressman, Roger S, 2001, “Software Engineering, A Practitioner’s Approach”, 5th Edition, McGraw-Hill, New York

[16] Prospero Consulting & Training, 2018, “Perancangan Perangkat Kerja Risiko Operasional RCSA – Risk Control Self Assessment”, Jakarta, Indonesia

[17] Putro, Bramantiyo E & Perdana, Ilham, 2013, “Analisa Control Self Assessment Audit Pada Klausul A.5 Security PPLICY Hingga Klausul A.9 Physical and Environmental Security Telkom Flexi Kebon Sirih Jakarta Pusat Menggunakan ISO/IEC 27001”, Telkom University, Bandung