UNIVERSITAS INDONESIA

EVALUATION OF BUSINESS CONTINUITY PLAN BASED ON COMPANY MAIN RISK SOURCES: CASE STUDY IN PT JAMSOSTEK (PERSERO)

THESIS

RUTH BEATRIX YORDAN
0906586133

FACULTY OF ECONOMICS
MASTER OF MANAGEMENT –
MASTER OF BUSINESS ADMINISTRATION
JAKARTA
JUNE 2011

UNIVERSITAS INDONESIA

EVALUATION OF BUSINESS CONTINUITY PLAN BASED ON COMPANY MAIN RISK SOURCES: CASE STUDY IN PT JAMSOSTEK (Persero)

THESIS

**Presented as partial fulfilment of the requirement
to obtain the degree of
Master in Business Administration**

**RUTH BEATRIX YORDAN
0906586133**

**FACULTY OF ECONOMICS
MASTER OF MANAGEMENT –
MASTER OF BUSINESS ADMINISTRATION
CONCENTRATION RISK MANAGEMENT
JAKARTA
JUNE 2011**

HALAMAN PERNYATAAN ORISINALITAS

Tesis ini adalah hasil karya saya sendiri, dan semua sumber baik yang dikutip maupun dirujuk telah saya nyatakan dengan benar.

Nama : Ruth Beatrix Yordan

NPM : 0906586133

Tanda Tangan : . . . .

Tanggal :28 Juni 2011

HALAMAN PENGESAHAN

Tesis ini diajukan oleh:

Nama	:	Ruth Beatrix Yordan
NPM	:	0906586133
Program Studi	:	Magister Manajemen – Magister Administrasi Bisnis
Judul Tesis	:	Evaluation of Business Continuity Plan Based on Company Main Risk Sources: Case Study in PT Jamsostek (Persero)

Telah berhasil dipertahankan di hadapan Dewan Penguji dan diterima sebagai bagian persyaratan yang diperlukan untuk memperoleh gelar sebagai Magister Manajemen – Magister Bisnis Administrasi pada Program Studi Manajemen Fakultas Ekonomi, Universitas Indonesia.

DEWAN PENGUJI

Pembimbing:	Dr. Dewi Hanggraeni	( )
Penguji:	Dr. Tengku Ezni Balqiah	( )
Penguji:	Rofikoh Rokhim, Ph.D	( )

Ditetapkan di:	Jakarta
Tanggal:	28 Juni 2011

PREFACE

Thanks to God Almighty and praise for His mercy and blessing that I am able to finish this thesis to fulfilled one of the requirements to gain the title of Magister Manajemen and Master Business Administration in Universitas Indonesia.

The writing of this thesis is not free from obstacles and barriers. Without helps and supports from all related parties, this writing will never be accomplished. I am highly thankful to:

1. Professor Rhenald Kasali, Ph.d as Head of Study Program of Magister Manajemen of Universitas Indonesia.
2. Dr. Dewi Hanggraeni as the thesis advisor for her constant support, supervision, and assistance for the duration of my thesis.
3. Mr. Hotbonar Sinaga as president director of PT Jamsostek (Persero) who gave chance to do research observation.
4. Mr. Teguh Purwanto, Mrs. Murti Djayanti, Mrs. Deva, and Risk Management Team of PT Jamsostek for the help, time allocation, and support of this thesis.
5. My beloved parents for the support and prayer.
6. My beloved husband for the consistently help and support from the beginning up until the completion of thesis.
7. The joy of my life that always become the source of strength, my daughters Rebecca and Reina.

Cibubur, June 2011,

The author

HALAMAN PERNYATAAN PERSETUJUAN
PUBLIKASI KARYA ILMIAH

Sebagai civitas akademik Universitas Indonesia, saya yang bertandatangan di bawah ini:

Nama : Ruth Beatrix Yordan
NPM : 0906586133
Program Studi : Magister Manajemen – Magister Administrasi Bisnis
Fakultas : Ekonomi
Jenis Karya : Tesis

Demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada Universitas Indonesia **Hak Bebas Royalti Non-eksklusif** (*Non-exclusive Royalti Free Right*) atas karya ilmiah saya yang berjudul:

EVALUATION of BUSINESS CONTINUITY PLAN BASED ON COMPANY MAIN RISK SOURCES: CASE STUDY in PT JAMSOSTEK (PERSERO).

beserta perangkat yang ada (jika diperlukan). Dengan hak bebas royalty noneksklusif ini Universitas Indonesia berhak menyimpan, mengalihmedia/formatkan, mengelola dalam bentuk pangkalan data (*database*), merawat, dan mempublikasikan tugas akhir saya selama tetap mencantumkan nama saya sebagai penulis/pencipta sebagai pemilik Hak Cipta.

Demikian pernyataan ini saya buat dengan sebenar-benarnya

Dibuat di : Jakarta
Pada tanggal :28 Juni 2011
Yang menyatakan

(Ruth Beatrix Yordan)

ABSTRACT

Name : Ruth Beatrix Yordan
Program Study : Master of Management – Master of Business Administration
Title : Evaluation of Business Continuity Plan Based on Company Main Risk Sources Case Study in PT Jamsostek (Persero).

This thesis intended to perform the evaluation of main risk sources in current Business Continuity Plan (BCP) in PT Jamsostek (Persero) and compare this BCP with the BCP model to have an effective BCP for PT Jamsostek (Persero). The BCP model itself is created based on some expert theories about BCP and implementation of BCP best practices. The analysis result is obtained in the form of gap between the current BCP and BCP. There are many parameters that need to be improved in the BCP of PT Jamsostek (Persero), starting from BCP revision, risk assessment, risk response, control activities, monitoring, information and communication.

Keywords: Business Continuity Plan (BCP), BCP model, risk assessment.

ABSTRAK

Nama : Ruth Beatrix Yordan
Program Studi : Magister Manajemen – Magister Bisnis Administrasi
Judul : Evaluasi terhadap Perencanaan Kelangsungan Bisnis Berdasarkan Potensi Resiko Utama Studi Kasus pada PT Jamsostek (Persero)

Tesis ini bertujuan untuk melakukan evaluasi terhadap potensi resiko utama pada perencanaan kelangsungan bisnis (Business Continuity Plan (BCP)) yang sudah diterapkan di PT Jamsostek (Persero) dan membandingkan BCP tersebut dengan model BCP sehingga terbentuknya BCP yang efektif untuk PT Jamsostek (Persero). Model BCP tersebut dibentuk berdasarkan teori dari beberapa pakar mengenai BCP dan implementasi terbaik dari BCP yang pernah ada. Analisa yang dilakukan menghasilkan suatu kesenjangan antara BCP saat ini dan model BCP. Ditemukan beberapa parameter yang harus ditingkatkan pada BCP dari PT Jamsostek (Persero), dimulai dari revisi BCP, *risk assessment*, respons terhadap resiko, *control activities*, pengawasan, informasi dan komunikasi.

Kata kunci : Perencanaan Kelangsungan Bisnis (BCP), model BCP, *risk assessment*.

TABLE OF CONTENT

LIST OF FIGURES

LIST OF TABLES

CHAPTER 1
INTRODUCTION

1.1 Thesis Background

In driving the business operation, it is an important matter for a company to prepare itself in facing threats or negative warning indications which can affect the business process. These threats or negative warning indications can turn up to become unavoidable casualty that could impact a lot on financial losses, fraudulence, company reputation, and morbidity losses for business operations such as activities, products and services. Besides, the board of director will become more accountable for losses if they did not take appropriate action to prevent stakeholder's losses. (Momani, 2010)

There are many risk sources that could damage businesses operations which in the end will cause a lot of financial losses. The risk sources can take the form of technology, people, process, and natural disaster. These are possible to have immediate impact to business risk, crime risk, disaster risk, informational technology risk, reputational risk, and system risk loss (Momani, 2010).

Technology could fail due to several reasons whether accidentally or purposely which cause delay and disruption to business process, activities, and product. For instance, the failure of system application in investment division will be reflected in investment optimization. The failure of security access or the low level of security access will also be reflected to incorrect report. Related to people, failure of user accessibility can lead to fraud. This error will lead to crisis of trustworthy. As another example, incorrect customer's claim status will cause incorrect balance statement and there will be a possibility of overstated in financial statement. Fire or damage can cause the loss of important documents and back up program such as in-house development of investment system.

Beside financial losses, there is another issue which can be categorized as a critical one: reputation issue. (Momani, 2010). This issue can drop down the CEO of a company and can also serve as a competitive advantage for competitor. The *Business Continuity Plan* (BCP) will help an organization to manage the disruption so that the business process can resume operation as soon as possible. (Broder, 2006). BCP is mostly implemented in banking indusry, but it is also important for non-banking institutions. According to the official website of Ministry of State Enterprises, www.bumn.go.id (accessed on May, 05 2011 at 08:30 pm), PT Jamsostek (Persero) as one of the biggest non-banking institutions in Indonesia commands the total assets reaching to around 94.5 trillions rupiahs in August 2010. As stated by the company's CEO, 90% of the total assets are in the form of investment funds. Thus, PT Jamsostek (Persero) needs a BCP to support and to protect the business continuity.

PT Jamsostek (Persero) is a state-owned enterprise with the task to administer employees' social security. It has successfully proven its commitment as a business partner in providing workers with protection towards possible socio-economical risk. PT Jamsostek (Persero) was founded based on the government's noble vision to improve people's welfare through the development of the workforce sector, the role of workforce are increasingly vital to support the national development. The increase in the role is followed by the increase in challenges and risks accompanied with it.

Based on Jamsostek's Corporate Risk Profile there are two critical functions of PT Jamsostek (Persero) which are ensuring service to the employee customers and maintaining customer's fund through investments. These are related to company reputation. Related to these functions, there are unavoidable casualties that may happen. They can be in the form of internal factors, such as the disconnection of network system from data center. As example, while the customers service must be ready from 8 o'clock in the morning, the failure mentioned above cause the service to be ready only after 12 o'clock noon. Thus, the service to the customers is negatively impacted. The unavoidable casualties may also take the form of external factors such as flood. In the past, due to flood, water overflew the place where the electricity generator was placed. The generator exploded and the electricity is shut down for several hours. This incident hampered PT Jamsostek (Persero) from carrying out its critical functions.

The risk factors mentioned above are the most contributors to business disruption and require effective business continuity plan in order to minimize business's losses. Based on the information obtained from Jamsostek official website www.jamsostek.co.id (accessed on May, 03 2011 at 09:15 pm). The number of active and passive memberships of PT Jamsostek (Persero) as of October 2010 is around 36,000,000. The total of one-year-period installments as per 30 September 2010 amounts 2.052 trillions rupiahs. Due to the number of participating companies, the service process to the members takes a significant role. To support the service process, the author conducted a research about the BCP in PT Jamsostek (Persero) so that a right BCP can be implemented in the company.

1.2 Problem Statements

Business continuity plan (BCP) is proven to be essential in the life of a company, and thus requires a special consideration. As cited from Mitroff and. Pearson. (1992), in a book titled "Crisis Management and Strategic Management: Similarities, Differences, and Challenges", crisis management should take a strategic role within organizations and top managements should give resources and priorities to save lives and property. Doughty (2000) stated BCP must be an integrated part of organization's change in management processes, life cycle of system development, corporate planning cycle. According to Doughty (2000), BCP must be an integrated part of organization's change in management processes, life cycle of system development, corporate planning cycle.

The implementation of BCP in the whole of PT Jamsostek (Persero) was started in 2010. Prior to 2010, the core principal of BCP was already implemented in some divisions such as technology division. The implemented BCP helps all participating divisions in PT Jamsostek (Persero) to be able to integrate preliminary actions before or when the unavoidable casualties or disaster happened or soon after it is happened.

The BCP also helps to measure the level of a critical condition due to unavoidable casualties or disasters that may impact the company's job function. In the meantime, there are several important things related to the BCP implementation in PT Jamsostek (Persero) which needed to be improved. Firstly, the awareness of the importance of BCP is acknowledged in technology division and risk management division only. Secondly, supporting documentation that contains detailed specification and standard operating procedure which should be embedded to the BCP is not created yet. Thirdly, throughout the infrastructure of PT Jamsostek (Persero), the routine testing for precondition for the eventual occurrence of unavoidable casualties or disaster is still not being implemented yet.

In the research reported by this thesis, the following questions that will be given in-depth discussion and sought for answers:

1. What is the condition and overall picture of the current BCP in PT Jamsostek (Persero)?
2. After knowing the current situation, find the gap between the current BCP and the effective BCP. What improvements can be made so that PT Jamsostek (Persero) can have an effective BCP?

1.3 Thesis Objectives

The objectives of this thesis can be listed as follows:

1. Obtaining the current condition and overall picture of the BCP in PT Jamsostek (Persero).
2. Analyzing the gap between the current BCP with the effective BCP for PT Jamsostek (Persero) and finding the improvement that can be made so that PT Jamsostek (Persero) can have an effective BCP.

1.4 Thesis Benefits

The points mentioned in Section 1.2 convey a picture that BCP must protect the process continuity while keep adapting itself in accordance to the changes in the company and the business objectives of the company. If a company possesses an effective BCP, then there are several achievements obtained by the company, such as:

- The company will be able to identify the scope of the critical services to be provided, define the minimum acceptable levels of service or outputs for each business process and establish time-frames in which the services should be resumed.
- The company has prepared well to mitigate its losses and consequently reduce the potential cost of an insurance claim. This will be attractive to insurance brokers so that they can offer attractive premium.
- The company has a major selling point to customer, because BCP can help enhancing customer service level. This will differentiate the company from the competitors. For example, PT Jamsostek (Persero) already launched "SIPT online" which is beneficial for the company's employee members. The members can easily access the information they need and the claim procedure can be initiated in any branch. It will be a benefit to PT Jamsostek (Persero) if the employee members know that it is already well prepared for the business continuity plan by doing well thought out and rehearsed in terms of plans that will protect the business of "SIPT online."

More benefit can also be mentioned to be obtained by the State Ministry of State Enterprises (*Kementerian Negara BUMN*) as the super ordinate of PT Jamsostek (Persero), which are:

- By providing an integrated service, PT Jamsostek (Persero) will be well prepared to mitigate the business process and to minimize the potential risk by establishing an effective BCP. This will eventually be reflected by the increase of PT Jamsostek (Persero)'s employee member.

- The resulting improved BCP which is applied in PT Jamsostek (Persero) can become a standard to others state enterprises under the ministry.

For the future research, the benefits that can be given by this thesis are:

- Contribution to the further development and improvement so that the BCP in PT Jamsostek (Persero) can be analyzed and effectively implemented to its perfection.
- Accurate overview of how the main risk sources in a company can be identified and how the minimum acceptable levels of each potential risk for each business process can be determined.
- An approach of how to establish time-frames for the company so that it will be able to measure the effectiveness of BCP.

1.5 Thesis Scope and Limitations

In doing the analysis in this thesis, there are some limitations:

1. The topic discussed will focus only for BCP in the head office of PT Jamsostek (Persero) and a handful number of company branches around Jakarta.
2. The risk assessments that are conducted will cover the enterprise risk management which specifically limited to the operational risk, technological risk, and reputational risk of BCP owned by PT Jamsostek (Persero).

1.6 Research Operational Model

1.6.1 Research methodology

This thesis utilizes descriptive qualitative and quantitative research method. Data collection is conducted through literature study on risk management, enterprise risk management, business continuity management, business continuity plan, operational risk management, business continuity plan. The type of the research used in this thesis is case study. The research instruments used by the researcher to obtain primary data in this thesis are questionnaire and interview.

1.6.2 Reasoning frame

There are some points highlighted in designing flow process to produce an effective BCP:

- In designing an effective BCP, an in-depth analysis about the main risk sources of the company must be undertook.
- This thesis will seek the business impact analysis to identify different kinds of risks related to business continuity of PT Jamsostek (Persero). The risk analysis will be checked based on enterprise risk management approach which includes the operational risk, technology risk and reputational risk.
- Furthermore, the result of risk analysis will be checked against the corporate risk profile of PT Jamsostek (Persero) on the purpose to highlight the critical risk. The model of BCP will be created based on expert theories and guidance based on enterprise risk management, business continuity management, and business continuity planning.
- Based on the research, the effective BCP will be pictured and compared to the current BCP which is already being implemented by PT Jamsostek (Pers ero).

The research will be conducted based on the followings:

1. Literature Study. Using this method, relevant theoretical frame will be advised. This will be used to analyze and evaluate the problem to be discussed. Thus, it is expected that the field data research will be focused to fulfill the need of the research. Therefore, and overview about the structure and the direction of the research can be obtained.

2. *Field research*. This will be done by performing a related study case in PT Jamsostek (Persero), by doing observations, interviews with competent parties who directly in touch with daily company operations.

3. *Design Proposal*. This thesis will propose the improvement process by designing the effective BCP which cover the whole risk assessment from identification up to the monitoring process toward the current BCP as the result of main risk source analysis that may directly impact the business planning of PT Jamsostek (Persero).

1.7 Thesis Originality

Table 1.1 Similar research ever conducted by other researchers

Title	Name of Researchers	Research Description	Research Methodology
Business Continuity Planning: Are We Prepared for Future Disasters (Journal)	Momani, (2010)	In this study, major risk factors related to business disruption and strategies to prevent losses were discussed	The analysis is done by using qualitative methodology
Business Continuity Planning: A Risk Manager's Agenda for Operational and Credit Risk Management (Journal)	Lanz (2002)	In this study, identification of risk manager action concerning about strengthen their business continuity strategies	The analysis used qualitative methodology
Develop Business Continuity Plan in Bumiputera (Thesis)	Wardhana (2005)	This thesis contains improvement of current Bumiputera BCP	The analysis is based on case study within the qualitative perspective
Business Continuity in the Pharmaceutical Industry	Stohr& Rohmeyer (2004)	This thesis contains evaluation model for business continuity and disaster Recovery in the pharmaceutical company	The analysis is based on case study within the qualitative perspective

(to be continued)

Table 1.1 Similar research ever conducted by other researchers (continued)

Title	Name of Researchers	Research Description	Research Methodology
A Disaster Recovery Planning Guide (Thesis)	Hellman & Karlsson, (2008)	This thesis contains disaster recovery planning guide to ensure the continuity of critical activities when disruption comes	The analysis is based on case study within the qualitative perspective

Sources: Researcher’s Journal and papers

The factors that differentiate this thesis from other researches are:

1. *Object of research*. This thesis presents the case study conducted in PT Jamsostek (Persero). It is chosen because the company is one of the largest non-banking finance institutions and the one and only employee protection institution under the Ministry of State Enterprises.
2. *Instrument of research*. This research uses in-depth interview as one of the tools. This tool will be check using *Spearman’s Rho* coorelation.on the theme coorelation and respondent coorelation.
3. *Point of emphasis*. This thesis will check the effectiveness of BCP in PT Jamsostek (Persero) especially in critical divisions and also the supporting division based on risk analysis related to enterprise risk management and business continuity management. Afterwards, the BCP model is created and compared with BCP PT Jamsostek then find the improvements to mitigate the risk.

1.8 Thesis Outline

The thesis consists of six chapters and is outlined as follows:

Chapter 1: Introduction. This chapter consists of thesis background, problem statement, thesis objectives, thesis benefits, thesis scope and limitations, thesis methodology, thesis originality, and completed by thesis outline.

Chapter 2: Theoretical Background. In this chapter, fundamental theories on enterprise risk management, operational risk, and business continuity strategies will be presented. Furthermore, qualitative methodology as the logical mindset of the thesis will be introduced.

Chapter 3: Research Methodology. This chapter will point out the types of research, research models, research stages, data mining methodology, and the used method of analysis.

Chapter 4: Company Profile of PT Jamsostek (Persero). This chapter contains the founding and the history, the vision and mission, core value, and organizational structure of PT Jamsostek (Persero). Besides, the business activity and risk management, as well as the BCP in the company will be presented.

Chapter 5: Analysis and Discussion: This chapter describes the analysis done to the data, based on the prescribed research stages. Also, the discussion on the result will be presented. The solution that will cope with the problem statements will be written, based on the theory already mentioned in Chapter 2.

Chapter 6: Conclusions and Suggestions. This chapter will mention in detail the conclusions obtained during the whole research process. The conclusion will also be based on the analysis undertook upon the problem statement. Some suggestion related with the implementation of BCP in PT Jamsostek (Persero) will be mentioned, with the hope that PT Jamsostek (Persero) will have an effective BCP.

CHAPTER 2
THEORETICAL BACKGROUND

2.1 Risk

The International Organization for Standardizations' (ISO/IEC) defines risk as: *the combination of the probability of an event (a set of circumstances) and its consequences (*ISO/IEC, 2002: 9). An event can have several consequences, both of positive and negative nature (ISO/IEC, 2002).

Hamilton (1996: 21) has another approach to risk applied to the corporate world: "*Risk is the danger of a random event negatively affecting the ability to achieve an objective*".

2.2 Risk Management

There are three steps contain in the risk management process such as risk analysis, risk evaluation and risk reduction/control, see Figure 2.1. Determining the scope of analysis is the first step in the risk analysis. After this, an identification of all potential hazards takes place. There are many risk analysis methods available that can be used in the identification phase and which to choose depends on the circumstances and the resources available. An evaluation of the probability and impact for each risk then takes place. This probability represents the possibility that a given occurrence will occur, while impact represents its effect if it occurs (IEC, 1995).

In the second step of the process, the risk evaluation, a judgment whether the risk is acceptable or not, shall be made. The risks which need to be concern on is risk which are not acceptable, this will become target for an option analysis. In the other hand risk-reducing options are investigated and compared. The risk analysis together with the risk evaluation represents the risk assessment (IEC, 1995).

The third and last step is risk reduction/control. In this step the most suitable risk-reducing aernative in the previous step is chosen and implemented. Enhancing risk monitoring to be within the company's risk appetite is a process that never ends. This is because of any new risks come up all the time and the new risk analysis has to be carried out regularly. Managing a company's risks will need a continuous process. (IEC, 1995).

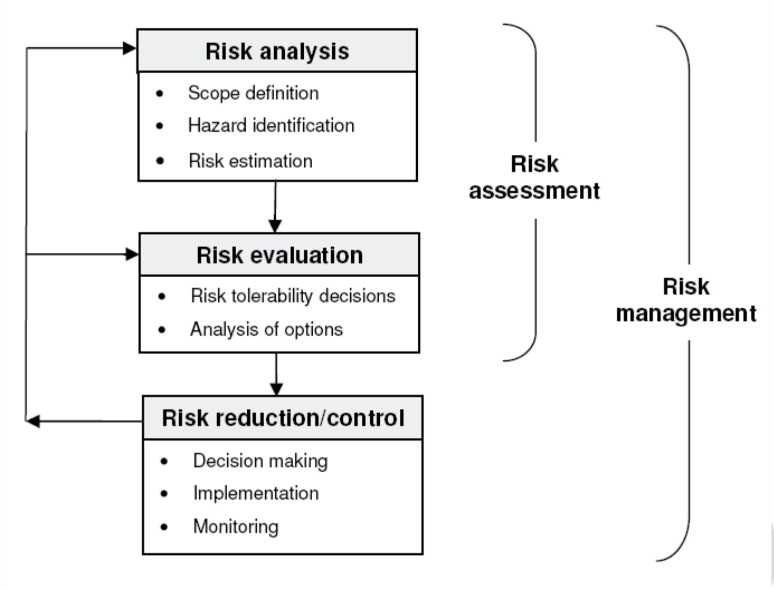


Figure 2.1 Risk Management Process according to International Electrotechnical Commission

Source: IEC (1995)

2.3 Risk Analysis Methods

There are three different risk analysis methods that can be found in a wide spectrum overview, see Figure 2.2. Which method to use depends on the target of the analysis. As there are many kind of risks it is hard to express the result in a single way. A classification of risk analysis methods are usually made with respect to the level of qualitative and quantitative elements (Olsson 1999, Nilsson 2003).

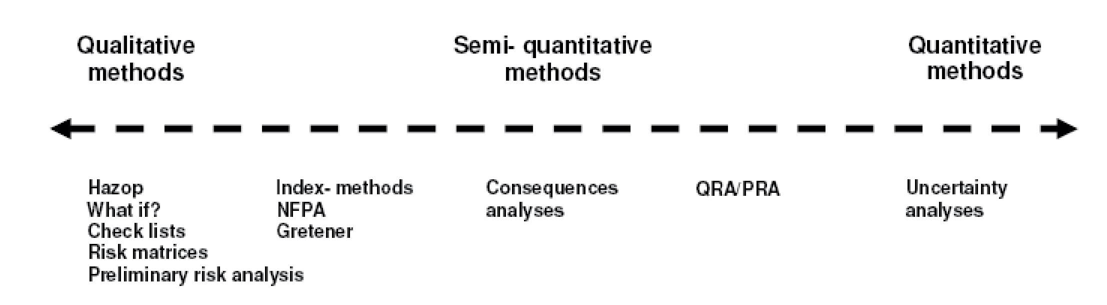


Figure 2.2 The spectrum of the different risk analysis methods with respect to the level of qualitative and quantitative elements

Source: Olsson (1999) and Nilsson (2003)

Qualitative Methods

This method is the most useful in the risk identification phase. This is the first part of the risk analysis. The purpose is mainly to describe occurrences at different conditions. The estimation is needed in an ordinal of probability and consequence that can be made to compare risks with each other. Common methods are “What if?”, checklists, and preliminary hazard analysis. (Olsson 1999, Nilsson 2003). Correlation of Spearman’s Rho is an example of qualitative methodology that can be used to analyze the result of interview (Trochim, 2006).

Semi-quantitative Methods

This method is more detailed in its composition and contains partly of numerical measures of probability and consequence. The numerical measures are not fixed but facilitate to choose between different alternatives associated with risk. A risk matrix with numerical elements is an example of a semi-quantitative method (Olsson 1999, Nilsson 2003).

Quantitative Methods

This method is completely numerical. The uncertainties in calculation models and input are taken into account and these uncertainties are reproduced to the end result. The calculation can be either deterministic or probabilistic. QRA, *quantitative risk* *analysis* is an example of quantitative method used commonly in the process industry (Olsson 1999, Nilsson 2003).

2.4 Enterprise Risk Management

The core objective for any business is to convey products and service to the market in order to generate profit for stakeholders. The effective to supply of these products and service is enabled by number of processes, which exist both on the inside and on the outside the organizations. In all businesses there are certain products and service regarded as critical to continued success, because they generate a lot of value. This means that it is very critical to the business for each process that deliver the critical product and service (Global, 2007). If such process considered as critical process is potentially to be failed for any reason, the consequence can be an interruption in the delivery of critical products and service, which will reduce the profit generated for stakeholders. That’s why as a business, it needs to protect their critical processes to ensure that it is able to offer resistance to disruption and to continue the delivery of products and services. To achieve this objective the business has to be sufficiently resilient (Global, 2007). Enterprise Risk Management (ERM) constitutes not only a tool for companies to create sustainable value, it also facilitates for management to communicate the value created to stakeholders (COSO, 2003).

The Committee of Sponsoring Organizations of the Treadway Commission (COSO, 2003: 87) definition of ERM can be more suitable in several cases:

Enterprise Risk Management is a process, effected by an entity’s board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risks to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives”.

COSO is an independent private sector initiative with the purpose to improve the quality of financial reporting and its recommendations has become a guideline for the evaluation of internal control systems (Henke, 2008). The definition is broad and adapted to suit all companies regardless of size or structure (Eichler and Bungartz, 2004). In this thesis, the COSO definition of ERM will be applied and the focus will be on such risks that threaten the achievement of the enterprises core objectives.

COSO has visualized the relationships between an enterprise's objectives and the components of risk management in form of a cube as can be seen on Figure 2.3.

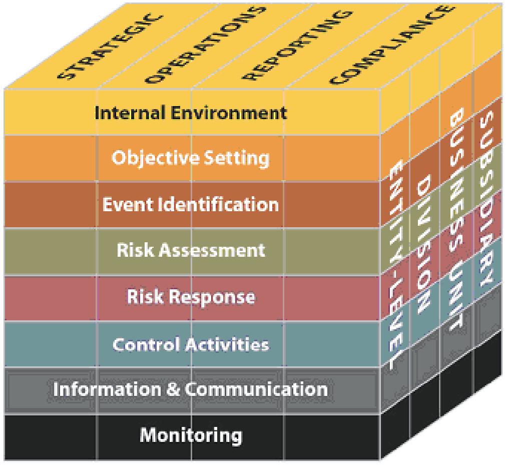


Figure 2.3 COSO's depicture of the relationships between an enterprise's objectives and the components of risk management

Source: COSO (2003).

The cubes three dimensions contain:

- The four objectives categories – strategy, operations, reporting and compliance – are represented by the vertical columns.
- The eight components are represented by horizontal rows.
- The entity and its organizational units are depicted by the third dimension of the matrix.

Internal Environment

The entity's internal environment is the foundation for all other components of ERM. The board of directors constitutes a key part of the internal environment because their attitude significantly influences other internal environment elements. As part of the internal environment, management establishes a risk management philosophy, establishes the entity's risk appetite, forms a risk culture and integrates ERM with related initiatives (COSO, 2003).

The ERM philosophy is the entity's minds about risk and how it chooses to manage risk. The philosophy shall be communicated by the management to all personnel and understood by them. This will improve the way the employees recognize and manage risk. It is a major importance that the management not only communicates the philosophy by words, but with everyday actions as well (COSO, 2003).

The risk appetite, established by management constitutes an important part of setting the company's strategy. It is important that the management chooses a strategy which is consistent within its risk appetite. Risk culture is the set of shared attitudes, values and practices characterizing how an entity considers risk in its day to day activities. Establishing an ERM philosophy and determine the company's risk appetite help creating a good risk culture (COSO, 2003).

There are seven steps for the risk assessment according to COSO:

1. *Objective setting*. Management has to set strategy and related objectives before the event identification can start, this is because of the event identification focuses on the achievement of the entity's core objectives. According to COSO (2003), entity objectives can be viewed in the context of four categories:

    - *Strategic* – relating to high-level goals, aligned with and supporting the entity's mission/vision
    - *Operations* – relating to effectiveness and efficiency of the entity's operations, including performance and profitability goals. They vary based on management's choices about structure and performance
    - *Reporting* – relating to the effectiveness of the entity's reporting. They include internal and external reporting and may involve financial or non-financial information

- *Compliance* – relating to the entity's compliance with applicable laws and regulations

2. *Event Identification*. This step focuses on identifying event that can affect the achievement of the entity's core objectives. There are two factors that management needs to be concerned on. They are external and internal factors that affect event occurrence. The techniques utilized to identify events can vary among different companies. It is wise to use a technique focusing on both trends in the past as well as predicting future exposures. Events that happened could have positive impact, and also negative impact which represent risks.

3. *Risk Assessment*. In the risk assessment, management estimates the likelihood and impact of the identified events and discusses option to deal with risks that are not tolerable. COSO's view of the risk assessment is quite similar to IEC's definitions of the risk management process presented in Chapter 2.2 (at the above passage). A difference is that COSO (2003) have slightly emphasized the picture of functional relation between entity and the whole view of the risks within a company. COSO stresses that events can correlate and create combinations of events with much deeper impact than the events have separately. COSO provides the risks that are being assessed into the context of the company's strategy and objectives.

4. *Risk Response*. Management shall choose an appropriate response to bring the risk within the entity's risk tolerance. There are four main categories to respond to a risk which are avoidance, reduction, sharing, and acceptance. Avoidance implies actions taken to exit the activities which create the risk. A risk reduction can be conducted either by reducing the likelihood or the impact of the risk or reducing both these parameters.

   The purpose with sharing the risk is to transfer it to another company, usually an insurance company. This is common with risks characterized with low likelihood and high impact. Acceptance means the risk is being ignored and no action taken to affect the likelihood or cost effective to manage all risks. The important thing is that the entity's risks are within its risk appetite (COSO, 2003).

5. *Control Activities*. Control activities are the policies and procedures that help ensure risk responses are properly executed. These activities take place all over the organization. The two elements that usually are involved in control activities are policy establishing and procedures to affect the policy. Information systems constitute a vital part of every organization. Therefore there have to be control activities regarding these systems (COSO, 2003).
6. *Information and Communication*. Large volumes of information, from both internal and external sources flow through an organization. An important task for management is to refine the information and make it useful for the work with ERM. Without relevant information it is hard to identify, assess and respond to risks in a proper way. Information constitutes the foundation for the communication within an organization and with external parties. Therefore it is important to have good communication channels throughout the enterprise. This is a condition for successful ERM. One of the most important communications channels is between top management and the board of directors (COSO, 2003).
7. *Monitoring*. To monitor ERM is a process that assesses both the presence and functioning of its components and the quality of their performance over time. Monitoring can be done either through ongoing activities or separate evaluations. Problems will probably be identified faster by ongoing monitoring routines compared to separate evaluations, since the latter take place after the fact. A suitable level of documentation of the monitoring process usually makes it more effective (COSO, 2003).

It is important when ERM deficiencies are discovered that they are being reported *in the right way through the right communication channels. If deficiencies not are* reported it will complicate improving ERM. There should also be alternative communication channels for reporting sensitive information (COSO, 2003).

ISO 31000 define risk as “The effect of uncertainty on objectives.” The emphasis is now on the ‘effect’ rather than the ‘chance’ (ISO, 2009: 57). The definition of risk management has changed to “coordinated activities direct and control an organization with regard to risk,” rather than listing various components such as culture, processes, structure. (ISO, 2009). This ISO 31000 noted that: “to be successful, risk management should function within a risk management framework which provides the foundations and organizational arrangements that will embed it throughout the organizations at all levels.” (ISO, 2009: 67). The standard aims to provide organization with guidance and a common platform for managing different types of risks, from many sources irrespective of the organizations size, type, complexity, structure, activities or location (ISO, 2009).

The risk management process in ISO 31000 comprises of five key activities, as can be seen in Figure 2.4.

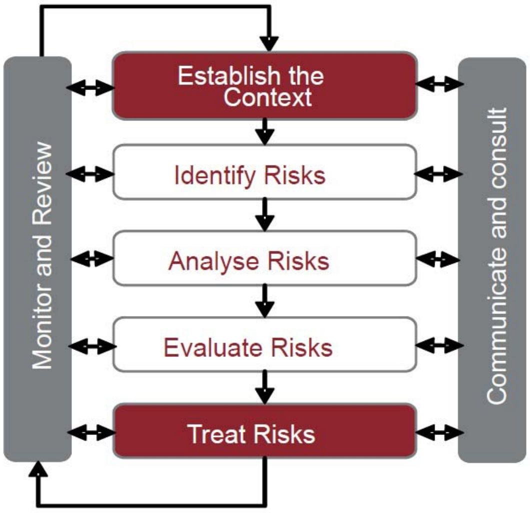


Figure 2.4 ISO 31000 depicture of the risk management process

Source: ISO (2009)

There are five key activities related to this ISO 31000:

1. *Communication and consultation*. This is concerned with engaging internal and external stakeholders throughout the risk management process. From the outset, good communications with key stakeholders will help establish expectations, shape the context of risk management and ensure their needs are considered very important for buy in. Throughout the risk management process, various written and verbal communications between the risk manager, risk owner and stakeholders will continue to occur (ISO, 2009).
2. *Establishing context*. Establishing context is about setting the parameters or boundaries around the organizations risk appetite and risk management activities. It requires consideration of the external factors such as social, resources and capabilities, strategy, resources, and capabilities. The risk manager will then need to establish context of the risk management processes which includes among other things establishing a risk management policy, processes, methodologies, plans, risk rating, training and reporting processes (ISO, 2009).
3. *Risk assessment*. It comprises of the processes for identifying, analyzing and evaluating risk. Ideally, the organization will utilize a range of risk identification techniques including brainstorming, work breakdown analysis, and expert facilitation. Risk analysis considers possible causes, sources, likelihood and consequences to establish the inherent risk. Existing management controls should be identified and effectiveness assessed to determine the level of residual risk. After this analysis, an evaluation of the level of risk is required to makes decisions about further risk treatment (ISO, 2009).
4. *Risk treatment*. The aim of risk treatment is that all risk level remains intolerable. Risk owners can treat risks by avoiding the risk, treating the risk sources, modifying likelihood, changing consequences or sharing elements of

the risk. The remaining level of risk retained should be within risk appetite (ISO, 2009).

5. *Monitoring and review*. Planned, regular monitoring of the risks and the risk management framework including processes is critical to keep the risk management framework relevant to the changing needs of the organization and external influences. Monitoring and review will be undertaken by risk owners, management and the board. An independent review of the risk management framework should be undertaken from time-to-time (ISO, 2009).

2.5 Operational Risk Management

Operational Risk Management is part of internal processes. The operational risk is part of the enterprise risk management process. Based on the Financial Services Authority in 2002 express its interest in operational risk as it considers "operational risk is present in all firms and can affect a firm's solvency, the fair treatment of its customers and the incidence of financial crime.

Basel Committee states: *"Operational risk is the risk of loss resulting from inadequate or failed internal processes, people and system or from external events."* (2004: 142). The business need to classify the specific condition of the operational risk based on its activities and its operating environment (Chapman, 2006).

Based on FSA (2001) describes operational risk as covering:

- Business risk which include adverse changes to a firm's market, customer or products, changes to the economic and political environments in which the firm operates and strategic risk which a firm faces if business plans, supporting system and the implementation of these plans adversely affect the firm
- Crime risk including potential theft, fraud and computer hacking
- Disaster risk such. as fires, floods and other natural disasters and terrorist activity

- Information technology risk, including unauthorized access and disclosure, and data corruption
- Legal risk including loss arising from legal action against it and from inadequate, incomplete or otherwise unsound legal documentation and practices
- Regulatory risk relating to the lack of observance of rules set by a regulatory body
- Reputational risk relating to the lack of observance of rules by a regulatory body
- Reputational risk from negative publicity about its business practices or internal controls
- System risk loss as a result of failure caused by the breakdown of business procedures, processes or systems and controls
- Outsourcing

In this thesis, crime risk, disaster risk, information technology risk, reputational risk, and system risk loss will be included in the analysis.

There are four elements within operational risk which are strategy, people, processes and system, and external event. This will be discussed in the following subsections.

2.5.1 Strategy risk

Since the company objective is to gain profit to the stakeholder, then the business's strategy is the business's overall approach to achieve its objective. Strategy is a description of what the business will do and the logic behind it (Chapman, 2006).

The strategy risk will determine the structure of a business, the key function that must be concern on and the allocation of people to tasks. The strategy risk will need a clear stated and understood objective. Chapman (2006: 224), determines the objective of strategy risk as "*the foundation for designing both the organizational structure and* *processes of a business and the work of individual business units and individual managers*"**.** This means that each business will use the objective as a tool to asses several key areas (Chapman, 2006).

2.5.2 People risk

Based on Chapman (2006: 228), "*People risk may be described as a combination of the detrimental impact of employee behavior (which may occur anywhere on the continuum between profit erosion and business failure) and employer behavior (which impairs employee efficiency, health and safety or loyalty).*"

There are some types of people risk that will be assess in this thesis such as risk management culture which is reflected through employee behavior.

2.5.3 Process and system risk

Based on Chapman (2006: 245), it can be cited that "*process and system risk may be defined as the failure of processes or systems due to their poor design, complexity or non-performance, giving rise to operational losses*".

There are some parameters which related to processes and systems risk such as:

a. *Controls*. Control is a tool that helps to measure the measurable and non measurable events. This need to be focus on result and it can neither be objective nor neutral. Control is needed to record event in the past and providing strategic direction in the future events to be aligned with business objective plans. The risk of control is related to the lack of quality. The control itself needs to be meaningful, simple, and easy to be understood (Chapman, 2006).

b. *Regulatory and statutory requirement*. Each company is required to follow the listing rules based on the regulation. This requirement includes notification of a significant failure in its systems and controls and also pre-agreed triggered points to be notified (Chapman, 2006).

c. *Continuity*. Arrangement for the operations continuity is needed when the significant process or system becomes unavailable or destroyed (Chapman, 2006).

d. *Indicator of loss*. Based on Chapman, 2006, "*The risk indicators are used to facilitate regular quantitative assessment and monitoring of risk exposures and mitigating responses.*"

e. *Transactions*. The risk of transaction to business derived from not honoring commitment to customer in terms of time, quality and quantity (Chapman, 2006).

f. *Computer/IT systems*. There are some parameters that need to be assessed such as the IT system should align with business needs and the organization is exploiting the system to be fully advantage, the automation will reduce the human error, data integrity, electronic data security, system capacity, and data recovery (Chapman, 2006).

g. *Knowledge management*. According to Chapman 2006 stated that "*How successful a company is in this task depends on a company's information culture. This can be defined as the values, attitudes and behavior that influence the way employees collect, organize, save, discuss, process, communicate and use the information.*"

h. *Project management*. The project management will relate to planning, controlling and coordinating projects from the starting point upon completion. Each project will have its own unique risk profile and will require the discipline of risk management to provide greater certainty to achieve the objective (Chapman, 2006).

2.5.4 External event

External events are events that occur outside of business, which may require a response in the form of change management or the instigation of contingency events such as natural disaster.

a. *Change of Management*. The change in management should be handled carefully to avoid a series of common risk. The radical changes in IT need to be planned and the implications need to be assessed to the whole business (Chapman, 2006).

b. *Business continuity*. Business continuity management us a holistic management process that identifies potential impacts that threaten an organization and provides a framework for building resilience and the capability for an effective response, which safeguards the interests of its key stakeholders, reputation, brand and value creating activities (*Business Continuity Institute*, 2002).

2.6 Technological Risk

Technological risk is an element of the operational risk. As of the business need to create effectiveness to supply of these products and service, the effectiveness use of technology has the ability to transform enterprises to enhanced stakeholder value. Chapman (2006: 263) defined technology risk as "*events that would lead to insufficient, inappropriate or mismanagement of investment in technology, in terms of manufacturing processes, product design and/or information management*"**.** This potential risk will be impacted or align with crime risk, information technology risk, and system risk loss. The mismanagement would include poor business continuity planning and protection of security level.

2.7 Reputational Risk

Reputational risk is very critical for the company's image. Fombrun & Foss(2005 :2) stated that "*a corporate reputation is a collective representation of a firm's past actions and results that describe firm's ability to deliver outcomes to multiple stakeholders*".

There is another definition of reputational risk as stated from Zaman (2004: 99) as follows "Ther range of risks that arise from the company's relationships, brand name which are threats to long-term trust with customers, employees, shareholders, and can include everything from specify policy misjudgements to scandals".

Effectively managing reputational risk can be achieved by applying the well-known framework of identification, assessment and management. A business need to elaborate the details of risk sources that could impact to the reputation of company, try to classify that from the criticality categories and in the end try to manage the risk by mitigation or transfer the risk.

2.8 Business Continuity Management

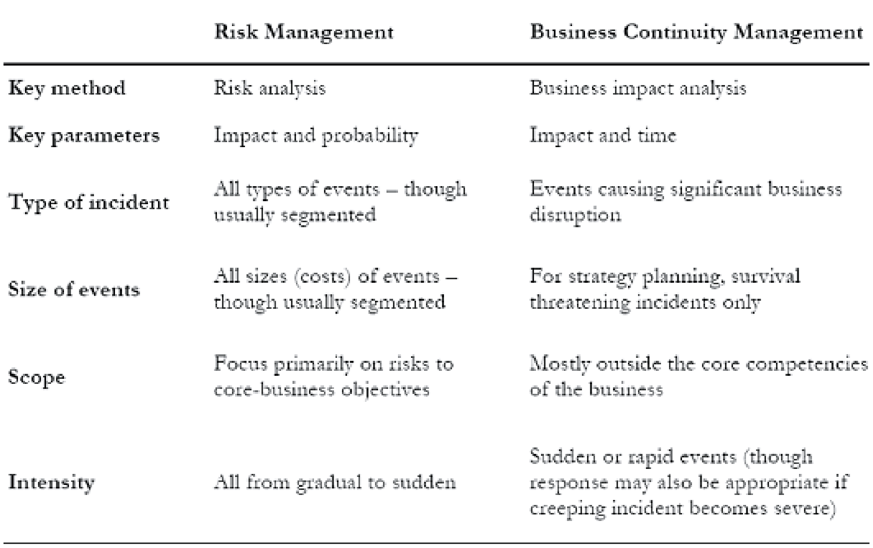
One problem with the risk management and crisis management processes is that in the risk identification phase it is difficult to detect all possible scenarios. Especially events with devastating consequences tend to be not foreseen just because they seem to unlikely (Andersen, 2003). A company which is not prepared for large catastrophes is very vulnerable. The trend today goes towards an increasing complexity of the world community with a deeper integration of networks in all areas resulting in an increased probability of unforeseen events to occur (Andersen, 2003). Therefore every company today has to be aware that an unforeseen event can occur and must be prepared to handle a crisis. This is the reason for the growing interest in Business Continuity Management (BCM), with focus on the process after an unforeseen event has occurred.

The Business Continuity Institute (BCI) Good Practice Guidelines (2008: 58) defines BCM as:

A holistic management process identifies potential impact threatening an organization and provides a framework for building resilience with the capability for an effective response that safeguards the interests of its key stakeholders, reputation, brand and value creating activities.

BCM is used on management level and the goal is to achieve a resilient business. The goal is achieved by identifying the potential impacts in advance. It provides a certain level of comfort in knowing that if a major disaster occurs, it will not result in financial disaster (Geoffrey, 1997). BCM can be seen as a subset of larger risk management process within the area of Enterprise Risk Management (Krell, 2006). BCM has several similarities with risk management, but there are also some differences, see Table 2.1. The main difference between the two processes is that BCM focuses on which strategies and tactics to apply after an unforeseen event have occurred, and the objective is to restore the business normal operations to the lowest possible cost. The risk management process focuses on strategies to avoid or mitigate risks before they occur (Krell, 2006).

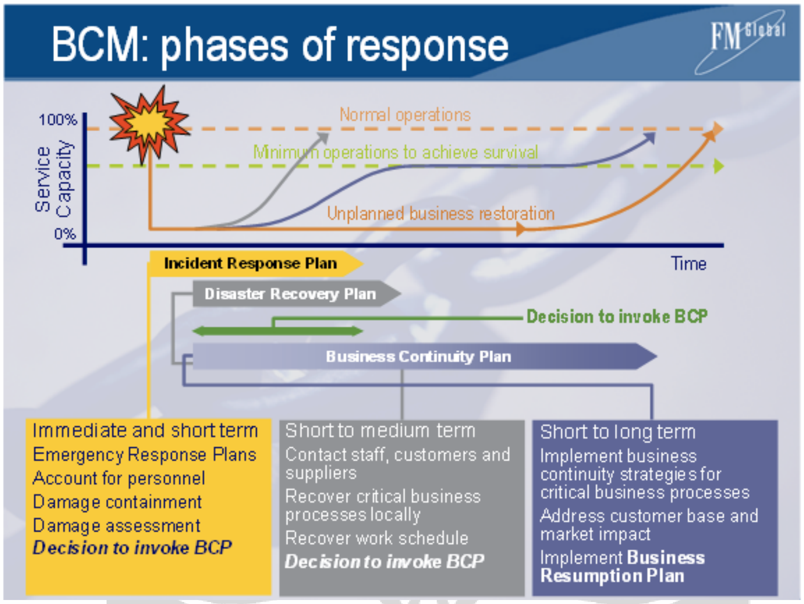
Table 2.1 Differences between Risk Management and BCM



	Risk Management	Business Continuity Management
Key method	Risk analysis	Business impact analysis
Key parameters	Impact and probability	Impact and time
Type of incident	All types of events – though usually segmented	Events causing significant business disruption
Size of events	All sizes (costs) of events – though usually segmented	For strategy planning, survival threatening incidents only
Scope	Focus primarily on risks to core-business objectives	Mostly outside the core competencies of the business
Intensity	All from gradual to sudden	Sudden or rapid events (though response may also be appropriate if creeping incident becomes severe)

Source: Business Continuity Institute, (2005).

A perspective on BCM was presented by Global (2007). According to them BCM can be divided into different phases of response which are illustrated in Figure 2.5. The content of each phase is described below.



Immediate and short term
Emergency Response Plans
Account for personnel
Damage containment
Damage assessment
Decision to invoke BCP

Short to medium term
Contact staff, customers and suppliers
Recover critical business processes locally
Recover work schedule
Decision to invoke BCP

Short to long term
Implement business continuity strategies for critical business processes
Address customer base and market impact
Implement **Business Resumption Plan**

Figure 2.5 Phases of response in BCM

Source: Global (2007)

The BCM model should contain BCP (Business Continuity Planning) and DRP (Disaster Recovery Planning). In this research, the author will elaborate BCP only, with the limitation already mentioned in Chapter 1.

2.9 Business Continuity Planning

Business continuity planning (BCP) can be defined as: *a process of developing and documenting arrangements and procedures that enable an organization to respond to an event that lasts for an unacceptable period of time and return to performing its critical functions after an interruption* (DRII, 2008 : pp.3).

Beside, there is another definition based on Broder (2006) that defined business continuity planning is a process that identifies the critical functions of an organizations and that develop strategies to minimize that effect of an outage or loss of service provided by these functions. Business continuity planning implies recovery planning for all the critical functions or business units of an organization. The difference between BCP and disaster recovery planning (DRP) is DRP refers to the re-establishment or continuity information technology and data systems; BCP refers to the recovery or continuity of business unit operations (system versus people).

The content of the definition is that BCP shall be seen as one part of the whole BCM process. The purpose of BCP is to mitigate the effect of an unforeseen event. BCP focuses on the negative impact and the process after an unexpected event has occurred. The plan highlights what shall be done to get back to normal business as soon as possible and how to keep the losses to a minimum. A vital part of the BCP is to identify the company’s critical business processes in a holistic view and determine where more specific action plans and strategies will be needed and prioritized (*Business Continuity Institute*, 2008).

When there is a disruption, it is often too late to do anything very radical about it, unless the actions have taken in advance. This is why the organizations have to work proactively. BCM means working systematically in advance to prevent disruptions from happening and if it happens anyway, the BCP shall consist of plans that get the processes quickly and safely back to order. This means that the action plans which are a part of the BCP will allow the organization to return to normal activity after a disruption has occurred (Broder, 2006).

An organization has thousands of different activities, but only a few percent of them are critical to the business. It is around these activities the specific action plans shall be directed, (Norrman, 2004). When first creating the plans, focus on the worst-case scenarios of the identified risks. Plans for the most serious consequences means also minor disruptions can be handled (*London First*, 2003).

Gallagher (2005) described a model on which elements BCP shall include, see Figure 2.6. The model consists of seven steps which are explained below.

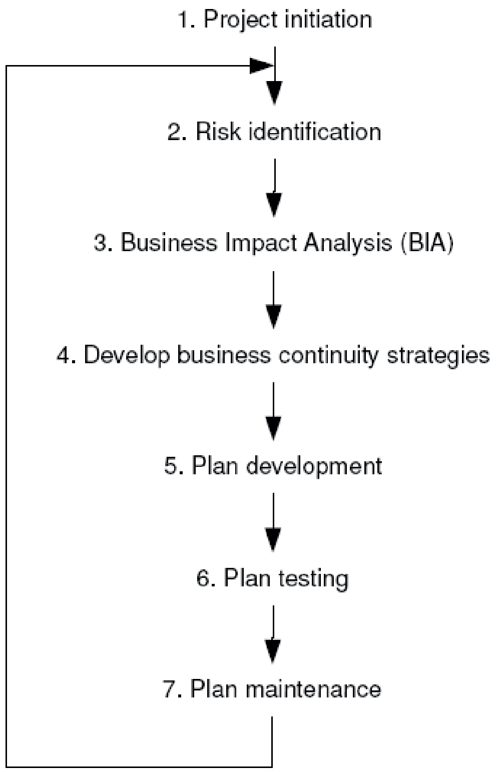


Figure 2.6 Seven phases which should be included in BCP

Source: Gallagher (2005)

1. *Project Initiation*. The initiation of the project is very important. Support from the management shall be established and the framework and scope of the project shall be decided. As mentioned above, in the chapter how to create a resilient supply chain, one of the conditions in creating a resilient supply chain is to get support from the top management. The same thing goes for BCP. If the project does not get fully support from the management it is likely it will encounter unnecessary resistance and perhaps even self die. (Gallagher, 2005). Based on DRII there are some broaden point of view to produce an effective plan which can be listed as project initiation:

    - *Identify the planning coordinator*. A person within the organization is designated as the planning manager, coordinator, leader, or other appropriate title. This person is responsible for the management of the project (that is, the completion of the plan) and possibly for coordinating or leading the recovery effort subsequent to a disaster. The coordinator may also have major responsibilities for plan activation. Ideally, this person should be a management-level employee who has good people and project management skills and a good understanding of the organization, and is detail oriented.

- *Obtain management support and resources*. No planning effort or project will be successful without the support of upper management. This support must be communicated to all levels of management. Absent the support of the board of directors or senior (executive) management as a group, it is often necessary to get the attention of and support from at least one member such as the CFO. This person becomes the business and continuity plan "sponsor."
- *Define the scope and planning methodology*. Narrow the scope of the project to a single division, site, or building, something small enough to allow a positive outcome. A successful project will add momentum for the completion of subsequent projects throughout the remainder of the organization. Be prepared to go beyond the established scope when identifying interdependencies and strategies. Many methods exist to manage the project. These include the following:
    - Planning standards for the business units or divisions
    - Steering or planning committee
    - Facilitation of internal development
    - Use of template plans

Greatest success is achieved when the corporate planner develops the "*basic plan"* and allows the divisions to concentrate on planning for only themselves.

According to FEMA, the basic plan should contain the following elements or sections introductory material (promulgation document, signature page, dated title and revisions page, distribution list, table of contents), purpose statement, situation and assumptions, concept of operations, organization and assignment of responsibilities, administration and logistics, plan development and maintenance, authorities and references.

2. *Risk Identification*. In this step a risk analysis is conducted to identify the main risks on company level and the impact and probability that they will arise (Gallagher, 2005).

   According to Broder (2006), there are some points that need to be identify based on thinking through the cause and effects of likely scenarios and offer recommendation to mitigate their effects, such as Inspect the buildings, grounds, and community for any hazard that may injure employees, damage equipment or facilities, or cut off the supply of materials, resources, or services.

   Question the general manager, facilities manager, and other appropriate people on what could prevent emergencies, outages, and disasters. Does the company have an evacuation procedure? Are first aid, food, and water supplies stockpiled? Are critical systems or equipment connected to uninterruptible power supplies? Are computer files backed up on a regular basis and stored off site?

3. *Business Impact Analysis*. The purpose of the Business Impact Analysis (BIA) is to identify which impact disruption and disaster scenarios has on the organization (Gallagher, 2005). The BIA will show which parts of a company that will be most affected by an incident and what effect it will have upon the company as a whole. The BIA is the base the site specific action plans are based on. The critical processes which generate most value within a company have to be identified and documented (ASIS, 2005).

According to Broder (2006), it is fundamental in the understanding of the amount of risk to retain, transfer, or mitigate. It will assist management to make timely decisions about future business issues. This is accomplished by examining impacts over significant blocks of time (hours or days) on service objectives, cash flow and financial position, regulatory requirements, contractual issues, and competitive advantage. It presents management with a financial basis for selecting the most cost-effective recovery strategies.

Refer to Broder (2006), a BIA will also help to accomplish the following:

1. Identify which processes and computer applications are critical to the survival of the organization.
2. Identify critical resources of the organization
3. Gain support for the recovery process from senior management
4. Increase management's awareness of the issues and resources required for a workable program, as well as introduce a basic planning structure to the management group
5. Potentially satisfy regulatory requirements and standards
6. Potentially reveal inefficiencies in normal operations
7. Help to justify or allocate better recovery planning budgets (cost/benefit)

A major objective of the BIA is to establish the recovery time objectives (RTOs) and recovery point objectives (RPOs) of business functions and data processes. The recovery time objective is the amount of time by which the organization would like to have the process or function back in service (Broder, 2006).

The RTO is the maximum downtime before the function or process is critically affected or the deadline in which the function or process must be restored to prevent severe impact to the business. The RPO is the point in time to which systems and data must be recovered after an outage or the acceptable amount of data that can be lost before a function or process is critically affected (Broder, 2006).

Another objective of the BIA is to show the business cycle criticality of various functions and refine strategies or reallocate resources accordingly during a continuity situation. Companies are composed of individual business functions that work together to deliver services or products (Broder, 2006.)

The result of the BIA is a priority list of which business processes to restore first in occurrence of a disaster. To be able do achieve this some key factors has to be taken into considerations. This includes knowledge about which products generate the main part of the revenues, which are the key markets and which are the most important customers (Global, 2007).

The approach taken to initiate and manage a BIA is very similar to that used in a risk analysis. It must begin with senior management's commitment. Because a top-down approach provides the fastest and often most accurate results, management must emphasize that this is a task not to be delegated downward in the organization. The planners' discussions with these managers in the process of collecting impact data will help to build relationships that will be useful later on if the business continuity planning process becomes stalled, or if resistance is encountered (Broder, 2006).

4. *Develop Business Continuity Strategies*. The risk analysis and the BIA identify which parts of the organizations are most vulnerable and important to the business. Based on those, continuity strategies will be formulated and specific plans will be developed to meet the needs identified in the risk analysis and the BIA (ASIS, 2005). The strategies can comprise policies for reducing the dependency on key suppliers or customers, human resources issues like succession planning, training, and retention of skilled workers, as well as the use of recovery centers and geographic dispersion of facilities and offices. The specific plans will focus more on actions to be taken when an unforeseen event has occurred. The development of business continuity

strategies is a very important step in the development of the plan because a lot of people are involved and key managers discuss essential questions and priorities. In this way all people affected are aware of the strategies (Gallagher, 2005).

5. *Plan Development*. The development of the plan is individual for each organization. There is no general plan that fits all because every single organization is unique. The plan will therefore vary in size and layout depending on the needs and size of the organization (Gallagher, 2005).
6. *Plan Testing*. To discover weaknesses, to keep employees updated and to avoid that the plan results in a folder in the bookshelf it is important that the plan is regularly tested. One way to test the plan is to execute crisis training exercises (Gallagher, 2005). Exercising of plans validates the business continuity procedures and confirms that the people involved know what to do in the event of a disruption (Global, 2007).
7. *Plan Maintenance*. Change occurs constantly in the company’s supply chain and in the environment. In order to assure that a company is always prepared for disruptions, it is therefore important that companies continually update their plans (Gallagher, 2005). If the plans are to complex with too many people involved, it is probable that they are less frequently studied. Therefore it is important that someone within the company is responsible for the main plan and to ensure that each entity in the company assign one person to be responsible for updating their plans (Global, 2007).

The author will use some theories related to the BCP analysis from COSO, ISO 31000, Gallagher, DR II, and FEMA, to create a BCP model. The model will be used to analyze the gap. The reason is, because the theories mentioned above support practical and detailed steps that should be done to produce a standard and complete BCP.

2.10 Business Continuity Model

The basic concept of business continuity as stated by Meglarthy (2000: 85**)** stated, "*Corporate business continuity planning specifies the methodology, structure, discipline, and procedures needed to back up and recover functional units struck by a catastrophe. Therefore, every functional unit must accept responsibility for developing and implementing the business continuity plan, and the plan must have the total support of management.*" The above statement describe Business continuity (BC) as a complex structure that includes multiple elements of planning and, by its very nature, is dependent on the involvement of all functional units.

Business continuity model that is used in this thesis is based on the result analysis which consist a form of combination from business continuity study, business continuity theory, and business continuity practice in some companies. Hasil olahan tersebut menjadi model yang di suggest oleh peneliti yang selanjutnya dipakai penelti menjadi acuan BCP model The development of a comprehensive model of Business Continuity (BC) is essential to facilitate a broad-based study of organizational BC practices across meaningful sample. The Business Continuity Institute (Smith, 2003) recommended a six-phase approach, summarized as follows:

1. Understand your business strategy
2. Define a business continuity strategy at varying levels of abstraction such as organizational, functional, and resource-level
3. Develop plans to execute your business continuity strategy
4. Build a "business continuity culture" through training and awareness program
5. Periodically audit and test your program
6. Institute appropriate governance processes.

NIST (2000) asserted that the success of BC activities is dependent upon an understanding of their recommended baseline BC process, development of a plan with all requisite components, and emphasis on plan maintenance, training, and testing. NIST (2000) recommended a contingency planning process consisting following steps:

1. Develop the contingency planning policy statement
2. Conduct the business impact analysis (BIA)
3. Identify preventive controls
4. Develop recovery strategies
5. Develop an IT contingency plan
6. Plan testing, training, and exercises
7. Plan maintenance

A more direct approach of BC assessment is provided by Ream (2003) who developed a Business Continuity Management (BCM) maturity model. The BCM maturity model uses a variety of characteristics to “grade” overall organizational competence on BC and related processes. Ream graded organizational as follows:

- Level 1 – Self- Governed – Business continuity management has not yet been recognized as strategically important by senior management.
- Level 2 – Supported Self- Governed – At least one business unit or corporate function has recognized the strategic importance of business continuity and has begun efforts to increase executive and enterprise-wide awareness.
- Level 3 – Centrally –Governed –Participating business units and departments have instituted a rudimentary governance program, mandating at least limited compliance to standardized BCM policy, practices and processes to which they have commonly agreed.
- Level 4 - Enterprise Awakening - All critical business functions have been identified and continuity plans for their protection have been developed across the enterprise.

- Level 5 – Planned Growth. Business continuity plans and tests incorporate multi-departmental considerations of critical enterprise business processes.
- Level 6 - Synergistic - All business units have a measurably high degree of business continuity planning competency. Complex business protection strategies are formulated and tested successfully.

Ream considered organizations at Level 1 – Level 2 to be “at risk” with respect to response capabilities based on the overall weakness of their respective BC programs. Similarly, organizations at Level 3 – Level 4 were labeled “competent performers.” Firms at Level 5 – Level 6 were described as exhibiting the highest levels of preparedness.

This Business Continuity Assesment helps to assess and create a comprehensive business conntinuity model. There are some guidance or best practices that can be used to create the business continuity model, such as:

A. BC-EM Model

This model is taken from a journal titled “Business Continuity in the Pharmaceutical Industry” (Edward & Paul, 2004). This model is a research result from business continuity in five organizations. The research involves:

a. A review of the literature and the identification of a number of models for business continuity and disaster recovery

b. Interviews with five business continuity experts, four from major pharmaceutical companies and one from the telecommunications industry

The interview also conducted with ten executives in the Pharmaceutical Companies. Beside the interview, there is a survey that already conducted to develop the model. The period of survey is started from December 2003 up to March 2004. The respondents come from high level managers and executives, and also lower to middle level managers.

The BC-EM Planning Model integrates concepts from the business continuity model devised by Smith (2003), Ream (2003), the NIST contingency planning guidelines, and Barnes (2001). The model includes suggested process steps related to plan development, risk and impact analysis, control architecture, and contingency plans, and governance constructs such as budgeting.

- *Planning*.There are some important questions that need to be asked, such as organization identified and ranked its assets, business impact or risk analysis which uses a formal risk assessment methodology, explicit security strategy been formulated, security budget been developed, and existence of BCP mission statement, BCP policies and procedures, BCP goals & strategies, and inclusion of internal and external business partners in planning phase.
- *Management Model*. The first issue to be addressed in the Management Model concerns whether the organization has developed a separate BC organization. The key issues in this area are the existence of a formal entity, formal budgets devoted to business continuity and the organizational location of these budgets, the role of general business continuity organization, and the existence of a crisis management center

  The following is a summary of each of the five levels of the model that represent the mechanism available to the security organization in its efforts to ensure a secure environment for the organization as a whole.

  - *Manager/Leadership Layer*. The ability of both general management and the security officers in a corporation to provide security is the key to the success of any BC effort. The important things are top management awareness of security risks and willingness to communicate the importance of security throughout organization, the experience and skill of the security managers and their formal reporting relationships in the organization.

At this level, BC-EM seeks to capture certain characteristics of the manager(s) who are responsible for planning and executing business continuity plans within their organization. Specific security manager characteristic include management title, percentage of activities in current position that are dedicated to business continuity planning and/or disaster recovery, reporting lines, level of budget authority, and professional experience in business continuity planning and disaster recovery

- *Governance Layer*. Based on (Luftman, 2003), Governance is “the operating model for how the organization will make decisions" Governance in the security/BC domain involves the allocation and direction of security resources, the delegation of responsibility for different aspects of security to various members of the organization, prioritization of projects, development of performance measures, the development and communication of clear roles in the event of a disaster, and the development and enforcement of security policies.
- *Human Resource Layer*. Employee awareness and understanding of security issues and their motivation to adopt security measures is a crucial aspect of a secure organization. At this level of the system models shows the role of the security organization in monitoring employee behavior and influencing sound security practices throughout the organization. The Human Resources aspect of BC-EM includes identification of characteristics associated with BC team members.

  The HR evaluation domain also seeks measures of the awareness of IT and other employees of the need for security and the understanding of the measures that are to be taken in the event of a disaster. The model similarly seeks to determine how diligent are employees in following best security practices, and whether or not IT personal take BC considerations into account in the development of new software applications and the implementation of system security procedures.

- *Process Layer*. The model has two aspects. First, security breaches often occur in business processes and it is the revenue producing processes such as order entry and service delivery that must be restored first in the event of an attack or natural disaster. The assessment model must therefore address the safeguards that are in place to protect and restore the essential processes of the organization.

  The second aspect of the process level is the security and BCP planning processes themselves. The security organization must develop and practice security procedures and an essential part of its role is to help the business units (including the information technology department) to understand and practice security measures and disaster recovery drills.

  Specific process concerns are as follows:

  - Involvement of senior management in BC and DR activities
  - Involvement of the business units and IT
  - Frequency of testing
  - Testing approaches, including broad discussion of BC issues throughout the organization, restoration of critical systems and applications, completion of sample transaction processing by IT and by business units, movement of business users to recovery site, testing by third party consultants, surprise testing, and participation of external business partners
  - Frequency of update of the BCP
  - The existence of recovery time objectives for various processes and platforms

- *Technology Layer*. Technology is the final layer of our system model. At this layer, security technologies such as encryption, digital signatures, mirrored databases, firewalls and virtual private networks are engineered to provide protection for the organization both from internal misuse, from attack by outsiders, or from natural or man-made disasters. The security organization investigates the available secure technologies and champions their use in the wider organization. IT and senior management should jointly determine the technologies that will be adapted and the IT projects that will be executed given limited resources.

- *Customer Relations*. The organization must also be prepared to protect its reputation and handle media inquiries. These include documentation of logistics processes, development and maintenance of customer contact lists, knowledge current customer orders, and lists of company individuals who maintain relationships with customers and who will be responsible for customer relations in an emergency situation.
- *Service Provider*. Every company depends crucially on many service providers including utility companies supplying water, power and communications, contracted disaster recovery outsourcers and insurance companies.

B. Business Continuity Plan in Bank ABC

Bank ABC is one of the multionational banking in Indonesia. Bank ABC headquarters is in the US. This bank already implemented the BCP since 1980s.

There is some highlighted point that can be highlighted related to this process:

- *BCP Objective Setting***.** The BCP which already implemented in this bank are driven from reputation, regulation, and leading practices. Based on the observation in this bank, the principal services that must be delivered during an interruption are manage risk, clear & settle transactions (all outstanding transactions), provide customer liquidity, and communication to all related parties.

  The key objectives for Business Continuity in this bank are:

- Adherence to policies and standards enterprise-wide
- Accurate identification of functional requirements via risk assessment
- Identification of cost effective strategies to mitigate risk
- Validation of the Business Continuity Plans through testing exercises
- Maintenance and update to the plan to reflect changes in people, process, or technology
- Managing initial crisis situations
- Activation of plan in event of business interruption

- *Business Impact Analysis*. This will be related to the impacts of business which may be caused by business interruptions. The analysis will determine the recovery objectives and priorities.

  Business impact analysis should consist:

  - Identify business processes and sub-processes
  - Identify qualitative and quantitative impacts caused by business interruptions
  - Identify process recovery priorities
  - Identify Recovery Time Objectives (RTO)
  - Identify Recovery Point Objectives (RPO)

  Based on RTO (the maximum time allowed by business to back to the normal position), there are segregation on the criticalities such as:

  - Criticality 1: 0 <= RTO < 4 hours
  - Criticality 2: 4 <= RTO < 24 hours
  - Criticality 3: 24 <= RTO < 72 hours
  - Criticality 4: RTO >= 72 hours

There are threat and vulnerability needed to be included in the analysis, both for natural disaster as well as man-made disaster.The assessment of business process will be assessed by the business itself. The crisis management center or Business Continuity Team needs to asses the Business Recovery Plan (BRP) also and aligns with its goals.

- *Escalation Process*. The crisis management team needs to manage the business recovery center. It should be done based on the organization chart crisis management team and follow the escalation process. The escalation process itself is segregated based on impact levels, starting from low impact up to critical impact. These levels need to be structured and specified in detail.
- *Testing*. The structure organization will be applied during an interruption or in the testing phase. The testing will simulate a real/production situation in the recovery (should be there is no different with the "As-Is" processes) to ensure that all back-up systems, processes, staffs, and locations are readily available. The activities that will be applied before, during, and after the testing period are:
    - Business Continuity Plan updated: Business Impact Analysis, Business Recovery Plan, CoBTrac
    - Process step from technology technical side for the drills.
    - Communication to all staff through Call Tree Testing to ensure that the staff is contactable and they are ready to take actions during testing
    - Independent Plan Review, this is included as review of plan that are needed to be tested during the testing period
    - Technical maintenance such as hardware, software, seating, and other resources
    - Country Business Continuity Plan update such as The Testing Test Result and Lesson Learn

- *Training*. Training is defined as the process of providing continuity of business personnel with the skills and knowledge necessary to plan for and respond to crisis events and business disruptions. The basic goals are:
    - Ensure that designated recovery staff is properly trained in business continuity
    - Ensure that designated recovery staff participate in corporate and regional level training courses
- *Awareness*. Awareness initiatives enforce training program message and are also used to communicate important business continuity topics. The basic goal are:
    - Keep Business Continuity prominent, enabling employees to know “What to do”
    - Educate staff so they understand their role within the business continuity plan
    - Enhance employees understanding of Business continuity and its importance to the short – and long term benefit and health of the organization
    - Emphasize the impact of non-compliance to regulatory and internal policy and the impact to the company and its customers

C. Business Continuity Plan in Public Sector

This procedure is already implemented in most of the public area in US, and in some government sectors such as Angkasapura I & II, POLRI. This BCP is In POLRI, the implementation started in 2009, titled. “Sistem Manajemen Keadaan Darurat (SSMKD)” (*Emergency Situation Management System*), divided into 2 disaster handling systems: Field Control Command System and Inter-unit Coordination

There are some points that need to be highlighted, such as:

- *Crisis Management*. SSMKD has 5 response levels known as “Emergency Situation Management Organization”. The level are:
    - *Field*. The level where the personnel and other emergency response resources execute the decision and tactical activities under authorized command, related with the direct response to emergency events and threats.
    - *Local*. With the task to coordinate the whole emergency response and recovery activities.
    - *Operational Region*. The intermediate level in national emergency situation service organization. The Operational Region manages and/or coordinates the information, resource, and also set the priorities for the local level.
    - *Regional*. This level manages and coordinates the information and resources between operational regions within a certain geographical region.
    - *National*. This level is responsible in coordinating the requests on resources and solves the problems emerging from regional level or between regional levels.

  Besides the points mentioned above, there are several important points that must be taken care of, such as:

    - Facility needed to be formed depends on the type and the complexity of an event/phenomenon. There is specific and detailed explanation on the facility to be used and the sort of the facility, characteristics, type of deployment, and the formation of the facility itself.
    - Specific and detailed activity planning on emergency event must be made far before the date of occurance to ensure the availability of the resources, including a clear and specific resource management.

- Monitoring on the maximum quantity of resources that still can be handled effectively. Besides, there is an assessment on the personal accountability, conducted by the supervisors in each level.
- In process activation of emergency response, a security guarantee must be given and described in detail.
- Managerial control so that the performance and emergency event activity planning can be evaluated, whether it is adequate or not.
- The expense must always be the main consideration. Head of Field Control Commando must ensure that the objectives are achieved using cost-effective strategies, by choosing the right type and quantity of the resource.
- Communication strategy must be structured in detail and in clear explanation; also escalation process must be structured and formalized.
- Recovery Time Objective (RTO) must be less than 24 hours, even must be able to be handled within 2 to 4 hours if the disaster of event is not large and complicated.
- Special assigmenment on supervisory task on regional command, with the function to monitor the management activities so that the response is conducted based on priority, directed to the objective, and can be managed properly.

The personnel on the SSMKD must obtain a special assignment order, where they will do the job in one operational period or until rotated. The main position and role for SSMKD is command and management. Several points important to be mentioned as job description of this position is:

- Special assignment must be the result of an assessment based on the competency of responsible jurisdiction, statement must be written clearly on the characteristics of effective command.

  - Clear statement on the authority to form a special team and to delegate authority, in case the disaster getting wider.
  - Clear job description in directing, ordering and/or controlling the resources.

- *Operation*. Several important points to be considered in the job description of this position are:
  - The command decides whether this position is required or not, depending on the event or phenomena that happens. The organizational structure of point can grow one layer deper, depends on the need.
  - Clear and detailed job description on the mapping related with the field operation, this can be based on region, geographical position, or even involving different function, based on the need of the emergency event.
- *Planning*. Several important points to be considered in the job description of this position are:
  - Clear and detailed job description related on collection of evaluation, documentation, and the use of information related with the emergency event.
  - Long-term planning development must be included also in the job description
- *Logistics*. Several important points to be considered in the job description of this position are:
  - The command decides whether this position is required or not, depending on the event or phenomenon that occurs. The organizational structure of this position can grow one level below if needed.
  - Clear and detailed job description related with providing the service facility, personnel, tools, and material in response to emergency event.

- *Finance/Administration.* Several important points to be considered in the job description of this position are:
    - The command decides whether this position is required or not, depending on the event or phenomenon that occurs. The organizational structure of this position can grow one level below if needed.
    - Clear and detailed job description on financial analysis and costs, as well as administrative aspects not yet handled by other function.

The activation of position or organization structure mentioned above highly depends on the need due to certain event/phenomenon. Thus, the organization is flexible. Besides, there is a procedure, ensuring the accountability of the assigned personnel.

CHAPTER 3
RESEARCH METHODOLOGY

3.1 Type, Method, and Object of the Research

This thesis utilizes descriptive qualitative and quantitative research method. Data collection is conducted through literature study on risk management, business continuity management, corporate governance, operational risk management, business continuity plan, and comprehensive emergency management.

Quantitative methodology test theory deductively from existing knowledge, through developing hypothesized relationships and proposed outcomes for study, qualitative approach are guided by certain ideas, perspectives or hunches regarding the subject to be investigated (Cormack, 1991). Qualitative research aims to achieve an in-depth understanding of a situation (Cooper and Schindler, 2008). Therefore, the important aspect is how to collect experience, opinion, feeling and the knowledge from the participants and afterwards adapting it to the aforementioned disciplines (Patton, 1990). All perspectives mentioned above become valuable for the author.

The type of the research used in this thesis is case study. The objective of the case study is to collect detail information using various data collection procedures while the phenomenon happens so that a deep understanding about the behavior and the reasons behind it can be obtained. Qualitative method investigates why and how aspects of a decision making, not only find the answers of what, where, and when. Thus, a small but well-directed sample is better than a large sample (Denzin and Lincoln, 2005).

The research instruments used by the author to obtain primary data in this thesis are questionnaire and interview. The content of questionnaire is being modified from BCP questionnaire that already being conducted by Stohr & Rohmeyer (2004) and based on corporate risk profile Jamsostek. By that means, the true picture of the situation can be gained and the analysis on the research object, PT Jamsostek (Persero) can be strengthened. Before the instruments are used to the respondents, an instrument test in the form of validity test and reliability test (*Cronbach's Alpha*) are conducted. The interview is using in depth interview. "In depth interview is a qualitative research techniques that involves conducting intensive individual interview to explore their perspectives on a particular idea, program, or situation" (Boyce & Neale, 2006: 3).The analysis of the result of in-depth interview will be done by using Spearman's Rho correlation. Based on the information obtained from www.statisticssolutions.com (accessed on June, 30 2011 at 07:15 pm). Spearman's Rhocoorelation is a non parametric test that is measured the degree of association between two variables. The aim of this coorelation is to analyze whether there is any hubungan saling mempengaruhi between respondents to answer the question and to analyze whether there is apakah ada hubungan saling mempengaruhi between the themes.

PT Jamsostek (Persero) is a state enterprise that organizes social security program for employees in Indonesia. One of the missions of PT Jamsostek (Persero) is to improve and develop the service quality and benefit to the member employees based on principles of professionalism. There are two critical functions of PT Jamsostek (Persero) which are operational- and service-related function and investment-related function. In this case, a business continuity plan (BCP) is required on the purpose to keep the continuity of the critical functions of PT Jamsostek (Persero) mentioned above. The BCP is already implemented in the company since 2010.

The phenomenon that can be observed are the awareness of the importance of BCP, the supporting documents, routine testing of infrastructure of PT Jamsostek (Persero). Based on the reasons mentioned above, the research conducted by the author will specifically focus on divisions related to the business continuity.

3.2 Research Stages

The research is initiated by the collection of primary and secondary data. The primary data was collected through in-depth interview and questionnaire. The secondary data is obtained directly from PT Jamsostek (Persero). The detailed stages of the research can be listed in detail as follows:

1. Initiation of the research by data collection through literature study and data analysis of information in PT Jamsostek (Persero).
2. Analysis of divisions directly related with critical business function of PT Jamsostek (Persero), such as Operation and Service Division and Investment Division, and also directs supporting of critical business function, such as Finance Division, Information Technology Division, Risk Management division based on questionnaire and interview.
3. Review the steps in creating BCP PT Jamsostek (Persero) based on interview result and review its documentation.
4. Risk identification by conducting risk assessment based on main risk sources of divisions directly related with business process. The identification is performed by using input, process, and output analysis of the corresponding divisions, which is also based on field study, literature study, questionnaire and interview.
5. The result of risk identification in relations of the divisions is being checked with the corporate risk profile of PT Jamsostek (Persero). This will be used to assess main risk identification (potential of critical risk) in ensuring the business continuity can be maintained.
6. Based on field study, literature study, data analysis, and analysis process already completed in the previous stages, an overview of BCP implementation in PT Jamsostek (Persero), since the BCP is created until now, can be obtained. As the result, risk sources, especially highest risk source in critical business function, can be identified. Then an assessment of how the implemented BCP can anticipate this risk source can be done.
7. Based on the identification, the current BCP in PT Jamsostek (Persero) will be compared with the effective model of BCP for the company. The objective in

this point is to find the gap between BCP model and BCP PT Jamsostek (Persero).

8. Propose recommendation for the improvement of BCP of PT Jamsostek (Persero) can be aligned with the BCP model to minimize the potentiality of risk.

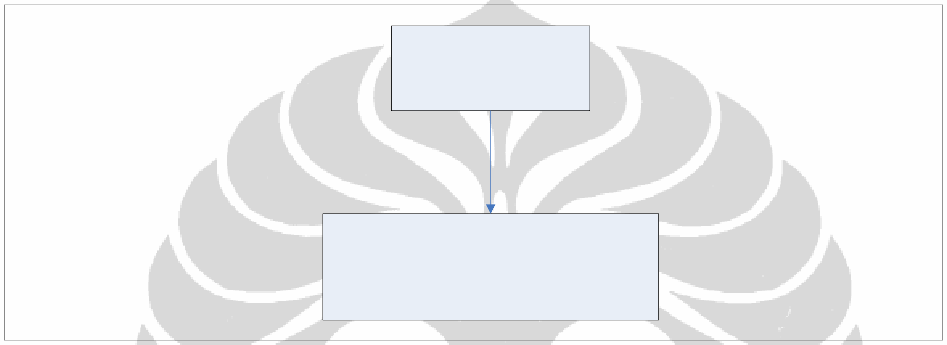


Figure 3.1 Research Stages: Data Analysis

Source: Primary Data Analysis

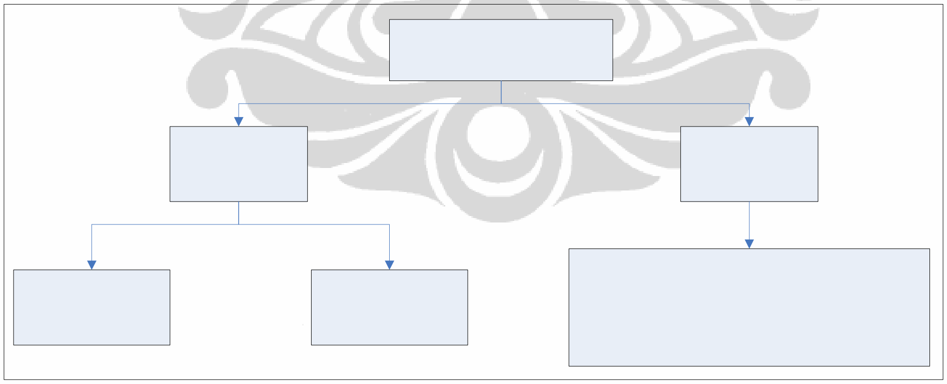


Figure 3.2 Research Stages: Data Collection Method

Source: Primary Data Analysis

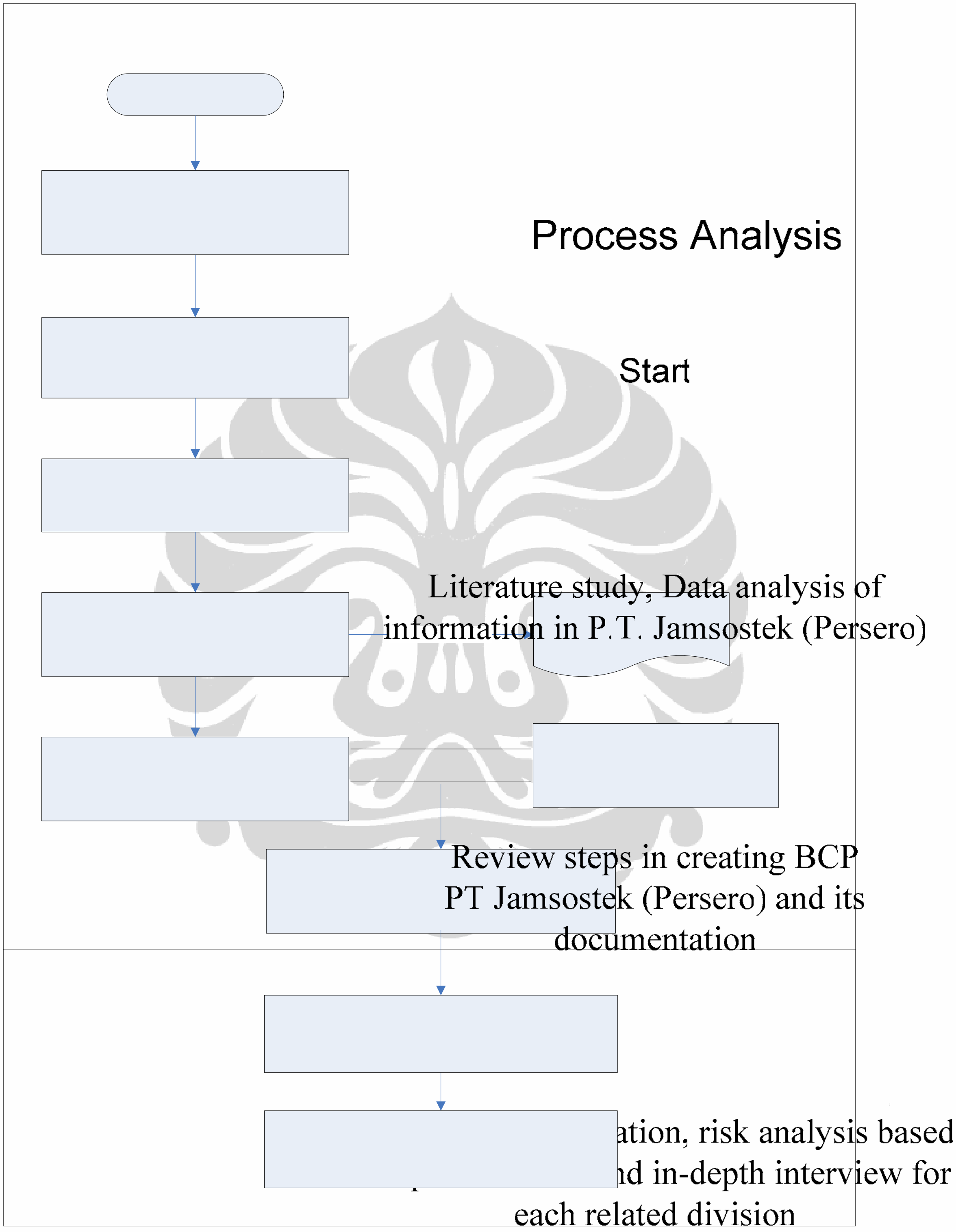

Process Analysis
Start
Literature study, Data analysis of
information in P.T. Jamsostek (Persero)
Review steps in creating BCP
PT Jamsostek (Persero) and its
documentation
ation, risk analysis based
nd in-depth interview for
each related division
Risk Assessment based on Main Risk
Sources of divisions
(Input/Process/Output)
C

Figure 3.3 Research Stages: Process Analysis

Source: Primary Data Analysis

3.3 Data Collection Method

3.3.1 Primary data

Primary data is the data that is never being published by any party before and must be obtained directly. There are several ways to obtain primary data such as interview, survey, case study, and observation. (Cooper and Schindler, 2008)

Primary data collection in this research is obtained by using questionnaire and interview. The questionnaire contains data directly sourced from respondents who are staffs of PT Jamsostek (Persero). Using the approach of qualitative research which involves non probability sampling, the method used in this thesis is purposive sampling. The respondent selection process is conducted by choosing participants arbitrarily based on the experience, job function, perception, and participation with business continuity plan in PT Jamsostek (Persero). The objective is to gain a valid and reliable opinion from the respondents regarding to the questions in the questionnaire. Questionnaires are distributed to the executives and lower to middle level management. The purpose of giving the questionnaire also the executives is to obtain a picture to measure their concern, their position to operational risk source in the work unit related with business continuity, how far the corporate governance regulates points in BCP that are related with company's main risk source, and lastly, how far the company already implemented business continuity best practice.

Meanwhile, the purpose of conducting questionnaire to lower to middle level management is to obtain a picture of the awareness level to BCP practice in the corresponding divisions, to perform cross-validation to the questionnaire result of the executives by mean of response and opinion test.

Interview will be conducted to the executives and lower to middle management, especially parties directly related to the creation and implementation of BCP in PT Jamsostek (Persero). The purpose is to shape a deeper understanding regarding main risk sources, issues, and matters that are related with BCP, as well as conducting cross-validation findings of the questionnaire result.

The choice of sample size for the questionnaire is based on finite sample size (Yamane and Taro in Israel, 1992). Mathematically, it can be written as follows:

$$n = \frac{N}{1 + N(e)^2}, \tag{3.1}$$

with:

n : total sample of respondent;

N : total population;

e : margin error or level of precision;

Total population is taken from some related divisions which are Operations and Service, Investment, Finance, Compliance and Risk Management, Planning, Development and Information. The total population is 132 staffs. With assumption the margin error is around 15%. Thus, the total sample required can be calculated as 33 respondents.

In this research, the samples of respondents are already given from PT Jamsostek (Persero), with the total number of respondents equals 34. Meanwhile, 33 respondents submit the filled questionnaires back. The respondents come from various divisions across the company. This is done to get an overall picture related to the BCP Jamsostek. The respondent are comes from:

1. Risk Management PT Jamsostek (Persero)
2. Information and Technology PT Jamsostek (Persero)
3. Planning and Development PT Jamsostek (Persero)
4. Corporate Secretary PT Jamsostek (Persero).
5. Money Capital Market division PT Jamsostek (Persero).
6. Portfolio Analysis division PT Jamsostek (Persero).
7. Facility and Infrastructure division PT Jamsostek (Persero).
8. Operation division PT Jamsostek (Persero).

9. Health Treatment Services PT Jamsostek (Persero)
10. Technical and Services PT Jamsostek (Persero)
11. Protocol and Household Affairs PT Jamsostek (Persero).
12. Finance Controller PT Jamsostek (Persero)

3.3.2 Secondary data

Secondary data is the data obtained by other party that already published before. The publication can be for general purpose like government census or specific purpose such as research projects (Blaikie in Hanggraeni, 2009). The common sources of secondary data are census, survey, organization records, collected through either qualitative or quantitative method.

The secondary data in this research is obtained from the company, such as the profile, BCP procedure, risk profile, and system and procedure of related divisions (operational and service, investment, finance), problem data log given by end users to Information Technology Division. The observation results are then used as the evaluation base of the BCP currently implemented in PT Jamsostek (Persero).

3.4 Data Analysis Method

3.4.1 The choice of data analysis method

The data analysis method is chosen based on the type of the data and the purpose of the analysis. The research uses the descriptive qualitative and quantitative method that describes the evaluation of the research objects. The analysis method in this research thus uses the instrument test.

The instrument which is tested in this research is the questionnaire. Before distributed to all related respondents, the validity and reliability of the questionnaire is tested by using *Cronbach's Alpha*) method. The purpose of the analysis is to obtain an accurate, credible, and reliable questionnaire.

The researcher used semi-structured interview and used analysis method of *Spearman's Rho* correlation is chosen to analyze the in-depth interview because the thematic code numbers extracted from the interview is still an ordinal data.

3.4.2 Validity and reliability test

Before the questionnaire, as the instrument of research, is distributed to all the respondents, it undergoes the validity and reliability.

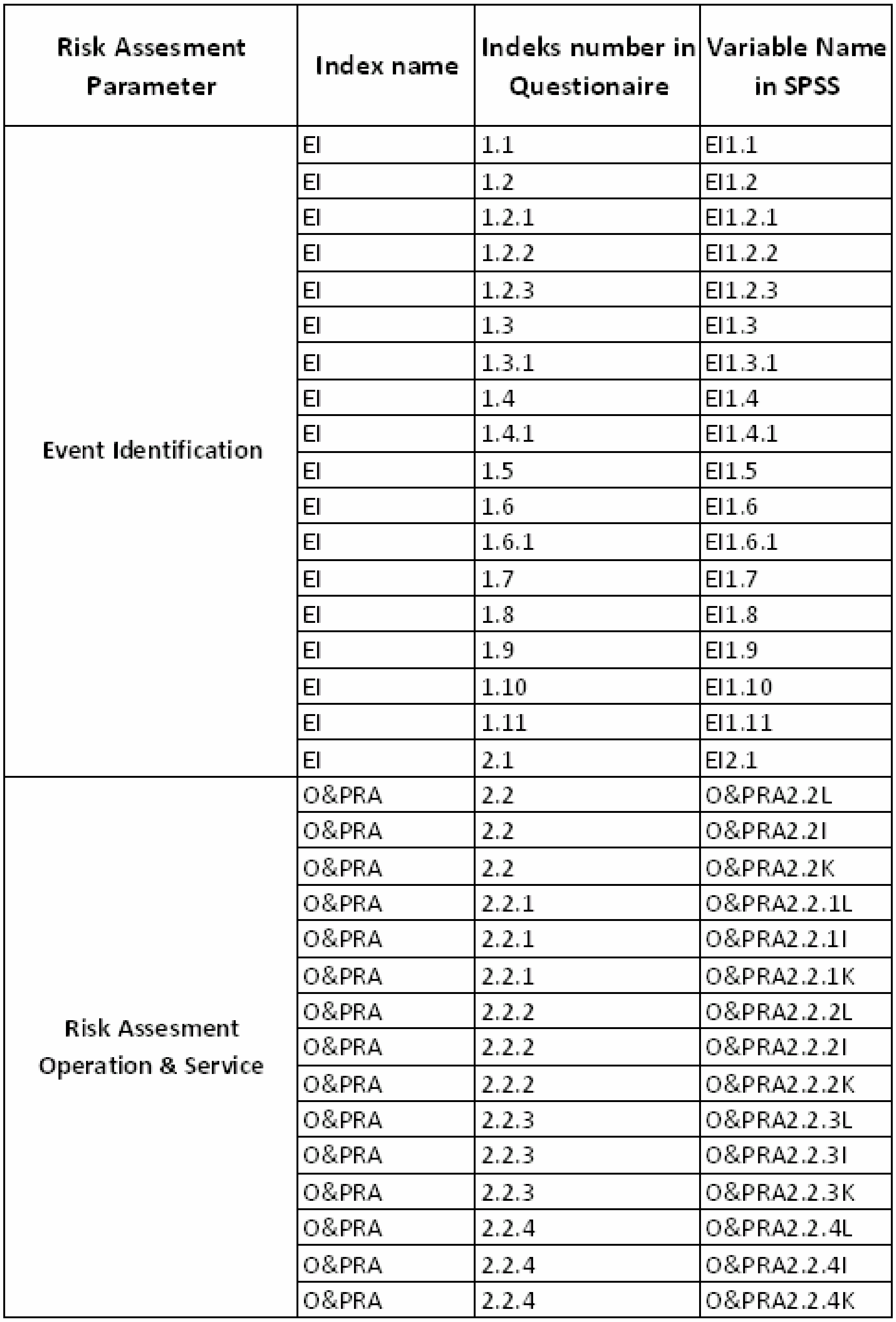
Validity Test

Validity Test shows the level of accuracy of the instrument in measuring the phenomenon of interest. Validity test is conducted by utilizing a factor analysis. The objective is to know how well every construction done during the thesis research can be defined by the measuring indicator variable (Hair et al., 2006).

In this research the validity test is already being assessed by using factor analysis. In doing the factor analysis, the main requirement that must be fulfilled is that the KMO (Keyser-Meyer-Olkin) number must be greater than 0.5 and the loading factor on the rotate component factor must be below 0.3 (Sarwono, 2006).

In this research, the questions are populated based on some parameters of enterprise risk management. Each parameter is categorized as class of population. The validation of each question will be tested based on the class of population. Please find below the population category align with the variable name which used in this category.

Table 3.1 Risk Assessment Parameters

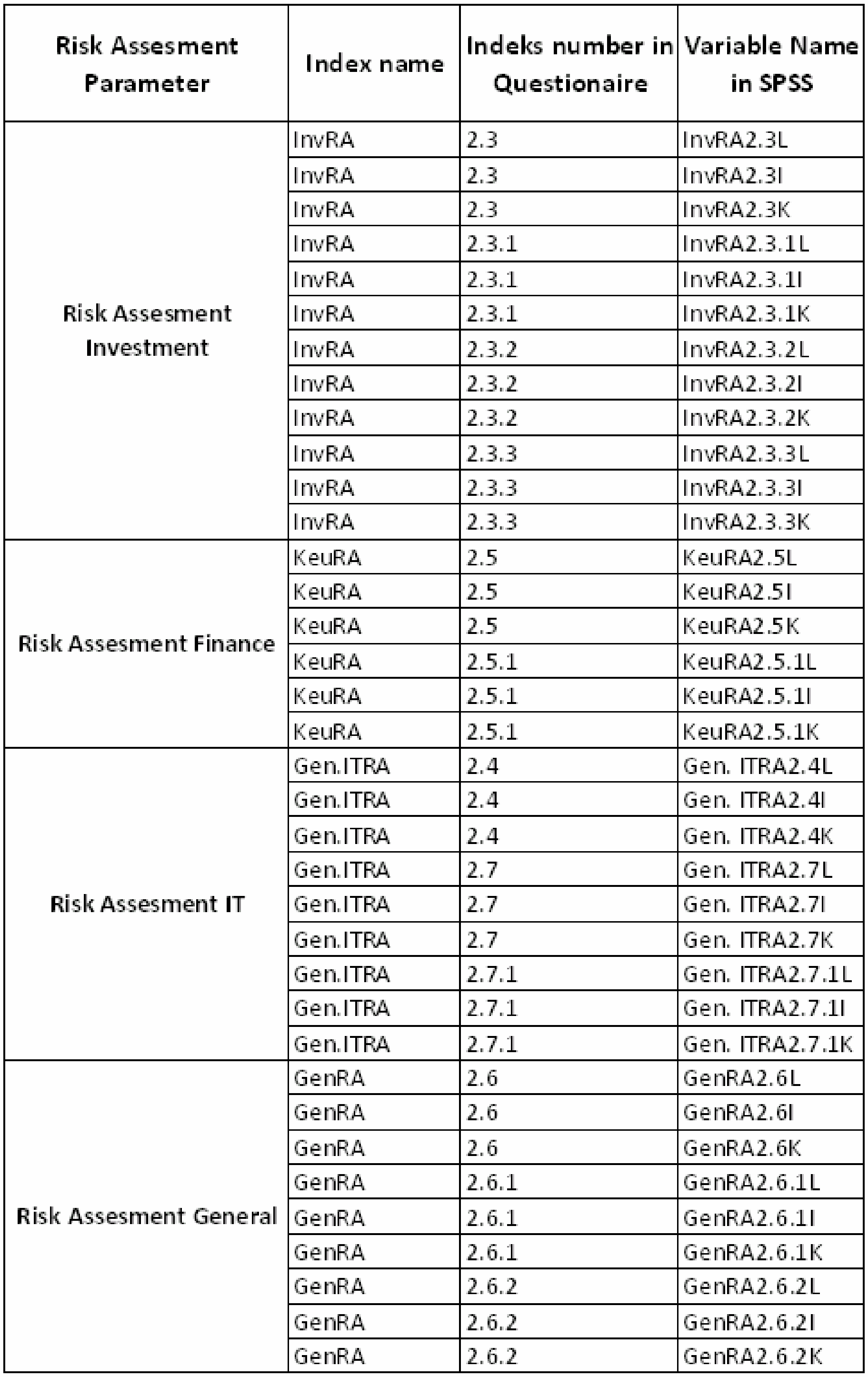


Risk Assesment Parameter	Index name	Indeks number in Questionaire	Variable Name in SPSS
Event Identification	EI	1.1	EI1.1
	EI	1.2	EI1.2
	EI	1.2.1	EI1.2.1
	EI	1.2.2	EI1.2.2
	EI	1.2.3	EI1.2.3
	EI	1.3	EI1.3
	EI	1.3.1	EI1.3.1
	EI	1.4	EI1.4
	EI	1.4.1	EI1.4.1
	EI	1.5	EI1.5
	EI	1.6	EI1.6
	EI	1.6.1	EI1.6.1
	EI	1.7	EI1.7
	EI	1.8	EI1.8
	EI	1.9	EI1.9
	EI	1.10	EI1.10
	EI	1.11	EI1.11
	EI	2.1	EI2.1
Risk Assesment Operation & Service	O&PRA	2.2	O&PRA2.2L
	O&PRA	2.2	O&PRA2.2I
	O&PRA	2.2	O&PRA2.2K
	O&PRA	2.2.1	O&PRA2.2.1L
	O&PRA	2.2.1	O&PRA2.2.1I
	O&PRA	2.2.1	O&PRA2.2.1K
	O&PRA	2.2.2	O&PRA2.2.2L
	O&PRA	2.2.2	O&PRA2.2.2I
	O&PRA	2.2.2	O&PRA2.2.2K
	O&PRA	2.2.3	O&PRA2.2.3L
	O&PRA	2.2.3	O&PRA2.2.3I
	O&PRA	2.2.3	O&PRA2.2.3K
	O&PRA	2.2.4	O&PRA2.2.4L
	O&PRA	2.2.4	O&PRA2.2.4I
	O&PRA	2.2.4	O&PRA2.2.4K

Source: Primary data analysis

(to be continued)

Table 3.1 Risk Assessment Parameters (continued)

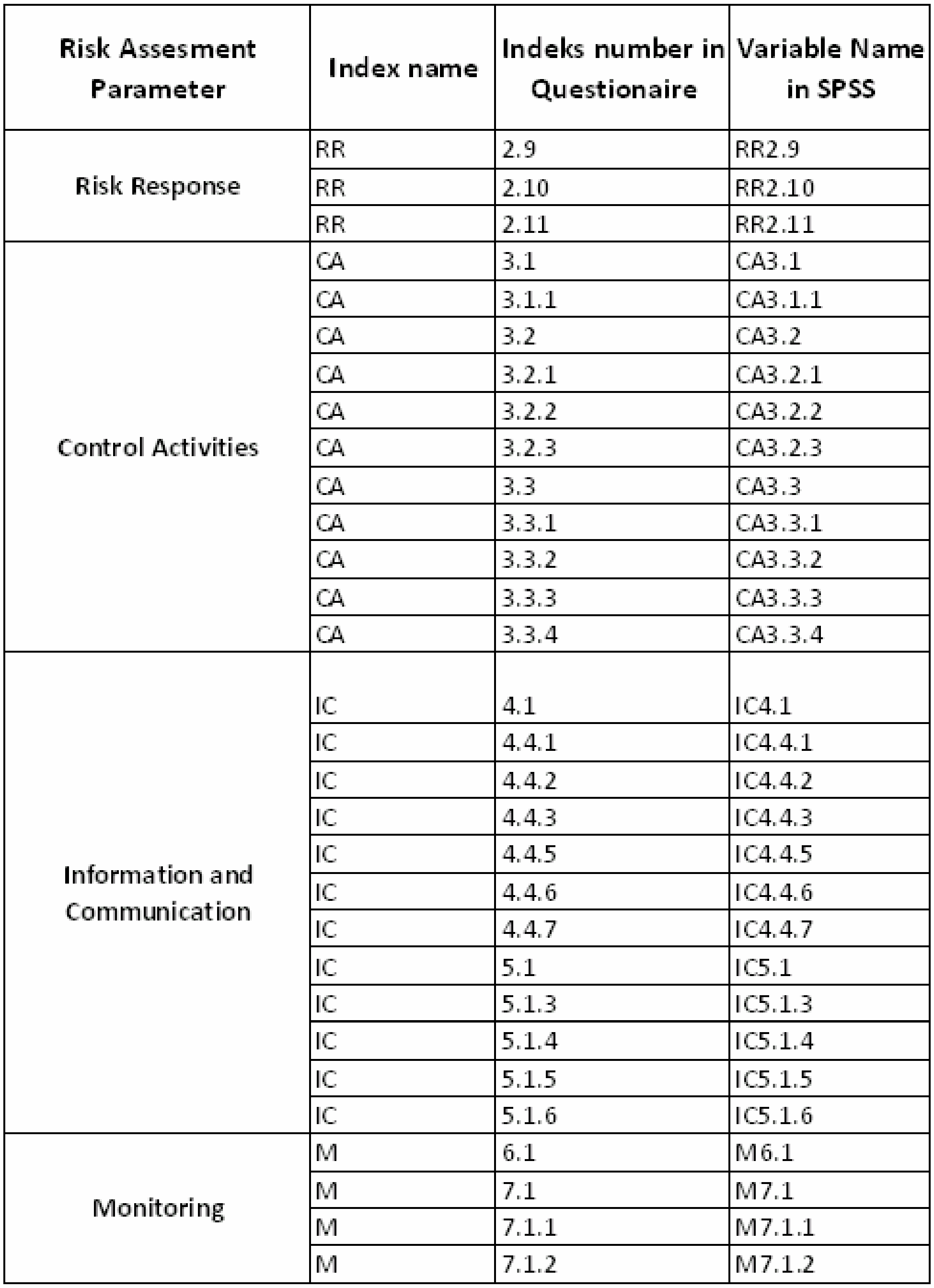


Risk Assesment Parameter	Index name	Indeks number in Questionaire	Variable Name in SPSS
Risk Assesment Investment	InvRA	2.3	InvRA2.3L
	InvRA	2.3	InvRA2.3I
	InvRA	2.3	InvRA2.3K
	InvRA	2.3.1	InvRA2.3.1L
	InvRA	2.3.1	InvRA2.3.1I
	InvRA	2.3.1	InvRA2.3.1K
	InvRA	2.3.2	InvRA2.3.2L
	InvRA	2.3.2	InvRA2.3.2I
	InvRA	2.3.2	InvRA2.3.2K
	InvRA	2.3.3	InvRA2.3.3L
	InvRA	2.3.3	InvRA2.3.3I
	InvRA	2.3.3	InvRA2.3.3K
Risk Assesment Finance	KeuRA	2.5	KeuRA2.5L
	KeuRA	2.5	KeuRA2.5I
	KeuRA	2.5	KeuRA2.5K
	KeuRA	2.5.1	KeuRA2.5.1L
	KeuRA	2.5.1	KeuRA2.5.1I
	KeuRA	2.5.1	KeuRA2.5.1K
Risk Assesment IT	Gen.ITRA	2.4	Gen. ITRA2.4L
	Gen.ITRA	2.4	Gen. ITRA2.4I
	Gen.ITRA	2.4	Gen. ITRA2.4K
	Gen.ITRA	2.7	Gen. ITRA2.7L
	Gen.ITRA	2.7	Gen. ITRA2.7I
	Gen.ITRA	2.7	Gen. ITRA2.7K
	Gen.ITRA	2.7.1	Gen. ITRA2.7.1L
	Gen.ITRA	2.7.1	Gen. ITRA2.7.1I
	Gen.ITRA	2.7.1	Gen. ITRA2.7.1K
Risk Assesment General	GenRA	2.6	GenRA2.6L
	GenRA	2.6	GenRA2.6I
	GenRA	2.6	GenRA2.6K
	GenRA	2.6.1	GenRA2.6.1L
	GenRA	2.6.1	GenRA2.6.1I
	GenRA	2.6.1	GenRA2.6.1K
	GenRA	2.6.2	GenRA2.6.2L
	GenRA	2.6.2	GenRA2.6.2I
	GenRA	2.6.2	GenRA2.6.2K

Source: Primary data analysis

(to be continued)

Table 3.1 Risk Assessment Parameters (continued)



Risk Assesment Parameter	Index name	Indeks number in Questionaire	Variable Name in SPSS
Risk Response	RR	2.9	RR2.9
	RR	2.10	RR2.10
	RR	2.11	RR2.11
Control Activities	CA	3.1	CA3.1
	CA	3.1.1	CA3.1.1
	CA	3.2	CA3.2
	CA	3.2.1	CA3.2.1
	CA	3.2.2	CA3.2.2
	CA	3.2.3	CA3.2.3
	CA	3.3	CA3.3
	CA	3.3.1	CA3.3.1
	CA	3.3.2	CA3.3.2
	CA	3.3.3	CA3.3.3
	CA	3.3.4	CA3.3.4
Information and Communication	IC	4.1	IC4.1
	IC	4.4.1	IC4.4.1
	IC	4.4.2	IC4.4.2
	IC	4.4.3	IC4.4.3
	IC	4.4.5	IC4.4.5
	IC	4.4.6	IC4.4.6
	IC	4.4.7	IC4.4.7
	IC	5.1	IC5.1
	IC	5.1.3	IC5.1.3
	IC	5.1.4	IC5.1.4
	IC	5.1.5	IC5.1.5
	IC	5.1.6	IC5.1.6
Monitoring	M	6.1	M6.1
	M	7.1	M7.1
	M	7.1.1	M7.1.1
	M	7.1.2	M7.1.2

Source: Primary data analysis

The tools that used to testing the validity is SPSS verse 17. Based on the validity testing some questions already passed the validation testing and in the further consideration it can be analyzed. Meanwhile for the rest questions that need to be eliminated from the questionnaire. The detail of the tests step can be shown in the attachments regarding “Result of Validity & Reliability Test.”

There are some questions that need to be dropped from the questionnaire. The reasons are:

1. The questions about the category of disaster. The disasters are classified into several levels as written in BCP of PT Jamsostek (Persero), but yet being acknowledged in detail and specifically by all respondents. Clear segregation does not exist until the time being and the clear examples for each disaster level are not yet given.
2. The BCP test covering all divisions has never been done. This causes the fact that not all of the respondents clearly know about that certain information and the result of the test.
3. Not all of the respondents participate actively and has a role in composing, evaluation, and improvement of the BCP in PT Jamsostek (Persero).
4. There is not clear and specific structure in the organization of BCP activation. This makes the answers of the respondents invalid.
5. The involvement and awareness of the respondents to training program is still low. Thus, deep knowledge about details in the BCP is very inferior.

Reliability

Cited from Ho (2006), the reliability of a measuring instrument is defined as its ability to consistently measure the phenomenon it is designed to measure.” Reliability refers to the consistency of the test itself. The procedure used for this purpose is from the category of Internal Consistency Procedures. It measures to what extend the items in a test measure the same construct. The method used is *Cronbach’s Alpha*. This method uses a single correlation coefficient which is an estimate of the average of all the correlation coefficients of the items within a test. If alpha is high, then this suggests that all of the items are reliable and the entire test is internally consistent. Otherwise if alpha is low, that means that at least one of the items is unreliable. In this case, the unreliable items must be identified through item analysis procedure.

The statistic *Cronbach's Alpha* (α) of the questionnaire used along the research reported in this thesis can be calculated by using the following formula:

$$\alpha = \frac{k(\mathrm{cov}/\mathrm{var})}{1+(k-1)(\mathrm{cov}/\mathrm{var})} \tag{3.2}$$

where:

α : statistic *Cronbach's Alpha*

k : number of questions in the questionnaire

cov : average covariance between questions in the questionnaire

var : average variance of the questions in the questionnaire

The value of α is the indication that the tested questionnaire is reliable. The software tool that is used to test the validity is SPSS verse 17. The approach to test the reliability is categorized based on the class of population. Each question that already passed the validity test will be now tested against reliability.

The tables below show the reliability result for each class of population. The source of each of them is the analysis of the primary data.

1. Event Identification

Table 3.2 Result of Reliability Result Event Identification

Reliability Statistics

Cronbach's Alpha	N of Items
.930	7

Source: Primary data analysis

2. Risk Assessment Operation and Service

Table 3.3 Result of Reliability Result Risk Assessment Operation and Service

Likelihood		Impact		Category	
Reliability Statistics		**Reliability Statistics**		**Reliability Statistics**	
Cronbach's Alpha	N of Items	Cronbach's Alpha	N of Items	Cronbach's Alpha	N of Items
.953	5	.841	4	.893	5

Source: Primary data analysis

3. Risk Assessment Investment

Table 3.4 Result of Reliability Result Risk Assessment Investment

Likelihood		Impact		Category	
Reliability Statistics		**Reliability Statistics**		**Reliability Statistics**	
Cronbach's Alpha	N of Items	Cronbach's Alpha	N of Items	Cronbach's Alpha	N of Items
.971	4	.893	4	.920	4

Source: Primary data analysis

4. Risk Assessment Finance

Table 3.5 Result of Reliability Result Risk Assessment Finance

Likelihood		Impact		Category	
Reliability Statistics		**Reliability Statistics**		**Reliability Statistics**	
Cronbach's Alpha	N of Items	Cronbach's Alpha	N of Items	Cronbach's Alpha	N of Items
.968	2	.969	2	.960	2

Source: Primary data analysis

5. Risk Assessment Information Technology

Table 3.6 Result of Reliability Result Risk Assessment Information Technology

Likelihood		Impact		Category	
Reliability Statistics		**Reliability Statistics**		**Reliability Statistics**	
Cronbach's Alpha	N of Items	Cronbach's Alpha	N of Items	Cronbach's Alpha	N of Items
.807	3	.852	3	.800	3

Source: Primary data analysis

6. Risk Assessment General

Table 3.7 Result of Reliability Result Risk Assessment General

Likelihood		Impact		Category	
Reliability Statistics		**Reliability Statistics**		**Reliability Statistics**	
Cronbach's Alpha	N of Items	Cronbach's Alpha	N of Items	Cronbach's Alpha	N of Items
.954	3	.953	3	.957	3

Source: Primary data analysis

7. Risk Response

Table 3.8 Result of Reliability Result Risk Response

Reliability Statistics

Cronbach's Alpha	N of Items
.851	3

Source: Primary data analysis

8. Control Activities

Table 3.9 Result of Reliability Result Control Activities

Reliability Statistics

Cronbach's Alpha	N of Items
.876	6

Source: Primary data analysis

9. Information and Communication

Table 3.10 Result of Reliability Result Information and Communication

Reliability Statistics

Cronbach's Alpha	N of Items
.888	5

Source: Primary data analysis

10. Monitoring

Table 3.11 Result of Reliability Result Monitoring

Reliability Statistics

Cronbach's Alpha	N of Items
.820	4

Source: Primary data analysis

All Tables 3.2 up to 3.11, as the result of primary data analysis, show the value of *Cronbach's Alpha* for each class population is higher than 0.6. This means that the questions is already valid and can be trusted, since it is reliable as an instrument to collect primary data.

3.4.3 Analysis of in-depth interview

The research variables can be measured by using quantitative and qualitative data. Quantitative data is verbal description, such as transcripts, textual data, words, and intentions. Different compare to quantitative data which is confirmatory and analyzed using deductive approach, qualitative data is explorative and is analyzed using inductive approach (Trochim in Hanggraeni, 2009). Qualitative data is also directed to obtain concecpt understanding, synthesis of theory, and delivering deep explanation about a concept or theory.

Analysis of qualitative data in the form of verbal description obtained from in-depth interview and answers of open questions from respondents is conducted by using qualitative thematic code table. The verbal description of respondents initially categorized into a number of themes that will be identified. Afterwards, a qualitative thematic code table can be built, and the table provides relations between each respondent and the themes already identified, as suggested by Trochim in Hanggraeni (2009). An example of the table code mentioned above can be given as follows.

Table 3.12 Example of Thematic Qualitative Code Table

Respondent	Theme 1	Theme 2	Theme 3	Theme 4	Theme 5
1	✓	✓		✓	
2	✓		✓		
3	✓	✓		✓	
4		✓		✓	
5		✓		✓	✓
6	✓	✓			✓
7			✓	✓	✓
8		✓		✓	
9			✓		✓
10				✓	✓

Source: Trochim in Hanggraeni (2009)

Qualitative thematic code above is further modified to become qualitative thematic code number so that a deeper analysis on the qualitative result of in-depth interview to the respondents can be conducted. Table 3.13 presents the qualitative thematic code number table of the example presented in Table 3.12.

Table 3.13 Example of Thematic Qualitative Code Number Table

Respondent	Theme 1	Theme 2	Theme 3	Theme 4	Theme 5
1	1	1	0	1	0
2	1	0	1	0	0
3	1	1	0	1	0
4	0	1	0	1	0
5	0	1	0	1	1
6	1	1	0	0	1
7	0	0	1	1	1
8	0	1	0	1	0
9	0	0	1	0	1
10	0	0	0	1	1

Source: Trochim in Hanggraeni (2009)

Interviews are conducted deeply to a set of respondents that are selected by using the referred sampling method. The interviewed respondents come from:

1. Risk Management division
2. Information Technology division
3. Investment division
4. Operation and service division
5. Investment division
6. Head of Protocol and Household Affairs division

3.4.4 Spearman’s Rho correlation

Based on the table of code number, a simple correlation matrix of inter-thematic and inter-respondent is made, and further a useful analysis result can be yielded. Spearman’s Rho correlation can be calculated by using the following formula (Trochim in Hanggraeni, 2009):

Spearman’s of:

$$\rho = 1 - {6\sum D^2}\Big/{N\left(N^2 - 1\right)} \tag{3.3}$$

with:

D : difference

N : the number of issues being observed

3.4.5 Descriptive statistics

Descriptive statistics is a kind of statistic analysis techniques that is related with illustrating and summarizing research data, so that it can be easily understood (Santosa and Ashari in Hanggraeni, 2009). By using descriptive statistics, a general view of respondent profile can be obtained. This view is based on gender, duration of service, highest education level, position, department, and relation with business continuity team in PT Jamsostek (Persero). Further classifications are the position of direct supervisor, percentage of time devoted by the respondent to matters related to business continuity planning, and total amount of work experience that is related directly with business continuity planning. From the descriptive statistics, a general view of respondent answer to each question in the questionnaire can also be obtained. The result of descriptive statistic analysis can be presented in the form of frequency table or graph.

CHAPTER 4
CORPORATE GENERAL OVERVIEW

4.1 PT Jamsostek (Persero) at a Glance

PT Jamsostek (Persero) is closely related to the Government seriousness in managing social security. Along the process of government effort to excel the social security regulation by issuing regulations related to the social security services to workface. Then in 1977, the Government issued its regulation No. 33 about the Employees Social Insurance, known in Indonesian abbreviation as ASTEK. The regulation required all employers, private businesses, state owned enterprises and regional companies to join the ASTEK scheme. This regulation was then excelled with the Law No. 3 year 1992 compelling all employers and employees to have social security. This law is the milestone of the establishment of PT Jamsostek (Persero). The Government Regulation No. 36/1995 ascertains PT Jamsostek (Persero)'s position as the administrating body of Workers Social Security.

Jamsostek program/schemes ensure guarantee workers' in obtaining basic protections to fulfil their basic requirement. The schemes ensuring offer employee's income flow to compensate partial or total loss of income due to social risks. Jamsostek scheme also acts as appreciation to employees for their contributions and dedication to the company they work with.

4.2 PT Jamsostek (Persero) Objective, Vision, Mission and Core Value

Below are the objective, mission, vision, and core value of PT Jamsostek (Persero).

The objective

To provide basic protection for employees and their families against social and economic risks which arises due to a decline or loss in the flow of their income as a result of work related accident, old age or death, as well as against the risk of illness.

The Vision

To become a trustworthy provider of employee social security scheme, emphasizing quality service and benefits to all members.

The Mission

1. To improve and develop the service quality and benefits to members based on the principles of professionalism;
2. To increase the number of members of employees social security scheme;
3. To enhance a Work Culture through the increasing quality of Human Resources and the implementation of Good Corporate Governance;
4. To manage members fund in a prudent manner;
5. To improve the corporate values and corporate image.

Core Values

1. Strong commitment and integrity, as well as responsibility.
2. Prioritize the interest and satisfaction of all members.
3. Honesty and creativity.
4. Dynamic and harmonious teamwork.
5. Continuous learning and improvements
6. Trust and mutual respect.
7. Effective leadership.
8. Cost consciousness.
9. Based on competency.

4.3 Organizational Structure

Organizational structure in PT Jamsostek (Persero) can be described as below.

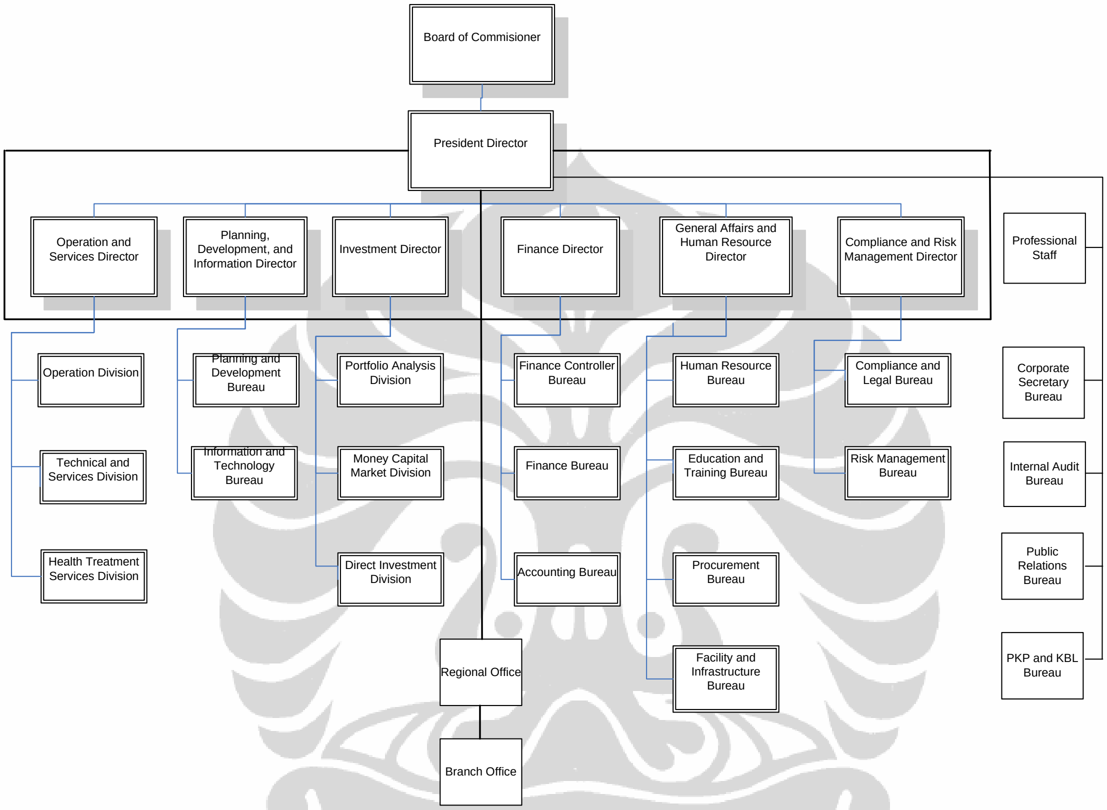

Board of Commisioner
President Director
Operation and Services Director
Planning, Development, and Information Director
Investment Director
Finance Director
General Affairs and Human Resource Director
Compliance and Risk Management Director
Professional Staff
Operation Division
Technical and Services Division
Health Treatment Services Division
Planning and Development Bureau
Information and Technology Bureau
Portfolio Analysis Division
Money Capital Market Division
Direct Investment Division
Finance Controller Bureau
Finance Bureau
Accounting Bureau
Human Resource Bureau
Education and Training Bureau
Procurement Bureau
Facility and Infrastructure Bureau
Compliance and Legal Bureau
Risk Management Bureau
Corporate Secretary Bureau
Internal Audit Bureau
Public Relations Bureau
PKP and KBL Bureau
Regional Office
Branch Office

Figure 4.1 Organizational Chart of PT Jamsostek (Persero)

Source: Jamsostek documents *(Organisasi Kantor Pusat Jamsostek* (2007))

PT Jamsostek (Persero) consists of 2 main core divisions and several supporting divisions.

The main core divisions are:

1. Operation and Services Division

This division handles anything related with the operation and service to the employee members and the prospective members of PT Jamsostek (Persero). The division is divided into 3 subdivisions:

- Operation Division

  The objective of this division is to publish guideline, technical direction, and Jamsostek membership card.

- Service Division

2. Investment Division

The supporting divisions can be listed as:

1. Finance Division
2. General Affairs and Human Resource Division
3. Planning, Development, and Information Division
4. Compliance and Risk Management Division
5. Task Unit under direct coordination of CEO

4.4 Products and Services PT Jamsostek (Persero)

Jamsostek designs all products based on the noble idea of providing workers and their families with basic protections in order to secure workers' social security.

Jamsostek is the business partner to state-owned enterprises, joint venture, foreign investment companies, foundations, cooperatives and small-medium enterprises that employ at least ten workers or pay their workers wages of Rp 1,000,000 minimum per month. Participations in all Jamsostek programs are legally administered by the Law No. 3 year 1992 about Employee Social Security and the implementation is stipulated in the Government Regulation No. 14 year 1993, the President Decree No. 22 year 1993 and the Labor Minister Regulation No.PER.05/MEN/1993. However, in order to guarantee the rights of members, the service quality of PT Jamsostek

(Persero) was improved by enacting the Minister/Secretary of Man Power and Transmigration Regulation No. PER-12/MEN/VI/2007 in December 1st 2007, also in replacement for the previous regulation, the Minister/Secretary of Man Power and Transmigration Regulation No. PER-05/MEN/1993.

In December 2006, Government of Republic Indonesia Regulation No. 76, year 2007 was enacted, regarding the fifth amendment of Government Regulation No. 14 year 1993, in regards to the Social Security program operation.

This government regulation enactment resulted in the increasing benefit of the Social Security Service of its members.

There are some programs related with Social Security Services:

1. *Employment Accident Benefit* (JKK). This program deals with work-related accidents or permanent handicap/diseases.
2. *Old Age Benefit* (JHT). The Old Age Benefit is a saving mechanism managed by collecting members' funds that provide certainty of flow of income in the case of employee loses of income due to several conditions including death, total disability or retirement.
3. *Death Benefit* (JKM). This program is a benefit provided to employee's beneficiaries in the case of death resulted from non-work related accidents. JKM is provided to alleviate the burdens of the families in the forms of funeral expenses and financial benefits.
4. *Health Care Benefit* (JPK). This program is helped to assists workers and their families to take care of their health. This program provides benefits starting from preventive, curative, and rehabilitative services.

4.5 Business Process PT Jamsostek (Persero)

The general overview of the business process in PT Jamsostek (Persero) can be classified into Business model of PT Jamsostek (Persero), Operational & Service Process, Investment Process, and Supporting Process.

Each business process in the company will now be discussed in more detail:

1. Business Model of PT Jamsostek (Persero)

   The business model applied in the company is divided into 3 parts: management process, main process, and supporting process. In the following figure, the overview of PT Jamsostek (Persero)'s business model is presented:

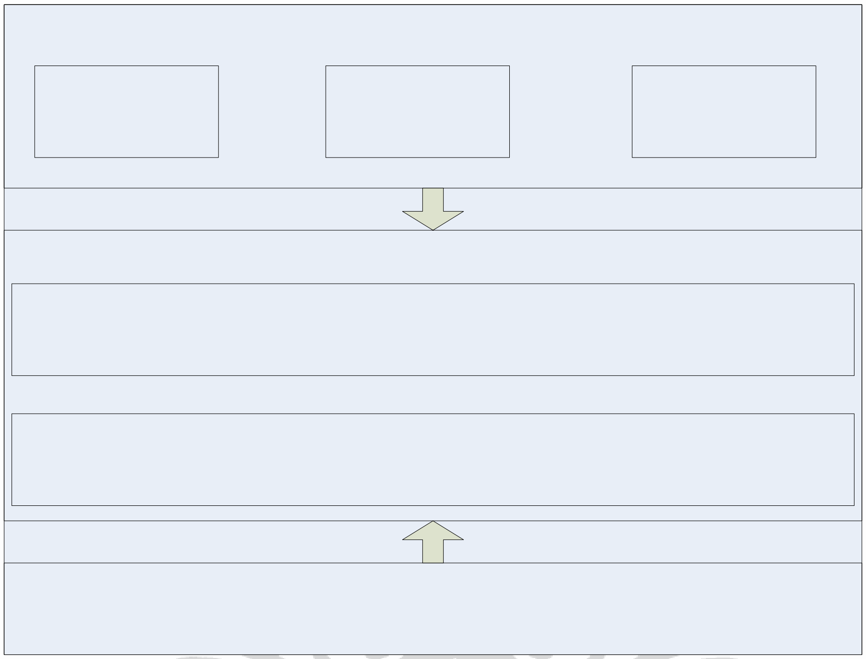

MANAGEM
SET DECISION OF VISION, MISSION, POLICY, OBJECTIVE OF COMPANY
SET D COMP
MAIN
OPERATION
INVES

Figure 4.2 Business Model PT Jamsostek (Persero)

Source: Jamsostek documents (*Manual Mutu* (2008))

2. Operation and Service Process

   This business process is one of the main business processes in PT Jamsostek (Persero). There are 4 processes in the Operational and Service Division, which are:

   - *Membership Expansion Process*. This process is related with the making of plans and programs on the purpose to achieve the target quantity of new membership. This process has a tight relation with the providing and maintenance of potential data, arrangement of socialization and supply control, and partnership in membership expansion.

- *Membership Maintenance Process*. This process is related with the making of plans and programs on the purpose to develop and improve good communication with parties related directly to the membership of PT Jamsostek (Persero). It also serves as an instrument to improve the service. The membership maintenance process organizes the management events and activity through partnership, membership management, and membership administration. Besides, it also deals with supply assurance and socialization to the members.
- *Security Service Process*. This process related with the determination of security service policy that closely related with control, statistic analysis, medical collaboration, and health and medical service. Besides, this process also manages processes related with product design and development delivered by the Operation and Service Division. The end result should be the increase of security benefit to the employee members of PT Jamsostek (Persero).

  There are several serviced programs that can be ordered under the Security Service Process:

  - *Retirement Benefit Service*. This process manages things related with retirement such as document acceptance service, value determination service, and the payment of pension to retired employee members.
  - *Death Benefit Service*. This process is related with matters such as death document acceptance, value determination service, and the payment of death compensation.
  - *Work Accidence Security Service*. This process specifically related with the identification, follow-up of accidence report, trauma handling

scheme, up to detailed things related with hospital bills and periodic handicap compensation.

- *Health and Medical Service*. This process deals with health and medical related matters such as capitation, claim consolidation, acceptance of capitation claim from provider, payment of capitation to provider, and administration of guarantee letters and other supporting documents.

- *Monitoring and Performance Evaluation Process*. This process is related with the observation and measurement of operational performance in PT Jamsostek (Persero) on the purpose to improve the service quality. This process has a strong connection with the arrangement of information system management, account officer performance assessment, branch office performance assessment, indicator setting and regional unit target, and lastly the class status evaluation of branch office.

  Two sub-processes related with Monitoring and Performance Evaluation can be mentioned as:

  - *Expansion and Maintenance of Health Service Centers*. This process is related with the data processing, the assignment of health service center, and matters related with the cost calculation, provider analysis up to the quality assurance and quality management.

  - *Construction Service*. This process is related with the membership expansion, data processing, planning, follow-up of unregistered membership projects, membership maintenance, and maters closely linked with construction process such as installment payment, determination of collection fee, payment of collection fee, as well as the acceptance of installment.

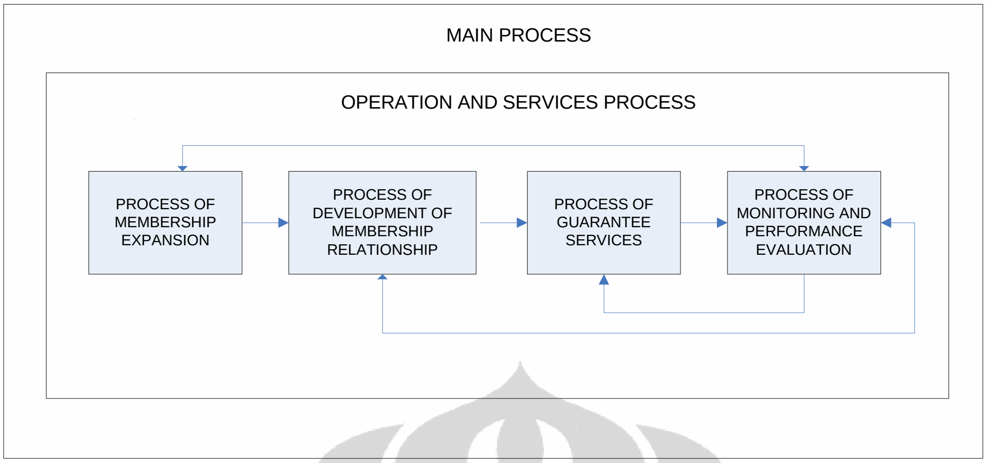

MAIN PROCESS
OPERATION AND SERVICES PROCESS
PROCESS OF MEMBERSHIP EXPANSION
PROCESS OF DEVELOPMENT OF MEMBERSHIP RELATIONSHIP
PROCESS OF GUARANTEE SERVICES
PROCESS OF MONITORING AND PERFORMANCE EVALUATION

Figure 4.3 Operation and Services Process PT Jamsostek (Persero)

Source: Jamsostek documents (*Manual Mutu* (2008))

3. Investment Process

There are 2 investment objectives claimed by PT Jamsostek (Persero), which are:

- Retirement Program Investment Objective
- Non-Retirement Program Investment Objective

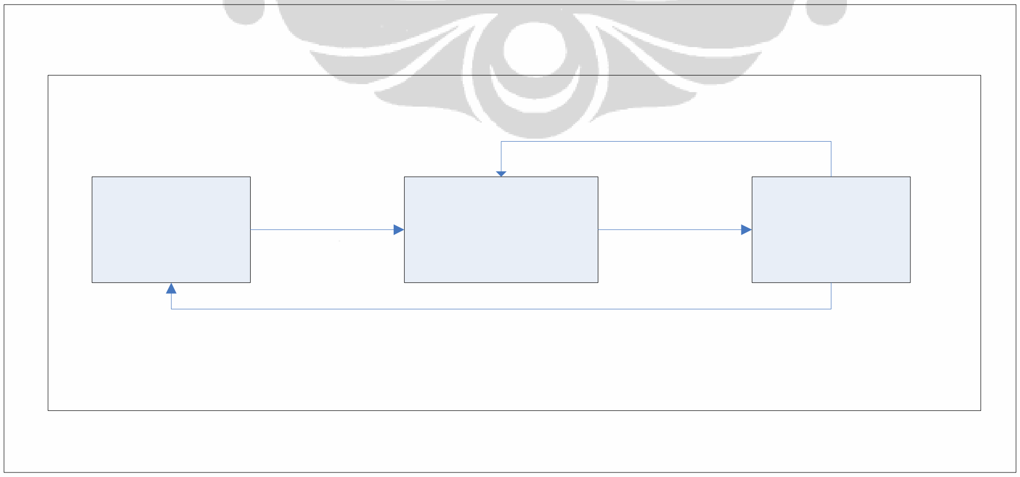


Figure 4.4 Operation and Services Process PT Jamsostek (Persero)

Source: Jamsostek documents (*Manual Mutu* (2008))

4. Supporting Processes

   The supporting processes consist of:

   - Finance Process
   - General Affairs and Human Resource Process
   - Planning, Development, and Information Process
   - Compliance and Risk Management Process
   - Work Unit under the supervision of CEO

4.6 Risk Management of PT Jamsostek (Persero)

The policy of risk management of PT Jamsostek (Persero) serves as a reference in the implementation of integrated and consistent risk management. The job description of Work Unit Risk Management includes the development of risk management policy, marketable security, direct investment, finance and portfolio, and operational. The risk management system will give orientation to all activities to achieve the vision and mission of the company. At the same time, a stable long-term profit achievement and optimal capital allocation to support healthy business activity are also becoming the objective while keep delivering accurate finance and management reports.

There are several processes related with risk management:

1. *Development of policy guideline on risk management*. The objective of this process is to develop a guideline that can be used as reference in managing the company’s risk.
2. *Development of risk review result*. Risk review can be related with several different aspect:

   - *Investment Risk*. Some examples of this risk are marketable securities, currency market risk, stock exchange risk, obligation risk, mutual funds risk, direct investment risk, property investment risk, and investment portfolio risk.

- *Financial Risk*. This is related with the fulfillment of liquidity standard such as finance, portfolio, risk, and capital demand risk.
- *Operational Risk*. This is related with the risk reviews of business process, information technology risk, general risk, human resource risk, and law risk.

4.7 Business Continuity Plan of PT Jamsostek (Persero)

The initiation of BCP in PT Jamsostek (Persero) is based on the determination to achieve the vision of PT Jamsostek (Persero) to become a trustworthy institution that arranges the employee' social security and gives priority in excellent service and optimal benefit to all its member. The company must continually improve the operational capacity and resilience in providing service in social security program even when disturbance or disaster/catastrophe happens.

The BCP of PT Jamsostek (Persero) is aimed to guarantee the continuity of the main business processes of the company in case disturbance or disaster/catastrophe occurs. The main business processes of the company covers:

1. Integrated social security program service for employee as instructed by ministry regulation of Peraturan Menteri Tenaga Kerja dan Transmigrasi Nomor Per-12/Men/VI/2007 obout the technical direction on membership registration, installment payment, compensation payment, an social security service to the employee in Republic of Indonesia.
2. Development and administration of member funds

The framework of BCP of PT Jamsostek can be listed as:

1. *Disaster Mitigation Plan*. Done based on actions with strategic, tactical, and technical values. This is done from the time when the disaster happens, the recovery phase, until the business activity can be normalized and the operation back to normal again.

- *Strategic Plan*. This plan is intended to tackle strategic issues related with the occurrence of the disturbance or disaster along with their impacts.
- *Tactical Plan*. This includes procedures and processes required to run the business continuity and the mobilization of resources, if in case disturbance or disaster occurs in various locations of main office and/or branch office(s).
- *Technical Plan*. This includes the recovery plan and business restoration, done on the level of work unit in main office or branch office so that they can operate normally as soon as possible.
- *Emergency response against disaster*. Emergency Response is identified as basic and spontaneous activities when and shortly after a disaster occurs.

2. *Organization Business Continuity*. The structure of the organization business continuity owned by PT Jamsostek (Persero) is developed so that various strategic, tactical, and operational problems in handling disaster can be done effectively and efficiently. The structure of this organization consists of several stages as follows:

    - *Executive Crisis Management Team* (*ECMT*). ECMT is an organization under the responsibility of CEO, membered by all executive officers. The function is to make decisions in critical issues. The responsibility is separated into 2 aspects, financial aspects (under the coordination of Director of Investment and Director of Finance), and Operation Aspects (under the coordination of Director of General Affairs and Human Resources and Director of Planning, Development, and Information).
    - *Crisis Management Team* (*CMT*). CMT is a team made up by several division heads or bureau heads, directly supervising work unit for operational activity to support the recovery process of critical business when a disturbance/disaster occurs.

- *Business Continuity Team* (*BCT*). BCT is the operational action team for BCP in the level of division/bureau work unit and branch office, with the responsibility to maintain the business continuity in each work unit and its recovery when a disturbance/disaster occurs. The coordinator of BCT is the division/bureau head and the head of branch office.

3. *BCP Maintenance*. The purpose of maintaining BCP is to ensure that all BCP documents are ready to use in case disturbance/disaster occurs in unpredicted time.

4. *BCP Training and Testing*. The purpose of BCP training is to improve the knowledge and awareness on how to prepare and response to emergency condition that may have impacts to business continuity. Besides, to improve the ability and to provide direct experience to all employee of PT Jamsostek (Persero).

   The purpose of BCP testing is to validate the business continuity plan (BCP) and to ensure the readiness of the business supporting system in facing emergency condition. After that, identification must be done to know certain aspects needed to be improved.

CHAPTER 5
ANALYSIS AND DISCUSSION

5.1 Preliminary Remarks

In the analyzing phase, the researcher uses some theories and best practices to create foundation of Business Continuity model. The theories used come from enterprise risk management, business continuity management, and business continuity plan from a number of sources such as Gallagher, DRII, COSO and ISO 31000. Besides, the model will follow some BCP best practices that already being applied as BCP public society in US and already being implemented in some government institutions such as POLRI and Angkasapura I & II. Also, there is a business continuity model known as BC-EM model that is already published as a research result.

5.2 Observation of PT Jamsostek (Persero)

5.2.1 Descriptive statistic of respondent profile based on questionnaire

The questionnaires are distributed to divisions or unit in the main office that will be directly involved in BCP PT Jamsostek. The division that are involved such as Risk Management, Information Technology, Investment, Finance, Operation and Services division, planning and development, facility and infrastructure, and protocol and household division. Total number of employees is 132 staffs. The respondent is chosen by risk management division. This is intended based on the knowledge and experience related to contingency procedure in each division and when it is integrated as BCP PT Jamsostek (Persero). The content of questionnaire is being modified from BCP questionnaire that already being conducted by Stohr & Rohmeyer (2004) and based on corporate risk profile Jamsostek. Total questionnaires that already distributed are 34 questionnaires. Meanwhile, the number of returned questionnaires is 33.

Total questionnaires that are valid to be analyzed are 32 questionnaires out of 33 returned questionnaires. The analysis cannot be done for the one questionnaire due to there are lots of questioned that are not being filled in. The composition of the respondents based on their formal title can be presented as bureau head (24%), unit head (49%), officer/analyst (15%), and others (12%), as again depicted on Figure 5.1.

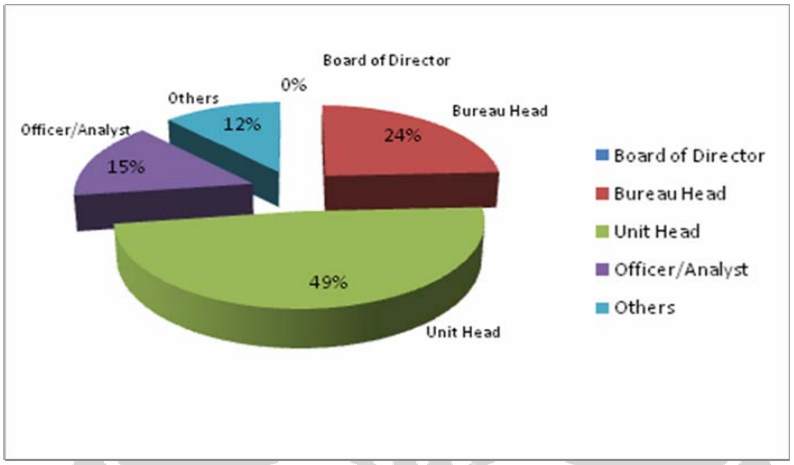


Figure 5.1 Respondent composition based on formal title

Source: Primary data analysis

The working tenor vary and its composition is categorized on three time intervals, which are: less than 10 years (< 10 years), between 10 and 20 years (10 – 20 years), and more than 20 years (>20 years).

From the three categories above, the biggest proportion (58%) is represented by respondents with more than 20 years working experience. The data taken from this group of respondents is intended to gather the information from the ones who should know the organization better. Beside, respondents with within 10 and 20 years working experience constitute 33% and less than 10 years around 9%.

For the majority, the respondent's gender is male (around 73%), meanwhile the rest (around 27%) are female.

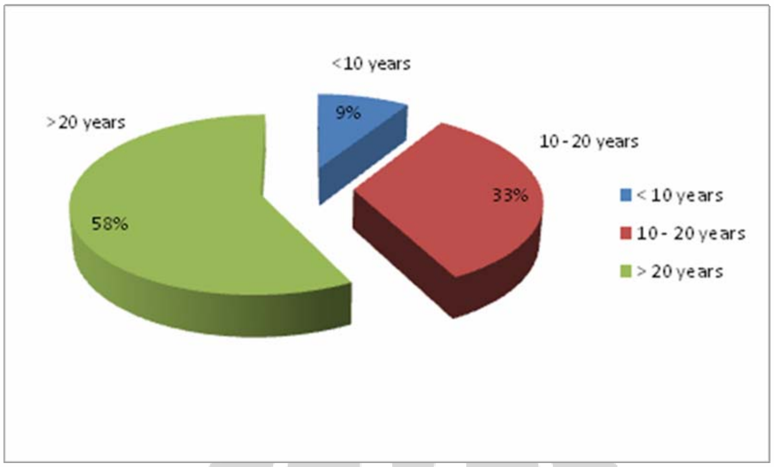


Figure 5.2 Respondent profile based on working tenure

Source: Primary data analysis

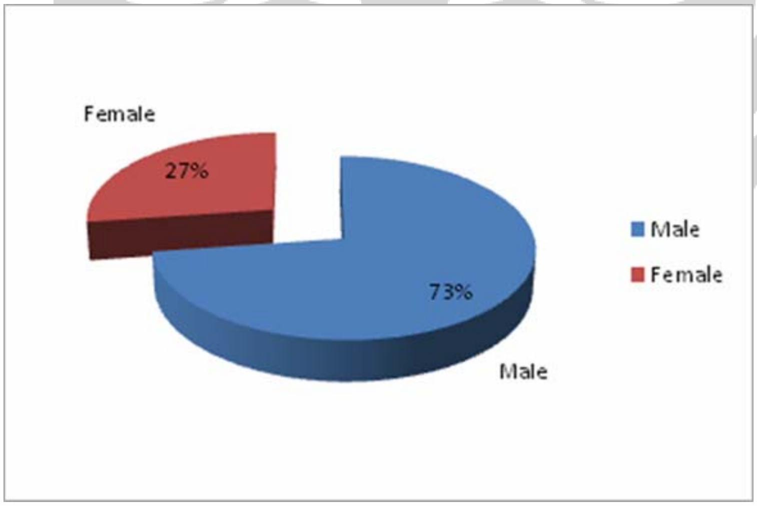


Figure 5.3 Respondent profile based on gender

Source: Primary data analysis

Based on the highest education level, around 6% of the respondents possessed diploma, 47% bachelor degree, and 47% master degree. Meanwhile, no respondent has a doctorate degree. From this education profile, it can be seen that the employee quality of PT Jamsostek (Persero) is sufficient, especially for employee with strategic level. In this stage, the employee should know how to manage and implement the strategy so that the business continuity can be sustained in PT Jamsostek (Persero).

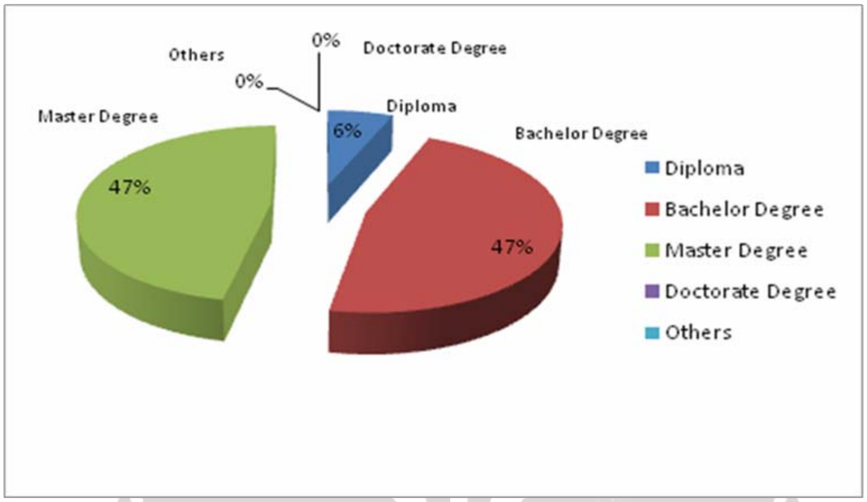


Figure 5.4 Respondent profile based on highest education

Source: Primary data analysis

Based on the business unit category, the respondents are coming from different business units such as risk management (around 21%), information technology (around 21%), operation and service (around 25%), investment (around 15%), and finance (around 5%). From development and planning unit comes around 3% respondents, others are 12%. The respondents are selected from various business units to gather complete information related to the business continuity plan of PT Jamsostek (Persero) in each unit/division. This will help a lot on the analysis since the related functions will enrich the information to be analyzed.

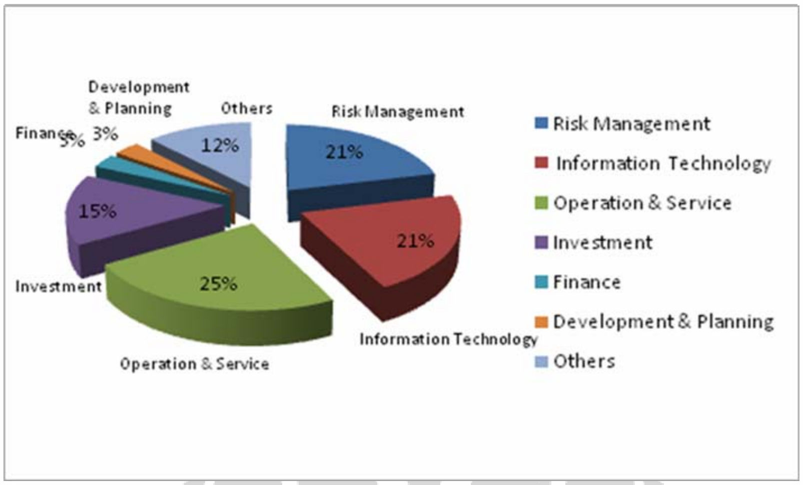


Figure 5.5 Respondent profile based on business unit

Source: Primary data analysis

The respondents are also being categorized based on the BCP positions that are already stated in the BCP handbook of PT Jamsostek (Persero) BCP. The categories are divided into:

- Bureau Head and Coordinator Crisis Management Team (CMT), around 9%.
- Bureau Head Member of Crisis Management Team (CMT), around 9%.
- Bureau Head besides member of Crisis Management Team (CMT), none.
- Coordinator Executive Crisis Management Team (ECMT), none.
- Coordinator Executive Crisis Management Team (ECMT) Finance, none.
- Coordinator Executive Crisis Management Team (ECMT) Operational, around 3%.
- Coordinator Business Continuity Team (BCT), around 9%.
- Member of Business Continuity Team (BCT), 43%.
- Others, 27%.

From the positions listed above, the largest group of the respondents is members of business continuity team (BCT), which is around 43%. This number indicates that almost half of the respondents should know about the structure organization of BCP. On the other side, there are still around 27% respondents who choose others as their role in BCP function.

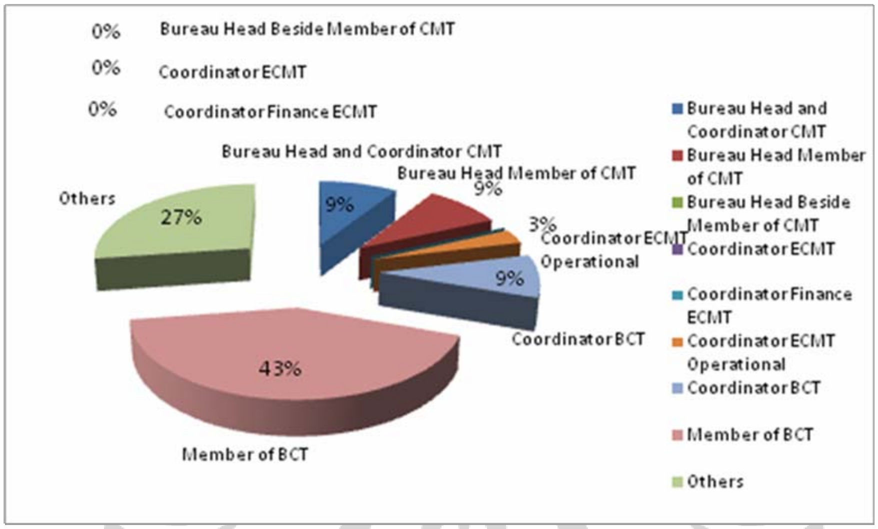


Figure 5.6 Respondent profile based on BCP position

Source: Primary data analysis

Furthermore, the respondent also being categorized based on their own supervisor in the BCP structure of the organization. From the analysis, it can be shown that the possible options in the questionnaire are almost evenly selected. The respondent whose supervisor is a bureau head and coordinator CMT are around 6%, bureau head member of CMT around 12%, bureau head besides member of CMT around 22%, coordinator ECMT around 15%, Finance ECMT coordinator around 6%, coordinator of ECMT Operational around 9%, coordinator of BCT around 18%, and member of BCT around 3%. Meanwhile, missing information is around 9%. It can be observed from this profile, around 22% respondents stated that their direct supervisor are categorized as bureau heads but not categorized as members of CMT. This means that there is a part of formal titles which are not categorized in the BCP organization structure. On the other hand, there are 15% responding that their direct supervisor is a coordinator of ECMT, meanwhile the coordinator of ECMT in the BCP organizational structure is stated as the Chief Executive Officer. No respondent comes from Board of Director (see Figure 5.1).

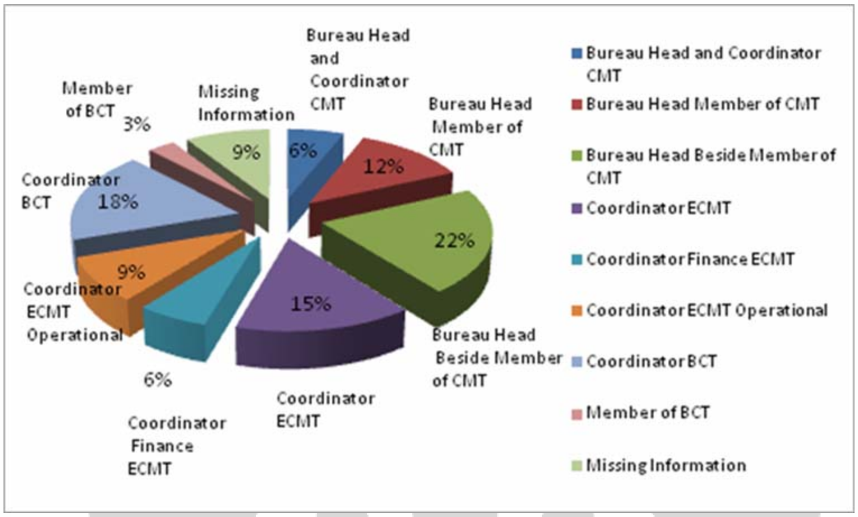


Figure 5.7 Respondent profile based on own supervisor in BCP organization structure

Source: Primary data analysis

Based on the percentage of activities in respondent's current position that are dedicated to business continuity planning, three categories are available:

- Less than 25% (< 25%)
- Between 25% and 50% (25% - 50%)
- More than 50% (>50%)

Assessing this aspect, it can be seen that around 55% of the respondents dedicate less than 25% of their working time to BCP. This number is high, more than half of the respondents. Meanwhile for time dedicated to BCP between 25% and 50% are received from 24% of the respondents and 21% of the respondents said that more than half of their time is invested for BCP-related matters.

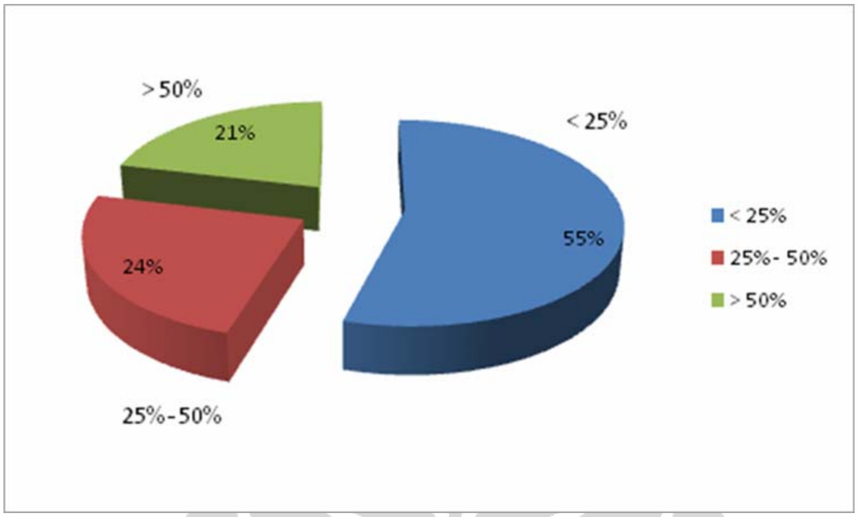


Figure 5.8 Respondent profile based on time percentage for BCP activities

Source: Primary data analysis

The last category asked to the respondents is their professional experience related to business continuity, distinctive in five time intervals: less than 1 year (< 1 year), between 1 and 3 years (1 - 3 years), between 3 and 6 years (3 - 6 years), between 6 and 9 years (6 - 9 years), and more than 10 years (> 10 years).

The analysis of proportion can be used to clarify the analysis of business continuity knowledge of the respondents. The respondents with less than 1 year professional experience are around 43%, between 1 and 3 years is around 30%, between 3 and 6 years is around 3%, between 6 and 9 years around 6%, more than 10 years around 18%.

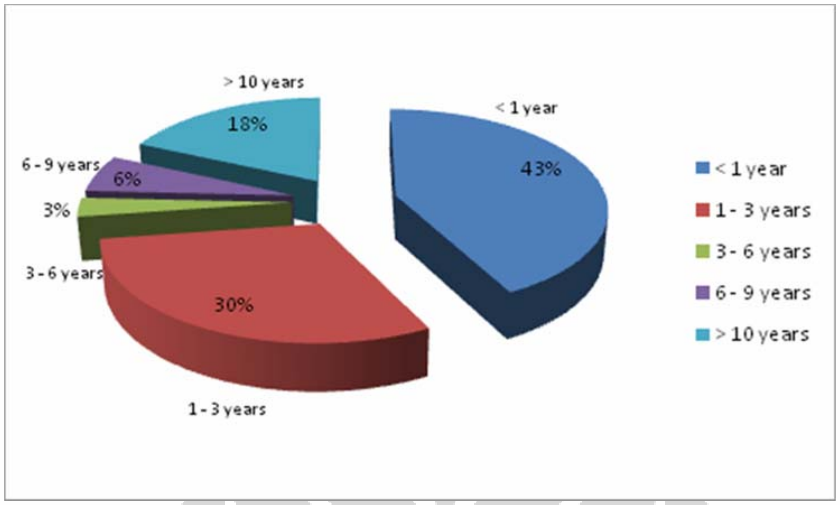


Figure 5.9 Respondent profile based on professional experience related to business continuity

Source: Primary data analysis

Based on the analysis on respondents' profile (formal title, working tenure, highest education), it can be assumed that most of the respondents can analyze the question related to their own business unit and are aware of the organizational interrelation in PT Jamsostek (Persero). Based on the BCP position, time percentage for BCP activities, professional experience related to business continuity, one can also predict how the respondents respond to each question related to the BCP control activities, monitoring, and information & communication.

5.2.2 Statistic descriptive of survey

There are some parameters that are assessed related to the risk assessment, based on enterprise risk management guidance from COSO and ISO 31000. The questions in the questionnaire are related to the theory and business continuity plan of PT Jamsostek (Persero). The question population is differentiated based on two options of answers. The first option of answers is for general answer, containing five options. It starts from "strongly disagree" up to "strongly agree." The second option of answer is specified to get the risk assessment answer. It has three categories with six options to answer based on the standard risk assessment of PT Jamsostek (Persero). Beside, the questionnaire also asked for respondent's opinion related to the questions. The table below shows the options of answer that are used in the questionnaire.

Table 5.1 Options of answer in the questionnaire

General Option

1	2	3	4	5
Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree

Specified Option

Risk Assessment Likelihood

1	2	3	4	5	6
Rare	Unlikely	Moderate	Likely	Almost Certain	Definitely

Risk Assessment Impact

1	2	3	4	5	6
Nil	Insignifica nt	Minor	Moderate	Major	Catas-trophic

Risk Assessment Category

1	2	3	4	5	6
Low	Moderate to low	Medium to low	Medium to high	Moderate to high	High

Source: Standard value questionnaire and risk assessment being used in PT Jamsostek (Persero)

Table 5.2 shows the statistic descriptive result of the valid and reliable questions from the questionnaire. It refers to questionnaire's required responses on a five point likert scale (1 = Strongly disagree (SD), 2 = Disagree (D), 3 = Neutral (N), 4 = Agree (A), and finally 5 = Strongly agree (SA)).

The mean of the population is denoted with $\overline{x}$ and standard deviation with σ.

Table 5.2 Descriptive Statistics

No	Questionnaire Statement	Respondent Answers					$\overline{x}$	σ
		SD	D	N	A	SA		
A.	Event Identification							
1.3	BCP already covered when the activation contingency procedure related to IT failed for Operational & Service division	3%	3%	24.2%	36.4%	33.3%	3.94	0.998
1.3.1	Contingency procedure in Operational & Service division already included in BCP procedure	3%	3%	21.2%	54.5%	18.2%	3.82	0.882
1.4	BCP already covered when the activation contingency procedure related to IT failed for Investment division	3%	9.1%	24.2%	51.5%	12.1%	3.61	0.933
1.4.1	Contingency procedure in Investment division already included in BCP procedure	3%	3%	30.3%	57.6%	6.1%	3.61	0.788
1.5	Contingency procedure in Supporting divisions already included in BCP procedure	9.1%	0%	30.3%	60.6%	0%	3.42	0.902
1.6	Contingency procedure in Finance divisions related to liquidity fulfillment already included in BCP procedure	3%	6.1%	27.3%	51.5%	12.1%	3.64	0.895
1.6.1	Contingency procedure in Finance division related to settlement already included in BCP procedure	3%	6.1%	30.3%	36.4%	24.2%	3.73	1.008

(to be continued)

Table 5.2 Descriptive Statistics (continued)

No	Questionnaire Statement	Respondent Answers					$\overline{x}$	σ
		SD	D	N	A	SA		
B.	Risk Response							
2.9	Business continuity testing ever being done	6.1%	21.2%	33.3%	39.4%	0%	3.06	0.871
2.10	Frequency of review and updated of BCP	6.1%	6.1%	60.6%	27.3%	0%	3.09	0.765
2.11	The involvement of business users in BCP is high	3%	3%	48.5%	39.4%	6.1%	3.42	0.792
C.	Control Activities							
3.2	BCP scope already includes the maintenance of inventory accuracy of components	0%	3%	36.4%	60.6%	0%	3.58	0.314
3.2.1	Preparedness of network communication	0%	0%	27.3%	63.6%	9.1%	3.82	0.584
3.2.2	Preparedness of network communication already being identified by employee	9.1%	9.1%	0%	75.8%	6.1%	3.79	0.696
3.3.2	Business Continuity Team already knew about BCP of service provider	0%	0%	45.5%	51.5%	0%	3.55	0.506
3.3.3	Service Level Agreement with service provider explicitly stated guarantee about business continuity in PT Jamsostek (Persero)	0%	0%	21.2%	78.8%	0%	3.79	0.415
3.3.4	Service Level Agreement with service provider ensured that the emergency procedure is already adequate.	0%	0%	27.3%	66.7%	6.1%	3.79	0.545

(to be continued)

Table 5.2 Descriptive Statistics (continued)

No	Questionnaire Statement	Respondent Answers					$\overline{x}$	σ
		SD	D	N	A	SA		
D.	Internal Controls							
4.4.3	BCP team is responsible for Crisis Management	9.1%	6.1%	21.2%	60.6%	3%	3.42	1.001
4.4.5	Formal assignment for Business Continuity Team	9.1%	9.1%	30.3%	48.5%	3%	3.27	1.008
4.4.6	Business Continuity Team have adequate qualification to implement the BCP	9.1%	6.1%	24.2%	57.6%	3%	3.39	0.998
4.4.7	Business Continuity Team have knowledge about overall divisions to implement the effective BCP	0%	6.1%	42.4%	48.5%	3%	3.48	0.667
E.	Monitoring							
6.1	Post testing evaluation is included in the BCP testing	0%	0%	60.6%	36.4%	3%	3.42	0.561
7.1	BOD involvement is high and support the BCP activities	0%	0%	15.2%	63.6%	21.2%	4.06	0.609
7.1.1	Senior Management involvement is high and support the BCP activities	0%	0%	33.3%	54.5%	12.1%	3.79	0.65
7.1.2	Information Technology involvement is high and support the BCP activities	0%	0%	6.1%	78.8%	15.2%	4.09	0.459

Note: There is 1 missing answer for Question 3.3.2
Source: Primary Data Analysis

A. Event Identification

This event identification is related to the term and procedure that already being implemented, especially for the contingency procedure, and also the opinion concerning of business continuity. The questions of contingency procedure are asked to each division such as operational and service division, investment division, supporting division, and finance division. The highest percentage of respondents answered with “Agree”. This highest percentage is due to before the BCP is implemented, each division already set up the procedure of contingency to prevent the business discontinuity that needs help from IT. For example, there is already backup data implemented in IT. Thus, when there disruption occurs, the data still can be recovered. There are some opinions related to the event identification that can be highlighted such as:

1. There are two main critical points that need to be included in the contingency procedure which are business data and business process continuity. These seen as the most crucial asset to be protected by Information Technology.
2. From the concerned answer related with the crucial asset, the IT respondents stated that the infrastructure should be adequate to enhance the crucial asset. Also, it needs to be tested in a frequent basis. The Operational & Service division stated that they have some concerns about the quantity and quality of people needs to be aligned so that the business process continuance can be sustained.

B. Risk Response

Risk Response questions are related to the activities that are conducted to mitigate the risk so that the business can still be sustained when the disruption appears. Based on the question of BCP testing, the selected options show that there are 39.4% respondents answering with “Agree”, meanwhile 33.3% answered with neutral position. The “Agree” answers are confirmed by the respondents who are involved directly in the BCP testing or who known about the BCP testing. The formal conduct of BCP is still not being implemented yet since the BCP is implemented. Only one test has ever been done after the implementation of BCP, and it is related to contingency procedure in IT division about the server connection. From the frequency of review and updated of BCP, more than a half of the respondents, 60.6%, answered in “Neutral” condition. This is because of they are not sure about the update or review of BCP procedure. The respondents answering with “Agree” contributes 27.3%, because they referred to their unit or division contingency procedure. About the involvement of business user, the highest percentages of the respondents respond with “Neutral”, 48.5%. If a respondent chooses to be neutral, the author cannot derive conclusion from the answered. The exploration of this statement will be answered in the in depth interview. In summary related to risk response, it seems that PT Jamsostek (Persero) could do much more in terms of communicating and rehearsing their BC plans.

C. Control Activities

Control activity questions are related to procedure or policy that already being implemented regarding business continuity plan. The highest percentage of the answer of this question is “Agree”. The agree answer of the respondents are related to the procedure of the information technology preparedness to mitigate the disruption and the preparedness of service provider who help the Information Technology division.

D. Internal Controls

Internal controls questions are related to the procedure in strengthening the internal control of BCP. In this section, the highest percentage of answers is “Agree”. Respondents agree for some critical questions such as:

1. BCP team is responsible for Crisis Management Team
2. There is already formal assignment for Business Continuity Team
3. BCT already have adequate qualification to implement the BCP
4. BCT have knowledge about how to implement the effective BCP.

The analysis from the above answers does not imply that all are based on the real facts. This will elaborate in the in-depth interview analysis.

E. Monitoring

Monitoring questions are related to the activities to control the process of BCP implementation. From the respondent answers for post testing evaluation, about 60.6% of the respondents answered in “Neutral” position. This is as inherent result from the question about BCP testing. BOD and senior management support for the BCP implementation exist. This is shown by the highest percentage of respondents giving “Neutral” as the answer. The category of support itself will be given details in the in-depth interview analysis.

F. Risk Assessment

In discussing matters related with risk assessment, 3 tables are constructed and analyzed.

Table 5.3 refers to questionnaires required responses on a six point likert scale (1 = Rare, 6 = Definitely). Rare is abbreviated with R, Unlikely U, Moderate M, Likely L, Almost Certain AC, and Definitely D.

Table 5.4 refers to questionnaires required responses on a six point likert scale (1 = Nil, 6 = Catasthrophic). Nil is denoted with N, Insignificant I, Minor MI, Moderate MO, Major MA, and Catastrophic C.

Table 5.5 refer to questionnaires required responses on a six point likert scale (1 = Low, 6 = High). Low is shorted with L, Moderate to low MOL, Medium to low ML, Medium to High MH, Moderate to high MOH, and lastly High with H.

Table 5.3 Statistic Descriptive of Assessment Specified Answered Option for Likelihood

No	Questionnaire Statement	Respondent Answered						$\overline{x}$	σ
		R	U	M	L	AC	D		
A.	Risk Assessment for Likelihood Operation and Service								
2.2	Contingency procedure not related with IT failed to be activated	29.6%	22.2%	33.3%	11.1%	0%	3.7%	2.52	1.424
2.2.1	Contingency procedure related to application system failed to be activated	11.1%	37%	37%	0%	14.8%	0%	2.7	1.171
2.2.2	Contingency procedure related to INPUT failed to be activated	22.2%	37%	18.5%	3.7%	18.5%	0%	2.59	1.394
2.2.3	Contingency procedure related to OUTPUT failed to be activated	22.2%	37%	14.8%	7.4%	18.5%	0%	2.63	1.418
2.2.4	Contingency procedure related to SERVER failed to be activated	3.7%	40.7%	33.3%	11.1%	7.4%	3.7%	2.89	1.155
B.	Investment								
2.3	Contingency procedure not related with IT failed to be activated	34.6%	46.2%	3.8%	7.7%	3.8%	3.8%	2.12	1.306
2.3.1	Contingency procedure related to INPUT failed to be activated	23.1%	53.8%	7.7%	11.5%	3.8%	0%	2.23	1.177
2.3.2	Contingency procedure related to OUTPUT failed to be activated	34.6%	34.6%	15.4%	3.8%	7.7%	3.8%	2.27	1.402
2.3.3	Contingency procedure related to SERVER failed to be activated	23.1%	42.3%	15.4%	11.5%	3.8%	3.8%	2.42	1.301
C.	Finance								
2.5	Contingency procedure related to settlement failed to be activated	54.5%	27.3%	0%	13.6%	4.5%	0%	1.86	1.246
2.5.1	Contingency procedure related to PROCESS, INPUT, OUTPUT failed to be activated	36.4%	45.5%	0%	4.5%	13.6%	0%	2.14	1.356

(to be continued)

Table 5.3 Statistic Descriptive of Assessment Specified Answered Option for Likelihood (continued)

No	Questionnaire Statement	Respondent Answered						$\overline{x}$	σ
		R	U	M	L	AC	D		
D.	General IT								
2.4	Contingency procedure related to server is failed. The connection to branches is disabled	6.3%	65.6%	18.8%	3.1%	3.1%	3.1%	2.41	1.012
2.7	Service provider who helps IT division cannot activate system application, database, and DRC due to threat or disaster	28.1%	53.1%	6.3%	3.1%	6.3%	3.1%	2.16	1.247
2.7.1	Network communication failed to be activated	9.4%	31.3%	50%	0%	9.4%	0%	2.69	0.998
E.	General								
2.6	More than 50% staff/personnel in Executive Crisis Management Team is changed	25%	40.6%	21.9%	6.3%	6.3%	0%	2.28	1.114
2.6.1	More than 50% staff/personnel in Crisis Management Team is changed	15.6%	50%	21.9%	6.3%	6.3%	0%	2.38	1.04
2.6.2	More than 50% staff/personnel in Business Continuity Team is changed	15.6%	37.5%	28.1%	15.6%	3.1%	0%	2.53	1.047

Source: Primary Data Analysis

Table 5.4 Statistic Descriptive of Assessment Specified Answered Option for Impact

No	Questionnaire Statement	Respondent Answer						$\overline{x}$	σ
		N	I	MI	MO	MA	Cc		
A.	Risk Assessment for Impact Operation and Service								
2.2	Contingency procedure not related with IT failed to be activated	0%	25.9%	7.4%	3.7%	29.6%	0%	3.7	1.171
2.2.1	Contingency procedure related to application system failed to be activated	0%	7.4%	14.8%	40.7%	25.9%	11.1%	4.19	1.075
2.2.2	Contingency procedure related to INPUT failed to be activated	3.7%	14.8%	25.9%	25.9%	29.6%	0%	3.63	1.182
2.2.3	Contingency procedure related to OUTPUT failed to be activated	0%	14.8%	29.6%	33.3%	14.8%	7.4%	3.7	1.137
2.2.4	Contingency procedure related to SERVER failed to be activated		14.8%	7.4%	18.5%	37%	22.2%	4.44	1.34
B.	Investment								
2.3	Contingency procedure not related with IT failed to be activated	0%	26.9%	15.4%	19.2%	26.9%	11.5%	3.81	1.415
2.3.1	Contingency procedure related to INPUT failed to be activated	7.7%	15.4%	26.9%	15.4%	26.9%	7.7%	3.12	1.395
2.3.2	Contingency procedure related to OUTPUT failed to be activated	7.7%	7.7%	30.8%	19.2%	26.9%	7.7%	3.08	1.468
2.3.3	Contingency procedure related to SERVER failed to be activated	7.7%	11.5%	11.5%	15.4%	38.5%	15.4%	3.5	1.421
C	Finance								
2.5	Contingency procedure related to settlement failed to be activated	4.5%	31.8%	9.1%	22.7%	22.7%	9.1%	3.55	1.503
2.5.1	Contingency procedure related to PROCESS, INPUT, OUTPUT failed to be activated	4.5%	36.4%	4.5%	31.8%	9.1%	13.6%	3.45	1.535

(to be continued)

Table 5.4 Statistic Descriptive of Assessment Specified Answered Option for Impact (continued)

No	Questionnaire Statement	Respondent Answer						$\bar{x}$	σ
		N	I	MI	MO	MA	Cc		
D.	General IT								
2.4	Contingency procedure related to server is failed. The connection to branches is disabled	0%	9.4%	0%	50%	31.3%	9.4%	4.31	0.998
2.7	Service provider who helps IT division cannot activate system application, database, and DRC due to threat or disaster	3.1%	3.1%	31.3%	12.5%	25%	25%	4.28	1.397
2.7.1	Network communication failed to be activated	0%	6.3%	28.1%	9.4%	28.1%	28.1%	4.44	1.343
E.	General								
2.6	More than 50% staff/personnel in Executive Crisis Management Team is changed	9.4%	28.1%	31.3%	21.9%	9.4%	0%	2.94	1.134
2.6.1	More than 50% staff/personnel in Crisis Management Team is changed	9.4%	31.3%	28.1%	25%	6.3%	0%	2.88	1.1
2.6.2	More than 50% staff/personnel in Business Continuity Team is changed	18.8%	31.3%	18.8%	15.6%	15.6%	0%	2.78	1.362

Source: Primary Data Analysis

Table 5.5 Statistic Descriptive of Assessment Specified Answered Option for Category

No	Questionnaire Statement	Respondent Answer						$\bar{x}$	σ
		L	MOL	ML	MH	MOH	H		
A.	Risk Assessment for Likelihood Operation and Service								
2.2	Contingency procedure not related with IT failed to be activated	3.7%	18.5%	44.4%	11.1%	18.5%	3.7%	3.33	1.209
2.2.1	Contingency procedure related to application system failed to be activated	3.7%	7.4%	33.3%	25.9%	25.9%	3.7%	3.74	1.163

(to be continued)

Table 5.5 Statistic Descriptive of Assessment Specified Answered Option for Category (continued)

No	Questionnaire Statement	Respondent Answer						$\overline{x}$	σ
		L	MOL	ML	MH	MOH	H		
2.2.2	Contingency procedure related to INPUT failed to be activated	14.8%	11.1%	29.6%	11.1%	29.6%	3.7%	3.41	1.5
2.2.3	Contingency procedure related to OUTPUT failed to be activated	3.7%	29.6%	22.2%	11.1%	25.9%	7.4%	3.48	1.451
2.2.4	Contingency procedure related to SERVER failed to be activated	11.1%	22.2%	37%	18.5%	11.1%	0%	3.96	1.16
B.	Investment								
2.3	Contingency procedure not related with IT failed to be activated	11.5%	38.5%	11.5%	19.2%	11.5%	7.7%	3.04	1.509
2.3.1	Contingency procedure related to INPUT failed to be activated	15.4%	19.2%	23.1%	26.9%	11.5%	3.8%	3.12	1.395
2.3.2	Contingency procedure related to OUTPUT failed to be activated	19.2%	11.5%	34.6%	19.2%	7.7%	7.7%	3.08	1.468
2.3.3	Contingency procedure related to SERVER failed to be activated	11.5%	15.4%	11.5%	42.3%	11.5%	7.7%	3.5	1.421
C.	Finance								
2.5	Contingency procedure related to settlement failed to be activated	27.3%	31.8%	9.1%	13.6%	13.6%	4.5%	2.68	1.585
2.5.1	Contingency procedure related to PROCESS, INPUT, OUTPUT failed to be activated	31.8%	13.6%	22.7%	13.6%	9.1%	9.1%	2.82	1.68
D.	General IT								
2.4	Contingency procedure related to server is failed. The connection to branches is disabled	0%	15.6%	31.3%	40.6%	3.1%	9.4%	3.59	1.103

(to be continued)

Table 5.5 Statistic Descriptive of Assessment Specified Answered Option for Category (continued)

No	Questionnaire Statement	Respondent Answer						$\overline{x}$	σ
		L	MOL	ML	MH	MOH	H		
2.7	Service provider who helps IT division cannot activate system application, database, and DRC due to threat or disaster	3.1%	31.3%	12.5%	40.6%	3.1%	9.4%	3.38	1.314
2.7.1	Network communication failed to be activated	0%	15.6%	28.1%	6.3%	40.6%	9.4%	4	1.32
E.	General								
2.6	More than 50% staff/personnel in Executive Crisis Management Team is changed	6.3%	46.9%	28.1%	9.4%	6.3%	3.1%	2.72	1.143
2.6.1	More than 50% staff/personnel in Crisis Management Team is changed	6.3%	43.8%	31.3%	6.3%	12.5%	0%	2.75	1.107
2.6.2	More than 50% staff/personnel in Business Continuity Team is changed	15.6%	34.4%	28.1%	6.3%	12.5%	3%	2.75	1.344

Source: Primary Data Analysis

The questions related to risk assessment is being answered based on the category of division to get the valid answer option. The questions are answered based on division category or from supporting division who knows about the risk assessment based on the business process of that division. Below is the mapping of the answer:

1. *Risk assessment for Operations and Service*. This assessment is answered by operations and service team, the bureau head or head of protocol affairs as he previously was a former team of operations and service team, risk management team, and technology team.
2. *Risk assessment for Investment*. This assessment is answered by investment team, the bureau head of risk management team as he was previously a former team of investment team, risk management team, and technology team.

3. *Risk assessment for Finance*. This assessment is answered by finance team members, risk management team, and technology team.
4. *Risk Assessment for Technology*. This assessment is answered from technology team, risk management team, and some respondent from various divisions who know the technology process.
5. *Risk Assessment for General Questions*. This assessment is answered from technology team, risk management team and also from operations and service team, investment team, and finance team, as they know the process.

The categorization of answers depends on the highest percentage of answer option and the mean analysis.

F.1 Risk Assessment for Operations and Service

The risk assessment for operations and service is related to some questions such as:

1. *Contingency procedure of not related with IT failed to be activated*. The analysis found out that the highest percentage of respondents state the likelihood that it will happen is “Moderate” (33.3%), with mean 2.52. From the mean value the position is in “Unlikely” to “Moderate” to be happened. This derived that the condition can be happened or not. The probability is fifty percent. Based on the category, this event is categorized as Medium to low, with mean 3.33.
2. *Contingency procedure related to application system failed to be activated*. The analysis stated that the highest percentage of respondents answered the likelihood to be happened equal on the “Unlikely” and “Moderate”, to be happened (37%). The mean value is on 2.7. From the mean value, the position can be categorized on “Moderate” position. From the impact, this event is categorized as “Moderate”. It is being categorized in between “Medium to high” (25.9%) and “Moderate to high” (25.9%), with mean 3.74.
3. *Contingency procedure related to INPUT failed to be activated*. The analysis found out that the highest percentage of respondents answered the likelihood

to be happened is “Moderate”, mean value is 2.59. The impact is relatively categorized as “Major” (29.6%). This impact should be heavy to the organization. This be categorized as “Medium to low” to “Medium to high” since the mean value is 3.41 rather than categorized as “Moderate to high” (29.6%).

4. *Contingency procedure related to OUTPUT failed to be activated.* The analysis stated that the highest percentage of respondents answered the likelihood to be happened is “Unlikely” to “Moderate”, with mean 2.63. This can be stated also that the category can be in the Moderate. The impact is Moderate (33.3%). This be categorized in between Medium to low (22.2%) and medium to high (11.1%) rather than moderate to low (29.6%) or moderate to high (25.9%) since the mean is 3.48 with standard deviation is 1.451.

5. *Contingency procedure related to SERVER failed to be activated.* The analysis stated that the highest percentage of respondents answered the likelihood to be happened is “Unlikely” (40.7%) to “Moderate”, with mean 2.89. This can be stated also that the category can be in the “Moderate”. The impact is “Major” (33.3%). The impact should be heavy to the organization. This be categorized in between “Medium to low” (37%) and “Medium to high” (18.5%), since the mean is 3.96 with standard deviation is 1.16.

F.2 Risk Assessment for Investment

The risk assessment for investment is related to some questions such as:

1. *Contingency procedure of not related with IT failed to be activated.* The analysis stated that the highest percentage of respondents answered the likelihood to be happened equal on the “Unlikely” (46.2%), with mean 2.12. From the impact of this event is categorized as “Moderate” with (19.2%) rather than “Insignificant” (26.9%) or “Major” (26.9%), since the mean is on 3.81 and standard deviation 1.415. It is being categorized in between

“Moderate to low” (38.5%) and “Medium to low” (11.5%), with mean 3.04 and standard deviation is 1.509.

2. *Contingency procedure related to INPUT failed to be activated*. The analysis stated that the highest percentage of respondents answered the likelihood to be happened equal on the “Unlikely” (53.8%), with mean 2.23. From the impact of this event is categorized as “Minor” (26.9%), since the mean is on 3.12. It is being categorized as “Moderate to high” (26.9%), with mean 3.12 and standard deviation is 1.395.
3. *Contingency procedure related to OUTPUT failed to be activated*. The analysis stated that the highest percentage of respondents answered the likelihood to be happened equal on the “Unlikely” (34.6%), with mean 2.27. From the impact of this event is categorized as “Minor” (30.8%), with mean is on 3.08. It is being categorized as “Medium to low” (34.6%), with mean 3.08.
4. *Contingency procedure related to SERVER failed to be activated*. The analysis stated that the highest percentage of respondents answered the likelihood to be happened equal on the “Unlikely” (42.3%), with mean 2.42. From the impact of this event is categorized as “Major” (38.5%), with mean is on 3.5. It is being categorized as “Medium to high” (42.3%), with mean 3.5 and standard deviation is 1.421.

F.3 Risk Assessment for Finance

The risk assessment for finance is related to some questions such as:

1. *Contingency procedure related to settlement failed to be activated*. The analysis stated that the highest percentage of respondents answered the likelihood to be happened equal on the “Rare” (54.5%), with mean 1.86. From the impact of this event is categorized as “Minor” (9.1%) since the mean is on 3.55 rather than “Insignificant” (31.8%) and “Major” (22.7%). It is being categorized in between “Moderate to low” (31.8%) and “Medium to low”, with mean 2.68 and standard deviation is 1.585.

2. *Contingency procedure related to PROCESS, INPUT, OUTPUT failed to be activated*. The analysis stated that the highest percentage of respondents answer the likelihood to be happened equal on the "Unlikely" (45.5%), with mean 1.356. From the impact of this event is categorized as "Minor" (4.5%) since the mean is on 3.45 rather than "Insignificant" (36.4%) and "Moderate" (31.8%). It is being categorized in between "Moderate to low" (13.6%) and "Medium to low" (22.7%), with mean 2.82 and standard deviation is 1.68.

F.4 Risk Assessment for Information Technology

The risk assessment for information technology is related to some questions such as:

1. *Contingency procedure related to server is failed. The connection to branches is disabled*. The analysis stated that the highest percentage of respondents answered the likelihood to be happened is in "Unlikely" (65.6%), with mean 2.41. From the impact of this event is categorized as "Major" (31.3%), with mean is 4.31. It is being categorized in between "Medium to low" (31.3%) and "Medium to high" (40.6%), with mean 3.59 and standard deviation is 1.103.

2. *Service provider that help IT division cannot activate system application, database, and DRC due to threat or disaster*. The analysis stated that the highest percentage of respondents answered the likelihood to be happened is in "Unlikely" (53.1%), with mean 2.16. From the impact of this event is categorized as "Moderate" (12.5%), with mean is 4.28 rather than "Minor" (31.3%) and "Catastrophic" (25%). It is being categorized as "Medium to high" (40.6%), with mean 3.38.

3. *Network communication failed to be activated*. The analysis stated that the highest percentage of respondents answered the likelihood to be happened is in "Moderate" (50%), with mean 2.69. From the impact of this event is categorized as "Major" (25%), with mean is 4.28. This should be heavy

impact to the organization. It is being categorized as “Medium to high” (40.6%), with mean 3.38 and standard deviation is 1.314.

F.5 Risk Assessment for General

The risk assessment for general overview is related to some questions such as:

1. *More than 50% staff/personnel in Executive Crisis Management Team are changed*. The analysis stated that the highest percentage of respondents answered the likelihood to be happened is in “Unlikely” (40.6%), with mean 2.28. From the impact of this event is categorized as “Minor” (31.3%), with mean is 2.94. It is being categorized as “Moderate to low” (46.9%), with mean 2.72 and standard deviation is 1.143.

2. *More than 50% staff/personnel in Crisis Management Team are changed*. The analysis stated that the highest percentage of respondents answered the likelihood to be happened is in “Unlikely” (50%), with mean 2.38. From the impact of this event is categorized as “Insignificant” (31.3%) to “Minor” (28.1%), with mean is 2.88. It is being categorized in between “Moderate to low” (43.8%) and “Medium to low” (31.3%), with mean 2.75 and standard deviation is 1.107.

3. *More than 50% staff/personnel in Business Continuity Team are changed*. The analysis stated that the highest percentage of respondents answered the likelihood to be happened is in “Unlikely” (37.5%), with mean 2.53. From the impact of this event is categorized as “Insignificant” (31.3%), with mean is 2.78. It is being categorized in between “Moderate to low” (34.4%) and “Medium to low” (28.1%), with mean 2.75 and standard deviation is 1.344.

5.2.3 In-depth-interview analysis

Based on result of in-depth interview for 8 respondents there are eight main themes that can be shown in Table 5.6.

Table 5.6 Eight Main Themes of Interview Result

Theme Number	Description
Theme 1	The most severe disaster/disturbance criticality for business continuity in PT Jamsostek (Persero)
Theme 2	Risk assessment performed/compound events considered
Theme 3	Delineation of BCP roles and governance
Theme 4	Integration of BCP among divisions
Theme 5	Testing of functions and processes
Theme 6	Use of outsourcers
Theme 7	The involvement of BOD & Senior Management is relatively high
Theme 8	Separate BCP budget

Source: Primary Data Analysis

The interview results are classified based on the themes on the table above. The respondents' answers can be shown in Table 5.7.

Table 5.7 Eight Main Themes Result of Interview

Theme	R1	R2	R3	R4	R 5	R 6	R7	R8
The most severe disaster/disturbance criticality for BC in PT Jamsostek	Process Business Continuity	Business data	Process Business Continuity	Process Business Continuity	Process Business Continuity	Business data	Process Business Continuity	Business data
Risk Assessment performed/compound events considered	Yes. Not all cover and in detail	Yes. The risk awareness still low	Yes. The risk awareness still low	Yes. Risk mapping only	No comment	Yes. Still in early stages need time.	No comment	No comment
Delineation of BCP roles and governance	Yes. For DRP procedure and governance	Yes. There is a project for BCP roles and governance underway	Yes. It is stated in BCP procedure about the governance	No.	No comment	No comment	Yes. But It still needs to be significantly improved	No comment
Integration of BCP among divisions	No. Need improvement	Yes. Its on the way of integration	No. Need a lot of works to do	No. Concern of BCP valuet	No comment	No. It still on the way to go	No comment	No comment. Under construction
Testing of functions and processes	Yes. Only once.	Yes. Not in the work hour.	Yes	Yes. Once, but not participated	No comment	No comment. Not participate	No comment.	No comment
Use of outsourcers	Yes. For DRP only	Yes. For DRP only	Yes. For DRP only	Yes. For DRP only	No comment	Yes. For DRP only	Yes. For DRP only	Yes. For DRP only
The involvement of BOD & Senior Management is relatively high	Yes. For the detail of support still under discussion.	Yes. The support should be embedded as integration.	Yes.	Yes. For general support.	No comment	No comment. The result of support still cannot be seen	Yes. The involvement is high especially when there is critical issue	No comment
Separated BCP budget	No. Distributed to business line	No. Distributed to business line	No comment	No. Distributed to business line	No. Distributed to business line	No. Distributed to business line	No. Distributed to business line	No comment

Source: Primary Data Analysis

Below are the important aspects which are the inherent results for the 8 respondents in each main theme based on Table 5.7.

1. There are two most critical assets that need to be taken care off: process business continuity and business data. The majority of the respondents choose process business continuity as the top priority to be recovered, followed then by the business data. These critical assets need to be recovered as the top priority when the disaster happens. The contingency procedure expected to become the backbone of this critical asset is from information technology, especially since PT Jamsostek (Persero) already implements the online application system. Meanwhile, from the process out of information technology, the contingency procedure refers to the manual activities.
2. The majority of the respondents stated that the risk assessment is already being conducted especially in the critical division such as critical function in operations & service division and investment division. Meanwhile, the risk assessment is not covered in detail and all functions related to the critical asset. This is mentioned, for example, by a respondent from information technology. This means that the analysis should update the recovery time objective (RTO) and recovery point objectives (RPO) with cost to be recovered. Then the assessment can be aligned with the factual condition. From operation & service division and investment division, the opinion regarding the same matter is that the risk analysis is still in the early stages, since it still begin with risk profile assessment. This should be enhanced. The risk management division itself stated that the risk awareness in overall divisions is still low. On the other side, the risk analysis is still not detailed for the overall process of contingency procedure and not covering the situation when the contingency procedure is failed to be activated. The only division that already created the contingency procedure step is the Information Technology division. Meanwhile, the IT team itself stated that when the

contingency procedure step is failed to be activated then they will executed the process manually.

3. The majority of the respondents stated that there is already delineation of BCP roles and responsibility. Meanwhile, the BCP roles and responsibility is still within the procedure in the handbook. From the role itself, as stated from risk management division, they are planning to create the roles of BCP team in the formal job description. Furthermore, will be part of every division responsibility. On top of that, the risk management team will increase the weight of BCP performance in their Key Performance Indicator (KPI). A suggestion comes from the household affair division that BCP should be included and formalize in the corporate governance. It should also be included in each division KPI. As wished by IT division and Operations and service division, there should be directorate segregation, such as segregation between IT directorate and Research and Development directorate, and segregation between Operations directorate and Service directorate. This segregation will help a directorate to focus on the function of the directorate itself.

4. The majority of the respondents stated that the integration of BCP among divisions is not yet available. Most of the respondents submit “no comment” response whether the BCP is on the way to be integrated in overall division. This is somehow logical because the implementation of BCP in PT Jamsostek (Persero) is just initiated since less than 2 years ago. There are a lot of works to be done to create the integration of BCP within the overall divisions. When that point is reached, then the value of BCP can present/exist in the overall division.

5. The majority respondent agreed that the testing process is already executed. Meanwhile, the testing that already being done since the implementation of BCP is just once time. This is being done not in the work hour time, and not involving all divisions, especially critical divisions such as operations and service and investment division. The testing scope is only to test the server

capabilities. There is no testing yet for the DRP-TI. On the other hand, this condition will reflect to the confidentiality of contingency procedure activation when the disruption comes. As per the experienced from previous disaster such as earthquake in Padang, the branches can still run the business. But, the contingency procedure was not needed to be activated since the infrastructure of both system and building are not destroyed by the earthquake. The level of confidence that IT can activate the contingency procedure seems to be in the mediocre level, since the frequency of testing is still low. The only measurement that can be used currently is the frequency of issue and problem solving report from IT log report.

6. The majority of the respondents agreed that to mitigate the risk, PT Jamsostek (Persero) should use outsourcers. The outsourcers are intended for DRP-IT only. These outsourcers will create the DRP and propose to the IT division. The recommendation for the involvement of these outsourcers is relatively high around 50% up to 90%.
7. The majority of the respondents agreed that the involvement of BOD & Senior Management is relatively high. The support of BOD & Senior management is acknowledged as the pillar of BCP implementation itself. Meanwhile, the support itself still felt as the general support for the overall corporate governance. In implementing the best BCP, it is agreed that the support should be present enough to increase the awareness of BCP and not only after the event or disaster exists, such as the budget, special control for BCP budget and activities.
8. The majority of the respondent stated that there is still no budget separation for BCP. The budget is still included in the budget of the business units.

Based on Table 5.7 above, the encryption is being done by dividing Theme 1 in the table into 2 themes. The encryption of the in-depth interview results that is already being done to 8 respondents can be shown in Table 5.8 that follows.

Table 5.8 Encryption code result of the interview

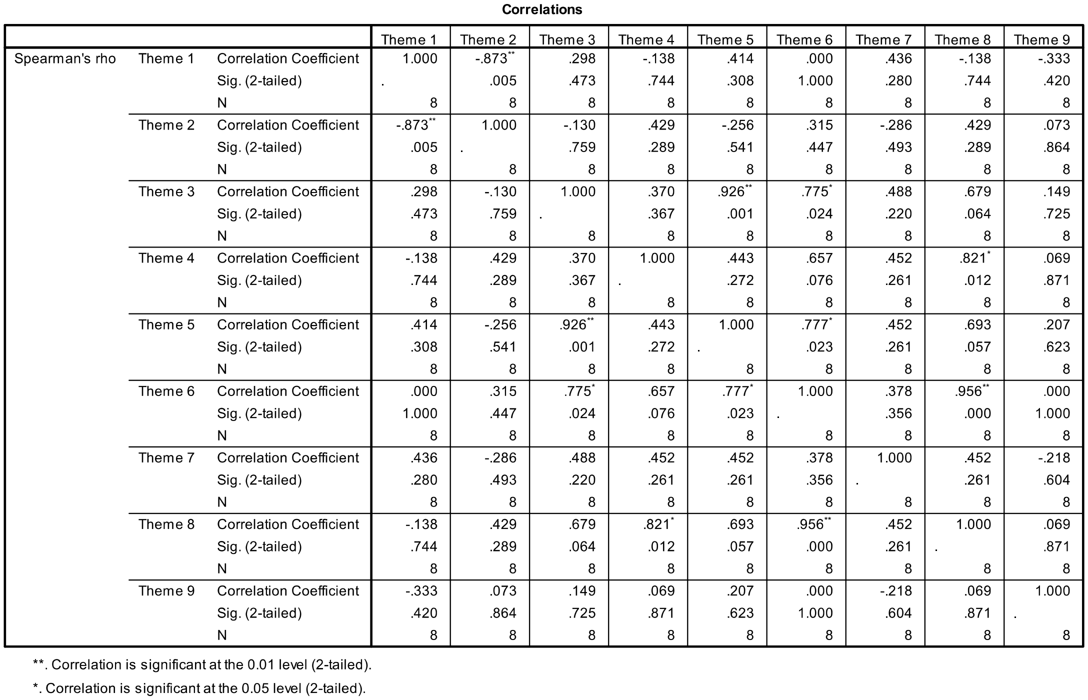
Theme	Respondent							
	R1	R2	R3	R4	R5	R6	R7	R8
The most severe criticality for BC in PT Jamsostek is business data	1	2	1	0	0	2	0	2
The most severe criticality for BC in PT Jamsostek is process of business continuity	2	1	2	2	2	0	2	1
Risk assessment performed/compound events considered	2	2	2	2	0	2	0	0
Delineation of BCP roles and governance	2	2	2	1	0	0	2	0
Integration of BCP among divisions	1	2	1	1	0	1	0	0
Testing functions and processes	2	2	2	2	0	0	0	0
Use of outsourcers	2	2	2	2	0	2	2	2
The involvement of BOD & senior management is relatively high	2	2	2	2	0	0	1	0
Separated BCP budget	1	1	0	1	1	1	1	0

Note: The meanings of numbers inside the cells are 0 denoted “No comment”, 1 “Disagree with the theme, 2 “Agree with the theme”
Source: Primary Data Analysis

The analysis of Spearman’s Rho to the 9 themes in the Table 5.8, based on in-depth interview result, can be shown in Table 5.9.

Table 5.9 gives information that the majority of the respondent answers in one theme do not affected to agree with other theme. This is shown by the insignificant coefficient of correlation within questions at α = 5%. There is an exception for correlation for some themes such as between Theme 6 and Theme 3 (0.775), Theme 5 and Theme 6 (0.777), Theme 6 and Theme 8 (0.956), Theme 4 & Theme 8 (0.821). From this result, it can be concluded that if the respondent agrees with one theme which has significant correlation with other theme, then there is a tendency that the respondent agrees with the other theme also, and vice versa. For example Theme 6, then there is a tendency that the respondent agrees with Theme 8.

Table 5.9 Spearman Rho Correlation Theme as Result of Interview



Correlations

			Theme 1	Theme 2	Theme 3	Theme 4	Theme 5	Theme 6	Theme 7	Theme 8	Theme 9
Spearman's rho	Theme 1	Correlation Coefficient	1.000	-.873**	.298	-.138	.414	.000	.436	-.138	-.333
		Sig. (2-tailed)	.	.005	.473	.744	.308	1.000	.280	.744	.420
		N	8	8	8	8	8	8	8	8	8
	Theme 2	Correlation Coefficient	-.873**	1.000	-.130	.429	-.256	.315	-.286	.429	.073
		Sig. (2-tailed)	.005	.	.759	.289	.541	.447	.493	.289	.864
		N	8	8	8	8	8	8	8	8	8
	Theme 3	Correlation Coefficient	.298	-.130	1.000	.370	.926**	.775*	.488	.679	.149
		Sig. (2-tailed)	.473	.759	.	.367	.001	.024	.220	.064	.725
		N	8	8	8	8	8	8	8	8	8
	Theme 4	Correlation Coefficient	-.138	.429	.370	1.000	.443	.657	.452	.821*	.069
		Sig. (2-tailed)	.744	.289	.367	.	.272	.076	.261	.012	.871
		N	8	8	8	8	8	8	8	8	8
	Theme 5	Correlation Coefficient	.414	-.256	.926**	.443	1.000	.777*	.452	.693	.207
		Sig. (2-tailed)	.308	.541	.001	.272	.	.023	.261	.057	.623
		N	8	8	8	8	8	8	8	8	8
	Theme 6	Correlation Coefficient	.000	.315	.775*	.657	.777*	1.000	.378	.956**	.000
		Sig. (2-tailed)	1.000	.447	.024	.076	.023	.	.356	.000	1.000
		N	8	8	8	8	8	8	8	8	8
	Theme 7	Correlation Coefficient	.436	-.286	.488	.452	.452	.378	1.000	.452	-.218
		Sig. (2-tailed)	.280	.493	.220	.261	.261	.356	.	.261	.604
		N	8	8	8	8	8	8	8	8	8
	Theme 8	Correlation Coefficient	-.138	.429	.679	.821*	.693	.956**	.452	1.000	.069
		Sig. (2-tailed)	.744	.289	.064	.012	.057	.000	.261	.	.871
		N	8	8	8	8	8	8	8	8	8
	Theme 9	Correlation Coefficient	-.333	.073	.149	.069	.207	.000	-.218	.069	1.000
		Sig. (2-tailed)	.420	.864	.725	.871	.623	1.000	.604	.871	.
		N	8	8	8	8	8	8	8	8	8

**. Correlation is significant at the 0.01 level (2-tailed).

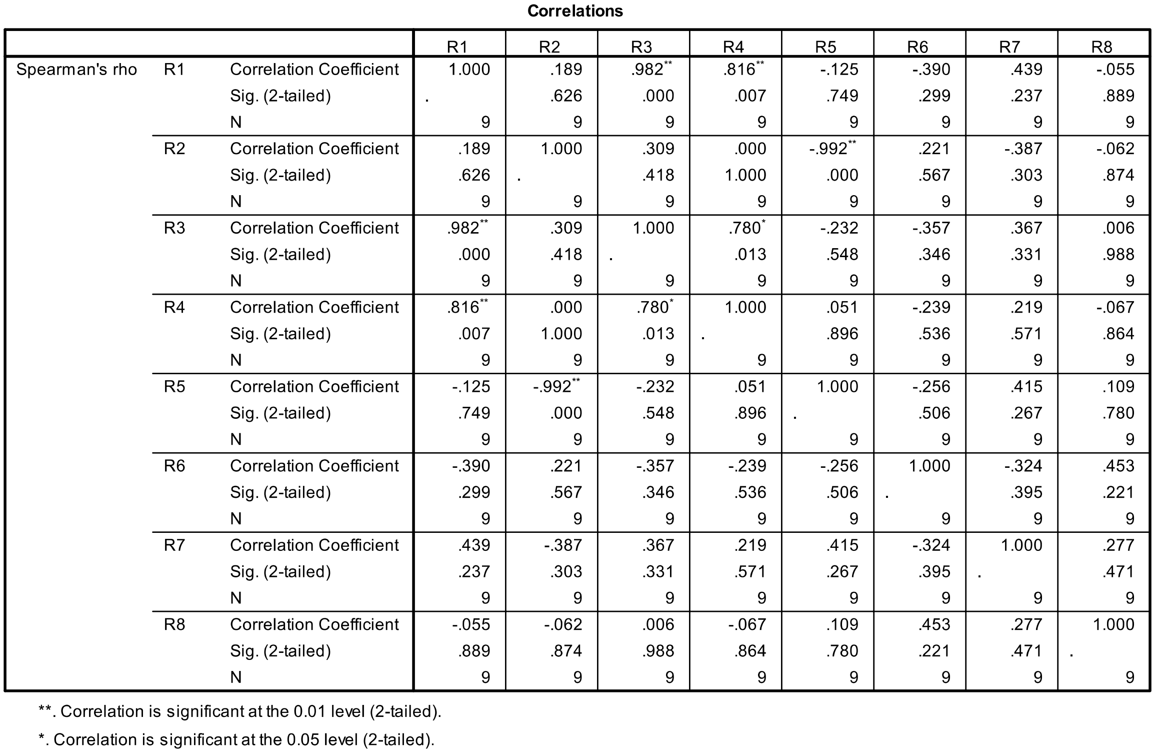
*. Correlation is significant at the 0.05 level (2-tailed).

Source: Primary Data Analysis

Correlation analysis of Spearman’s Rho is also being done to know the correlation between respondent opinions. The result is shown in Table 5.10.

Table 5.10 shows that in majority there is no correlation between one respondent to the other respondent, excePT for respondent 3 and 4. The correlation for respondent 3 and 4 is + 0.78. This is because of respondent 3 and 4 comes from same division which is risk management division. From this analysis, it can be implied that each respondent share the opinion based on the division, experience level, and knowledge about the BCP itself. It is shown by the insignificant level of correlation between respondent at $\alpha = 5\%$.

Table 5.10 Spearman's Rho Correlation Respondent as Result of Interview



Correlations

			R1	R2	R3	R4	R5	R6	R7	R8
Spearman's rho	R1	Correlation Coefficient	1.000	.189	.982**	.816**	-.125	-.390	.439	-.055
		Sig. (2-tailed)	.	.626	.000	.007	.749	.299	.237	.889
		N	9	9	9	9	9	9	9	9
	R2	Correlation Coefficient	.189	1.000	.309	.000	-.992**	.221	-.387	-.062
		Sig. (2-tailed)	.626	.	.418	1.000	.000	.567	.303	.874
		N	9	9	9	9	9	9	9	9
	R3	Correlation Coefficient	.982**	.309	1.000	.780*	-.232	-.357	.367	.006
		Sig. (2-tailed)	.000	.418	.	.013	.548	.346	.331	.988
		N	9	9	9	9	9	9	9	9
	R4	Correlation Coefficient	.816**	.000	.780*	1.000	.051	-.239	.219	-.067
		Sig. (2-tailed)	.007	1.000	.013	.	.896	.536	.571	.864
		N	9	9	9	9	9	9	9	9
	R5	Correlation Coefficient	-.125	-.992**	-.232	.051	1.000	-.256	.415	.109
		Sig. (2-tailed)	.749	.000	.548	.896	.	.506	.267	.780
		N	9	9	9	9	9	9	9	9
	R6	Correlation Coefficient	-.390	.221	-.357	-.239	-.256	1.000	-.324	.453
		Sig. (2-tailed)	.299	.567	.346	.536	.506	.	.395	.221
		N	9	9	9	9	9	9	9	9
	R7	Correlation Coefficient	.439	-.387	.367	.219	.415	-.324	1.000	.277
		Sig. (2-tailed)	.237	.303	.331	.571	.267	.395	.	.471
		N	9	9	9	9	9	9	9	9
	R8	Correlation Coefficient	-.055	-.062	.006	-.067	.109	.453	.277	1.000
		Sig. (2-tailed)	.889	.874	.988	.864	.780	.221	.471	.
		N	9	9	9	9	9	9	9	9

**. Correlation is significant at the 0.01 level (2-tailed).

*. Correlation is significant at the 0.05 level (2-tailed).

Source: Primary Data Analysis

5.2.4 Risk assessment against corporate risk profile

In this section, the risk assessment that is already being analyzed in the above section (risk assessment section) will be checked against the corporate profile. The analysis checks the linkage about the risk analysis between them. The risk analysis is related to operational risk, technological risk, and reputational risk. This assessment is intended to know about the critical risk that should be identified.

Corporate Risk Profile of PT Jamsostek uses the same perspective with BCP risk assessment; meanwhile there is a different in the name or description. Below table 5.9 shown the category:

Table 5.11 Category of risk profile assessment

Scale	Description
1-2	Low
3-4	Moderate low
5-9	Medium low
10-12	Medium high
13-20	Moderate high
21-36	High

Source: Jamsostek documents (Profil Resiko PT Jamsostek (2010))

Table 5.12 Risk assessment against corporate risk profile

Division	Process	Risk Assessment	Corporate Risk Profile	Risk Category
Operations and Service	Contingency procedure related to business process excludes any IT related it is failed to be activated. Concern: Claim fraud; verification on claim to provider; staff capability and competencies; processing time; low satisfaction level of service; standard level of service	Likelihood : Moderate; Impact: Moderate; Category: Medium to low	Inherent: Likelihood : Moderate Low (4); Impact: Medium Low (5); Category: Moderate High (20)	Operational; Reputational
	Contingency procedure related to business process related to IT is failed to be activated. Concern: Matrix level to access the system; the database accuracy; application contingency, expert system to minimize human error, server bandwidth, capacity DRC compared to DC	Likelihood : Moderate; Impact: Moderate; Category: Between Medium to high to Moderate to high	Inherent: Likelihood : Moderate Low (4); Impact: Medium Low (5); Category: Moderate High (20)	Technology

(to be continued)

Table 5.12 Risk assessment against corporate risk profile (continued)

Division	Process	Risk Assessment	Corporate Risk Profile	Risk Category

Investment	Contingency procedure related to business process excludes any IT related it is failed to be activated.
	Concern : Lack of source information for analysis, standard procedure to assess partner of investment, fraud and default investment, Staff competencies & capabilities; economic macro condition or regional deteriorated, facilities and infrastructure is not operate maximal in internal basis; facilities and service to tenant still not operate in maximal basis, deposit default.
		Likelihood : Unlikely;
		Impact: Moderate;
		Category: Between Moderate to low to Medium to low
			Inherent:
			Likelihood : Medium Low (5);
			Impact: Medium Low (5);
			Category: High (25)
				Operational
				Reputational

	Contingency procedure related to business process which related to IT is failed to be activated.
	Concern: Matrix level to access the system; the accuracy of database; application contingency, expert system to minimize human error, server bandwidth.
		Likelihood : Unlikely;
		Impact: Major;
		Category: Medium to high
			Inherent:
			Likelihood : Moderate Low (4);
			Impact: Medium Low (5);
			Category: Moderate High (20)
				Technology

(to be continued)

Table 5.12 Risk assessment against corporate risk profile (continued)

Division	Process	Risk Assessment	Corporate Risk Profile	Risk Category

Finance	Contingency procedure related to PROCESS, INPUT, OUTPUT is failed to be activated Concern: Overstated in financial report, moral hazard	Likelihood : Unlikely;
		Impact: Minor;
		Category: Medium to Low
			Inherent:
			Likelihood : Moderate Low (4);
			Impact: Medium Low (3);
			Category: Medium High (12)
				Operational
				Reputational

Source: Primary Data Analysis

The above table shows the critical risk that need to be identified specifically in BCP procedure. As based on corporate risk profile, the above potentiality of inherent risk is in the category of High Category even though the likelihood is moderate to low. This is being strengthened also based on Risk Assessment from primary data, with majority for the impact when the event is occurred is in Moderate level.

5.3 Gap Analysis

In the Gap analysis, researcher will use a model that is derived from some theory and best practices to create foundation of Business Continuity model in this research. The theory that used are comes from Enterprise Risk Management, Business Continuity Management, Business Continuity Plan from some sources such as Gallagher, DR II, FEMA and then followed by COSO and ISO 31000. Beside, it will follow some BCP best practices which already being used as BCP public society in US and some government industries such as POLRI and Angkasapura I & II. Also, there is Business Continuity model which known as BC-EM model from a research that already being published.

The model categorization is compared directly with the reality that found in the implementation. This category is then compared with the situation of the BCP of PT Jamsostek (Persero). Based on first step which have to be taken to create the BCP, there are some concerns need to be done which are:

1. *Project Identification*. Planning is the important part in starting the project. A good planning remarks a good stewardship. Success in any endeavor requires careful preparation and planning. The project identification need to be taken care seriously since it will align with the result that we want to achieve. Some steps that are included in the project identification can be shown in below table.

Table 5.13 Project Identification

Step	BCP Model	BCP Jamsostek (Actual)	Gap Analysis
Identify planning coordinator	There should be detail responsibility and job description.	Job description is issued on the field	The responsibility and job description is not captured in detail for both the planning coordinator and the team member when starting or initiate the BCP project.
	The person in charge should be detail in the capability assessment such as: • Should be from management-level employee, • He/She has people skill, project management skill • Good understanding of the organization, • Detail oriented.	• There is no capability assessment special to manage project • The candidate is only 1 specifically unit head of operational risk (line managers)	The planning coordinator is based on function assignment in Risk Management unit. This function is just embedded as additional task of the operational risk management unit head. As based on the corporate governance of organizational structure of PT Jamsostek (Persero) for the capability assessment for this title.

(to be continued)

Table 5.13 Project Identification (continued)

Step	BCP Model	BCP Jamsostek (Actual)	Gap Analysis
Identify planning 0coordinator	• Able to commit sufficient time to the project to ensure it can be completed within the agree time frame This PIC will coordinate with management operations team,		There is no assessment needed about how many times this person managing the project, how about the skill to manage project, and specified about the detail orientation.
Obtain management support and resources	The support must be communicated to all levels of management. There must be a ranging from senior level management teams on down: • The management decision-making team • The business continuity steering committee • The BCP coordinator • The management operations team • Department coordinators • The emergency operations team • The damage assessment and post investigation team	The support is communicated between Risk Management department and Information Technology Department. The team member consist: • BCP planning coordinator • Subordinate of BCP planning coordinator	The BCP initiative to be implemented is comes from the initiative of former Director Risk Management. The discussion is started in the Risk Management Unit and diverge to Informational Technology to others divisions. There is a lack of support and resources as a ranging from senior level management teams on down when managing this project. Even though the core resources is not fulfilled in when managing this project. There is no BCT steering committee and department coordinator to be appointed.

(to be continued)

Table 5.13 Project Identification (continued)

Step	BCP Model	BCP Jamsostek (Actual)	Gap Analysis
Obtain management support and resources	The attention of and support from at least one member of senior management level such as the CFO as BCP "sponsor". The management should responsible for making major decision, deliver the resources.	The support is from Risk Management Director. The Risk Management director is giving direction. Meanwhile there is no special budget of this activities	There is attention from senior management but it is limited to giving direction in managing this project.
Define the scope and methodology	Planning standards for the business units or divisions. There should be: • Business risk assessment • Recovery strategy development • Writing the recovery plan • Testing and Maintenance of Plans • Information Systems BCP • Business Unit Resumption Planning • Corporate Contingency Planning	The planning is based on input from risk management director and consultant. Meanwhile for the methodology is using the same technique as creating the corporate risk profile.	The methodology used is as per the standard basis as per already used in business as usual assessment. There are some points that need to be delivered in details such as: • Detail business risk assessment • Recovery plan should be in detail especially for the process outside IT • Recovery strategy development should embedded in BCP, not just related to IT division only • The testing and maintenance of plans need to detailed and there must be time line in detail basis

(to be continued)

Table 5.13 Project Identification (continued)

Step	BCP Model	BCP Jamsostek (Actual)	Gap Analysis
Define the scope and methodology			• There should be Work Breakdown Structure, Time Schedule planner, Standardized instruments and any Aothers related to help identify the project scope.
	Steering or planning committee. There should be planning committee which contains person in charge for each division.	There is no planning committee created.	There is no special planning committee to do the BCP process. The driver is comes from Risk Management gather information from others division.
	Facilitation of internal development should include: • Standard Questionnaire for BCP • Interview • Focus group discussion This is intended to do problem mapping then it can be focused to the internal development.	The facilitation used is based on interview and meeting discussion to mapping the problem.	The discussion is to mapping the problem and still not focuses to the internal development itself.

(to be continued)

Table 5.13   Project Identification (continued)

Step	BCP Model	BCP Jamsostek (Actual)	Gap Analysis
Define the scope and methodology	Use of template plans. The elements such as: • Introductory material which consists • Promulgation document (outlines the authorithy and responsibility of the plan) • Signature page (demonstrates that all response organization have participated in its development and are committed to its success) • Dated title and revisions page • Distribution list • Purpose statement • Situation and assumptions • Concepts of operations • Organization and assignment of responsibilities • Administration and logistics • Plan development and maintenance • Authorities and references	The project initiation is not formalized in the form of proposal. There is a template plans just used to assess the Business Impact Analysis for each division or unit which related to main critical function in each critical division.	The pilot project should be formalize in the form of proposal with the standardize template as per the model suggested. This will help to evaluate the result of BCP to the project initiation procedure.

Source: Gallagher, DR II, FEMA, COSO, ISO 31000)

2. Risk Assessment

Table 5.14 Risk Assessment

Step	BCP Model	BCP Jamsostek (Actual)	Gap Analysis
Event Identification/Risk Identification	Identify event that can affect the achievement of the entity's core objective. The identification should be in detail: • Source of risk in each division which comes from internal and external factor • When/Where/Why and How that this risk can be happened? • Event that can be happened which implied to the target from internal factors and external factors • Triggered that derived the event • Consequence or the effect to the organization • Who/Which part will be impacted when the risk occurred? Control to avoid the event to be happened.	Based on the approved BCP. The risk identification: • Analyzing source of risk comes from natural disaster, manmade disaster, and technology. Most of them is from external factors. • Assess the risk impact based on infrastructure loss and important document • Risk Mapping, based on the value of likelihood, impact from some source of risk. • Contingency procedure that is being described in detail is from IT division	The risk identification both for the source of risk and event is already being done. Meanwhile there are some identify to be concerned such as: • Identification is not covered all the possible source of risks especially for critical functions. • The critical asset need to be identified in detail for each business function • There should be list of risk priority to be recovered. • The event identification should be from internal factors also.

(to be continued)

Table 5.14 Risk Assessment (continued)

Step	**BCP Model**	**BCP Jamsostek (Actual)**	**Gap Analysis**
Event Identification/Risk Identification	• How about the effectiveness current mitigation or to cover the event Beside, the identification of event occurrence should include the external and internal factors		• The consequence when the event is occurred should be covered in detail and measurable such as cost estimation, risk owner to be responsible. • The contingency procedure should be identified in detail for each business function especially for critical business. There is no assessment for each factor that affects the event to be occurred, for event occurrence in the BCP.
	Choose techniques to use to identify events. The techniques can be chosen such as: • Brainstorming, • Work breakdown analysis, • Expert facilitation	The techniques to use to identify events from brainstorming.	The brainstorming techniques is one of the tools, meanwhile it should follow with the work break down analysis and expert facilitation.

(to be continued)

Table 5.14 Risk Assessment (continued)

Step	BCP Model	BCP Jamsostek (Actual)	Gap Analysis
Event Identification/Risk Identification	Offer recommendation to mitigate their effects, by: • Question the general manager, facilities manager, and other appropriate people on what could prevent emergencies, outatges, and disasters • Question about the evacuation procedure? • Question about critical systems or equipment connected to uninterruptible power • supplies? • Question about files backed up on a regular basis and stored off site?	The recommendation to be offered: • Specifically related with Information Technology procedure only. This is proposed by IT team. • Question and answered being done to find the root cause for some business critical	Gap analysis: • The overall risk assessment should mitigate the risk which related to the strategy, people, and process. Then the overall process can be checked and mitigated before the event is occurred. • The question and answered need to be done to prevent the event to be occurred • Offered the recommendation as a prevent action both internal event and external event The evacuation procedure still not defined in BCP

(to be continued)

Table 5.14 Risk Assessment (continued)

Step	**BCP Model**	**BCP Jamsostek (Actual)**	**Gap Analysis**
Risk Assesment/Risk Analysis/Business Impact Analysis	Some identification that need to be assessed in detail: • Using formal risk assessment methodology • Identify the scope of Business Continuity with detail parameter • Existence of BCP Mission Statement, BCP policies and procedures, BCP goals & strategy • Identify the critical processes which generate most value within a company • Identify critical resources and ranked its asset in terms of their strategic importance • Identify which parts of a company that will be most affected by an incident and what effect it will have upon the company as a whole • There must be a qualitative and quantitative impact to be assessed	The identification that already being assessed: • Already use formal risk assessment methodology • Critical process that need to be recovered when disaster is happened • BCP missions is aligned with overall Risk Management • The critical process is defined	There are some gap analysis: • Lack of scope of Business Continuity • The policies and procedures of BCP need to be enhanced and updated • The BCP needs to rank the critical resources and asset with exact measurement such as cost and the impact to the business. • To increase the risk awareness, each risk owner need to know about the most affected unit or process that will be affected when the disruption appeared.

(to be continued)

Table 5.14 Risk Assessment (continued)

Step	BCP Model	BCP Jamsostek (Actual)	Gap Analysis
Risk Assesment/Risk Analysis/Business Impact Analysis	• Identify threat and vulnerability assessment for unpredictable events especially external event		• The vulnerability assessment control the important function to check about the preparedness when that event is occurred
	Risk assessment need to concern on: • Considers possible causes such as sources, likelihood and consequences/impact of the identified event to establish the inherent risk. • Established some contingency procedure strategies related to each critical process, and list down the risks within the contingency procedure and assigned the risk rating. • Discusses option to deal with risks that are not tolerable • Identify process recovery priorities	Risk assessment: • Assessed the possible causes like likelihood, impact from external events or factors. Internal factors just in Information Technology • Contingency procedure is for IT division only	Gap analysis: • The risk sources, likelihood, and impact need to be identified both from external factors and also internal factors in detail for each critical division. • More than one strategy for contingency procedure need to be developed to find the effective and efficient action plan to be done • The intolerable risk need to be discussed and described, then the recovery priorities can be identified

(to be continued)

Table 5.14 Risk Assessment (continued)

Step	BCP Model	BCP Jamsostek (Actual)	Gap Analysis
Risk Assesment/Risk Analysis/Business Impact Analysis	Examining impacts for each event or contingency procedure which failed to be activated: • Calculated the significant blocks of time on service objectives, • Calculated the cash flow and financial position for each strategy for procedure contigency, • Regulatory requirements, • Contractual issues,	There are already regulatory requirements being implemented in the current BCP focused on DRP IT activation.	The gap for this section is big enough. There must be a huge improvement related to the failed contingency procedure to be activated. Since the contingency procedure just covered the process step related to DRP activation.
	• Examining some highlighted points: • Formal assignment for Business Continuity roles • Headcount dedicated to BC and the capability • Assignment oversight and implementation responsibilities • Use of formal change control over the plan • Competitive advantage,	Examining some highlighted points: BCP budget still embedded in each division	There are a lot of points that are not being owned in the current BCP. From the interview result, the respondent mentioned that it is in the plan to do for: • Formal BCP assignment • Gain the competitive advantage

(to be continued)

Table 5.14 Risk Assessment (continued)

Step	BCP Model	BCP Jamsostek (Actual)	Gap Analysis
Risk Assesment/Risk Analysis/Business Impact Analysis	• Potentially reveal inefficiencies in normal operations, • Help to justify or allocate better recovery planning budgets by calculated the cash, • Budget separation and level of budget authority • Designated Senior business management sponsor BC		
	• Establish the recovery time objective (RTO) and recovery point objectives (RPO) of business functions and data processes. • This should be followed also by cost to be expensed aligned with the RTO & RPO setting.	There is already RTO defined	The RTO defined in the most of the process step is in daily basis. This should be followed by the expenditure. Then, it can be calculated precisely. The criticality of the process will be determined by the RTO time frame.
Risk Response	Risk Mitigation: • Detection, Recognize potential threats to reduction or sharing the risk; Updated the BCP procedures and policies in frequently basis	Risk Mitigation: • The testing is already being done once time. The testing scope is related to DRP	To ensure about the confidentiality of risk mitigation. It needs to be:

(to be continued)

Table 5.14 Risk Assessment (continued)

Step	**BCP Model**	**BCP Jamsostek (Actual)**	**Gap Analysis**
Risk Response	• Prevention, Protect asset from accidental or misuse; Involvement of business user • Recovery, Effort to return the condition to normal condition; Testing of BCP; Using outsourcers	• Outsourcers for DRP IT	• Tested in frequent basis and involved participation from all business users. • The procedures of BCP need to be updated in frequent basis, especially to be aligned with current business process and need • Need to test the capabilities of the outsourcers itself to ensure the capabilities and consistency of the outsourcers
Control Activities & Monitoring	Policy establishing and procedures aligned with the BCP third party.	Procedure established is BCP document	The policy and procedure to control the activities should be established in detailed and includes the step procedures to do internal control the outsourcers instead of BCP document only to ensure the emergency procedure is adequate enough.

(to be continued)

Table 5.14 Risk Assessment (continued)

Step	BCP Model	BCP Jamsostek (Actual)	Gap Analysis
Control Activities & Monitoring	Build “business continuity culture” through training and awareness program. The training itself need to have basic goal such as the staff that follow the training is being properly trained. The training itself can be from internal organization or from the expert trainer The awareness itself needs to have basic goals also such as keep business continuity prominent, their role in BCP, understanding about business continuity.	Training program is only held once time by Risk Management Team.	The training program needs to be done in frequently basis. The training and awareness are the main point to gain success in BCP implementation. Since this is related to the end user of BCP.
	Periodically audit, test, and evaluate the program. There should be testing plan before it being tested. The testing activities should be done in the detail and formal procedure	There is only once testing related to DRP-IT	Before the testing is being done, there should be a plan related to these testing activities. Then, after the testing already being done there must be a post testing. The testing itself need to include participation from most of the business users.

(to be continued)

Table 5.14 Risk Assessment (continued)

Step	BCP Model	BCP Jamsostek (Actual)	Gap Analysis
	Increase management's awareness, such as: • Decision for major issues and resources required for a workable program • Involvement of senior management in BC activities	There is on the way to go to involve the senior management awareness.	The awareness of BCP needs to be communicated in all levels management especially for senior management. This will help to increase participation in all levels related to BCP.
Information & Communication	Refine the information and make it useful Effective communication and information BCT team should have adequate communication skill	Based on survey, there is already adequate communication skill in BCT team.	As per the respondent opinion, currently the value of BCP still not exists. Thus means, there is still works to do for the communication so the BCP value can be presence.

Source: Gallagher, DR II, FEMA, COSO, ISO 31000

CHAPTER 6
CONCLUSIONS AND RECOMMENDATIONS

6.1 Conclusions

As the result of the analysis, there are some answers the thesis objective, which will be summarized here.

The conclusion that can be driven aligned with BCP objectives are:

1. The overall picture about the BCP of PT Jamsostek is obtained. PT Jamsostek already created a BCP that focuses on IT-related disruptions. Meanwhile, for other disruptions non related to IT, the contingency procedure depends on the policy of each division, based on the existing normal procedures.The business continuity assessment of overall organizational competence as per REAM suggestion for organizational grading BCP to management on business continuity and related process is on the level 2 (supported self governed).

2. The gap between the current BCP with BCP model is already be shown in the Table 5.13 and Table 5.14. The gap is obvious especially in project initiation, risk assessment, control activities, and monitoring. BCP should be a structured and detailed integral unity of all contingency procedures of related divisions, especially critical divisions such as operation and service and investment. It should cover the process, the people, and the system of the whole organization. By doing this, the BCP can be effectively implemented when disruptions or threats occurs. In the other side, developing a BCP environment or culture in an organization is a significant undertaking, particularly because if the organization has traditionally seen BCP as an informational technology (IT) issue and not an organization-wide issue. IT is only one of many dependencies the organization has in the delivery of its products and services. Align with this, there are some points that need to be

improved related to BCP of PT Jamsostek (Persero). This will be elaborate further in the recommendation section.

As a summary, developing a business continuity plan is not a one-time static task. It is a process that requires the commitment and cooperation of the entire organization. In order to perpetuate the process, business continuity plan must be a company-stipulated policy as well as a company-sponsored goal. The organizations that adopt this company culture-oriented posture are the ones whose plans are actively maintained and tested, and whose employees are well-trained and poised to proactively respond to a crisis.

6.2 Recommendations

There are some recommendations that can be proposed for PT Jamsostek, *Kementerian BUMN*, and for future research.

For PT Jamsostek (Persero), based on result of analysis in the Chapter 5, there are some points that need to be improved based on the categories below:

1. *BCP revision/update*. As PT Jamsostek (Persero) intends to revise the BCP to be aligned with current business process, the first thing to do is to follow the process of planning with project identification as suggested by the BCP model. The process of building a plan is extremely valuable to Jamsostek. The purpose of identifying problems and developing a recovery process does not only force Jamsostek to examine the impact of a disaster on the company and its business, but also question the very mode of operations and process within business units.

2. *Risk Assessment*. Prevention is better than cure. As cited from Augustine (1995:121), "*The first stage (of a crisis), not surprisingly, is prevention. Amazingly, it is usually skipped altogether, even though it is least costly and simplest way to control a potential crisis*". There are several points that need to be improved in the current BCP of PT Jamsostek (Persero), such as:

- Event Identification. There are some points related to event identification that need to be improved, such as:
    - The event identification/risk identification should cover all of the possibilities risk in each critical business. The events that should be included are originated from the internal factors up to the external factors. From this analysis, the critical asset for each business function can be identified. The consequence or impact of an event, current contingency procedure, and the effectiveness of current contingency procedure must also be well identified. Based on the identification, the risk sources should be listed based on priorities.
    - There must be at least a standardized questionnaire that should be used to indicate the risk analysis in detail. This is important to gather the data. The question should be customized for each division. This is important to make sure about the operational impact categories.
    - The interview needs detailed question related to strategy, people, and process. By this mean, the potentiality of risk can be shown in detail. The way to mitigate this event before it occurs can be found. Along the interview, any suggestions offered to mitigate the event must be collected. The strength and weakness of each suggestion must be assessed.
    - Using tools such as work breakdown analysis will help a lot to map all risk potentialities.

3. Risk Assessment/Business Impact Analysis

- The scope of business continuity plan should be determined in detail, as shown by a BCP already implemented in Bank ABC. See Figure 6.1.

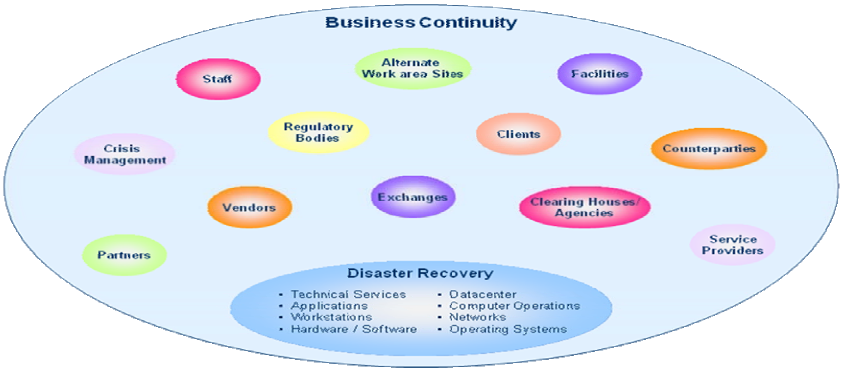


Figure 6.1 Business continuity scope in Bank ABC

Source: Bank ABC's BCP Training Material

- The critical resources such as processes, resources, and asset should be measurable agains several parameters such as: value within the organization and strategic importance. The measurement itself must have an exact standard, such as cost to be expensed and level of absolute improvement.
- Identification of divisions vulnerable to disaster should be conducted. Risk owner must know how a certain accient may affect the business. This will automatically increase the risk awareness of the risk owner. The impact itself needs to be measured qualitatively and quantitatively. Presented now as example is the impact measurement of Bank ABC such as from:

1. Qualitative Impact:

   The qualitative impact such as inability to settle outstanding trades, loss of new business, contractual penalties and regulatory fines, lost of interest on funds, borrowing expenses, loss of existing business, additional compensation paid to counterparties, effect on operational capital (values of funds inaccessible), extraordinary expenses (such as resources needed to address the disruption)

2. Quantitative Impact

   The quantitative impact such as cash flow, financial reporting and control, client services (customer perception), competitive advantage, legal or contractual violation, regulatory requirement, third party relations, public image, industry image, employee morale, backlog, professional embarrassment, employee turnover

- Threat and vulnerability assessment of event needs to be done precisely and in detail since this is required to check the quality of preparedness when the event is occurred.
- The risk sources, likelihood, and impact must be covered in detail. Beside there should be a proposed multiple strategies of contingency procedure for each identified process in order to manage the risk. The strategies need to be developed with exact measurement such as cost to be expensed. This is needed to check the effectivity and efficiency of the strategies.
- Related to the impact of risk, it needs to be calculated in the measurable way such as significant block of time in service the objectives, cash flow and financial analysis, follow the regulatory requirements, finding the contractual issues.
- The organizational structure of BCP must be ensured and given priority to meet the objectives as follows: formal assignment for BCP roles, head count for BC and the capability assessment, separation budget for BCP, and designated senior business management sponsor for BC.
- Establishment of Recovery Time Objective (RTO) and Recovery Point Objectives (RPO) of business functions and data process. This should be followed also by cost measurement.

4. Risk Response.

There are some basic points that need to be improved in the current BCP of PT Jamsostek (Persero) related to testing in order to check how effective the risk response is.

- *Testing Planning*. There must be a planning for testing. There are 2 example that can be follow such as:
    1. BCP of Bank ABC. There are risk assessments, drills, communication plan to employee, independent plan review, testing result, and lesson learned. There are multiple plans that can be used depending on the testing objective.
    2. BCP of "*Sistem Manajemen Keadaan Darurat*". There are complete procedures included the complete structural organization, special team assignment, facility and infrastructure, communication.
- *Testing Frequencies*. The testing itself needs to be done in a frequent basis. As per BCP of "*Sistem Manajemen Keadaan Darurat*" and BCP Bank ABC, there are scheduled testing and surprice testing

5. Control Activities/Monitoring

Control activities/monitoring is the important phase in controlling the effectiveness of implemented BCP. There are some steps that need to be highlighted such as:

- Policy and procedures of internal BCP must align with the third party's BCP
- Build "business continuity culture" through training and awareness program. This program should be in the frequent basis. The trainer should expert the risk management and communication skills.
- In each testing, there must be a post evaluation. Besides, the testing should gather participation from business users in each division.

- The awareness of BCP needs to involve senior management also. They need to be involved in the BCP activities

6. Information & Communication

   An important task related to BCP is to refine the information and make it useful for the work. Without relevant information it is hard to send the related information effectively. There are some points need to be considered such as:

   - Communication skill between business continuity team to the rest of the employees
   - Effectiveness of communication

Based on the interview result, until now there is no standard BCP in the form of rule or decree to be followed by all state enterprises under the Ministry of State Enterprises (*Kementrian BUMN*), especially for PT Jamsostek (Persero). The recommendations for the ministry are:

a. Issuing the rule or decree related to BCP policy and guidance and also conducting close supervision related to BCP.
b. Implementing the BCP to all others enterprises under the ministry.

As the recommendations for future research, this thesis can be improved related to the analysis, in the form of:

a. Using comparison of the BCP in companies under the Ministry of State Enterprises such as BCP of PT Telkom to get further analysis.
b. In data collection, using forum group discussion between divisions, holding a meeting to be attended by some divisions to get the inherent understanding.

REFERENCES

Alberts, Christopher & Dorofee, Audrey. (2003). *Managing Information Security Risks – The OCTAVEsm Approach*. New Jersey: Pearson Education.

Andersen, E. (2003), Be prepared for the unforeseen. *Journal of contingencies and crisis management*, Vol. 11, Number 3, 129-131.

ASIS. (2005). *Business Continuity Guideline, A Practical Approach for Emergency Preparedness, Crisis Management, and Disaster Recovery*.

AZ/NZS ISO 31000 – Australia/New Zealand International Organization for Standardization. (2009). *Risk Management – Principles and Guidelines*. Sydney: Author.

Barnes, James C. (2001). A Guide to Business Continuity Planning. Florida: John Wiley & Sons.

Basel Committee on Banking Supervision. (2004). *International Convergenge of Capital Measurement and Capital Standars, a Revised Framework*. Bank for International Settlements Switzerland: Author.

BCI – The Business Continuity Institute. (2002). Business Continuity Management: Good Practice Guidelines, version BCI DJS 1.0. http://www.thebci.org.

BCI. – The Business Continuity Institute. (2008). *Good Practice Guideline, Section 1 BCM Policy & Programme Management*, Version 2008.1, pp. 6. http://www.thebci.org.

Boyce, Carolyn & Neale, Palena (2006). *Conducting in-depth interviews: A guide for designing and conducting in-depth interviews for evaluation input.* Pathfinder International

Broder, James F. (2006). *Risk Analysis and the Security Survey*. (3rd ed.) United Kingdom: Butterworth Heinemann.

Chapman, Robert J. (2006). *Simple tools and techniques for enterprise risk management*. West Sussex: John Wiley & Sons.

Cooper, Donald R. & Schindler, Pamela S. (2008). *Business Research Methods.* Singapore:Mc Graw Hill.

Cormack, D.S. (1991). *The research process.* Black scientific: Oxford.

COSO – The Committee of Sponsoring Organizations of the Treadway Commission (2003). *Enterprise Risk Management - Integrated Framework*. New Jersey: Author.

Denzin, Norman K. & Yvonna S. Lincoln. (2005). *The Sage Handbook of Qualitative Research*. United Kingdon: Sage Publications

Doughty, Ken. (2000). *Business Continuity Plan: Protecting Your Organization's Life*. Florida: Auerbach Publications.

DRII The Institute for Continuity Management. (2008). May 5, 2011.http://www.drj.com/glossary/drjglossary.html.

FEMA. (1998). *Protecting Business Operations, Publication 331*. Washington, D.C.: US Government Printing Office.

Fombrun, C.J. and Foss, C. B.(2005). The Reputation Quotient Part I: Developing Reputation Quotient, The Gauge: Developing MediaLink's Newsletter of Worldwide Communications (Vol. 14, pp. 1-4).

FM Global. (2007). *Guide to practical business continuity planning, FM Global internal framework*. http://www.fmglobal.com.

FSA – The Financial Service Authority. (2001) Consultation Paper. *Annex C: Draft Rules and Guidance*. London: Author.

FSA – The Financial Service Authority Consultation Paper. (2002) *Operational Risk Systems and Controls*. London: Author.

Gallagher, M. (2005). The Road to Effective business continuity management. *Accountancy Ireland*, Vol. 37, Number 2, 89-123.

Geoffrey, H. (1997). Disaster recovery planning process. *Disaster Recovery World, Disaster Recovery Journal*, Vol 5, No 1, 55-63.

Hanggraeni, Dewi. (2009). *Pengaruh Privatisasi Terhadap Tata Kelola dan Kinerja Perusahaan P.T. Indofarma (Persero) Tbk*. Jogjakarta: Universitas Gajah Mada

Hamilton, G. (1996). *Risk Management 2000*. Studentlitteratur: Lund.

Hair, F. Joseph, Black, Willian C., Babin, Barry J.,Anderson, Rolph, Tatham, Ronald L. *Multivariate Data Analysis*, (6th ed.). (2006). New Jersey: Pearson Prentice Hall International.

Hellman, Linus & Karlsson, Magnus. (2008). *A Disaster Recovery Planning Guide*. Sweden: Department of Fire Safety Engineering and System Safety Lund University.

Henke, M. (2008). Enterprise and Supply Risk Management. In George & Ritchie (Ed.). *A Handbook of Assessment, Management, and Performance*. New York. (pp.125-135).

ISO/IEC – International Organization for Standardization / International Electrotechnical Commission. (2002). *Guide 73: Risk Management - Vocabulary Guidelines for Use in Standards*, Geneva: Author.

IEC - International Electrotechnical Commission. (1995). *International Standard, Dependability management* - Part 3:Application guide - Section 9: *Risk analysis of technological systems*, Geneva, Switzerland: Author.

International Criminal Investigative Training Assistance Program (ICITAP). (2010). *Standard Sistem Manajemen Keadaan Darurat Pelatihan Yang Disetujui*.

Israel, Glenn. D. (1992). Sampling The Evidence of Extension Program Impact. Program Evaluation and Organizational Development. Florida: University of Florida

Krell, E. (2006). Business continuity – creating a framework for success. CMA Management. Vol. 79, Nr. 8.

London First. (2003). *Expecting the Unexpected – Business continuity in an uncertain world*. http://www.thebci.org/London%20Firsts.pdf

Lanz, Joel. (March 2002). Business Continuity Planning: A Risk Manager's Agenda for Operational and Credit Risk Management. The Risk Management Association Journal, 50-54.

Meglarthy, S. (2000). *Overview of Business Continuity Planning.* Florida : Aurebach CRC Press LLC.

Mitroff, I.I., C. Pearson & T.C. Puchant. (1992). *Crisis management and strategic management: Similarities, differences and challenges*. Adv. Strat. Manage., p: 235-260.

Momani, Naill.M. (2010). *Business Continuity Planning: Are We Prepared for Future Disasters*. American Journal of Economics and Business Administration 2, 272-279.

Nilsson, J. (2003). *Introduktion till riskanalysmetoder*. Department of Fire Safety Engineering, Lund Institute of Technology, Lund, Sweden.

NIST - National Institute of Standards and Technology. (2000). NIST Special Publication 800-34, Contingency Planning Guide for Information Technology (IT) Systems, :Author.

Norrman A., Lindroth R. (2004). Chapter Risk Characteristics of the Supply Chain – A Contingency Framework. In Brindley, C. (Ed.). *Supply Chain Risk*. Hampshire: Ashgate Publishing Limited.

Olsson, F. (1999). *Riskanalysmetoder*. Brandteknik, Lunds Tekniska Högskola, Lunds Universitet.

Patton, M. Q. (1990). *Qualitative Evaluation and Research Method* (2nd ed.). Newburry Park, CA: Sage Publications, Inc.

Ream, S. (2003). *How Does Your Company Measure Up? The Business Continuity Management (BCM) Maturity Model*. http://www.virtual-corp.net/html/bc_model.html.

Robert Ho. (2006). *Handbook of Univariate and Multivariate Data Analysis and Interpretation with SPSS*. Boca Raton: Chapman & Hall/CRC.

Sarwono, Jonathan. (2006). *Analisis data penelitian menggunakan SPSS*. Jogjakarta : Andi.

Santosa and Ashari. (2005). *Analisa Statistik dengan Microsoft Excel & SPSS*. Jogyakarta:Andi.

Smith, D. (2003). *Learning from BCI's Good Practice Guidelines: Business Continuity Advice from Someone who Knows*. Business Continuity Institute. http://www.contingencyplanning.com.

Trochim, M.K. (2006). *The Qualitative Debate – The Research Methods Knowledge Base*. (April 30, 2011). http://www.socialresearchmethods.net/kb/qualdeb.php.

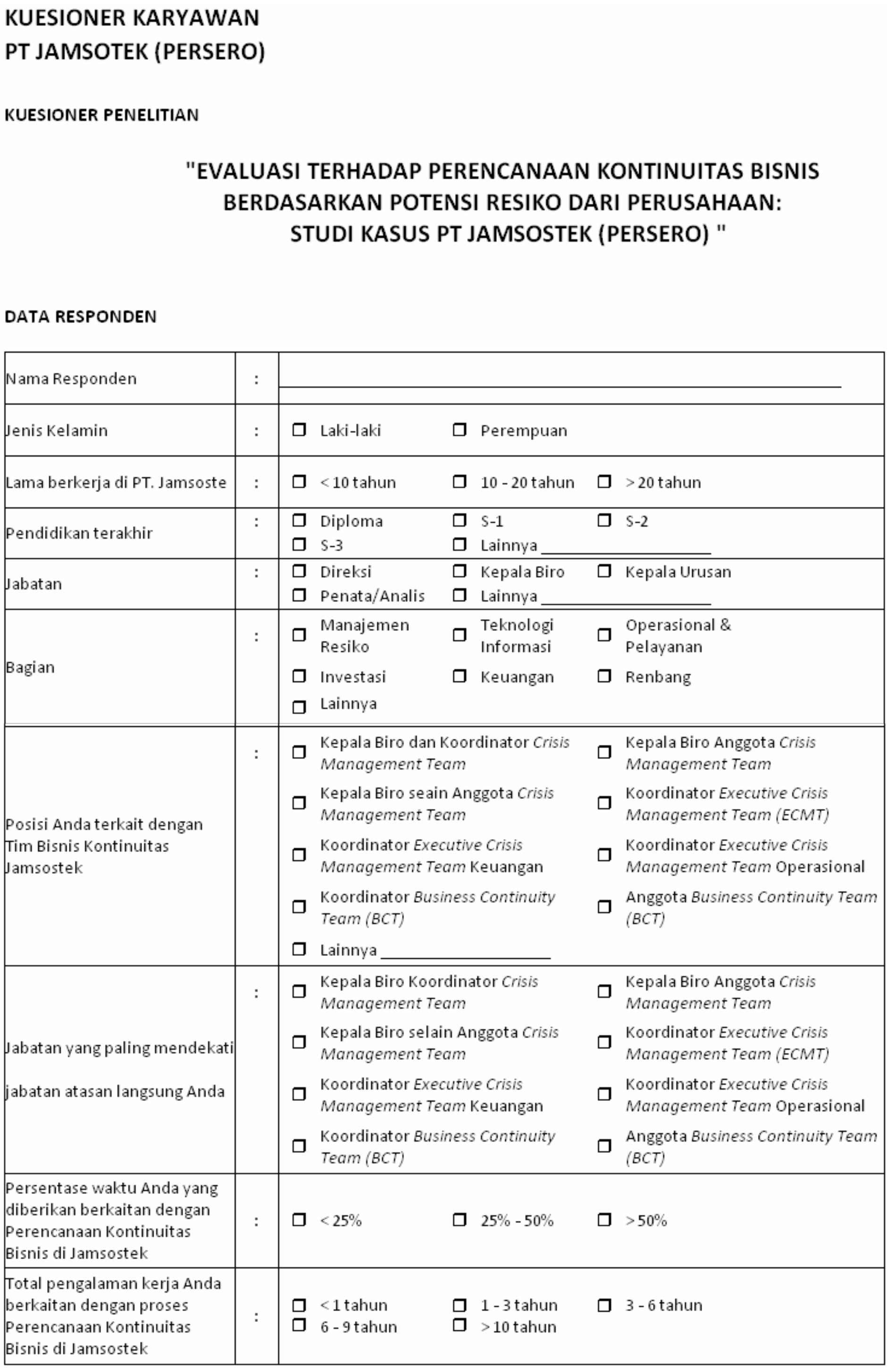
Van Maanen, John. (1979). *Reclaiming Qualitative Methods for Organizational Research: A Preface*. Administrative Science Quaterly. http://www.jstor.org/pss/2392358.

Yamane, Taro. 1967. *Statistics and Introductory Analysis,* 2nd ed. New York: Harper and Row.

Zaman, Arif. (2004). *Reputational Risk: How to manage for value creation.* United Kingdom: Pearson Education Limited.

.

APPENDIX A Research Questionnaire



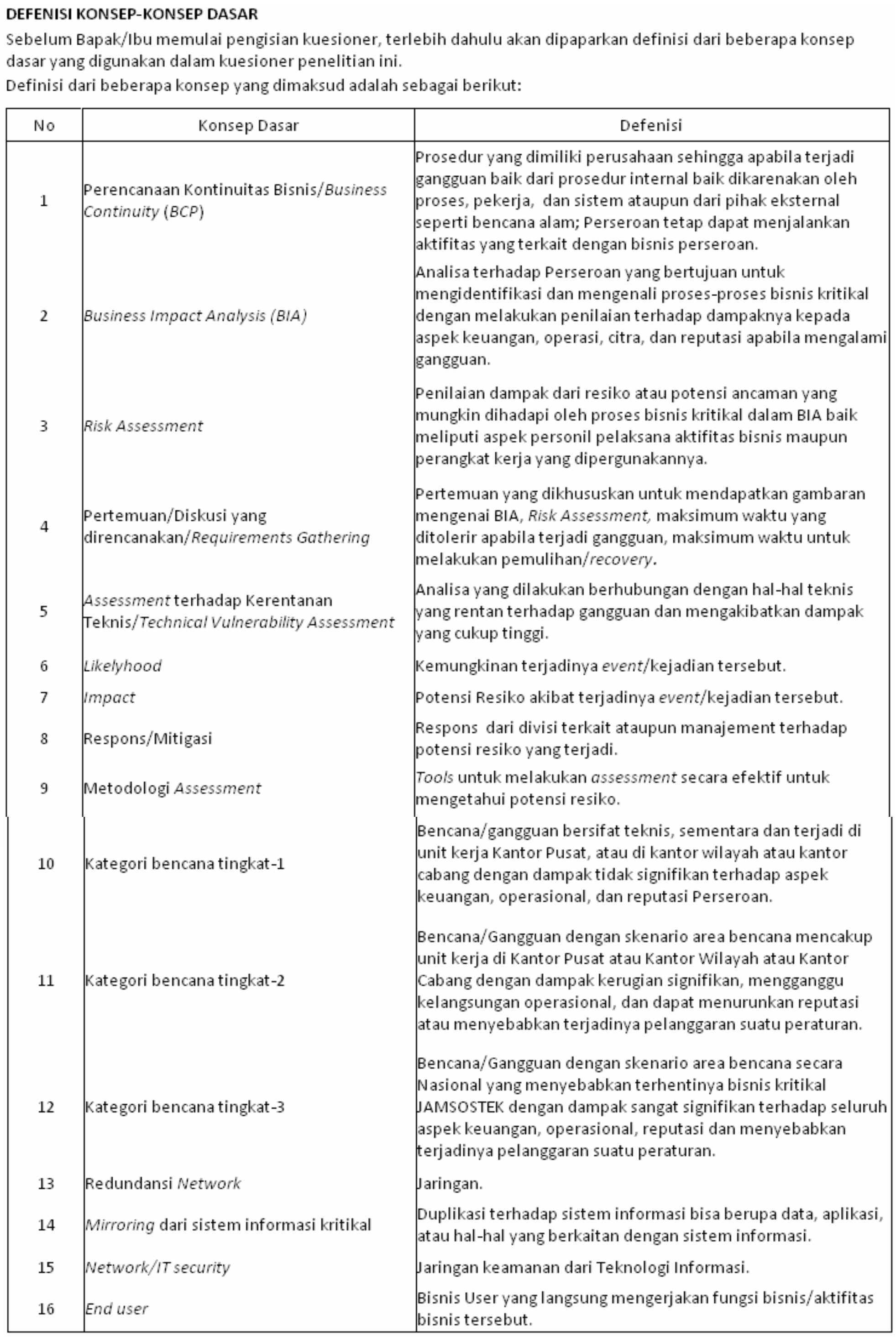
KUESIONER KARYAWAN
PT JAMSOTEK (PERSERO)

KUESIONER PENELITIAN

"EVALUASI TERHADAP PERENCANAAN KONTINUITAS BISNIS BERDASARKAN POTENSI RESIKO DARI PERUSAHAAN: STUDI KASUS PT JAMSOSTEK (PERSERO) "

DATA RESPONDEN

Nama Responden	:	____
Jenis Kelamin	:	□ Laki-laki □ Perempuan
Lama berkerja di PT. Jamsoste	:	□ < 10 tahun □ 10 - 20 tahun □ > 20 tahun
Pendidikan terakhir	:	□ Diploma □ S-1 □ S-2 □ S-3 □ Lainnya ____________________
Jabatan	:	□ Direksi □ Kepala Biro □ Kepala Urusan □ Penata/Analis □ Lainnya ____________________
Bagian	:	□ Manajemen Resiko □ Teknologi Informasi □ Operasional & Pelayanan □ Investasi □ Keuangan □ Renbang □ Lainnya
Posisi Anda terkait dengan Tim Bisnis Kontinuitas Jamsostek	:	□ Kepala Biro dan Koordinator *Crisis Management Team* □ Kepala Biro Anggota *Crisis Management Team* □ Kepala Biro seain Anggota *Crisis Management Team* □ Koordinator *Executive Crisis Management Team (ECMT)* □ Koordinator *Executive Crisis Management Team* Keuangan □ Koordinator *Executive Crisis Management Team* Operasional □ Koordinator *Business Continuity Team (BCT)* □ Anggota *Business Continuity Team (BCT)* □ Lainnya ____________________
Jabatan yang paling mendekati jabatan atasan langsung Anda	:	□ Kepala Biro Koordinator *Crisis Management Team* □ Kepala Biro Anggota *Crisis Management Team* □ Kepala Biro selain Anggota *Crisis Management Team* □ Koordinator *Executive Crisis Management Team (ECMT)* □ Koordinator *Executive Crisis Management Team* Keuangan □ Koordinator *Executive Crisis Management Team* Operasional □ Koordinator *Business Continuity Team (BCT)* □ Anggota *Business Continuity Team (BCT)*
Persentase waktu Anda yang diberikan berkaitan dengan Perencanaan Kontinuitas Bisnis di Jamsostek	:	□ < 25% □ 25% - 50% □ > 50%
Total pengalaman kerja Anda berkaitan dengan proses Perencanaan Kontinuitas Bisnis di Jamsostek	:	□ < 1 tahun □ 1 - 3 tahun □ 3 - 6 tahun □ 6 - 9 tahun □ > 10 tahun

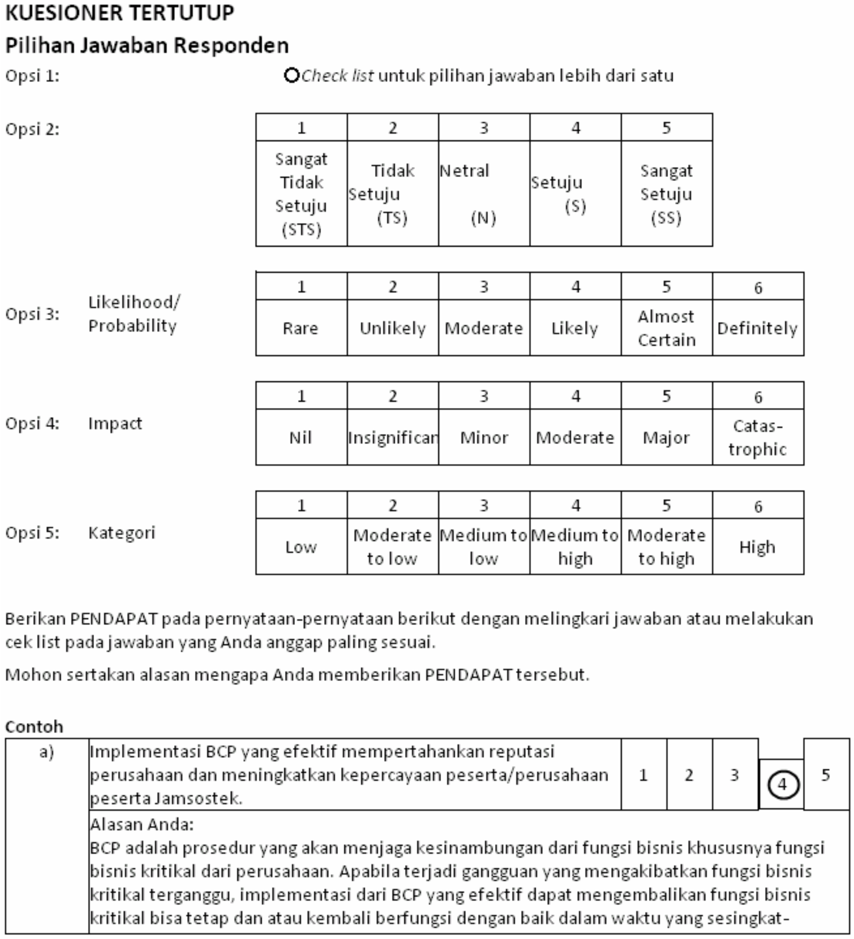


DEFENISI KONSEP-KONSEP DASAR

Sebelum Bapak/Ibu memulai pengisian kuesioner, terlebih dahulu akan dipaparkan definisi dari beberapa konsep dasar yang digunakan dalam kuesioner penelitian ini.

Definisi dari beberapa konsep yang dimaksud adalah sebagai berikut:

No	Konsep Dasar	Defenisi
1	Perencanaan Kontinuitas Bisnis/*Business Continuity* (*BCP*)	Prosedur yang dimiliki perusahaan sehingga apabila terjadi gangguan baik dari prosedur internal baik dikarenakan oleh proses, pekerja, dan sistem ataupun dari pihak eksternal seperti bencana alam; Perseroan tetap dapat menjalankan aktifitas yang terkait dengan bisnis perseroan.
2	*Business Impact Analysis (BIA)*	Analisa terhadap Perseroan yang bertujuan untuk mengidentifikasi dan mengenali proses-proses bisnis kritikal dengan melakukan penilaian terhadap dampaknya kepada aspek keuangan, operasi, citra, dan reputasi apabila mengalami gangguan.
3	*Risk Assessment*	Penilaian dampak dari resiko atau potensi ancaman yang mungkin dihadapi oleh proses bisnis kritikal dalam BIA baik meliputi aspek personil pelaksana aktifitas bisnis maupun perangkat kerja yang dipergunakannya.
4	Pertemuan/Diskusi yang direncanakan/*Requirements Gathering*	Pertemuan yang dikhususkan untuk mendapatkan gambaran mengenai BIA, *Risk Assessment,* maksimum waktu yang ditolerir apabila terjadi gangguan, maksimum waktu untuk melakukan pemulihan/*recovery*.
5	*Assessment* terhadap Kerentanan Teknis/*Technical Vulnerability Assessment*	Analisa yang dilakukan berhubungan dengan hal-hal teknis yang rentan terhadap gangguan dan mengakibatkan dampak yang cukup tinggi.
6	*Likelyhood*	Kemungkinan terjadinya *event*/kejadian tersebut.
7	*Impact*	Potensi Resiko akibat terjadinya *event*/kejadian tersebut.
8	Respons/Mitigasi	Respons dari divisi terkait ataupun manajement terhadap potensi resiko yang terjadi.
9	Metodologi *Assessment*	*Tools* untuk melakukan *assessment* secara efektif untuk mengetahui potensi resiko.
10	Kategori bencana tingkat-1	Bencana/gangguan bersifat teknis, sementara dan terjadi di unit kerja Kantor Pusat, atau di kantor wilayah atau kantor cabang dengan dampak tidak signifikan terhadap aspek keuangan, operasional, dan reputasi Perseroan.
11	Kategori bencana tingkat-2	Bencana/Gangguan dengan skenario area bencana mencakup unit kerja di Kantor Pusat atau Kantor Wilayah atau Kantor Cabang dengan dampak kerugian signifikan, mengganggu kelangsungan operasional, dan dapat menurunkan reputasi atau menyebabkan terjadinya pelanggaran suatu peraturan.
12	Kategori bencana tingkat-3	Bencana/Gangguan dengan skenario area bencana secara Nasional yang menyebabkan terhentinya bisnis kritikal JAMSOSTEK dengan dampak sangat signifikan terhadap seluruh aspek keuangan, operasional, reputasi dan menyebabkan terjadinya pelanggaran suatu peraturan.
13	Redundansi *Network*	Jaringan.
14	*Mirroring* dari sistem informasi kritikal	Duplikasi terhadap sistem informasi bisa berupa data, aplikasi, atau hal-hal yang berkaitan dengan sistem informasi.
15	*Network/IT security*	Jaringan keamanan dari Teknologi Informasi.
16	*End user*	Bisnis User yang langsung mengerjakan fungsi bisnis/aktifitas bisnis tersebut.



KUESIONER TERTUTUP

Pilihan Jawaban Responden

Opsi 1: ○*Check list* untuk pilihan jawaban lebih dari satu

Opsi 2:

1	2	3	4	5
Sangat Tidak Setuju (STS)	Tidak Setuju (TS)	Netral (N)	Setuju (S)	Sangat Setuju (SS)

Opsi 3: Likelihood/ Probability

1	2	3	4	5	6
Rare	Unlikely	Moderate	Likely	Almost Certain	Definitely

Opsi 4: Impact

1	2	3	4	5	6
Nil	Insignifican	Minor	Moderate	Major	Catas-trophic

Opsi 5: Kategori

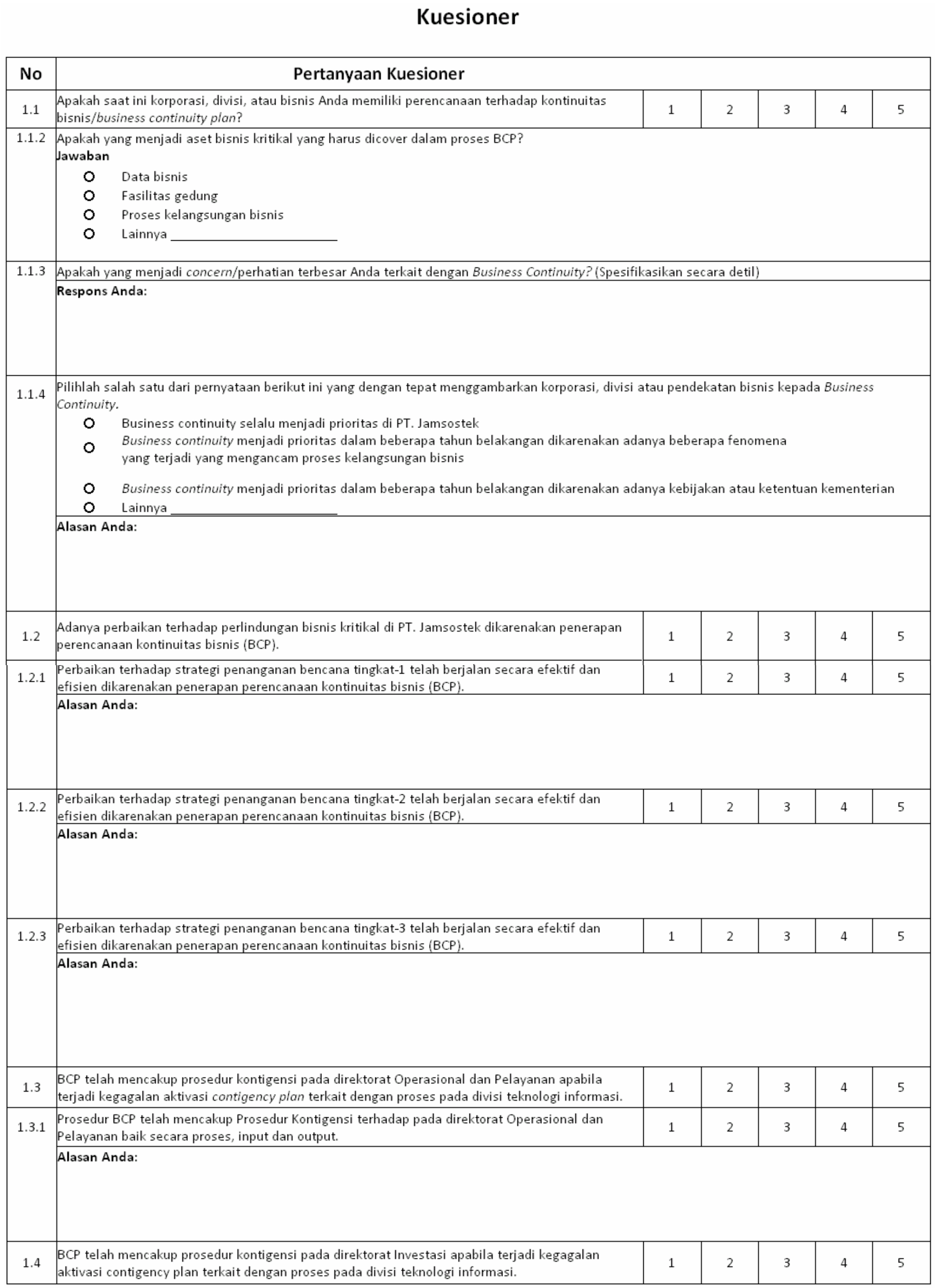
1	2	3	4	5	6
Low	Moderate to low	Medium to low	Medium to high	Moderate to high	High

Berikan PENDAPAT pada pernyataan-pernyataan berikut dengan melingkari jawaban atau melakukan cek list pada jawaban yang Anda anggap paling sesuai.

Mohon sertakan alasan mengapa Anda memberikan PENDAPAT tersebut.

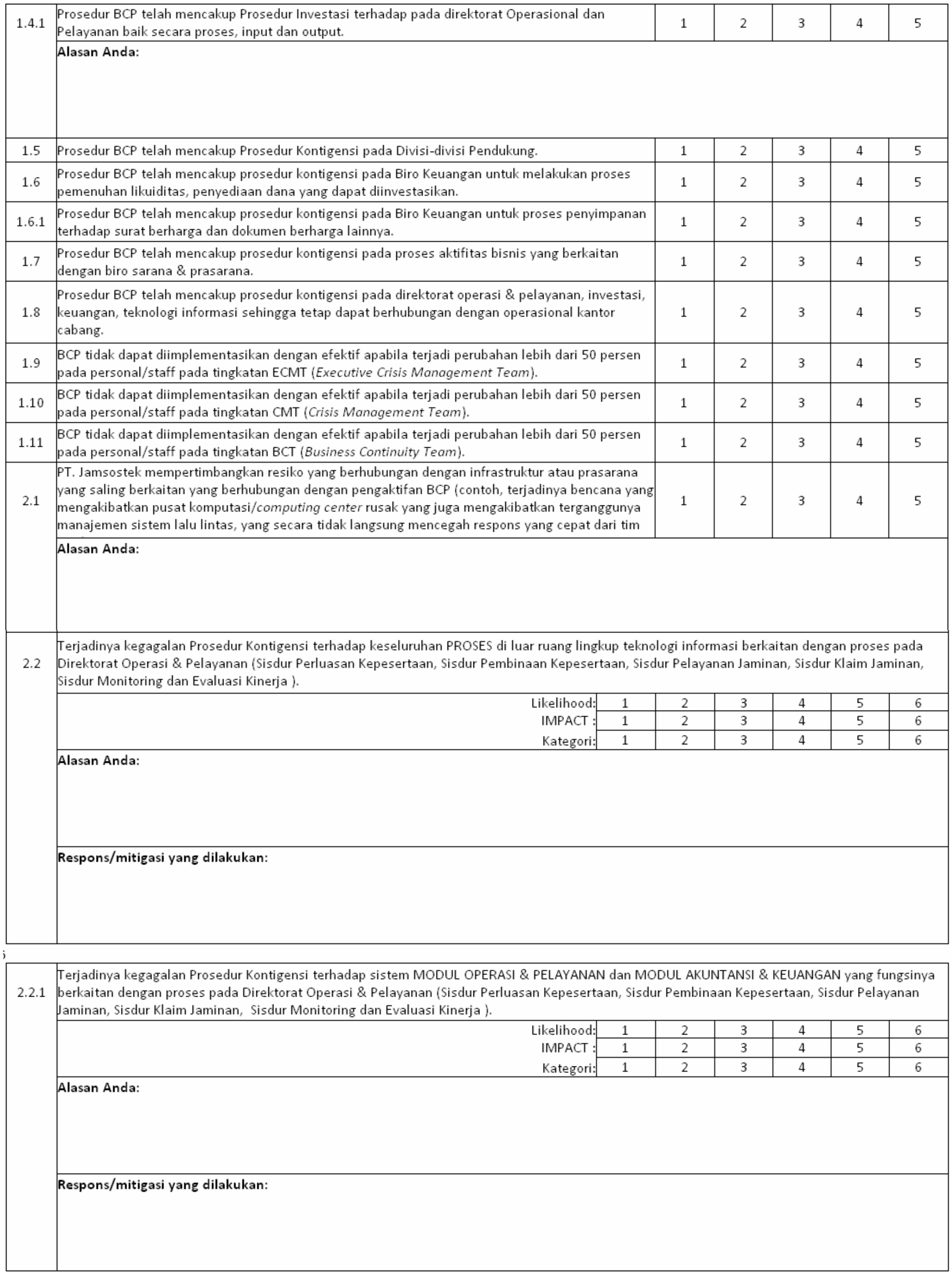
Contoh

a)	Implementasi BCP yang efektif mempertahankan reputasi perusahaan dan meningkatkan kepercayaan peserta/perusahaan peserta Jamsostek.	1	2	3	[✓ 4]	5
	Alasan Anda: BCP adalah prosedur yang akan menjaga kesinambungan dari fungsi bisnis khususnya fungsi bisnis kritikal dari perusahaan. Apabila terjadi gangguan yang mengakibatkan fungsi bisnis kritikal terganggu, implementasi dari BCP yang efektif dapat mengembalikan fungsi bisnis kritikal bisa tetap dan atau kembali berfungsi dengan baik dalam waktu yang sesingkat-					



Kuesioner

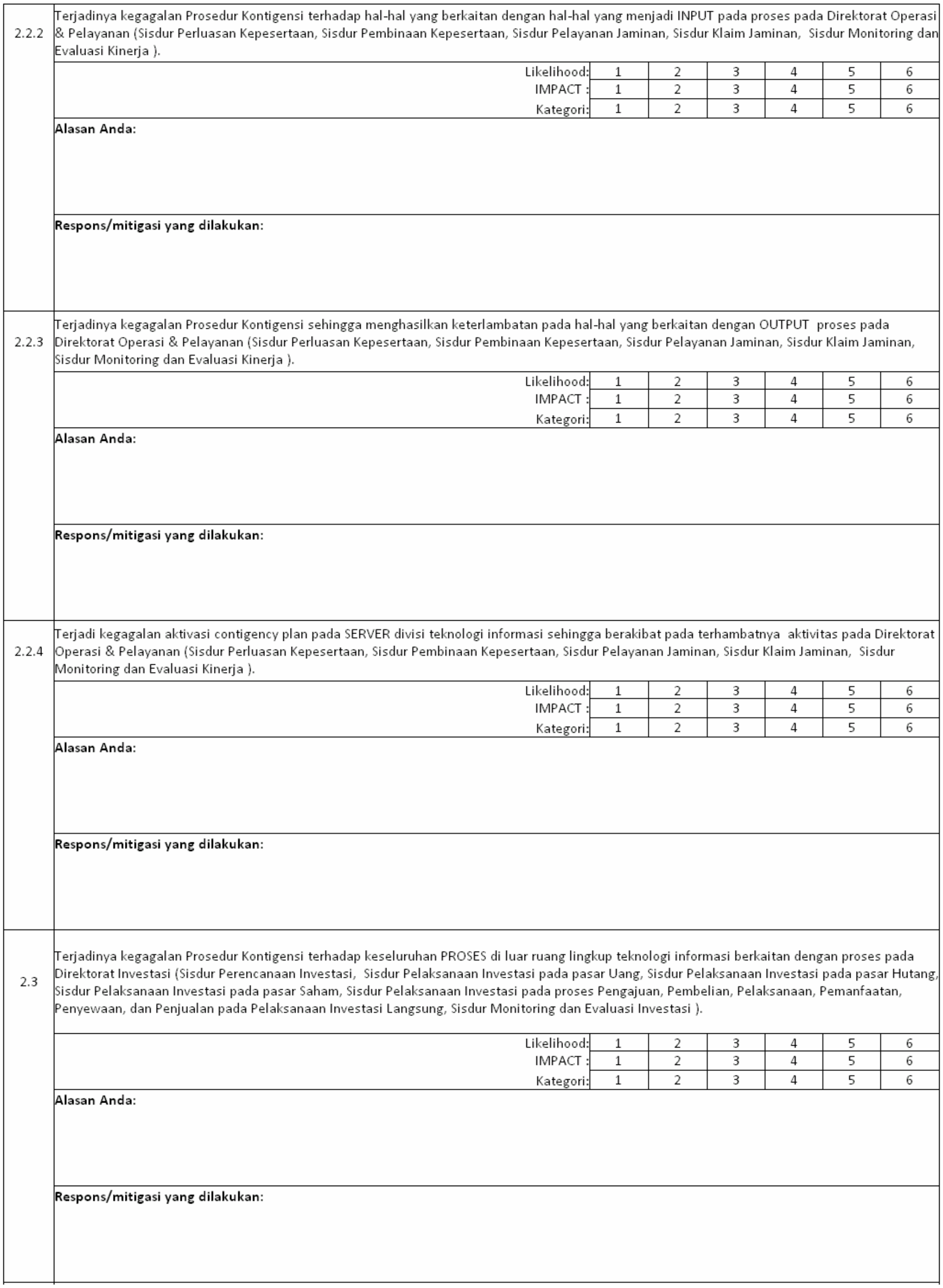
No	Pertanyaan Kuesioner					
1.1	Apakah saat ini korporasi, divisi, atau bisnis Anda memiliki perencanaan terhadap kontinuitas bisnis/*business continuity plan*?	1	2	3	4	5
1.1.2	Apakah yang menjadi aset bisnis kritikal yang harus dicover dalam proses BCP? **Jawaban** ○ Data bisnis ○ Fasilitas gedung ○ Proses kelangsungan bisnis ○ Lainnya ________________________					
1.1.3	Apakah yang menjadi *concern*/perhatian terbesar Anda terkait dengan *Business Continuity?* (Spesifikasikan secara detil)					
	Respons Anda:					
1.1.4	Pilihlah salah satu dari pernyataan berikut ini yang dengan tepat menggambarkan korporasi, divisi atau pendekatan bisnis kepada *Business Continuity*. ○ Business continuity selalu menjadi prioritas di PT. Jamsostek ○ *Business continuity* menjadi prioritas dalam beberapa tahun belakangan dikarenakan adanya beberapa fenomena yang terjadi yang mengancam proses kelangsungan bisnis ○ *Business continuity* menjadi prioritas dalam beberapa tahun belakangan dikarenakan adanya kebijakan atau ketentuan kementerian ○ Lainnya ________________________					
	Alasan Anda:					
1.2	Adanya perbaikan terhadap perlindungan bisnis kritikal di PT. Jamsostek dikarenakan penerapan perencanaan kontinuitas bisnis (BCP).	1	2	3	4	5
1.2.1	Perbaikan terhadap strategi penanganan bencana tingkat-1 telah berjalan secara efektif dan efisien dikarenakan penerapan perencanaan kontinuitas bisnis (BCP).	1	2	3	4	5
	Alasan Anda:					
1.2.2	Perbaikan terhadap strategi penanganan bencana tingkat-2 telah berjalan secara efektif dan efisien dikarenakan penerapan perencanaan kontinuitas bisnis (BCP).	1	2	3	4	5
	Alasan Anda:					
1.2.3	Perbaikan terhadap strategi penanganan bencana tingkat-3 telah berjalan secara efektif dan efisien dikarenakan penerapan perencanaan kontinuitas bisnis (BCP).	1	2	3	4	5
	Alasan Anda:					
1.3	BCP telah mencakup prosedur kontigensi pada direktorat Operasional dan Pelayanan apabila terjadi kegagalan aktivasi *contigency plan* terkait dengan proses pada divisi teknologi informasi.	1	2	3	4	5
1.3.1	Prosedur BCP telah mencakup Prosedur Kontigensi terhadap pada direktorat Operasional dan Pelayanan baik secara proses, input dan output.	1	2	3	4	5
	Alasan Anda:					
1.4	BCP telah mencakup prosedur kontigensi pada direktorat Investasi apabila terjadi kegagalan aktivasi contigency plan terkait dengan proses pada divisi teknologi informasi.	1	2	3	4	5



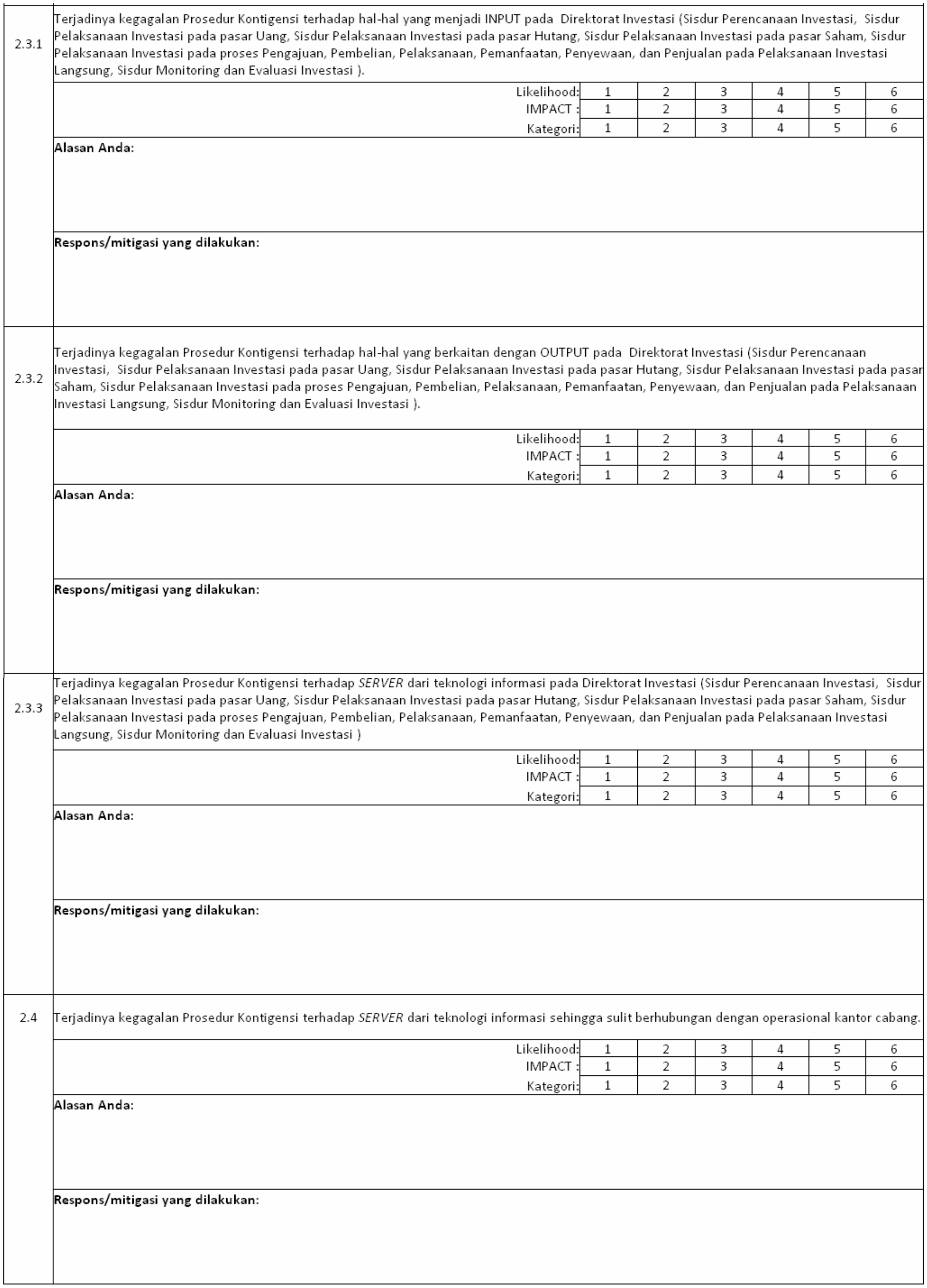
1.4.1	Prosedur BCP telah mencakup Prosedur Investasi terhadap pada direktorat Operasional dan Pelayanan baik secara proses, input dan output.	1	2	3	4	5
	Alasan Anda:					
1.5	Prosedur BCP telah mencakup Prosedur Kontigensi pada Divisi-divisi Pendukung.	1	2	3	4	5
1.6	Prosedur BCP telah mencakup prosedur kontigensi pada Biro Keuangan untuk melakukan proses pemenuhan likuiditas, penyediaan dana yang dapat diinvestasikan.	1	2	3	4	5
1.6.1	Prosedur BCP telah mencakup prosedur kontigensi pada Biro Keuangan untuk proses penyimpanan terhadap surat berharga dan dokumen berharga lainnya.	1	2	3	4	5
1.7	Prosedur BCP telah mencakup prosedur kontigensi pada proses aktifitas bisnis yang berkaitan dengan biro sarana & prasarana.	1	2	3	4	5
1.8	Prosedur BCP telah mencakup prosedur kontigensi pada direktorat operasi & pelayanan, investasi, keuangan, teknologi informasi sehingga tetap dapat berhubungan dengan operasional kantor cabang.	1	2	3	4	5
1.9	BCP tidak dapat diimplementasikan dengan efektif apabila terjadi perubahan lebih dari 50 persen pada personal/staff pada tingkatan ECMT (*Executive Crisis Management Team*).	1	2	3	4	5
1.10	BCP tidak dapat diimplementasikan dengan efektif apabila terjadi perubahan lebih dari 50 persen pada personal/staff pada tingkatan CMT (*Crisis Management Team*).	1	2	3	4	5
1.11	BCP tidak dapat diimplementasikan dengan efektif apabila terjadi perubahan lebih dari 50 persen pada personal/staff pada tingkatan BCT (*Business Continuity Team*).	1	2	3	4	5
2.1	PT. Jamsostek mempertimbangkan resiko yang berhubungan dengan infrastruktur atau prasarana yang saling berkaitan yang berhubungan dengan pengaktifan BCP (contoh, terjadinya bencana yang mengakibatkan pusat komputasi/*computing center* rusak yang juga mengakibatkan terganggunya manajemen sistem lalu lintas, yang secara tidak langsung mencegah respons yang cepat dari tim	1	2	3	4	5
	Alasan Anda:					

2.2	Terjadinya kegagalan Prosedur Kontigensi terhadap keseluruhan PROSES di luar ruang lingkup teknologi informasi berkaitan dengan proses pada Direktorat Operasi & Pelayanan (Sisdur Perluasan Kepesertaan, Sisdur Pembinaan Kepesertaan, Sisdur Pelayanan Jaminan, Sisdur Klaim Jaminan, Sisdur Monitoring dan Evaluasi Kinerja).						
	Likelihood:	1	2	3	4	5	6
	IMPACT :	1	2	3	4	5	6
	Kategori:	1	2	3	4	5	6
	Alasan Anda:						
	Respons/mitigasi yang dilakukan:						

2.2.1	Terjadinya kegagalan Prosedur Kontigensi terhadap sistem MODUL OPERASI & PELAYANAN dan MODUL AKUNTANSI & KEUANGAN yang fungsinya berkaitan dengan proses pada Direktorat Operasi & Pelayanan (Sisdur Perluasan Kepesertaan, Sisdur Pembinaan Kepesertaan, Sisdur Pelayanan Jaminan, Sisdur Klaim Jaminan, Sisdur Monitoring dan Evaluasi Kinerja).						
	Likelihood:	1	2	3	4	5	6
	IMPACT :	1	2	3	4	5	6
	Kategori:	1	2	3	4	5	6
	Alasan Anda:						
	Respons/mitigasi yang dilakukan:						



2.2.2	Terjadinya kegagalan Prosedur Kontigensi terhadap hal-hal yang berkaitan dengan hal-hal yang menjadi INPUT pada proses pada Direktorat Operasi & Pelayanan (Sisdur Perluasan Kepesertaan, Sisdur Pembinaan Kepesertaan, Sisdur Pelayanan Jaminan, Sisdur Klaim Jaminan, Sisdur Monitoring dan Evaluasi Kinerja).						
	Likelihood:	1	2	3	4	5	6
	IMPACT :	1	2	3	4	5	6
	Kategori:	1	2	3	4	5	6
	Alasan Anda:						
	Respons/mitigasi yang dilakukan:						
2.2.3	Terjadinya kegagalan Prosedur Kontigensi sehingga menghasilkan keterlambatan pada hal-hal yang berkaitan dengan OUTPUT proses pada Direktorat Operasi & Pelayanan (Sisdur Perluasan Kepesertaan, Sisdur Pembinaan Kepesertaan, Sisdur Pelayanan Jaminan, Sisdur Klaim Jaminan, Sisdur Monitoring dan Evaluasi Kinerja).						
	Likelihood:	1	2	3	4	5	6
	IMPACT :	1	2	3	4	5	6
	Kategori:	1	2	3	4	5	6
	Alasan Anda:						
	Respons/mitigasi yang dilakukan:						
2.2.4	Terjadi kegagalan aktivasi contigency plan pada SERVER divisi teknologi informasi sehingga berakibat pada terhambatnya aktivitas pada Direktorat Operasi & Pelayanan (Sisdur Perluasan Kepesertaan, Sisdur Pembinaan Kepesertaan, Sisdur Pelayanan Jaminan, Sisdur Klaim Jaminan, Sisdur Monitoring dan Evaluasi Kinerja).						
	Likelihood:	1	2	3	4	5	6
	IMPACT :	1	2	3	4	5	6
	Kategori:	1	2	3	4	5	6
	Alasan Anda:						
	Respons/mitigasi yang dilakukan:						
2.3	Terjadinya kegagalan Prosedur Kontigensi terhadap keseluruhan PROSES di luar ruang lingkup teknologi informasi berkaitan dengan proses pada Direktorat Investasi (Sisdur Perencanaan Investasi, Sisdur Pelaksanaan Investasi pada pasar Uang, Sisdur Pelaksanaan Investasi pada pasar Hutang, Sisdur Pelaksanaan Investasi pada pasar Saham, Sisdur Pelaksanaan Investasi pada proses Pengajuan, Pembelian, Pelaksanaan, Pemanfaatan, Penyewaan, dan Penjualan pada Pelaksanaan Investasi Langsung, Sisdur Monitoring dan Evaluasi Investasi).						
	Likelihood:	1	2	3	4	5	6
	IMPACT :	1	2	3	4	5	6
	Kategori:	1	2	3	4	5	6
	Alasan Anda:						
	Respons/mitigasi yang dilakukan:						



2.3.1 Terjadinya kegagalan Prosedur Kontigensi terhadap hal-hal yang menjadi INPUT pada Direktorat Investasi (Sisdur Perencanaan Investasi, Sisdur Pelaksanaan Investasi pada pasar Uang, Sisdur Pelaksanaan Investasi pada pasar Hutang, Sisdur Pelaksanaan Investasi pada pasar Saham, Sisdur Pelaksanaan Investasi pada proses Pengajuan, Pembelian, Pelaksanaan, Pemanfaatan, Penyewaan, dan Penjualan pada Pelaksanaan Investasi Langsung, Sisdur Monitoring dan Evaluasi Investasi).

Likelihood:	1	2	3	4	5	6
IMPACT :	1	2	3	4	5	6
Kategori:	1	2	3	4	5	6

Alasan Anda:

Respons/mitigasi yang dilakukan:

2.3.2 Terjadinya kegagalan Prosedur Kontigensi terhadap hal-hal yang berkaitan dengan OUTPUT pada Direktorat Investasi (Sisdur Perencanaan Investasi, Sisdur Pelaksanaan Investasi pada pasar Uang, Sisdur Pelaksanaan Investasi pada pasar Hutang, Sisdur Pelaksanaan Investasi pada pasar Saham, Sisdur Pelaksanaan Investasi pada proses Pengajuan, Pembelian, Pelaksanaan, Pemanfaatan, Penyewaan, dan Penjualan pada Pelaksanaan Investasi Langsung, Sisdur Monitoring dan Evaluasi Investasi).

Likelihood:	1	2	3	4	5	6
IMPACT :	1	2	3	4	5	6
Kategori:	1	2	3	4	5	6

Alasan Anda:

Respons/mitigasi yang dilakukan:

2.3.3 Terjadinya kegagalan Prosedur Kontigensi terhadap *SERVER* dari teknologi informasi pada Direktorat Investasi (Sisdur Perencanaan Investasi, Sisdur Pelaksanaan Investasi pada pasar Uang, Sisdur Pelaksanaan Investasi pada pasar Hutang, Sisdur Pelaksanaan Investasi pada pasar Saham, Sisdur Pelaksanaan Investasi pada proses Pengajuan, Pembelian, Pelaksanaan, Pemanfaatan, Penyewaan, dan Penjualan pada Pelaksanaan Investasi Langsung, Sisdur Monitoring dan Evaluasi Investasi)

Likelihood:	1	2	3	4	5	6
IMPACT :	1	2	3	4	5	6
Kategori:	1	2	3	4	5	6

Alasan Anda:

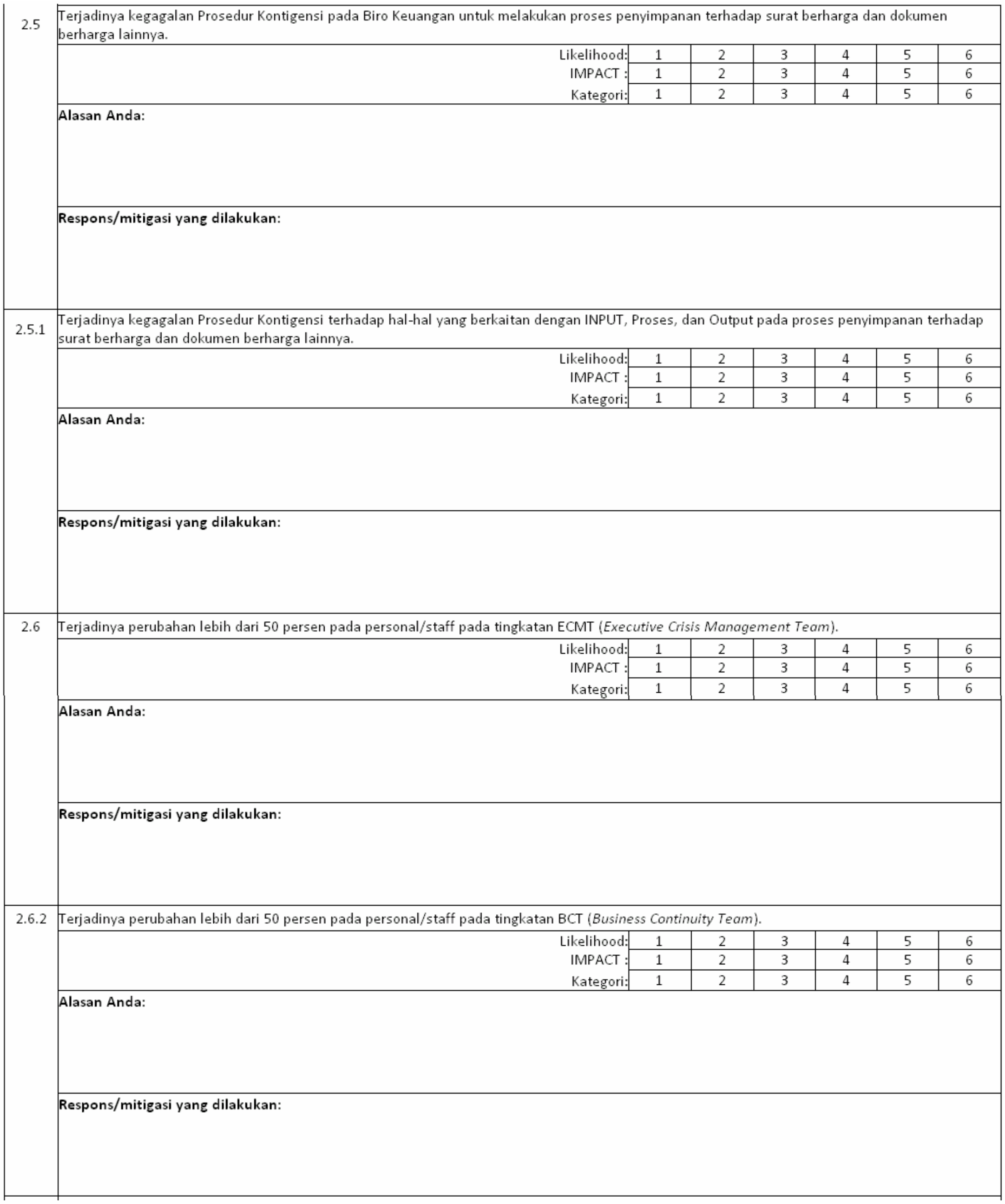
Respons/mitigasi yang dilakukan:

2.4 Terjadinya kegagalan Prosedur Kontigensi terhadap *SERVER* dari teknologi informasi sehingga sulit berhubungan dengan operasional kantor cabang.

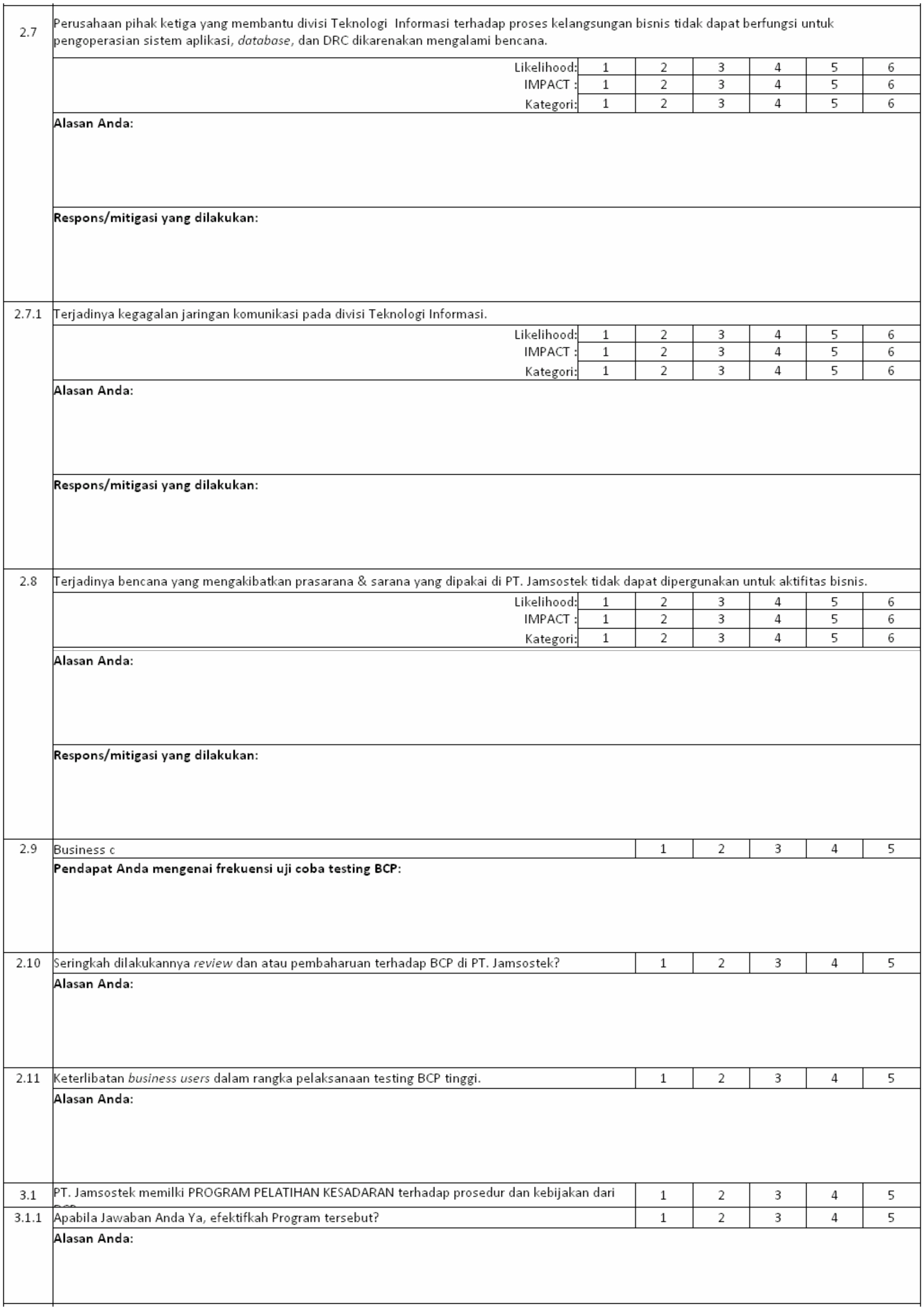
Likelihood:	1	2	3	4	5	6
IMPACT :	1	2	3	4	5	6
Kategori:	1	2	3	4	5	6

Alasan Anda:

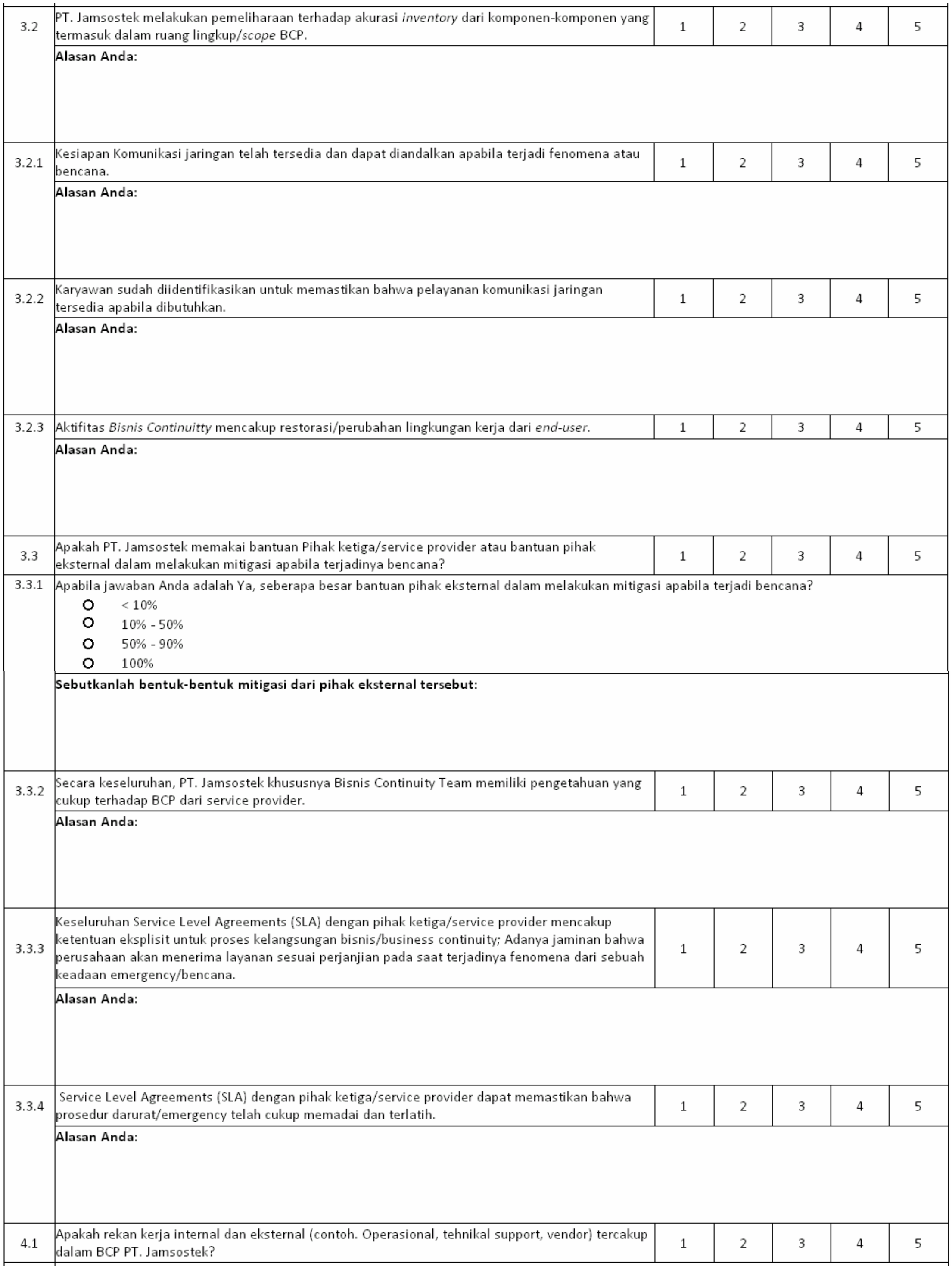
Respons/mitigasi yang dilakukan:



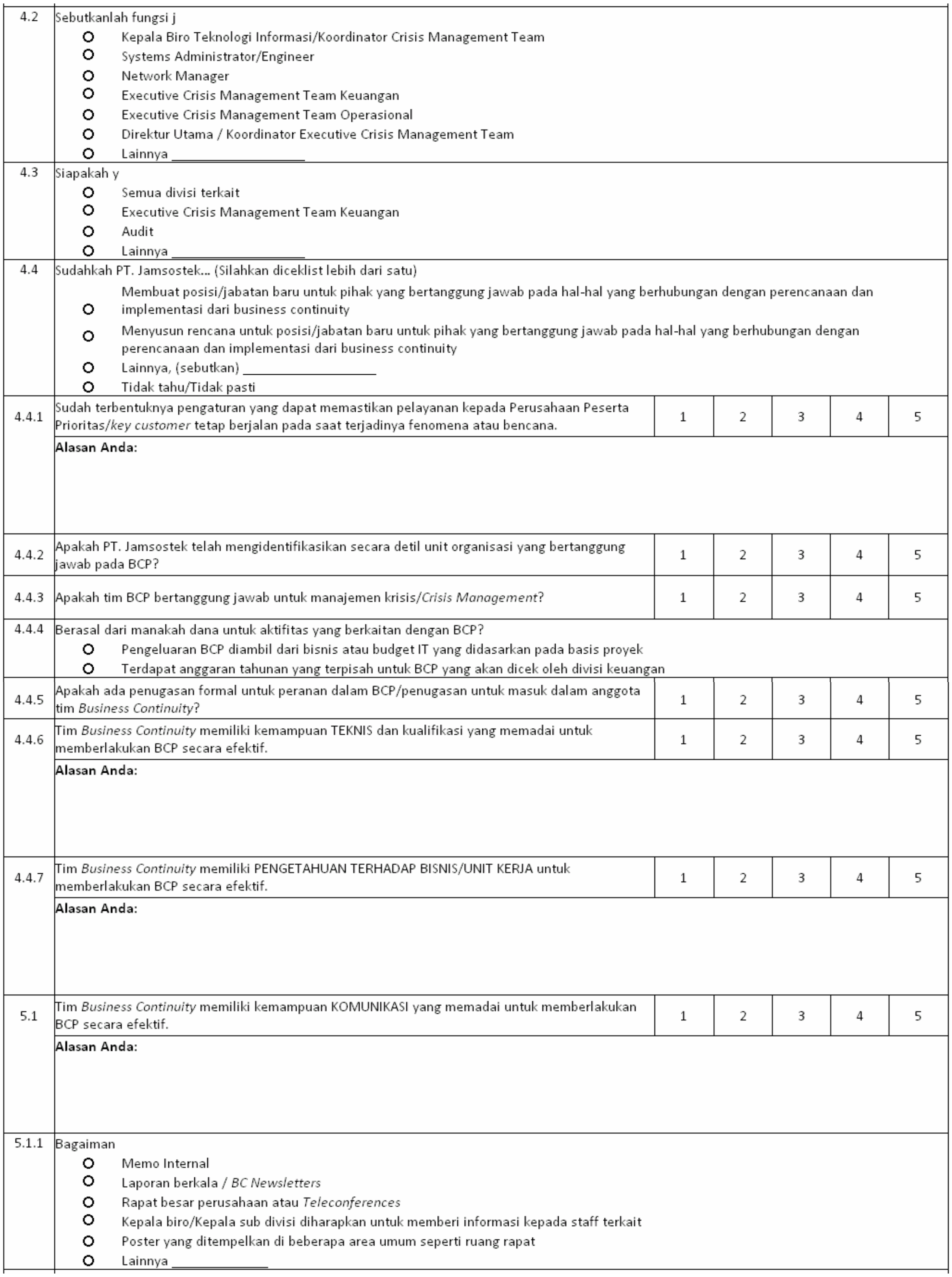
2.5	Terjadinya kegagalan Prosedur Kontigensi pada Biro Keuangan untuk melakukan proses penyimpanan terhadap surat berharga dan dokumen berharga lainnya.						
	Likelihood:	1	2	3	4	5	6
	IMPACT :	1	2	3	4	5	6
	Kategori:	1	2	3	4	5	6
	Alasan Anda:						
	Respons/mitigasi yang dilakukan:						
2.5.1	Terjadinya kegagalan Prosedur Kontigensi terhadap hal-hal yang berkaitan dengan INPUT, Proses, dan Output pada proses penyimpanan terhadap surat berharga dan dokumen berharga lainnya.						
	Likelihood:	1	2	3	4	5	6
	IMPACT :	1	2	3	4	5	6
	Kategori:	1	2	3	4	5	6
	Alasan Anda:						
	Respons/mitigasi yang dilakukan:						
2.6	Terjadinya perubahan lebih dari 50 persen pada personal/staff pada tingkatan ECMT (*Executive Crisis Management Team*).						
	Likelihood:	1	2	3	4	5	6
	IMPACT :	1	2	3	4	5	6
	Kategori:	1	2	3	4	5	6
	Alasan Anda:						
	Respons/mitigasi yang dilakukan:						
2.6.2	Terjadinya perubahan lebih dari 50 persen pada personal/staff pada tingkatan BCT (*Business Continuity Team*).						
	Likelihood:	1	2	3	4	5	6
	IMPACT :	1	2	3	4	5	6
	Kategori:	1	2	3	4	5	6
	Alasan Anda:						
	Respons/mitigasi yang dilakukan:						



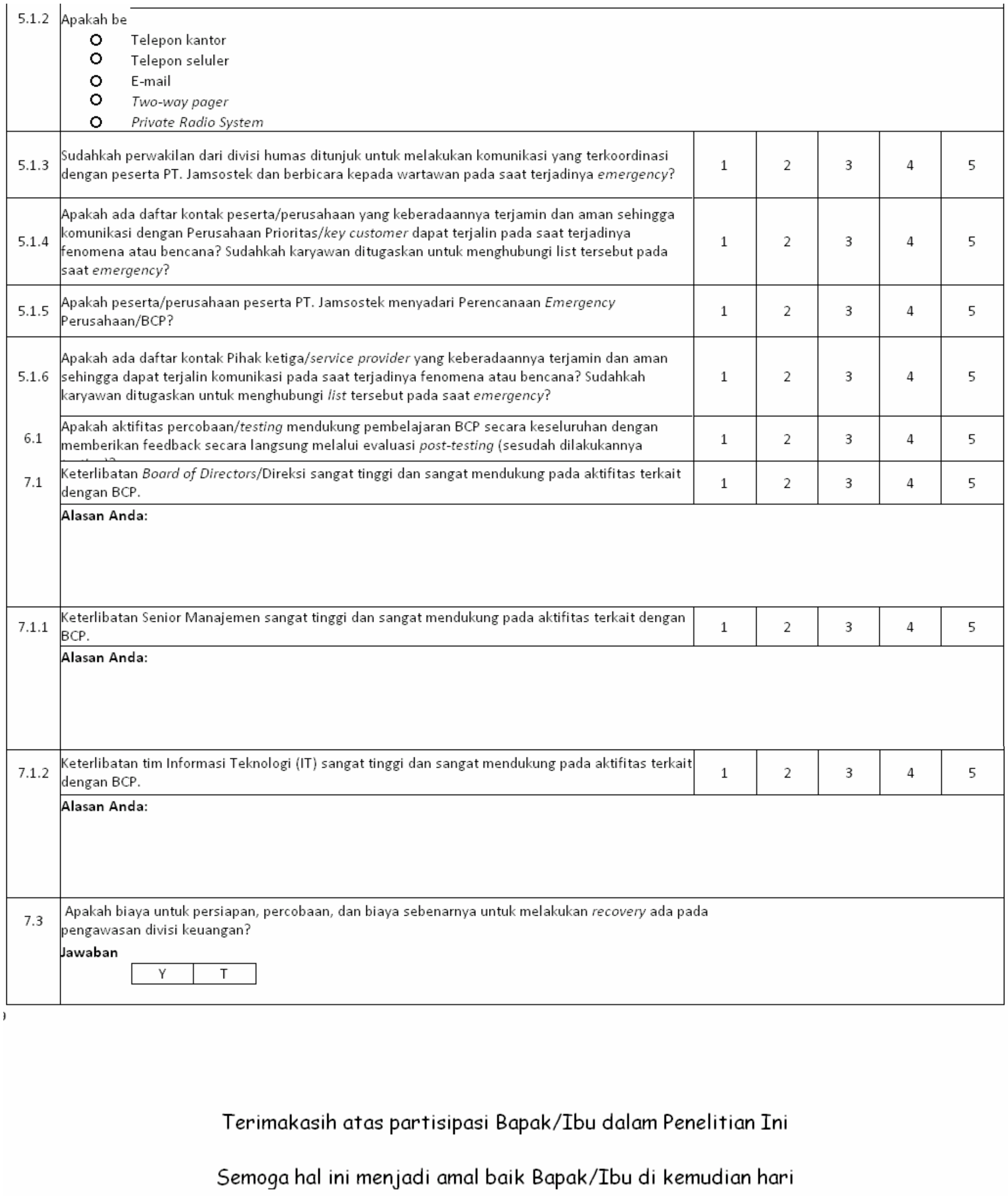
2.7	Perusahaan pihak ketiga yang membantu divisi Teknologi Informasi terhadap proses kelangsungan bisnis tidak dapat berfungsi untuk pengoperasian sistem aplikasi, *database*, dan DRC dikarenakan mengalami bencana.						
	Likelihood:	1	2	3	4	5	6
	IMPACT :	1	2	3	4	5	6
	Kategori:	1	2	3	4	5	6
	Alasan Anda:						
	Respons/mitigasi yang dilakukan:						
2.7.1	Terjadinya kegagalan jaringan komunikasi pada divisi Teknologi Informasi.						
	Likelihood:	1	2	3	4	5	6
	IMPACT :	1	2	3	4	5	6
	Kategori:	1	2	3	4	5	6
	Alasan Anda:						
	Respons/mitigasi yang dilakukan:						
2.8	Terjadinya bencana yang mengakibatkan prasarana & sarana yang dipakai di PT. Jamsostek tidak dapat dipergunakan untuk aktifitas bisnis.						
	Likelihood:	1	2	3	4	5	6
	IMPACT :	1	2	3	4	5	6
	Kategori:	1	2	3	4	5	6
	Alasan Anda:						
	Respons/mitigasi yang dilakukan:						
2.9	Business c		1	2	3	4	5
	Pendapat Anda mengenai frekuensi uji coba testing BCP:						
2.10	Seringkah dilakukannya *review* dan atau pembaharuan terhadap BCP di PT. Jamsostek?		1	2	3	4	5
	Alasan Anda:						
2.11	Keterlibatan *business users* dalam rangka pelaksanaan testing BCP tinggi.		1	2	3	4	5
	Alasan Anda:						
3.1	PT. Jamsostek memilki PROGRAM PELATIHAN KESADARAN terhadap prosedur dan kebijakan dari		1	2	3	4	5
3.1.1	Apabila Jawaban Anda Ya, efektifkah Program tersebut?		1	2	3	4	5
	Alasan Anda:						



3.2	PT. Jamsostek melakukan pemeliharaan terhadap akurasi *inventory* dari komponen-komponen yang termasuk dalam ruang lingkup/*scope* BCP.	1	2	3	4	5
	Alasan Anda:					
3.2.1	Kesiapan Komunikasi jaringan telah tersedia dan dapat diandalkan apabila terjadi fenomena atau bencana.	1	2	3	4	5
	Alasan Anda:					
3.2.2	Karyawan sudah diidentifikasikan untuk memastikan bahwa pelayanan komunikasi jaringan tersedia apabila dibutuhkan.	1	2	3	4	5
	Alasan Anda:					
3.2.3	Aktifitas *Bisnis Continuitty* mencakup restorasi/perubahan lingkungan kerja dari *end-user*.	1	2	3	4	5
	Alasan Anda:					
3.3	Apakah PT. Jamsostek memakai bantuan Pihak ketiga/service provider atau bantuan pihak eksternal dalam melakukan mitigasi apabila terjadinya bencana?	1	2	3	4	5
3.3.1	Apabila jawaban Anda adalah Ya, seberapa besar bantuan pihak eksternal dalam melakukan mitigasi apabila terjadi bencana? ○ < 10% ○ 10% - 50% ○ 50% - 90% ○ 100%					
	Sebutkanlah bentuk-bentuk mitigasi dari pihak eksternal tersebut:					
3.3.2	Secara keseluruhan, PT. Jamsostek khususnya Bisnis Continuity Team memiliki pengetahuan yang cukup terhadap BCP dari service provider.	1	2	3	4	5
	Alasan Anda:					
3.3.3	Keseluruhan Service Level Agreements (SLA) dengan pihak ketiga/service provider mencakup ketentuan eksplisit untuk proses kelangsungan bisnis/business continuity; Adanya jaminan bahwa perusahaan akan menerima layanan sesuai perjanjian pada saat terjadinya fenomena dari sebuah keadaan emergency/bencana.	1	2	3	4	5
	Alasan Anda:					
3.3.4	Service Level Agreements (SLA) dengan pihak ketiga/service provider dapat memastikan bahwa prosedur darurat/emergency telah cukup memadai dan terlatih.	1	2	3	4	5
	Alasan Anda:					
4.1	Apakah rekan kerja internal dan eksternal (contoh. Operasional, tehnikal support, vendor) tercakup dalam BCP PT. Jamsostek?	1	2	3	4	5



4.2	Sebutkanlah fungsi j ○ Kepala Biro Teknologi Informasi/Koordinator Crisis Management Team ○ Systems Administrator/Engineer ○ Network Manager ○ Executive Crisis Management Team Keuangan ○ Executive Crisis Management Team Operasional ○ Direktur Utama / Koordinator Executive Crisis Management Team ○ Lainnya ___________________					
4.3	Siapakah y ○ Semua divisi terkait ○ Executive Crisis Management Team Keuangan ○ Audit ○ Lainnya ___________________					
4.4	Sudahkah PT. Jamsostek... (Silahkan diceklist lebih dari satu) ○ Membuat posisi/jabatan baru untuk pihak yang bertanggung jawab pada hal-hal yang berhubungan dengan perencanaan dan implementasi dari business continuity ○ Menyusun rencana untuk posisi/jabatan baru untuk pihak yang bertanggung jawab pada hal-hal yang berhubungan dengan perencanaan dan implementasi dari business continuity ○ Lainnya, (sebutkan) ___________________ ○ Tidak tahu/Tidak pasti					
4.4.1	Sudah terbentuknya pengaturan yang dapat memastikan pelayanan kepada Perusahaan Peserta Prioritas/*key customer* tetap berjalan pada saat terjadinya fenomena atau bencana.	1	2	3	4	5
	Alasan Anda:					
4.4.2	Apakah PT. Jamsostek telah mengidentifikasikan secara detil unit organisasi yang bertanggung jawab pada BCP?	1	2	3	4	5
4.4.3	Apakah tim BCP bertanggung jawab untuk manajemen krisis/*Crisis Management*?	1	2	3	4	5
4.4.4	Berasal dari manakah dana untuk aktifitas yang berkaitan dengan BCP? ○ Pengeluaran BCP diambil dari bisnis atau budget IT yang didasarkan pada basis proyek ○ Terdapat anggaran tahunan yang terpisah untuk BCP yang akan dicek oleh divisi keuangan					
4.4.5	Apakah ada penugasan formal untuk peranan dalam BCP/penugasan untuk masuk dalam anggota tim *Business Continuity*?	1	2	3	4	5
4.4.6	Tim *Business Continuity* memiliki kemampuan TEKNIS dan kualifikasi yang memadai untuk memberlakukan BCP secara efektif.	1	2	3	4	5
	Alasan Anda:					
4.4.7	Tim *Business Continuity* memiliki PENGETAHUAN TERHADAP BISNIS/UNIT KERJA untuk memberlakukan BCP secara efektif.	1	2	3	4	5
	Alasan Anda:					
5.1	Tim *Business Continuity* memiliki kemampuan KOMUNIKASI yang memadai untuk memberlakukan BCP secara efektif.	1	2	3	4	5
	Alasan Anda:					
5.1.1	Bagaiman ○ Memo Internal ○ Laporan berkala / *BC Newsletters* ○ Rapat besar perusahaan atau *Teleconferences* ○ Kepala biro/Kepala sub divisi diharapkan untuk memberi informasi kepada staff terkait ○ Poster yang ditempelkan di beberapa area umum seperti ruang rapat ○ Lainnya ______________					



5.1.2	Apakah be ○ Telepon kantor ○ Telepon seluler ○ E-mail ○ *Two-way pager* ○ *Private Radio System*					
5.1.3	Sudahkah perwakilan dari divisi humas ditunjuk untuk melakukan komunikasi yang terkoordinasi dengan peserta PT. Jamsostek dan berbicara kepada wartawan pada saat terjadinya *emergency*?	1	2	3	4	5
5.1.4	Apakah ada daftar kontak peserta/perusahaan yang keberadaannya terjamin dan aman sehingga komunikasi dengan Perusahaan Prioritas/*key customer* dapat terjalin pada saat terjadinya fenomena atau bencana? Sudahkah karyawan ditugaskan untuk menghubungi list tersebut pada saat *emergency*?	1	2	3	4	5
5.1.5	Apakah peserta/perusahaan peserta PT. Jamsostek menyadari Perencanaan *Emergency* Perusahaan/BCP?	1	2	3	4	5
5.1.6	Apakah ada daftar kontak Pihak ketiga/*service provider* yang keberadaannya terjamin dan aman sehingga dapat terjalin komunikasi pada saat terjadinya fenomena atau bencana? Sudahkah karyawan ditugaskan untuk menghubungi *list* tersebut pada saat *emergency*?	1	2	3	4	5
6.1	Apakah aktifitas percobaan/*testing* mendukung pembelajaran BCP secara keseluruhan dengan memberikan feedback secara langsung melalui evaluasi *post-testing* (sesudah dilakukannya	1	2	3	4	5
7.1	Keterlibatan *Board of Directors*/Direksi sangat tinggi dan sangat mendukung pada aktifitas terkait dengan BCP.	1	2	3	4	5
	Alasan Anda:					
7.1.1	Keterlibatan Senior Manajemen sangat tinggi dan sangat mendukung pada aktifitas terkait dengan BCP.	1	2	3	4	5
	Alasan Anda:					
7.1.2	Keterlibatan tim Informasi Teknologi (IT) sangat tinggi dan sangat mendukung pada aktifitas terkait dengan BCP.	1	2	3	4	5
	Alasan Anda:					
7.3	Apakah biaya untuk persiapan, percobaan, dan biaya sebenarnya untuk melakukan *recovery* ada pada pengawasan divisi keuangan? **Jawaban** Y | T					

Terimakasih atas partisipasi Bapak/Ibu dalam Penelitian Ini

Semoga hal ini menjadi amal baik Bapak/Ibu di kemudian hari

APPENDIX B Researcher's Interviews

Researcher : RSC

Respondent : RPD

Interview 1: IT Division

RSC : "Apakah yang menjadi asset bisnis kritikal yang menjadi tolok ukur untuk proses kelangsungan bisnis yang ada di Jamsostek."

RPD : "Asset bisnis kritikal yang harus discover dalam BCP adalah proses kelangsungan bisnis. Perusahaan akan hidup minimum survive kalo proses kelangsungan bisnisnya jalan. Bisnis kritikal di Jamsostek, apabila terjadi disaster, kita sudah melakukan recover terhadap system yang bisa up dalam tempo beberapa saat, ini kan sudah di declare. Kalau semuanya hancur berarti harus ada yang lebih intinya lagi (red. yang harus discover),yaitu aplikasi SIPT online dari sisi aktivasi kepesertaan. Itukan titipan dan tabungan, ada asuransikan maka ada dari sisi investasi SIInvest. Dengan seperti itu diasumsikan bisnis kita berlangsung/langgeng. Pada saat bicara BCP lebih spesifik ke IT DRP. Kalau bicara BCP secara keseluruhan dari seluruh sisi Jamsostek. Kalau bicara IT DRP saya sbg kaur duktek, maka lebih ke arah IT DRP. Kebetulan operasional Jamsostek 85% sudah ditunjang dengan teknologi. Teknologi merupakan tulang punggung. Padahal mengenai IT DRP sendiri adalah SIPT & SI invest, padahal masih banyak spt meta data dari arsip, structure, data arsip-arsip yang lain, atau dari bank datanya profiling peserta."

RSC : "Bagaimana prosedur kontigensi terhadap BCP yang sudah diberlakukan di divisi IT?"

RPD : “Level kontigensi sudah yang paling berat, bicara mengenai BCP itu bsa dilihat level-levelnya. Misalnya paling sederhana: monitor, bagaimana kelangsungan, dilakukan laporan lewat via internet krn jaringan mati. Kebetulan operator saat ini adalah Telkom. Kita ada personal in charge di sini tapi tidak poll di system teknis. Mereka memiliki perangkat modem (ada router ada switch). Bagaimana kelangsungan monitor ini supaya 24/7, ada di command center. Kalau tidak bisa dilakukan selama 24 jam maka, ada VPN. Caranya dengan dial internet trus tunneling ke jamsostek pusat. Dari jamsostek pusat baru implementasi pusat akan dilakukan. Ada lagi disaster seperti Padang, tidak mungkin masuk gedung, maka pada saat itu, kan ada 2 bisnis kita yang sudah di sentral dan belum. Yang belum maka harus dikeluarkan perangkatnya. Ada perlengkapan standar kita 1 notebook dan modem atau biasa disebut tunelling, kalau sudah di scope kan lagi misalnya peserta tidak mungkin bayar iuran, tapi kewajiban jamsostek tidak dapat diberikan. Pola nya kesana.”

RSC : “Bagaimana dengan kegagalan prosedur kontigensi pada divisi Operasional & Pelayanan sebagai salah satu fungsi kritikal di PT Jamsostek (Persero)?”

RPD : “Yang menjadi fungsi kritikal di divisi ini apabila terjadi bencana adalah pada pengajuan klaim. Sebagai perusahaan yang memberikan pelayanan jaminan pada pesertanya, maka Jamsostek harus mengutamakan kewajibannya dahulu yaitu proses pengajuan klaim. Yang sudah diimplementasi, standard apapun yang dipakai Eropa atau yang Singapore sama aja. Kita bicara day to day operationnya, kita siapkan assembly hall nya, recovery site nya spt apa, kita bikin di lapangan parkir, bikin tenda, ada mobil belakangnya dibuka itu untuk tempat brankas, sementara yang lain dikunci. Tapi kita tidak ada pembayaran cash. Cash untuk operasional, kalau ada peserta dengan pembayaran lebih kecil dari 100ribu ya mungkin urunan. Di tenda darurat 2 PC cukup CSO &

verifikator jaminan (1PC) sementara yang lain kasir. Dari situ keliatan flow nya, penetapan karena ada besaran people, dll.”

RSC : “Bagaimana prosedur koneksi untuk ke bank apakah sudah diatur ketika terjadi bencana?” RPD : “Kita belum diatur terhadap pihak ketiga, asumsinya adalah jadi kita bayarkan kan surat perintah seperti cek, tapi cek 1 kasus 1 lembar, misalnya ada outstanding cek, sementara itu belum dibayarkan sehingga ada imbalance karena di Jamsostek sudah berkurang dari sisi cash. Sekian kita transaksi maka ada balance untuk jumlah cek yang telah dikeluarkan. Dengan pihak ketiga belum diatur untuk pencairan surat perintah bayar tenaga kerja, asumsinya sekarang sudah banyak ke rekening tabungan itu satu, yang kedua perbankan jauh lebih bagus dengan BCP. Jadi sama saja dengan pagelaran nasional. Dari sisi operasional, cash transfer.”

RSC : “Apabila secara menyeluruh perbankan juga terkena bencana. Sudah adakah prosedur kerjasama dengan pihak ketiga, dalam hal ini adalah perbankan atau service provider?”

RPD : “Dengan pihak ketiga belum, kami masih dalam usulan stuktur organisasinya, trus juga prosedur-prosedur terhadap dari sisi hardware, networking, database dan aplikasi. Untuk ke pihak ketiganya kita bisnisnya dulu, itu berarti teman-teman di operasi, pelayanan, investasi sudah clear. Jadi yang tatanan yang pertama dulu adalah dari mereka,(request dari bisnisnya). TI adalah tools aja, mau pake apapun silahkan. Ok sekarang TI adalah enabler bukan supporting aja tapi enabler, pada saat kita mau melakukan research untuk menjadi enabler ada resource yang harus kita serap. Resource yang mau kita serap juga manajemen belum sampai kesana. R&D untuk teknologi itu belum kesana, jadi agak-agak sulit juga kami untuk melakukan.Paling-paling kami duduk diskusi mencari solusi dengan pihak principal (red. vendor), kalau ada masalah tersebut gimana, kita usulkan, tapi harusnya pedoman pertamanya dari bisnis.”

RSC : “Berdasarkan pembicaraan prosedur backup plan akses data dari DRP TI sudah terjamin, bagaimana dengan level confidence nya apabila diimplementasikan?”

RPD : “Kebetulan belum dibahas secara teknis, belum pernah diuji coba tapi kita sudah buat. Kami dulu pernah melakukan maintenance server di data center kami, karena dia itu mau melakukan penambahan kapasitas listrik. Tadinya kita drill down dari jam 9 kegiatan- kegiatan yang sekuensial, netral dengan asumsi selesainya jam 9 malam di tangerang dimatiin semuanya, bener-bener uji coba thp data bisnis. Selesainya di jam 3 pagi. Uji coba itu di bukan di hari kerja.Terus itu di tahun 2010, kemarin di blln Februari di 2011 kita ada permasalahan di server, karena server kita beli butuh penyetaraan, bisnis ada peningkatan (grow up), tadinya user 1200, sekarang jadi 1800, 2100. Yang masuk ke database, staff internal jamsostek. Resourcenya tidak mampu. Coba kita ada solusi- solusi shortcut ada pengembangan saldo, disitu selesai proses pengembangan itu jam 3, kami laporkan ke kepala biro dan direksi, jam 6-9 pagi mesin bermasalh. Kita informasikan ke help desk agar diinformasikan system kita down, sepertinya kejadiannya di hari senin atau selasa. Sekarang yang bermasalah di DC kita adalah server aplikasi nya server, database tidak bermasalah. Kita alihkan aplikasi di DRC sementara datanya dari DC, jam 12 up. Aplikasi kita kan single tier dan database seiring sejalan di satu tempat, Cuma database pakai dari satu system, yang satu lagi pake yang lain. Dari confidence nya mampu juga sih kami.”

RSC : “Apa penyebab uji coba jarang dilakukan? Seberapa tinggi tingkat keyakinan dari BCP Jamsostek ini sendiri?”

RPD : “Rencana kami untuk tahun ini ada uji coba, dokumen ini kita cek kembali, kita belum sempat cek kembali, kita review, kemudian di uji coba. Level confidence level dari tataran sekitar 6 karena, belum di state dari bisnis untuk RTO nya untuk berapa sih harus direcover, targetnya saat ini adalah 24 jam, apabila sudah up maka dipindahkan ke DRC. Ya tidak apa-apa, tapi belum dihitung Jamsostek berapa biayanya dari sisi finance, bagaimana dengan reputasinya, saat ini bagaimana untuk mempertanggungjawabkan. Hal tersebut kenapa saya anggap ini kritikal. Standar yang kami lakukan, karena ada komitmen dari kepala biro sendiri kita bisa meminimalisir kegiatan sekuensial jadi parallel."

RSC : "Apabila terjadi kegalan terhadap proses kontigensi. Sejauh mana kemungkinan keberhasilannya?"

RPD : "Contoh ekstrim Aceh, agak sulit kalau kita bicara manual itu bisa jalan tidak sih? Karena tidak seperti membalikkan tangan yang dari sentralisasi ke desentralisasi. Secara manualnya kita harus punya database sentralisasi. Dengan cara semanual-manualnya kita harus punya database (red. dari sisi IT) sentralisasi, membagi dari sisi sentralisasi ke desentralisasi itu cukup sulit juga. Kedua dengan cara kami melayani integrity customer dipertanyakan benarkah peserta Jamsostek atau tidak, ya ngga, kalo benar peserta aktif atau tidak. Kemudian dasarnya dari mana kenapa harus dilayani, itu pasti butuh data. Itu yang sekarang sampai saat ini saya piikir bagaimana caranya? Ya pasti dengan VPN tidak usah pusing-pusing. Kalau punya provider GSM, ada 3 akan membuat menara mobile dalam waktu 24 jam. Dari sisi infrastruktur gimana, untuk pembentukan database itu gimana? Jadi agak sulit untuk berbicara hal itu, apakah manual menyelesaikan masalah. Event saya pernah di database, gimana cara mengeluarkan database. Secara manual-manualnya nya notebook ini apakah bisa dijadikan server, jadi dia bisa berjalan sendiri. Kita punya Oracle, oracle itu butuh 70 platform, ada juga yang masuk ke Windows."

Prosedur kontigensi yang sudah pernah terjadi misalnya di Aceh. Memang pada saat itu tidak bisa berfungsi sama sekali, semuanya stuck, ada masa recovery nya,trus begitu mulai berfungsi dari kanwil ada bantuan kesana, veriffikasi data bisa dilakukann di Aceh, jaringan masih ada tapi setelah recovery. Dulu begitu sebenarnya yang penting bisa kerja, ada modem diselamatkan dulu contoh banjir bandang. Ini yang dibicarakan khusus skala nasional DC nya hancur. Contoh di Aceh, semua sector memang tidak bisa berjalan bisa berjalan setelah masa recovery, ada tim yang membantu pada saat recovery tersebut."

RSC : "Dari TI sendiri dalam melakukan prosedur kontigensi, cenderung lebih melakukan prioritas pada investasi atau operasi & pelayaan?"

RPD : "BCP harus dua-dua nya ,bobot 100% 100%. Konsepnya itu ada mesin operasional dan ada mesin untuk investasi. Jadi jaringannya itu redundan dan itu hanya untuk bisnis kritikal saja. Prosedur kontigensi hanya PUPM yang melakukan day to day operational. Iniliah yang belum kami dapatkan apa sih/mana aja yang harus, whole system Investasi atau per modul demikian juga dengan operasional & pelayanan. Tapi yang kita asumsikan kalau per modul hidup harusnya whole sistemnya juga hidup. Kebetulan ini juga di modulnya, tapi kalo di aplikasinya. Contoh MC Office ada Word, excel, dll, jadi begitu office hidup maka modul-modulnya juga otomatis hidup."

RSC : "Dari sisi eskalasi proses, sejauh apa kepentingan BCP/DRP di mata manajemen?"

RPD : "Yang pasti untuk kelangsungan bisnis ada 2 profit taking atau dari sisi trust dari stake holder. Yang ga bisa dihitung adalah dari sisi pencitraan."

RSC : "Bagaimana bentuk dorongan dari manajemen level terhadap pelaksanaan BCP itu sendiri dengan mempertimbangkan faktor tadi, mengingat frekuensi uji coba, tingkat confidence level?"

RPD : "Kami memang belum berdiskusi lebih banyak mengenai how to manage DRP, tetapi dengan melihat kesepakatan kerjasama antara dirut Jamsostek & dirut Telkom dalam hal penyediaan tempat data center dan DRC, itu adalah hal yang serius. Kedua. Dengan kerjasama juga menyediakan link dan backup linknya itu adalah hal yang serius untuk kelangsungan bisnis & pencitraan. Ditambah lagi untuk strategisnya di tahun 2011 ini, kami mengajukan budget pemeliharaan IT DRP disetujui tanpa ada potongan sedikitpun. Tapi yang belum bukan dari manajemen tapi dari divisi resiko menghitung berapa sih kerugian apabila RTO 1 jam, 2 jam, sampai 24 jam. Itu yang harus dihitung jadi asumsinya, kami bagaimana caranya dengan perhitungan itu TI berhasil cost saving untuk menginvestasikan bagaimana system mati jadi hidup. Dari sisi manajemen juga bisa terlihat sudah ada bentukan pengukuran yang jelas."

RSC : "Dari sisi corporate governance, apakah yang harus ditingkatkan?"

RPD : "Di biro TI ada 32 orang, deskjob monitoring system, itu baru dari network belum dari database. Trus operasional, trus pengembangan. Dimana-mana TI itu bukan biro tapi minimum direktorat dengan 2 unit kerja. Operasional dan Pengembangan. Pengembangan itu dibagi 2 pengembangan seluruhnya dan operasional seluruhnya. Bagaimana operasional berjalan sampai dengan DR nya. Pengembangan juga seperti itu. Bisnis alignment dengan IT harusnya ada disini di analis bisnis nya. Bahasa bisnis dengan bahasa IT itu berbeda. Yang harus dilakukan adalah pengembangan di direktorat IT, pemisahan khusus operasional sendiri, pengembangan sendiri, alignment sendiri."

RSC : "Bagaimana bentuk keterlibatan dari pihak ke-3 dalam hal ini service provider?"

RPD : "Begitu terjadi bencana keterlibatan cukup tinggi karena mereka yang membuat DRP, involvement sampai 90%."

RSC : "Bagaimana dengan spesifikasi detil dari penanganan BCP pihak ke-3 apabila pihak ketiga tersebut terkena bencana?"

RPD : "Kami juga punya SOP dan masuk ke SLA. kami harapkan tidak ada bencana deh."

RSC : "Bagaimana dengan budget BCP? Apakah sudah ada pemisahan khusus?"

RPD : "Budget DRP-TI ada di TI, pada saat terjadi bencana, kami mengamankan dari sisi TI, uji coba DRP-TI tetap dari TI. Misalnya prasarana & sarana butuh assembly hall maka biro tersendiri yang melakukan uji coba. Kalo kita bicara BCM , IT-DRP hanya ada di information untuk recover, informasi yang di recover hanyalah SIPT & SIInvest, sisanya ada di tempat lain."

RSC : "Apakah ada pengawasan khusus pada budget BCP?" RPD : "Pengawasan da di biro keuangan, tapi secara khusus belum ada."

RSC : "Apakah dilakukan post testing setelah adanya uji coba?"

RPD : "Ya, secara IT ada feedback testing tapi uji coba yang dilakukan uji coba tidak langsung."

Interview 2: Risk Management Division (simultaneously with 3 respondents)

RSC : "Apakah yang menjadi asset bisnis kritikal yang menjadi tolok ukur untuk proses kelangsungan bisnis yang ada di Jamsostek"

RPD 1 : "Kalau saya lebih cenderung ke data nya. Katakanlah di investment kita salah mengenai datanya berapa posisi kita dimana itukan hancur juga begitu juga dengan pelayanan. Kalo gedung kan lebih bisa, katakanlah saya kunjungan di Surabaya, itukan bisa dilakukan dimana saja."

RPD 2, 3 : "Setuju pak."

RSC : "Bagaimana dengan proses bisnis?"

RPD 1 : “Kalo proses bisnis kita sudah tetapkan dalam acuan baku dalam tiap aktifitas dan sudah diimplementasikan. Apakah kita sudah mencoba proses nya RPD 2?”

RPD 2 : Iya tapi dilokalisir. Uji coba lebih kea rah infrastruktur, kapasitas DRC, kemampuan mesin-mesin yang digunakan.”

RSC : “Jadi uji coba lebih ke arah IT bukan keseluruhan proses?”

RPD 1 : “Belum. Iya kita sudah punya standarisasi tapi belum diujicobakan pada masa terjadinya.”

RSC : “Ketika uji coba dilakukan adakah pemindahan *end user*? ”

RPD 1 : “Yang terlibat di uji coba adalah divisi IT dan BMR. Mengenai pemindahan bisnis user baru akan, belum terjadi.”

RSC : “Apa kira-kira menurut bapak yang menjadi perhatian terbesar/concern/ highlight point dari BCP untuk improve atau major factor dari implementasi BCP yang sedang berlangsung?”

RPD 1 : “Saya jujur khawatir dengan DRC IT. Saat ini saya lebih melihat di resiko operasional salah satu penyebab kelemahan kita kan di IT. Saya khawatirkan di IT mampu tidak melakukan eksplorasi ini. Di kita kualitas IT dan data bisnis. Nah kemudian bisnis proses tidak terkoneksi secara utuh dalam satu rangkaian. Saya khawatir Bisnis proses A sama B ada pada unit berbeda untuk menangani satu flow dari bisnis proses/masalah ga nyambung. Karena bisnis proses dibuat dalam unit berbeda. Apakah ada dalam satu rangkaian yang utuh atau tidak. Katakanlah kalau terjadi force majour yang mau ga mau kita harus melakukan BCP itu sendiri apa bisa nyambung atau tidak karena tidak di uji coba sama sekali, takutnya tidak sustain. Harusnya bisa diujicoba IT & bisnis proses.”

RPD 2 : “Yang menjadi concern adalah bagaimana proses sosialisasi dari BCP tersebut terkait dengan tingkat awareness dari staff itu sendiri terhadap resiko yang akan dihadapi.”

RSC : “Apakah yang kira-kira tepat menggambarkan BCP secara manajemen/strategis/teknis?”

RPD 1 : “BCP harusnya iya menjadi prioritas di Jamsostek, karena di era yang tidak pasti seperti sekarang kita harusnya memiliki back up plan yang kita bisa diandalkan. Apalagi Jamsostek adalah bisnis kepercayaan memegang, pengelola dana amanah dari masyarakat. misalnya kita terjadi sesuatu yang terjadi sebenarnya kita harus sudah perhitungkan dan kita tidak bisa mendeliver apa yang menjadi kewajiban kita, apakah kita bisa tetap memegang amanah spt sekarang? Jangan sampai datang akibat dulu baru dilakukan. Saya selalu menganngaap penting, sesuatu yang disebutkan (bencana) misalnya terjadi, cth di investment dalam sehari dua hari opportunity sudah hilang, opportunity untuk mendapatkan gain dan peningkatan manfaat lebih di investasi peserta. Di operasi, tidak bisa pelayanan, tidak sepenuhnya siap melayani karena tidak sepenuhnya siap. Dengan uji coba kita bisa ukur seberapa siap kita, khususnya di hari kerja.”

RSC : “Di investasi, apa yang menjadi point supaya BCP berhasil?”

RPD 1 : “Sistem investasi stand alone, investasi tidak online agak beruntung karena semuanya ada di kantor pusat. Masih memungkinkan data penyimpanan lokalisir cepat, kita bisa menyimpan tapi kan itu tidak real data dan belum tentu secara disiplin untuk menyimpan data tersebut secara back up. Dan belum tentu terintegrasi. SI invest di pusat tidak perlu online, yang perlu online di cabang. Back up data apakah sudah di back up otomatis atau tidak? Belum begitu tau detil untuk DRC.”

RSC : “Apakah dalam pembentukan BCP di Jamsostek, ada pengaturan khusus atau dorongan dari pihak eksternal seperti kementrian terkait?”

RPD 1 : “Secara teknis tidak tapi spiritnya iya. Karena dari kementrian diminta, mereka sudah punya blue print enterprise risk management, BCP salah satu bagiannya, BCP adalah salah satu concernnya.”

RPD 2 : “Kalau kita belajar BCP dari kebijakan pemerintah, diatur salah satu manajemen, BCP bagian dari pengelolaan risk management. Di tahun 2006 berlaku amanah RUPS untuk mengimplementasikan manajemen resiko. Spiritnya di risk management, BCP melekat dalam risk management. Arahnya BCP kemana belum secara tegas diberikan.”

RSC : “Apakah ada turning point atau fenomena, maka BCP diimplementasikan di Jamsostek?”

RPD 1 : “Dorongan secara direct tidak tapi kita sadar sebagai pemegang amanah masyarakat kita sadar perlunya BCP. Di samping itu ada musim gempa di Padang, itu juga memicu semangat untuk iimplementasi BCP. Tapi sebelum kejadian kita sudah pikirikan, sudah dibuat sebagai bagian dari ERM. “

RPD 2 : “Tahun ini kita bangun infrastruktur untuk ERM di TI. Ketidakpastian tidak bisa diprediksi, kemudian ada BCP DRP, untuk mengurangi kemungkinan kita tidak mampu. Minimalisasi lebih kea rah dampak. Lebih ke arah IT.”

RSC : “Setelah BCP diimplementasi ada tidak perbaikan kontigensi?”

RPD 1 : “Kita tidak bisa bicara karena baru diimplementasikan. Baru mulai dikembangkan. Dinamika dokumen, berdasarkan perubahan-perubahan. Kalau masalah dari infrastruktur lebih detail bertanya ke Kepala Biro TI. Kalau di TI perbaikan kontigensi dari DRC harusnya lebih kelihatan. Kita juga ada sosialisasi awareness mengenai Risk Management di kantor cabang di akhir desember, kantor pusat di bulan april. Ini salah satu resiko kita, buka kesadaran mereka. Tahun 2011, akan dilakukan penyempurnaan/penyesuaian perpindahan provider (lebih kea rah DRC).

Kita juga akan membentuk tim, tim penyusunan penyempurnaan. Tim khusus/tim ad hoc itu lebih efektif hanya ada sebatas dalam kebijakan, tim masuk dari berbagai divisi, ini dibuat dari bulan Juni. Pelegalan terhadap struktur organisasi melalui pembentukan SK Kerja, masuk dalam system prosedur. Termasuk ada penunjukkan terhadap tiap unit terhadap PIC."

RSC : "Bagaimana dengan proses pembaharuan BCP tersebut?"

RPD 1 : "Baru mau dilakukan dalam program kerja di tahun ini."

RSC : "Bagaimana tingkat perubahan nilai/value dari pekerja/staff terhadap nilai BCP?"

RPD 1 : "Kita harus akui saat ini risk management masih terasa asing boro-boro BCP. Secara ini mereka pasti berpikir kalau terjadi bencana bagaimana, memang tidak pernah kita formalkan dalam satu system tapi ide-idenya ada. Kita memang meningkatkan awareness dengan melakukan sosialisasi, kita sudah bantu untuk menjelaskan BCP itu seperti apa? Sosialisasi baru dilakukan sekali tapi ke semua unit kerja. Kita sadarkan dengan membuka wawasan. Selama ini yang mengetahui BCP DRP hanya unit tertentu yaitu IT & Risk management. Di luar itu kan belum tentu tau atau belum tentu mau tau. Kita coba sosialisasikan dan kita paksa mereka membuat profil resiko dimana untuk unit-unit tertentu yang terkait. Misalnya IT atau investasi, operasi mereka harus memikirkan itu (apa yang harus di back up, kontigensi. Kalau di investasi mereka melakukan dengan back up external harddisk tapi belum tentu proses tersebut dilakukan secara kontinu. Ke depannya kita paksa apakah bisa berlangsung?"

RSC : "Bagaimana dengan perbaikan terhadap perubahan?"

RPD 1 : "Perencanaan sudah ada, mulai diimplementasikan Juni, adhoc nya, tiap unit kerja punya PIC nya. "

RSC : "Berhubungan dengan penanganan bencana berdasarkan tingkat bencana. Apakah ada perbaikan strategi?"

RPD 2 : "Misalnya bencana tingkat 1 ada hang local dalam RTO . Dari sisi TI, pada strategi ada perbaikan dalam infrastruktur TI, ada perbaikan strategi tapi hanya untuk pelayanan kritikal point saja misalnya. Untuk Operasional : Lokal sudah ada prosedur."

RSC : "Bagaimana dengan kecukupan likuiditas apabila terjadi interruption sehingga peserta berbondong-bondong ajukan klaim ke Jamsostek?" RPD 1: "Apabila dengan likuiditas sudah cukup sesuai dengan rasio yang ada, cadangan resiko thp likuiditas. Proses kontigensi terhadap likuiditas sudah berjalan untuk seluruh cabang yang ada di seluruh nasional."

RPD 2 : "Dari sisi proses: dari semua cabang yang memiliki jaringan tingkat provider sudah sesuai dengan jumlah rumah sakit. Contohnya penanganan di Aceh, Padang, adanya merekrut dari cabang terdekat, penanganan di Aceh tidak ada issue apakah ada issue mengenai klaim tidak bisa diklaim. Cadangan sudah sangat-sangat besar, terkecuali secara nasional semua klaim, pemerintah akan menjamin mengenai likuiditas tersebut. Tapi harus disadari belum ada dokumen pendukung, penanganan secara detil. Apabila bisnis proses Jamsostek terhenti sama sekali dan aktifasi IT sama sekali tidak mendukung. Manual process yang akan dilakukan. Prosedur IT sama sekali tidak mendukung maka prosedur manual yang akan diutamakan. Kritikal proses berhenti, menghidupkan kembali proses secara manual, secara dokumentasi cari berkas, dan instruksi nya berasal dari ECMT (direktur utama). Tidak ada lagi control secara system. Perbaikan strategi: secara corporate level: apabila terjadi bencana Organisasi normal tidak akan berlaku, langsung masuk ke organisasi ECMT. Secara menyeluruh apabila spesifik pada BCP sendiri, perbaikan belum ada karena belum dilakukan dikarenakan belum ada bencana, tetapi sudah ada best practice.

RSC : “Menurut bapak bagaimana dengan perbaikan strategi dari organisasi terhadap BCP itu sendiri?”

RPD 1 : “Dari organisasi masih belum terbentuk secara kongret SK kerja dan lain-lain, harusnya begitu dilakukan implementasi bakal ada proses kelanjutannya. Walaupun Belum dilakukan uji coba secara keseluruhan, tetapi satu dua sudah terjadi kan? Saat ini mungkin kita belajar prioritas di point-point kritikal di pelayanan, tapi nanti akan menyeluruh. Harus kita sadari bahwa tingkat awareness terhadap resiko yang sudah pernah diuji coba ada di bawah 50%.”

RSC : “Bagaimana dengan penyimpanan data surat berharga yang terkait dengan divisi investasi?”

RPD 1 : “Pertama, aktifitas investasi ada di luar, reliable, mereka punya back up data nasional (obligasi, saham, dll) di custodian. Untuk deposito yang dipegang di Jamsostek baik di pusat maupun cabang. Karena antara yang mencatat dan menyimpan berbeda.”

RSC : “Bagaimana dengan pihak ke-3 untuk penyimpanan data tersebut. Apakah Jamsostek dapat memastikan BC dari pihak ke-3 tersebut?”

RPD 1 : “Mereka adalah lembaga Negara yang tau kredibilitasnya, ada supervise langsung dari bapepam LK.”

RSC : “Bagaimana dengan biro Prasarana & Sarana?”

RPD 1 : “Kesiapan sudah ada, prosedur sudah ada kebjijakan tapi belum ada prosedur secara detil. Saya belum terlalu yakin jawaban mengenai hal ini.”

RSC : “Bagaimana bila terjadi perubahan personil yang cukup mendasar pada level ECMT, CMT, dan BCT terhadap BC di Jamsostek?”

RPD 1 : “Apabila terjadi perubahan direksi lebih dari 50%, tidak ada masalah, 100% juga tidak masalah karena kita sudah berjalan dengan system, strategi sudah ada, prosedur sudah ada, siapapun direkturnya kecuali arahnya berbeda ya ada perubahan lagi. Tidak ada pengaruh dengan perubahan organisasi di ECMT karena sudah berjalan benar. Dengan kantor wilayah dan BCT nya lebih tidak masalah, karena sudah ada pengganti yang menggantikannya, bukan orang yang ditunjuk tapi SOP nya yang perlu dicek. Itu clear, capability yang menggantikan ada assessment, apabila sudah lulus uji kompetensi, dan lain lain tidak masalah dan kita sudah punya core competency dan soft competency, kita sudah punya."

RPD 2 : "Kemungkinan ada interupsi atau gangguan pada pengaktivan BCP, apabila perubahan tersebut langsung disertai bencana atau gangguan mendasar yang membutuhkan eskalasi dan penanganan khusus."

RSC : "Bagaimana dengan kesiapan apabila terjadi kegagalan pengaktivan Prosedur Kontigensi?"

RPD 1 : "Resiko sudah dipertimbangkan pada saat terjadi bencana. Kita bicara pada saat ini., mengenai IT karena saya sudah ke Surabaya dan sudah melihat kesiapan infrastruktur sudah siap tapi belum diuji coba pada hari kerja. Masalah IT ada DRC, jaringan masalah server kita ada, masalah SDM kita mengatur di back up, masalah gedung kita beralih ke gedung terdekat."

RPD 2 : "Di BCP kita mengatur sampai level 3, klo prosedur 1 tidak berhasil naik ke prosedur 2 baru naik manual.

RPD 1 : "Menurut saya kemungkinan terjadi sangat kecil, relative ga mungkin terjadi kecuali gempa bumi tahun 2012, kita sustain, selama ada power listrik kita bisa jalan. Tapi kalau bicara impact pasti besar. Mitigasi yang dilakukan ya pasti manual. Tapi kan suda diatur manualnya."

RPD 3 : “Menurut saya mengenai kegagalan prosedur kontigensi di IT yaitu sistemnya gagal, kemungkinannya moderate. Hal ini dikarenakan banyak faktor eksternal. Mengenai impact nya pasti besar.”

RSC : “Apabila dilakukan mitigasi manual, bagaimana dengan surat-surat, terjadi klaim fiktif?”

RPD 1 : “Dokumen akan diproses kalau sudah lengkap, diluar itu akan dikembalikan. Kemungkinan kecil, karena tidak akan disimpan, apabila sudah lengkap maka akan diagendakan, kalau hilang di database kita tidak disimpan. Apa yang terjadi selama ini relative sangat kecil, karena kita bisa cover, klaim fiktif jrang karena kita sudah ada her registrasi, sehingga probability bisa sangat kecil. Hal ini juga terbukti dengan laporan permasalahan internal sudah berkurang frekuensi mengenai hal ini.”

RSC : “Bagaimana dari sisi Investasi?”

RPD 1 : “Kita sudah punya mekanisme khusus, ada SOP, intens untuk mengurangi potensi terjadinya kegagalan. Otomatis probabilitas kecil. Potensi terjadi fraud sangat kecil, sudah di minimalkan. Investasi juga sudah punya investment guideline. Implementasi guideline tersebut dibuat oleh risk management, dan sudah diimplementasikan. Contoh kasus bank XXX kita sudah bisa discover di Jamsostek. Contoh : Pelaporan yang ada dalam data dengan pengakuan dari bank tersebut, dilakukan sidak, ga cuma periodically, malah ada ambil sample. Kalau terjadipun impactnya kecil, misalnya penempatan pasti besar di bank besar, di bank kecil pasti kecil. Misalnya bank YYY, kemungkinan dropnya pasti kecil. Perlu diketahui bahwa spirit dari manajemen resiko lebih ke investasi, terlihat dengan adanya 3 kaur untuk menangani investasi.”

RSC : “Bagaimana dari sisi Keuangan?”

RPD 1 : “Untuk biro keuangan, kemungkinan frekuensi relatif kecil, mereka sudah punya aturan, sudah punya control kesana. Impactnya juga kecil karena sudah ada system. Mereka ada cek kesana, yang tidak dilakukan oleh bank XXX tidak pernah mengecek sama kalau dilihat di surat ada statement : bahwa deposito tidak bisa dijaminkan dan dipindahkan oleh ke pihak manapun juga. Hanya eksklusif untuk Jamsostek berlaku spt itu, kalau itu dilakukan masih bisa terjadi berarti itu ada kesalah di perbankan tersebut.” RSC : “Bagaimana apabila perusahaan pihak ke-3 dalam hal ini service provider yang membantu Jamsostek apabila tidak bisa berfungsi untuk aplikasi system?”

RPD 1 : “Kita pakai provider ZZZ, saya sudah mengunjungi lokasi dari sisi topografi, dan lain-lain. Selain itu ditarik garis Jakarta dengan Surabaya lempengannya berbeda.

RSC : “Bagaimana keterlibatan service provider dalam hal ini ZZZ dalam menangani BCP Jamsostek?”

RPD 1 : “Proses keterlibatan apabila terjadi bencana pasti ada, ada sampai 50-90%. Ada pembagian area, DC & DRC punya ZZZ. Mereka yang melakukan, SLA ada, mereka akan membantu. DRP juga disiapkan oleh ZZZ. BCP itu bicara mengenai bencana, BCP itu mengacu pada DRP, DRP IT mengacu pada ZZZ.”

RSC : “Bagaimana apabila prasarana&sarana tidak bisa dipakai lagi?”

RPD 1 : “Tidak besar, seperti misalnya Aceh bisa dilayani oleh kantor cabang sekitarnya, kita punya Networking sehingga bisa dilayani, dan ini sudah bisa dilakukan.”

RSC : ”Bagaimana pembaharuan BCP terhadap proses teknikal, khususnya yang terkait dengan IT?”

RPD 1 : “Jamsostek melakukan pemeliharaan infrastruktur, sudah ada, dan telah dilakukan pemeliharaan infrastruktur, dan pasti ada improvement, dulu

DRC tidak sebaik sekarang. Mengneai kesiapan komunikasi jaringan, sudah mengcover critical point, apabila keseluruhan rusak maka agak berat.”

RSC : “Bagaimana bentuk pengawasan terhadap BCP?”

RPD 1 : “Yang bertugas mengawasi BCP: Kita sudah membentuk, di TI, tapi resiko sebagai wakil. Koordinator IT dan Resiko.”

RSC : “Bagaimana dengan pembentukan struktur detil dari organisasi structural BCP itu sendiri?”

RPD 1 : “Core nya ada 2 kita & unit-unit kritikal tadi; pelegalan sudah mulai dibentuk. Penugasan formal sedang mau dilakukan. Tapi untuk divisi TI dalam penanganan DRP kemampuan teknis sudah ada harusnya karena mereka terkait dengan operasional tersebut. Selain itu untuk capability sudah ada.”

RSC : “Bagaimana dengan pembentukan budgeting?”

RPD 1 : “Dana/Budgeting, kita akan usulkan di luar, tapi saat ini, saya belum tau apakah tim masuk ke tempat TI apa tidak. Perencanaannya diharapkan terpisah. Budget diawasi oleh keuangan.”

RSC : “Kemampuan komunikasi & pengetahuan mengenai dampak: Harusnya mereka sudah diinformasikan dengan baik.”

RSC : “Bagaimana dengan keterlibatan Direksi terhadap pelaksanaan BCP?”

RPD 1 : “Tinggi pastinya. Sudah jadi sangat utuh yang tidak terpisahkan. Dukungan dari BOD bahwa ini adalah suatu hal yang sangat strategic, sehingga menjadi utuh dan tidak terpisahkan.”

RSC : “Bagaimana dengan keterlibatan humas di BCP?”

RPD 1 : “Perencanaan melibatkan humas, saat ini belum. Pelaksanaan belum karena baru di tahun 2010.”

RSC : “Menurut bapak, implementasi BCP karena baru 1 tahun. Secara corporate governance apa yang dibutuhkan untuk terjadinya improvement?”

RPD 1 : “Pertama di IT dan bisnis proses. Dua hal yg harus dipertimbangkan. Dari divisi lain : komunikasi terhadap sosialisasi BCP tersebut. Sebenarnya ini adalah value added buat perusahaan, pertama internal perlu komunikasinya, di internal paham mengenai pentingnya BCP,ada komitmen tersebut, barulah kita komunikasikan ke eksternal. Harusnya sudah siap untuk itu. Cara komunikasi biarlah humas yang merumuskan. Tapi harusnya mereka dikomunikasikan bahwa kita punya BCP,karena ini adalah nilai jual kita, stake holder harusnya convinience in case terjadi apa-apa dana anda aman, hak-hak tidak dikurangi. Dalam skala kecil dibuktikan oleh Tsunami kita bisa cover. Jangan sampai ketika terjadi hal-hal besar tidak bisa discover. Komunikasi sudah mulai 2010, dan di 2011 sudah mulai. Secara internal ini maunya dimasukkan pada internal diklat, dan e- learning. Sehingga mempercepat sosialisasi internal.”

RSC : “Bagaimana dengan hambatan terhadap sosialisasi BCP?”

RPD 1 : “Kesadaran terhadap manajemen resiko rendah, dan ini adalah bagian dari manajemen resiko. Kita pasti akan parallel untuk implementasi.”

RSC : “Bagaimana dengan value terhadap BCP itu sendiri? Prosedur kontigensi masing-masing divisi sdh ada, tapi integrasi BCP belum terlihat nilainya”

RPD 1 : “Karena belum diintegrasi secara utuh, secara parsial kita sudah punya contingency plan. Tugasnya tim yang harusnya mengintegrasikan secara proporsional. Sebenarnya sudah dibangun arahnya sudah kesana dan nantinya akan dilibatkan langsung. Kalau dilihat nantinya setiap unit kerja harusnya mempunyai tugas.”

RSC : “Bagaimana dengan structural organisasi, apakah ada yang harus diubah, misalnya memasukkan nilai ke KPI?”

RPD 1 : “Secara tidak langsung sudah masuk tapi bobotnya akan dinaikkan. Tapi di tahun-tahun pertama arahnya akan ke sana, unsur KPI sudah dimasukkann dalam kinerja mereka, karena apabila tidak dimasukkan ke dalam unsur KPI, dan dipaksa sistem tidak aka nada gunanya.”

Interview 3: Operation & Service Division (simultaneously with 2 respondents)

RSC : “Apakah yang menjadi perhatian terbesar dari BCP?”

RPD 1 : “Perhatian terbesar dari BCP adalah kecukupan dana, kemudian akurasi data kepesertaan kalau tidak akurat bisa keliru pembayarannya. Hal mutlak hubungannya dengan teknologi. Saat ini belum online dengan pihak teknologi. Kemudian tersedianya provider kesehatan, karena kalau mereka belum kita bentuk tidak bisa memberikan pelayanan atau begini, biaya berobat semakin naik/meningkat. Terkait dengan kecukupan dana baik waktu maupun dengan harga, kalau ini terputus akan bermasalah. Berbeda dengan santunan uang berapa kewajiban kalo kecil ya dapat kecil. Berbeda dengan kalo uang dikumpulkan tidak mampu membeli jasa itu akan bermasalah, karena peserta datang ke dokter tadi bukan bayar dulu tapi langsung dilayani, kemudian provider datang untuk menagih ke jamsostek. Berarti apa dana yang kita kumpulkan harus siap untuk membayarkan jumlah yang harus dibayar.”

RPD 2 : “Memang ada negoisasi dengan pihak rumah sakit sebelum penandatanganan perjanjian, kita buat IKS dengan rumah sakit berapa harganya sebelum tanda tangan perjanjian, tapi begitu deal ya sudah peserta tidak dibebani lagi. Tidak boleh ada sharing dengan peserta, misalnya obat tidak ada sesuai standar Jamsostek kemudian diberi standar di tingkatkan maka itu akan ditagihkan ke peserta. Jamsostek punya daftar obat standar yang sudah tertera di apotik dan di tempat lain, kemudian peserta merek tersebut yang ada dari dokter tidak ada dengan rumah sakit maka perjanjian dicarikan merek yang disetarakan dengan yang ada di kita selisihnya tanggung jawab peserta tapi dihindari selisihnya."

RPD 1 : "Bentuk kategorisasi sudah ada, ini kan termasuk manajemen resiko dengan adanya standar. Dengan bentuk negoisasi tapi belum dijabarkan dalam divisi manajemen resiko.Terus tadi apabila dihubungkan dengan dana, kecukupan dana dan provider pelaksana tersebut. Karena ini sangat riskan bahwa JPK tidak setengah-setengah, ada 2 hal yang diperhatikan take it or leave it, kalau mau menyelenggarakan harus sepenuhnya, ini yang harus benar-benar diperhatikan secara khusus. Di JPK ini adalah padat karya, peserta akan tumbuh terus apalagi kalau menjadi wajib, ini akan menjadi resiko reputasi karena hanya bisa mengumpulkan peserta tapi tidak bisa melayani dengan baik. Pelayanan dilakukan di cabang masing-masing, di cabang-cabang harus bisa melayani dengan baik, orangnya harus cukup. Kalau JHT orang bisa menunggu, tidak perlu diambil saat ini. Tapi kalau kesehatan tidak bisa ditunda, misalnnya operasi jantung, peserta bertanya dimana saya harus operasi, dan Jamsostek harus bisa menjawab kebutuhan peserta. Kesehatan dilakukan lebih dari satu kali berturut-turut, semua peserta pasti sakit cuman waktunya/frekuensi, kondisi sakit parah atau tidak."

RSC : "Bagaimana dengan proses yang terkait dengan prosedur kontigensi apabila terjadi gangguan pada operasi & pelayanan?"

RPD 1 : "Ada 1001 macam fraud yang bisa terjadi, apakah rumah sakit bisa melakukan penagihan (provider), cth: USG tidak pernah dilakukan tapi ada penagihan, kunjungan dokter fiktif. Seperti kemarin ada operasi usus buntu dokter menagih operasi besar, dianggap semuanya pecah, begitu kita melakukan review/implementasi manajemen ternyata bukan banyak. Organisasi belum sesuai dengan kebutuhan organisasi untuk pelayanan kesehatan, Pendek kata kalo Jamsostek disuruh fight dengan PT XXX (perusahaan pemerintah yang mengatur asuransi kesehatan untuk PNS) yang satu perusahaan tersendiri itu pasti kalahnya di jumlah personil, tapi upaya dan lain-lain kami sudah mengusahakan secara maksimal. PT XXX peserta nya adalah PNS yang tertib, sementara Jamsostek perusahaan swasta yang kritis. PT XXX pesertanya sudah ditetapkan oleh pemerintah/kementrian, tarif sudah ada, sduah gampang bargain dengan pihak rumah sakit, ini dari kementrian, mereka tinggal sharing pasien, udh gampang, apabila ada tambahan sharing disitulah askes baru menekan rumah sakit dalam negoisasinya. Kami dilepas harus bargain sendiri dengan pihak rumah sakit, ini harus keterampilan kami sendiri kantor cabang untuk bernegoisasi. Peraturan pun hanya misalnya pelayanan khusus untuk bantuan tenaga kerja, tapi itupun hanya bantuan sedikit, misalnya persalinan 500 ribu, kacamata 200 lebih dari situ peserta sendiri yang menambahkan. Maka kita harus mampu bernegoisasi kemudian dituangkan dalam peraturan/kontrak, nanti kalo ada perubahan maka di renegoisasi.

RSC : “Apakah Prosedur kontigensi selalu menjadi prioritas di PT Jamsostek? Bagaimana dengan prosedur kontigensi pada divisi Operasional & Pelayanan?”

RPD 1 : “Harusnya iya, karena ini ruh nya. Ada regulasi yang membahayakan kita di masa depan, misalnya iuran JPK ditetapkan 3% dari upah pekerja untuk lajang, 6% untuk keluarga, ditetapkan ceiling nya/ yang dihitung untuk menghitung iuran 1 juta, apabila pekerja upahnya 5 juta tetap dihitung 1 juta, itu tahun 1993 sampe sekarang belum dirubah. Pada tahun 1993 upah 1 juta 10 kali lebih UMP/inflasi, setelah 18 tahun ini sudah di bawah upah minimum. Ini harus diubah tapi sampe sekarang belum diubah. Itu yg menjadi prioritas dikarenakan adanya beberapa fenomena. Fenomena itu adalah peraturan yang harus diubah. Misalnya contoh ceiling dinamis, dialign dengan PTKP, kalo bisa 3 kali PTKP. Peraturan pemerintah harus berubah terhadap iuran. Selain itu ada kebijakan opting out (kebebasan bersyarat) dalam kompetisi. Jamsotek harus ikut iuran pemerintah yang tidak dinamis, swasta fleksibel tergantung perusahaan. Perusahaan tidak diwajibkan,sehingga yang upah besar masuk ke swasta, yang upah kecil masuk ke jamsostek. Sebetulnya asuransi social untuk perusahaan upah besar membantu upah kecil. Tapi ini tidak terjadi lagi karena ada opting out, justru kita harus melihat pada perusahaan upah besar harusnya membantu yang upah nya kecil. Andaikata PNS tidak wajib askes, untuk eselon yang upah besar pasti tidak masuk askes."

RSC : "Bagaimana dengan penanganan prosedur kontigensi apabila terjadi gangguan terhadap proses bisnis?"

RPD 1 : "Kita sama saja, kita kurang personil walaupun ada verifikator, tapi ada cabang yang personilnya hanya ada 1, tidak semua kantor cabang ada kabid JPK (red. ada aturannya sendiri), ada kabid pelayanan, belum tentu ada kabid tsb di cabang. Concern untuk kategori bencana sama."

RSC : "Bagaimana dengan perbaikan terhadap strategi prosedur kontigensi?"

RPD 1 : "Kalau kami sudah melakukan perbaikan secara terus menerus. Untuk integrasi di BCP, unit-unit/divisi-divisi terkait sudah melakukan prosedur kontigensi tapi sendiri-sendiri, tidak tertulis secara rinci. Contoh : tekpel, mereka sudah melakukan, misalnya SIPT online untuk mitigasi resiko supaya tidak menyimpang seenaknya penetapan ulang, bagaimana tidak terjadi fraud. Sekarang muncul apakah karna dari manajemen resiko, menurut kami tidak, tapi lebih menertibkan, supaya bisa berkoordinasi dengan baik. Prosedur kontigensi sudah melekat pada divisi terkait, embedded."

RPD 2 : "Ada improvement, Ada, improvement terus-menerus dalam proses kepesertaan walaupun kadang-kadang kita menjadi terlalu ketat,ada faktor penurunan pelayanan kalau tidak diikuti peserta. Kalau peserta tidak membantu kita, karena lebih kaku untuk masuk ke sistem, misalnya perusahaan nunggak maka di stop. Misalnya karena tidak bisa dilayani. Karena ada link antara biro keuangan.”

RSC : “Bagaimana penanganan BCP terhadap kemungkinan bencana yang terjadi?”

RPD 1 : “Saya khawatir disini. Kami sdah melakukan dari sisi JPK, tapi belum tentu BOD atau tingkat kementrian sepaham. Kami masih melihat setengah-setengah. Sebab kalau personil tidak ssi/tdk cukup, maka klaim tidak bisa diverifikasi/diproses. Kami minta kepala bidang untuk pelayanan JPK khusus, tidak dicampur aduk dengan kabid untuk menangani lainnya.karena bisnisnya banyak berbeda. Misalnya pada kenyataannya kabid tersebut ikut menangani pelayanan lain seperti cash benefit, penggantian, santunan. Di samping itu, harusnya ada 24 jam ada call center. Pemahaman terhadap program ini, SDM mengatakan selalu dipatok bahwa penambahan hanya 100 orang. Apalagi konon Jamsostek JPK hanya 23% dari total peserta Jamsostek, sekarang ini sudah cukup luar biasa sibuknya. Ini kan membutuhkan perubahan yang sangat radikal. Mungkin bukan salah BOD, mungkin hanya komunikasi antara BOD dan kementrian. Perbaikan sangat prinsip saat ini, karena persyaratannya tidak dipenuhi personil dan kompetensinya. Banyak terjadi di cabang pekerjaan di bawa ke rumah, hal ini tidak sehat untuk karyawan Jamsostek. Dari sisi kami penanganan sudah melakukan usaha-usaha yang maksimal, kami sudah melakukan perubahan kebijakan seperti silinguigish (batasan upah maksimal 1 juta), opting out sudah diajukan tinggal pemerintah melakukan. Karena kan ini bisa bangkrut kalau tidak bisa diandalkan.”

RSC : “Bagaimana dengan penanganan terjadinya fraud dari prosedur kontigensi BCP?

RPD 1 : “Secara proses bisnis normal dalam pencegahan fraud, sudah dilakukan prosedur ada fakta integritas, ada komisi medis independen 8 dokter spesialis, cash manajemen, ada pembinaan evaluasi. Di sini sangat komit dengan pengendalian. Ini setuju untuk dilakukan, tapi ini masalahnya untuk pengupayaan untuk mengejar tidak bisa untuk level divisi. Karena ini berhubungan dengan pihak divisi, sudah politis karena ada hubungan dengan pihak luar dari menaker, dll.”

RSC : “Bagaimana apabila terjadi perubahan susunan organisasi ECMT, CMT, BCT lebih dari setengahnya terhadap impact/dampak dari prosedur kontigensi BCP?”

RPD 1 : “Prosedur BCP bisa berjalan dengan baik. Saya kira system sudah ada, jadi siapapun penggantinya bisa menggantikan. Makin ke bawah semakin gampang.”

RSC : “Bagaimana dengan pengaktifan BCP yang berhubungan dengan TI?”

RPD 1 : “Ini sudah ada, Surabaya sebagai kontigensi system kalo terjadi apa-apa disini. Tapi saya tidak tau buktinya, belum pernah mati semua langsung diganti, tapi katanya sudah siap. Saya tidak tau sejauh mana testingnya. Selama ini masih dikendalikan disini.”

RSC : “Bagaimana proses kelangsungan bisnis apabila terjadi kegagalan aktivasi dari BCP?”

RPD 1 : “Kalau terjadi macet baik pada system (red.data) atau proses bisnis kita ga bisa bayar pada provider tingkat pertama. Gambaran kalau terjadi macet kita tidak bisa bayar pada tingkat pertama. Tingkat pertama dibayar berdasarkan jumlah daftar tertanggung yang dialokasikan.Itu dibayar mau sakit atau tidak sakit dibayar misalnya dengan satuan 500ribu per tertanggung. Mungkin provider ini ada masalah,kita ga bisa bayar sekarang ya, mungkin bisa memahami. Cuman nanti di tingkat lanjutan yang selanjutnya ada masalah pada daftar tingkat tertanggungnya mungkin itu yang menjadi masalah. Untuk klaim tingkat provider masih bisa menerima dengan kondisi belum dibayar dalam rentang waktu tertentu. Rentang waktu itu sekitar 1 minggu kalo tidak salah. Cuman peserta baru tidak tau (peserta baru Jamsos di provider tsb), karena tidak ada catatan, tapi mungkin kita bisa baik dengan hubungan baik pada provider. Surat rujukan masih bisa diberikan, maka dapat dibuat surat jaminan, selama kita tau. Kalaupun masih ada masalah antar kantor cabang, bisa saling contact surat kantor cabang, peserta cukup memberikan kartu jamsostek. Tapi itu kan membutuhkan waktu untuk pemrosesan tersebut."

RSC : "Apakah proses bisnis dapat berjalan apabila terjadi gagal aktivasi lebih dari waktu yang ditentukan?"

RPD 1 : "Saya kira masih bisa. Rumah sakit tidak bisa menolak pasien cuman siapa yang membayar yang masalah. Ya mungkin ya hanya citra saja yang dikorbankan, tapi pelayanan tetap berjalan. Proses penting ada di pusat yang paling penting, tapi untuk komunikasi dari kantor cabang, yang akan memastikan itu peserta. Customer relation ada di cabang. Dari system cabang bisa beralih ke pusat, tapi untuk hubungan ke provider adalah dari cabang.Apabila terjadi impact cukup tinggi, tapi tidak terlalu tinggi karena ini masih bisa ditelusuri, misalnya kalau kita keliru memasukkan JHT maka duitnya akan hilang , kalau pelayanan JHT resiko reputasi. Kalau misalnya pasien ada 100 cukup kerepotan."

RSC : "Apakah ada kemungkinan untuk menyalurkan resiko tersebut pada pihak ke-3?" RPD 1: "Tidak, tetap internal. Resiko masih bisa diterima, tapi apabila sering-sering terjadi maka reputasi dipertaruhkan. Minimalisir dilakukan dengan hubungan ke pusat. Hanya saja ada peserta yang keluar kita ngga tau, dia sakit dia bisa klaim. tapi itupun karena prosesnya perawatan dilakukan dulu, baru rumah sakit langsung ke Jamsostek. Kalau salah bayar maka Jamsostek bisa rugi untuk membayarnya kalau terjadi kesalahan.Ada resiko tapi masih bisa diatasi."

RSC : “Bagaimana apabila modul aplikasi untuk mengakses data kepesertaaan tidak berfungsi? Bagaimana bentuk mitigasi yang digunakan?”

RPD 1 : “Hal tersebut jarang, tapi dari sisi impactnya mungkin moderate kalau sampai terjadi. Harusnya tidak boleh lebih dari 1 hari, kalau bisa dalam 2-3 jam sudah bisa teratasi, karena pelayanan terus menerus dlakukan. Masih ada dokumen pendukung. Mitigasi yang dilakukan adalah data manual, satu-satu nya kontigensi, walaupun itu tidak praktis dan biasanya keuangan tidak mau.Karena harus membuka ledger. Biasanya yang paling tertib keuangan (terbenahi terlebih dahulu).”

RSC : “Bagaimana dengan uji coba dari BCP?”

RPD 1 : “Uji coba sudah pernah tapi saya tidak ikut, uji coba baru 1 kali dengan pihak service provider yang baru.” RSC : “Bagaimana dengan keterlibatan user? Sosialisasi dari BCP itu sendiri?”

RPD 1 : “Sepertinya review terhadap BCP terus dilakukan dan user terlibat. Program pelatihan kesadaran sudah ada program tapi baru 1 kali, dikatakan efektif mungkin tapi kan baru 1 kali, dan mereka tidak total dalam pemberlakuannya. Dalam uji coba juga belum ada perubahan tempat dari end user.” RSC : “Bagaimana dengan partisipasi atau keikutsertaan pihak ketiga/service provider dalam penanganan BCP?”

RPD 1 : “Pihak ketiga yang ikut serta dalam penanganan BCP adalah service provider khusus untuk TI. Kemungkinan satu provider kena bencana, bisa dipindah di provider berikutnya. Involvement antara 50-90%. Harusnya sudah ada perjanjian, dan mereka juga harusnya sudah mempunyai BCP dan membantu apabila terjadi bencana sesuai perjanjian SLA.” RSC : “Apakah sudah ada fungsi jabatan khusus untuk BCP di kuesioner?”

RPD 1 : “Tim khusus untuk BCP: Belum ada, yang ada hanya manajemen resiko, dia coordinator saja, memetakan saja, membagi bola saja. Sementara yang melakukan masing-masing divisi. Sampai saat ini belum ada identifikasi detil mengenai unit organisasi . Belum ada penugasan formal. Tim belum terbentuk secara detil dan menyeluruh”

RSC : “Bagaimana dengan bentuk komunikasi pada peserta apabila Jamsostek terjadi bencana?”

RPD 1 : “Walaupun belum menyeluruh, tapi pengaturan sudah ada. Sudah ada AO yang melakukan hal itu. Perusahaan peserta jamsostek belum tau BCP. Itu yang belum tentu semua perusahaan mengerti hal tersebut.”

RSC : “Bagaimana dengan budget BCP sendiri?”

RPD 1 : “Belum ada dana terpisah, masih pada budget IT.”

RSC : Dari sisi apa yg dilakukan Risk Management (dari sisi assessment, identifikasi yang sudah dilakukan) terhadap BCP. Apa kira-kira kekurangannya yang menurut bapak perlu ditingkatkan?

RPD 1 : “Kekurangan tidak pernah memantau, sejauh mana divisi tsb memahami, awarenessnya seperti apa, apakah dia mengerti atau tidak mengenai divisi operasional tsb, sosialisasi masih kurang. Perlu sosialisasi yang lebih menyeluruh.”

RSC : “Dari sisi keterkaitan/integrasi pada keseluruhan divisi. Ketika BCP terbentuk apakah sudah terasa atau belum?”

RPD 1 : “Ini masih dalam rencana, kemaren masih dalam tahap launching, membuat analisa resiko masing-masing, masih dalam proses. Belum secara khusus pada BCP. Yang masih dilakukan adalah masing-masing divisi belum terintegrasi. Kami belum merasakan manfaat nya secara khusus sampai saat ini. Bukan berarti manfaat BCP nya, tapi belum merasakan adanya BCP yang akan dibentuk itu jelas manfaatnya.”

RSC : “Menurut bapak prioritas BCP itu sejauh apa di mata manajemen?”

RPD 1 : “Mungkin secara manajemen paham secara umum tapi tidak diketahui detil dampaknya seperti apa. Belum paham apa perlu BCP itu sendiri, karena BCP itu semacam menu baru, belum terstruktur. Kalau pengendalian resiko sudah dipahami. BCP itu diharapkan menjadi sesuatu hal yang baru. Pembakuannya belum ada, belum terstruktur. Harusnya kan semua karyawan sudah tau, tahapan sudah tau. Ini kan bisa berbeda-beda persepsi. Redaksi nya yang benar bagaimana, orang tau atau tidak visi & misi di BCP. Perlu declare nya, value nya belum terasa. Mungkin kita sudah melakukan tapi belum sistematis, masih banyak naluri. Ibaratnya kalau service excellent di XXX bahasanya sama, tapi kalau ini belum ada pembahasan yang sama. JPK adalah fungsi kritikal di Jamsostek. Kalau JPK jelek maka akan berdampak ke program lainnya, karena ini sangat frekuen berhubungan dengan peserta. Resiko yang diperhatikan adalah resiko reputasi perusahaan, misalnya 1 pasien dipimpong, itu akan gaung kemana-mana."

RSC : "Dari sisi corporate governance, struktur organisasi, apakah sudah menjawab kebutuhan Jamsostek?"

RPD 1 : "Mungkin dikarenakan bisa digabung antara pelayanan. Pada saat Jamsostek lahir operasi & pelayanan terpisah, ini malah core bisnis jadi 1 dan divisi pendukung jadi banyak. Ibaratnya spt selimut pendek untuk menutupi tubuh. 1 direktur tidak focus. Harusnya lebih terfokus ke pelayanan.Pelayanan sendiri dan operasional sendiri. Kalau pemikiran saya harusnya beliau ini bisa berhubungan dengan departemen terkait, kementrian, dan semua yang berkaitan bisa dihimpun. Ini mungkin kurang teryakini, malah ada survey pelaksana untuk melihat market pelayanan apa yang diperlukan. Walaupun nanti renbang yang melakukan, tapi kan untuk pelaksanaan ini perlu dri divisi pelayanan. Dari sisi control: Ini perlu, Apakah setiap kepala cabang belum pernah melihat BPK nya, kabid belum melihat providernya, krn kabidnya digabung. Dari 121 kantor cabnag hanya ada 28 kabid untuk pelayanan JPK, sisanya digabung dengan pelayanan yang lain, hanya di kantor pusatnya digabung. Di cabang ini kan pelayanan langsung, cth di setiabudi untuk verify untuk bangkit dari t4 duduk sangat minim waktunya. Kalo staff yang bertemu langsung ke pelayanan providernya kan sangat tidak enak."

RSC : "Kalo dari control sendiri bagaimana, loop hole dari penggabungan?"

RPD 1 : "Karena digabung jadi semua divisi, tadi nya 1 direktorat untuk akuisisi, ada kemitraan, pembinaan khusus untuk mengajaak semua masuk, kemudian dibina apakah kepesertaannya sudah benar. Administrasi dari bulan ke bulan, berapa yang dicairkan. Betulkah datanya dimana ini sering misalnya AO yang melakukan untuk pengembangan apakah sudah pas rasionya, kompetensi dari AO itu, kemampuan SDM. Perlu ada yang mengatur. Tidak terurus mengenai reward thp AO. Perhatian thp hal-hal detil tidak tersedia. Approval processnya lama. Hubungan antara cabang dengan kantor wilayah akan lebih mudah kalau kantor pusat hubungannya baik dengan kementerian-kementerian. Kalau kementrian kurang lebih paham dengan Jamsostek,dan membuat peraturan yang memaksa daerah untuk perduli dengan jamsostek maka akan lebih mudah bagi jamsostek. Karena Jamsostek walaupun ada sisi bisnisnya tapi tetap perlu ada pemaksaan juga."

Terakhir digabung tahun 2000an sebelumnya terpisah, karene mungkin dulu direktur keuangan & investasi adalah 1 maka begitu ini dipisah maka ada yang lain yang dipisah. Pada saat pergantian direksi sekaligus organisasi diubah. Beda dengan askes, dananya given. Maka direkturnya direktur operasional dan 1 program. Jamsostek dengan program 4, bahkan ada tambahan program yaitu program pensiun."

Interview 4: Investment Division

RSC : "Apakah yang menjadi asset bisnis kritikal yang menjadi tolok ukur untuk proses kelangsungan bisnis yang ada di Jamsostek"

RPD : "Secara fisik kita tidak pegang apapun, karena saham-saham yang kita punya semuanya ada di KSEI custody, kecuali deposito ada di settlement dan beberapa branch. Yang paling penting adalah data bisnis.karena saat ini posisi ada berapa, untuk gedung karena ada di penyimpanan di gedung ini, proses bisnis lebih kepada software karena tracking menggunakan sarana elektronik langsung ke BEJ. Dari ketiga hal ini yang paling penting: Data bisnis, kalaupun tidak online kita masih bisa by phone ada alternative pilihan yan ada. Data untuk melihat opportunity cost dari harga market dan harga yang kita miliki saat ini."

RSC : "Apabila terjadi kegagalan dari data bisnis tersebut, bagaimana prosedur kontigensinya. Apakah bisa dilakukan?"

RPD : "Bisa, karena data sebelumnya dilakukan di print di hari sebelumnya, seandainya system elektronik terganggu. Kemungkinan kesalahan jelas lebih besar, karena system aplikasi kita mendeteksi seluruh kemampuan. Pedoman yang kita miliki memperlihatkan jenisnya, harga berapa lama,kalau menurut kita salah, maka system akan memberitahu, apakah ini bisa dilakukan atau tidak. Tapi ya pasti manual error lebih tinggi. Saya antara data dengan system, data merupakan informasi yang kita punya sementara system untuk akses ke data. Kalau system tidak ada maka human error lebih tinggi."

RSC : "Apa yang menjadi concern untuk dikembangkan mengenai proses BCP di jamsostek?"

RPD : "Saya kira system sudah jalan, mungkin yang perlu dikembangkan SOP otorisasi kewenangan yang bisa melakukan hal itu. Pengembangan itu lebih kepada perilaku dari pelaksananya. Saya kira yang belum optimal adalah pelaksana investasinya. Pengembangan itu yang belum ada, dengan batasan kewenangan tertentu, dia melakukan untuk kepentingan rekannya. Misalnya pengendalian dari sisi entitlement. Pengembangan terhadap back up system, kalau itu drop ada back up system aplikasi yang lain. Sistem ini down terpaksa melakukan manual. Walaupun tidak online tapi secara local area tetap terhubung."

RSC : "Adakah perbaikan terhadap prosedur kontigensi sejak dibentuknya BCP?"

RPD : "Kalau di kami belum terlalu terasa, karena disini sudah ada system yang memang sudah online dengan untuk saham online untuk bursa dan ada Bloomberg. BCP sendiri belum terasa manfaatnya tapi itu tetap harus ada, karena belum terjadi gangguan maka manfaat belum terasa."

RSC : "Bagaimana bentuk penanganan bencana khususnya di strategi, apakah ada perbaikan?"

RPD : "Ada perbaikan dari sisi system jarang drop. Apabila dari staff/orangnya capability sudah cukup baik, dari sisi kelangsungan bisnis sudah baik,dari sisi TI dampaknya jarang terjadi drop, dari seluruh organisasi sudah cukup baik, kita perlu apa mereka siap, ada kendala di aplikasi sudah bisa diturunkan team nya. Koordinasi kami dalam team work sudah ada perbaikan. "

RSC : "Bagaimana dari sisi keseluruhan proses, perbaikan nilainya BCP apakah ada atau tidak?"

RPD : "Sebetulnya sudah ada cuman mungkin belum didefenisikan dengan rinci, jadi belum semua memahami apa, siapa dan bagaimana saat terjadi.Ini pandangan saya."

RSC : "Dari sisi investasi ada proporsi portofolio untuk menjaga likuiditas, bagaimana confidence level prosedur kontigensi menjaga likuiditas tersebut?"

RPD : “Dengan adanya back up data kita ada juga backup di tempat lain, jadi harusnya data bisa diakses secra terus menerus. Secara likuditas, prosedur kontigensi tidak ada masalah, jumlah stock dana, berdasarkan laporan keuangan bahwa kewajiban kita lebih kecil dari asset kita, jadi masih bisa di back up.

RSC : “Bagaimana apabila nilai saham turun? “

RPD : “Tapi kan semua tidak seketika itu terjadi, harusnya ada proses. Apabila terjadi normal, deposito bisa ditarik, obligasi bisa dicairkan. Kecuali perbankan sudah drop, dan chaos negri ya susah semua sector juga susah memenuhi kewajibannya. Tapi kalo misalnya seperti krisis moneter harga saham jatuh, kami juga memiliki SOP dalam kondisi mana harus dilepas, dalam keadaan market sudah berjalan saya kira ga ada masalah. Keputusan terhadap itu ada SOP dan diimplementasi, ada perbaikan terhadap prosedur, ada strategi tactical aseet per tiga bulan. Kalau dalam tiga bulan berikutnya ada sesuatu (penurunan atau penaikan), untuk pembayaran yang besar, maka akan disiapkan dananya dari deposito, untuk saham. Hal ini sudah diimplementasikan sudah lama.”

RSC : “Bagaimana apabila terjadi potensi terjadi kesalahan dari perencanaan?”

RPD : “Kemungkinan terjadi kecil sekali, yang mungkin terjadiketika krisis moneter, saham turun. Dalam kondisi normal kecil dibawah 1 %. Dari portofolio saham tidak boleh banyak-banyak yang banyak di deposito dan obligasi Negara. Sekalipun terpengaruh di bawah 1% 1 per mil Dari total asset 80 T ga sampe 1 T, itupun bukan rugi, karena harganya naik misalnya spt skrg 2009 sudah balik sekarang. Itupun ada pedomannya, syarat & ketentuan tidak boleh masuk di saham-saham yang bukan blue chip.”

RSC : “Mengenai structural organisasi ECMT,CMT, BCT. Apakah bapak mengetahui secara jelas?”

RPD : “Rincian tugas mengenai siapa, bagaimana belum tau, informasi belum dapat.”

RSC : “Ini merupakan hal terkait dengan pengaktivan struktur organisasi baru apabila terjadi bencana, dimana berdasarkan BCP Jamsostek, anggotanya terkait dengan struktur organisasi saat ini. Apabila terjadi perubahan anggota secara mendasar pada tiap levelnya, apakah ada pengaruhnya?”

RPD : “Tidak ada pengaruh karena sudah ada struktur, job desk, hirarki sudah ada, jadi siapapun yang melaksanakan siapa saja pasti bisa. level di bawah lebih sering, direksi ada jarak 5 tahun. Perubahan tidak terlalu sering tapi lebih sering dibandingkan dengan level di atasnya”

RSC : “Apakah bapak mengetahui bagaimana proses kontigensi, back up plan komunikasi dari BCP Jamsostek?”

RPD : “Sepertinya belum ada informasi secara tertulis maupun lisan. Walaupun supporting tetap ada dari divisi-divisi pendukung seperti Resiko Management yaitu dari sisi kapasitas mereka sudah mulai, hanya saja dari sisi resiko masih profil resiko, tapi ke arah sana masih perlu waktu.”

RSC : “Bagaimana dengan hubungan ke cabang? Bagaimana dengan prosedur kontigensinya untuk komunikasi?

RPD : “Ada hanya deposito. Sekarang ini kita sedang mengimplementasikan sist Invest, nantinya apa yang dilakukan di cabang utk pencairan deposito bisa di monitor langsung. Jadi bisa dilakukan transfer antara data daerah cabang ke pusat, dan pusat cabang.”

RSC : “Bagaimana apabila prosedur kontigensi gagal untuk system investasi?”

RPD : “Apabila dari proses yang diluar TI, jarang tempat saya tidak ada orang tapi system bisa berjalan. Impactnya sedikit di bawah sedang, tidak signifikan. Kemungkinan proses terganggu terjadi di saham yang memperhatikan running trade: saham hanya 20% saja yang berdampak. Sementara kalau terjadi saham down paling hanya transaksi hari itu saja.

Di samping itu, masih bisa diandalkan secara manual, bisa dikerjakan tanpa system walaupun errornya makin besar karena berpengaruh pada keseluruhan portofolio yang besar. Saham & obligasi untuk trading. Kalau kupon paling telat terima kupon, kalau tidak punya data maka bisa jadi jumlah unit nya kurang atau terlambat diterima. Sementara itu kegagalan prosedur kontigensi dari TI so far sih sangat jarang. tapi yang kita punya hanya bilyed deposito, selain itu deposito ada di bank, mungkin hanya kehilangan data. Obligasi dan saham juga tidak ada disini, disimpan di XXX.”

RSC : “Sejauh mana keyakinan terhadap keamanan XXX sendiri?”

RPD : “XXX saya kira sudah system keseluruhan, saya bisa yakini sekitar 90%. berdasarkan dari branding . Tapi mengenai BCP mereka sendiri itu yang 10%.” Pihak ke-3 belum dipercaya sepenuhnya.”

RSC : “Apa yang menjadi concern dari investasi terhadap proses kontigensi?

RPD : “Menjaga kesinambungan system sehingga bisa berjalan seperti seharusnya, kita mau tanyakan adanya back up data hard copy, sehingga data dimiliki dalam bentuk file soft copy.”

RSC : “Selain yang membutuhkan IT, apakah ada step untuk proses kontigensi?”

RPD : “Tidak ada, masih spt BAU saja.”

RSC : “Bagaimana uji coba testing BCP?”

RPD : “Tidak pernah diikutsertakan.”

RSC : “Apakah mengetahui mengenai pembaharuan terhadap BCP di Jamsostek?”

RPD : “Netral, sedang, beberapa. Tidak terlalu sering juga, ada, Cuma tidak merasa terlalu banyak reviewnya.”

RSC : “Bagaimana keterlibatan bisnis user dari investasi terhadap pelaksanaan BCP itu sendiri?”

RPD : “Partisipasinya secara fakta masih biasa aja, harusnya PUPM tinggi, kalau belum ada spesifik dari.Kurangnya dari frekuensi review dan sosialisasi.”

RSC : “Pelatihan kesadaran?”

RPD : “Belum ada, ada pun tidak banyak. Tidak efektif karena sepertinya culture nya belum terbentuk terhadap BCP. Sense of BCP belum terasa.”

RSC : “Komunikasi terhadap karyawan mengenai BCP?”

RPD : “Belum ada, sudah ada informasi sedikit tapi belum clear.”

RSC : “Yang bertanggung jawab terhadp BCP itu sendiri, opini bapak?”

RPD : “Harusnya yang menjadi penanggung jawabnya DIRUT. Koordinator harusnya organisasi ECMT komitee, tapi pelaksanaan dari divisi harusnya dari tiap divisi terkait.”

RSC : “Bagaimana dengan Biayanya/Budget?”

RPD : “Biasanya pooling di biro TI, tapi masing-masing unit mengajukan tiap divisi. Anggaran masing-masing divisi dikoordinir di budget TI.”

RSC : “Bagaimana dengan komunikasi BCT ke tiap divisi?”

RPD : “Belum, kalau dari internal sudah disampaikan tapi apakah inline/up to date belum tau. Sudah ada tapi belum maksimal, bentuknya pada meeting evaluasi.”

RSC : “Bagaimana dengan peran humas untuk komunikasi ke medi?”

RPD : “Komunikasi belum ada yang terkoordinir.”

RSC : “Keterlibatan direksi & senior manajemen?”

RPD : “Netral, karena belum kelihatan.”

RSC : " Dari secara corporate governance, apakah ada sesuatu hal yang harus diperbaiki/diimprove untuk meningkatkan proses kelangsungan bisnis?"

RPD : "Apabila itu improvement harusnya selalu ada, misalnya dari sisi TI, dari sisi human resource nya : kompetensi, attitude, kedisiplinan,leadership & tanggung jawab. Untuk menumbuhkan sense of belonging, karena saya liat fighting spiriitnya masih agak kurang. Yang paling penting adalah koordinasi yang harus aware terhadap time table, sehingga harus menunggu implementasi sekuensial sehingga time processing menjadi lama."

Interview 5: Division Secretary Bureau

RSC : "Apakah yang menjadi asset bisnis kritikal yang menjadi tolok ukur untuk proses kelangsungan bisnis yang ada di Jamsostek"

RPD : "BCP sudah ada di Jamsostek, yang menjadi point kritikal di jamsostek adalah data bisnis. Data bisnis adalah subset dari proses kelangsungan bisnis. Data bisnis sangat penting misalnya data kepesertaaan bagaimana data tersebut bisa di retrieve sewaktu waktu. Selain itu yang berhubungan dengan proses kelangsungan bisnis adalah jumlah staff yang melayani, bagaimana bentuk pelayanan kepada peserta, pemberlakuan penyimpanan data ke system, tata ruang yang standard untuk melayani, keakuratan, kecepatan proses. Ini adalah hal yang sangat berkesinambungan yang harus diatur dalam pelayanan khususnya. Saat ini yang terjadi jumlah anggota staff untuk melayani dibandingkan dengan rasio peserta di bawh standard. Rasio tersebut di ambil tolok ukur dari sisi kuantitas dan kualitas. Mungkin saja secara kuantitas memadai tapi tidak secara kualitas. Rasio ketidakcukupan staff ada di keseleruhan daerah cabang di Indonesia, tapi untuk Jawa diperkirakan masih bisa memadai. Yang menjadi perhatian adalah bagaimana bisa memenuhi rasio kecukupan staff dan dat bisnis, untuk menunjang proses kelangsungan bisnis."

RSC : "Apakah yang menjadi point kritikal bagi PT Jamsostek?"

RPD : "Yang menjadi point kritikal bagi PT Jamsostek adalah mengenai pencitraan, belakangan terjadi image bahwa Jamsostek adalah perusahaan yang memiliki nilai korupsi yang cukup tinggi, dan pencitraan Jamsostek menjadi buruk. Namun demikian sudah ada upaya-upaya terkait untuk meminimalisir hal tersebut, seperti Jamsostek mengikuti organisasi anti korup (lupa namanya), Jamsostek mengikuti GeCG dimana ada pengaturan yang jelas mengenai tata kelola perusahaannya, Jamsostek sudah 4 tahun berturut-turut mendapat penghargaan dari sisi tata kelola perusahaan yang terbuka."

RSC : "Bagaimana dengan perbaikan terhadap perlindungan bisnis kritikal?"

RPD : "Saat ini masih sama dengan sebelum terjadi nya implementasi dari BCP. Belum ada perbaikan yang cukup jelas dan detil yang bisa dirasakan oleh unit terkait. Hal tersebut sejalan dengan perbaikan strategi pada bencana."

RSC : "Bagaimana dengan peran pada divisi pendukung khususunya Biro Sekertariat perusahaan?"

RPD : "Sudah menjalankan prosedur kontigensi, misalnya untuk kearsipan semua arsip sudah tersimpan dengan rapi sehingga bisa untuk di retrieve dengan baik, selain itu sudah dimasukkan ke dalam file, media elektronik, dan ada penyimpanan gudang di terogong."

RSC : "Bagaimana dengan prosedur kontigensi ada komuikasi ke cabang?"

RPD : "Sudah ada, dalam beberapa tahun terakhir komunikasi dapat berjalan dengan lancar antara pusat ke cabang."

RSC : "Bagaimana dengan perubahan struktur secara mendasar pada struktur organisasi ECMT< CMT, dan BCT?"

RPD : "Tidak begitu tahu mengenai struktur organisasi ECMT, CMT, dan BCT.Tetapi apabila berkaitan dengan struktur organisasi direksi, kepala biro, kaur prosedur sdh ada, sdh baku dan sdh diimplementasi dgn baik. Apabila sesuai dengan assessment maka orang tersebut dapat mengikuti prosedur yang sudah ada untuk melakukan tugasnya, mungkin untuk ide-ide itu yang agak berbeda satu pihak dan yang lainnya, tapi mengenai apa yang dikerjakan, tracking progress perencanaan yang sudah dijalankan, akan dijalankan, dipending sudah bisa berjalan sesuai dengan system."

RSC : "Bagaimana dengan prosedur kontigensi pada divisi operasi dan pelayanan?"

RPD : "Sudah ada dilakukan prosedur kontigensi. Hal ini dikarenakan untuk proses pelayanan sendiri sudah memiliki prosedur kontigensi dari system ada 2 Data center yaitu DC di Tangerang dan satu lagi di Surabaya. Apabila salah satu bermasalah maka bisa dipakai data yang lain."

RSC : "Bagaimana mengenai prosedur kontigensi pada proses di luar ruang lingkup TI pada divisi operasional & pelayanan?

RPD : "Prosedur kontigensi sudah ada dan berjalan dengan baik pada proses ini. Frekuensi terjadinya cukup kecil karena sudahd dicakup dengan baik, namun apabila tidak berjalan memiliki dampak yang cukup besar."

RSC : "Bagaimana mengenai prosedur kontigensi pada aplikasi & server?"

RPD : "Sudah ada prosedur kontigensi yang baik jadi frekuensi sangat kecil untuk terjadi. Kegagalan server dari TI sehingga sulit berhubungan dengan kantor cabang sangat jarang, ini terlihat dari pelaporan cabang kepada TI menurun dan selama beberapa tahun belakangan sudah ada perbaikan secara khusus pada servernya sendiri."

RSC : "Bagaimana kemungkinan kegagalan aktivasi prosedur kontigensi dari TI?"

RPD : “Kegagalan jaringan komunikasi pada divisi TI, frekuensi kecil karena sudah ada prosedur kontigensi yang jelas, adanya perubahan dan perbaikan pada divisi TI dalam hal penanganan jaringan komunikasi.”

RSC : “Bagaimana dengan partisipasi dari pihak ke-3 untuk membantu dari sisi TI? Bagaimana kapabilitinya”

RPD : “Pihak ke-3 cukup besar perannya dalam BCP. Perusahaan pihak ke-3 untuk membantu dari sisi data organisasi adalah YYY. Dalam hal ini YYY diyakini mampu untuk melakukan pengoperasian data khususnya apabila terjadinya bencana. Jadi dalam hal ini frekuensi terjadinya bisa dikategorisasikan kecil tapi impactnya cukup besar.”

RSC : “Bagaimana penanganan bencana terhadap prasarana & sarana?”

RPD : “Frekuensi kecil , impact sedang. Dibuktikan dengan kejadian gempa di Padang, prasarana & sarana aman.”

RSC : “Apa yang terjadi pada saat peristiwa gempa di Padang?”

RPD : “Peristiwa di Padang tidak mengakibatkan gedung Jamsostek rusak secara keseluruhan dan infrastruktur cabang tidak rusak, sehingga proses normal dapat dijalankan. Proses pengaktifan aktifitas di Padang dikarenakan adanya pemberitahuan untuk memberlakukan operasional pada hari ke-3 setelah bencana. Di samping itu jumlah peserta yang datang ke cabang dapat dikategorsasikan sedikit dikarenakan situasi & kondisi pada saat itu pada kondisi bencana.”

RSC : “Bagaimana dengan prosedur kontigensi pada likuiditas Jamsostek?”

RPD : “Jamsostek memiliki rasio kecukupan dana yang sangat tinggi, rasio likuiditas tidak usah diragukan lagi, sudah sangat cukup. Hal ini terjadi karena asset Jamsostek sangat tinggi untuk memenuhi kewajibannya. Jamsostek mempunyai 4 program, dan ke-4 program tersebut tidak dilakukan subsidi silang, masing-masing program wajib memenuhi kewajiban masing-masing, namun demikian likuiditas dapat dicukupi dengan baik. Contoh apabila hampir keseluruhan peserta melakukan klaim pada program Non JHT, Jamsostek mampu melakukan pembayaran dengan baik dan tidak akan kekurangan likuiditas. Di samping itu, walaupun untuk program JPK mengikuti peraturan pemerintah yang sudah ditetapkan sejak tahun 1993, dimana persentase yang ditagihkan kepada peserta sudah tidak sebanding dengan tingkat inflasi terhadap harga obat-obatan yang berlaku di pasaran dan harga pengobatan, saat ini rasio kewajiban dan rasio asset sudah hamper seimbang, namun Jamsostek tetap mampu membayar kepada peserta sesuai dengan prosedur dan tanggung jawab yang harus diberikan. Apabila peserta sudah mengikuti prosedur yang ada dan mengikuti jalannya proses yang ada, Jamsostek akan menunaikan kewajibannya sesuai dengan yang diharapkan dan seharusnya. Jamsostek berbeda dengan perusahaan asuransi swasta lainnya, Jamsostek adalah program jaminan yang dijaminkan pemerintah.”

RSC : “Bagaimana dengan BCP yang ada di Jamsostek? Sudahkan pernah diujicoba?”

RPD : “Testing tidak secara detil diketahui pernah dicoba atau tidak, tapi menurut informasi sudah pernah dilakukan di salah satu kantor cabang.”

RSC : “Bagaimana dengan review terhadap BCP?”

RPD : “Belum diketahui secara jelas dikarenakan BCP baru dibentuk dankejadian yang terkait bencana belum pernah terjadi, sehingga tidak bisa dilakukan review.”

RSC : “Bagaimana dengan tim yang terbentuk di BCP?”

RPD : “Jamsostek belum memiliki tim anggota yang terpisah untuk menangani BCP, Jamsostek memusatkan pada divisi Renbang dan Teknologi Informasi untuk pengembangan BCP tersebut. Mengenai perencanaan untuk dibuatnya tim divisi khusus tersebut belum diketahui informasi yang jelas. Jamsostek saat ini memiliki tim yang menangani BCP namun mereka bukan khusus untuk menangani BCP saja, mereka adalah bagian dari existing team yang sudah ada dan mendapat tanggung jawab untuk menangani BCP di dalamnya. Namun demikian belum ada pengesahan dalam SK kerja.”

RSC : “Tim yang manakah yang menangani BCP saat ini?”

RPD : “Tim yang menangani mengenai proses kelangsungan bisnis khususnya dari tim teknologi, sudah memiliki pengetahuan yang baik mengenai pengaktivasian BCP.”

RSC : “Bagaimana dengan anggaran mengenai BCP?”

RPD : “Saat ini belum ada anggaran khusus untuk pengeluaran terhadap BCP, anggaran masing-masing per divisi, namum dengan adanya BCP dan divisi tersebut menambahkan anggaran lebih untuk tahun itu, maka itu dapat di propose dan bisa diimplementasi.”

RSC : “Bagaimana keterlibatan BOD dan senior manajemen pada BCP?”

RPD : “Keterlibatan BOD cukup tinggi dalam pelaksanaan BCP tersebut. Keterlibatanya dalam hal apabila terjadi sesuatu fenomena atau event yang terkait, apabila ada *issue-issue* yang menjadi highlight point untuk tahap direksi.”

RSC : “Bagaimana mengenai komunikasi dari divisi humas pada pihak media?”

RPD : “Tidak terlalu mengetahui dengan jelas, namun sepertinya belum dilakukan.”

RSC : “Bagaimana concern bapak secra corporate governance terhadap BCP Jamsostek?”

RPD : “BCP seharusnya bisa dibakukan dalam tata kelola perusahaan, dibakukan bobot nya harusnya ditingkatkan dalam procedural tata kelola perusahaan, masuk dalam KPI masing-masing pihak yang berkaitan, adanya dilakukan proses audit/review, masuk dalam pengembangan performance pihak tersebut. Sehingga pelakasanaan dan implementasinya dapat berjalan dengan baik.”

Interview 6: Finance Division

RSC : “Bagaimana proses pada divisi keuangan? Bagaimana dengan kritikal proses di keuangan?”

RPD : “Surat berharga : asset bilyet, deposito. Kalau saham, obligasi di custody pihak ke-3. Data peserta yang sangat penting dan kritikal. Dari sisi TI sudah ada penyimpanan data salah satunya di Surabaya.”

RSC : “Bagaimana dengan proses, apa yang paling penting? Proses bisnis atau dokumen fisik?Kalau terjadi bencana, apa yang paling harus dijaga?”

RPD : “Sampai saat ini belum ada bencana yang signifikan. Proses penyimpanan di keuangan ini adalah hasil dari request dari investasi untuk menyimpan deposito. Baru kita simpan di deposito. Yang menjadi hal yang penting adalah aplikasi SisInvest yang akan menampilkan request dari investasi, kemudian proses di keuangan sampai dengan approval proses. Kemudian baru ke custody. Apabila terjadi bencana, maka kami melakukan manual aplikasi dengan excel. Tpi saya belum terbayangkan kalau terjadi bencana bagaimana ya. Saat ini masih mengikuti standard prosedur yang sudah ada, tapi apabila terjadi bencana belum terbayangkan.”

RSC : “Bagaimana dengan pencairan likuiditas?”

RPD : “Dari masalah klaim past bisa cair. Misalnya di cabang-cabang tinggal request kemudian langsung diminta ke pusat. Pusat langsung mencairkan dananya. Setiap minggu cabang akan melakukan fax mengenai kebutuhan dana biasanya sekali seminggu yang cabang butuhkan berapa. Kemudian akan dicadangkan dan cabang memberikan pada peserta. Nanti cabang bisa ambil melalui rekening induk dan nantinya cabang bisa ambil seberapa yang dibutuhkan sesuai dengan approval yang sudah diberikan.”

RSC : “Apabila terjadi suatu gangguan sehingga peserta secara bersama-sama mengambil dananya secara bersama-samaan, bagaimana dengan proses likuiditasnya?”

RPD : “Untuk likuiditas tidak masalah, tapi pasti untuk proses pencairannya pasti terganggu.”

RSC : “Apa yang menjadi asset yang paling penting yang harus dijaga?”

RPD : “Terutama pasti orangnya harus bagus dan bisa mengoperasikan aplikasi. Sistem kita sudah bagus, dan saat ini orang-orangnya sudah bisa mengoperasikan aplikasi. Selain itu manajemen SDM nya sudah jalan, apabila ada yang cuti, proses tetap bisa berjalan dengan normal.”

RSC : “Yang paling penting organisasi harus bisa menerapkan capabilities dan responsibility baru system akan mengikuti?”

RPD : “Iya, misalnya dari employee syarat pendidikannya harus S-1.“

RSC : “Bagaimana dengan prosedur kontigensi sudah berjalan dengan lancar?”

RPD : “Kontigensi deposito ada di brankas yang tahan api. Pemegang kuncinya hanya 1 orang dan cadangannya saya. Tapi apabila salah satu berhalangan ada backup nya, tapi informasi kombinasi tersebut bisa diganti-ganti untuk menjamin kerahasiaanya.”

RSC : “Apakah ada prosedur kontigensi lain terhadap brankas tersebut?”

RPD : “Kalau orang curi brankas tersebut juga tidak ada gunananya. Karena pencairan deposito tersebut juga harus ada tanda tangan direksi. Walaupun secara fisik itu rusak tapi tetap bisa dilakukan pencairan. Bank akan memberikan konfirmasi kepada Jamsostek, sehingga ada saling kontrol.”

RSC : “Bagaimana bila terjadi fraud?”

RPD : “Belum, prosedur kita standard ISO dan ada audit stock opname, selain itu ada pengawasan dari pihak luar dengan frekuensi setahun sekali dalam melakukan audit tersebut.“

RSC : “Bagaimana dengan prosedur kontigensi secara integrasi dengan divisi lain?”

RPD : “Untuk integrasi secara detil saya tidak dapat berbicara banyak.”

RSC : “Ada perubahan thp proses kontigensi sebelum dan sesudah BCP diimplementasi?”

RPD : “Perasaanya lebih enak dengan adanya BCP tersebut.“

RSC : “Bagaimana dengan awareness thp BCP?”

RPD : “Ada, staff keuangan punya tanggung jawab sendiri, job desk masing-masing. Mereka sudah melakukan routine prosedur, dan memiliki spontanitas tehadap proses routin yang terjadi untuk mencegah proses gagal bayar yang terjadi.”

RSC : “Dari sisi BCP sendiri, proses awareness itu seberapa dekat dengan staff terhadap proses rutin?”

RPD : “Belum adalah, karena testingnya juga belum ada langsung di divisi keuangan. Bencana juga belum terjadi. Paling yang bisa dilakukan kalau membayangkan itu terjadi adalah menunggu prosedur suspend yaitu menunggu kembali normal atau kondusif. Nantinya ketika proses sudah berjalan normal, baru bisa melakukan pelayanannya. Karena apabila terjadi bencana bank-bank lain juga kemungkinan mengalami yang sama. Misalanya di Aceh, setelah keadaan kondusif, staff dari pusat juga dikirimkan. Walaupun hal ini setelah ada instruksi langsung dari direksi. Yang jelas kalau rasio likuiditas tidak masalah.”

RSC : “Bagaimana hubungan antara cabang ke kantor pusat? Apa yang harus ditingkatkan untuk optimalisasi?”

RPD : "Cabang yang penting dananya siap, sehingga pembayaran klaim tidak terhambat. Gangguannya lebih kea rah perbankan atau system. Biasanya di perbankan dana yang diberikan lewat cek, tidak bisa dicairkan, karena dana yang ada adalah minimal. Padahal bisa refer ke cabang induk. Hal ini dikarenakan petugas bank belum mengerti mengenai pencairan tersebut. Tapi hal ini sudah jarang. Dari system proses lama karena kapasitas bandwith server, misalnya pada awal bulan banyak yang akses ke system tersebut. Apabila terjadi bencana dan IT tidak dapat melakukan aktivasi prosedur kontigensi, ini akan mengalami gangguan yang cukup memberikan impact signifikan karena proses nya menjadi lama dan akan berdampak pada resiko reputasi."

RSC : "Bagaimana dengan sosialisasi BCP, apakah efektif atau tidak secara integrasi?"

RPD : "Efektif untuk menyadarkan kita, karena sekarang-sekarang ini masih dalam batas normal."

RSC : "Apakah value BCP sudah merema dalam kepribadian staff yang ada?"

RPD : "Masih dalam pembentukan. Tapi memang apabila terjadi contoh di pusat ada gempa, orang-orang pada berebutan, prosedur detail juga belum ada. Tapi harusnya masih dalam pembentukan."

RSC : "Bagaimana bentuk komunikasi yang efektif?"

RPD : "Harusnya ada latihan uji coba yang dilakukan daripada sosialisasi lewat meeting atau pelatihan. Yang nomer 1 itu adalah latihan."

RSC : "Apa yang harus ditingkatkan untuk BCP?"

RPD : "Harusnya Biro Pengawasan Internal ikut mengawasi implementasi dari BCP ini sendiri. Sehingga awareness terhadap prosedur tersebut. Biro ini langsung bertanggung jawab ke direksi. Kalau belum ada uji coba, kita juga belum tau apabila prosedur kontigensi itu berhasil atau tidak.

Apalagi Jamsostek sangat concern terhadap resiko reputasi, apalagi kalau terjadi complain sampai masuk ke media. “

.

APPENDIX C Validity & Reliability Test

C.1 Event Identification

Validity Test

Correlation Matrix[a]

		EI1.3	EI1.3.1	EI1.4	EI1.4.1	EI1.5	EI1.6	EI1.6.1
Correlation	EI1.3	1.000	.910	.745	.723	.619	.779	.542
	EI1.3.1	.910	1.000	.783	.748	.571	.666	.399
	EI1.4	.745	.783	1.000	.717	.501	.571	.413
	EI1.4.1	.723	.748	.717	1.000	.591	.677	.647
	EI1.5	.619	.571	.501	.594	1.000	.739	.715
	EI1.6	.779	.663	.571	.677	.739	1.000	.856
	EI1.6.1	.542	.399	.413	.647	.715	.856	1.000
Sig. (1-tailed)	EI1.3		.000	.000	.000	.000	.000	.001
	EI1.3.1	.000		.000	.000	.000	.000	.011
	EI1.4	.000	.000		.000	.001	.000	.008
	EI1.4.1	.000	.000	.000		.000	.000	.000
	EI1.5	.000	.000	.001	.000		.000	.000
	EI1.6	.000	.000	.000	.000	.000		.000
	EI1.6.1	.001	.011	.008	.000	.000	.000	

a. Determinant = .000

KMO and Bartlett's Test

Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		.811
Bartlett's Test of Sphericity	Approx. Chi-Square	219.247
	df	21
	Sig.	.000

Anti-image Matrices

		EI1.3	EI1.3.1	EI1.4	EI1.4.1	EI1.5	EI1.6	EI1.6.1
Anti-image Covariance	EI1.3	.116	-.071	-.021	.013	.011	-.037	-.002
	EI1.3.1	-.071	.102	-.043	-.070	-.043	-.024	.056
	EI1.4	-.021	-.043	.344	-.076	-.008	.008	.002
	EI1.4.1	.013	-.070	-.076	.246	.028	.044	-.096
	EI1.5	.011	-.043	-.008	.028	.386	-.011	-.076
	EI1.6	-.037	-.024	.008	.044	-.011	.114	-.092
	EI1.6.1	-.002	.056	.002	-.096	-.076	-.092	.132
Anti-image Correlation	EI1.3	.854[a]	-.651	-.104	.077	.050	-.322	-.016
	EI1.3.1	-.651	.745[a]	-.232	-.441	-.218	-.219	.483
	EI1.4	-.104	-.232	.947[a]	-.261	-.023	.038	.007
	EI1.4.1	.077	-.441	-.261	.818[a]	.090	.262	-.531
	EI1.5	.050	-.218	-.023	.090	.932[a]	-.054	-.335
	EI1.6	-.322	-.219	.038	.262	-.054	.799[a]	-.747
	EI1.6.1	-.016	.483	.007	-.531	-.335	-.747	.658[a]

a. Measures of Sampling Adequacy(MSA)

Communalities

	Initial	Extraction
EI1.3	1.000	.822
EI1.3.1	1.000	.750
EI1.4	1.000	.644
EI1.4.1	1.000	.749
EI1.5	1.000	.636
EI1.6	1.000	.801
EI1.6.1	1.000	.590

Extraction Method: Principal Component Analysis.

Total Variance Explained

	Initial Eigenvalues			Extraction Sums of Squared Loadings		
Component	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	4.992	71.309	71.309	4.992	71.309	71.309
2	.963	13.750	85.059			
3	.372	5.317	90.376			
4	.314	4.481	94.858			
5	.236	3.370	98.228			
6	.071	1.014	99.242			
7	.053	.758	100.000			

Extraction Method: Principal Component Analysis.

Component Matrix[a]

	Component
	1
EI1.3	.907
EI1.3.1	.866
EI1.4	.802
EI1.4.1	.865
EI1.5	.797
EI1.6	.895
EI1.6.1	.768

Extraction Method: Principal Component Analysis.

a. 1 components extracted.

Reliability Test

Case Processing Summary

		N	%
Cases	Valid	33	100.0
	Excluded[a]	0	.0
	Total	33	100.0

a. Listwise deletion based on all variables in the procedure.

Reliability Statistics

Cronbach's Alpha	N of Items
.930	7

C.2 Risk Assessment Operation and Service

C.2.1 Likelihood

Vakidity Test

Correlation Matrix[a]

		O&PRA2.2L	O&PRA2.2.1L	O&PRA2.2.2L	O&PRA2.2.3L	O&PRA2.2.4L
Correlation	O&PRA2.2L	1.000	.949	.847	.841	.761
	O&PRA2.2.1L	.949	1.000	.819	.812	.715
	O&PRA2.2.2L	.847	.819	1.000	.991	.664
	O&PRA2.2.3L	.841	.812	.991	1.000	.632
	O&PRA2.2.4L	.761	.715	.664	.632	1.000
Sig. (1-tailed)	O&PRA2.2L		.000	.000	.000	.000
	O&PRA2.2.1L	.000		.000	.000	.000
	O&PRA2.2.2L	.000	.000		.000	.000
	O&PRA2.2.3L	.000	.000	.000		.000
	O&PRA2.2.4L	.000	.000	.000	.000	

a. Determinant = .000

KMO and Bartlett's Test

Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		.769
Bartlett's Test of Sphericity	Approx. Chi-Square	201.268
	df	10
	Sig.	.000

Anti-image Matrices

		O&PRA2.2L	O&PRA2.2.1L	O&PRA2.2.2L	O&PRA2.2.3L	O&PRA2.2.4L
Anti-image Covariance	O&PRA2.2L	.073	-.068	.003	-.006	-.060
	O&PRA2.2.1L	-.068	.098	-.003	.002	.012
	O&PRA2.2.2L	.003	-.003	.016	-.016	-.025
	O&PRA2.2.3L	-.006	.002	-.016	.016	.025
	O&PRA2.2.4L	-.060	.012	-.025	.025	.375
Anti-image Correlation	O&PRA2.2L	.782[a]	-.802	.081	-.166	-.365
	O&PRA2.2.1L	-.802	.807[a]	-.082	.061	.063
	O&PRA2.2.2L	.081	-.082	.726[a]	-.971	-.325
	O&PRA2.2.3L	-.166	.061	-.971	.718[a]	.321
	O&PRA2.2.4L	-.365	.063	-.325	.321	.848[a]

a. Measures of Sampling Adequacy(MSA)

Communalities

	Initial	Extraction
O&PRA2.2L	1.000	.921
O&PRA2.2.1L	1.000	.879
O&PRA2.2.2L	1.000	.892
O&PRA2.2.3L	1.000	.875
O&PRA2.2.4L	1.000	.659

Extraction Method: Principal Component Analysis.

Total Variance Explained

Component	Initial Eigenvalues			Extraction Sums of Squared Loadings		
	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	4.225	84.500	84.500	4.225	84.500	84.500
2	.461	9.223	93.723			
3	.259	5.186	98.909			
4	.046	.928	99.837			
5	.008	.163	100.000			

Extraction Method: Principal Component Analysis.

Component Matrix[a]

	Component
	1
O&PRA2.2L	.959
O&PRA2.2.1L	.937
O&PRA2.2.2L	.944
O&PRA2.2.3L	.935
O&PRA2.2.4L	.812

Extraction Method: Principal Component Analysis.

a. 1 components extracted.

Reliability

Case Processing Summary

		N	%
Cases	Valid	27	100.0
	Excluded[a]	0	.0
	Total	27	100.0

a. Listwise deletion based on all variables in the procedure.

Reliability Statistics

Cronbach's Alpha	N of Items
.953	5

C.2.2 Impact

Validity Test

Correlation Matrix[a]

		O&PRA2.2.1I	O&PRA2.2.2I	O&PRA2.2.3I	O&PRA2.2.4I
Correlation	O&PRA2.2.1I	1.000	.480	.675	.581
	O&PRA2.2.2I	.480	1.000	.831	.400
	O&PRA2.2.3I	.675	.831	1.000	.519
	O&PRA2.2.4I	.581	.400	.519	1.000
Sig. (1-tailed)	O&PRA2.2.1I		.006	.000	.001
	O&PRA2.2.2I	.006		.000	.019
	O&PRA2.2.3I	.000	.000		.003
	O&PRA2.2.4I	.001	.019	.003	

a. Determinant = .102

KMO and Bartlett's Test

Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		.679
Bartlett's Test of Sphericity	Approx. Chi-Square	54.364
	df	6
	Sig.	.000

Anti-image Matrices

		O&PRA2.2.1I	O&PRA2.2.2I	O&PRA2.2.3I	O&PRA2.2.4I
Anti-image Covariance	O&PRA2.2.1I	.454	.069	-.147	-.193
	O&PRA2.2.2I	.069	.297	-.192	-.003
	O&PRA2.2.3I	-.147	-.192	.206	-.046
	O&PRA2.2.4I	-.193	-.003	-.046	.633
Anti-image Correlation	O&PRA2.2.1I	.722[a]	.188	-.479	-.361
	O&PRA2.2.2I	.188	.629[a]	-.776	-.007
	O&PRA2.2.3I	-.479	-.776	.625[a]	-.127
	O&PRA2.2.4I	-.361	-.007	-.127	.840[a]

a. Measures of Sampling Adequacy(MSA)

Communalities

	Initial	Extraction
O&PRA2.2.1I	1.000	.679
O&PRA2.2.2I	1.000	.687
O&PRA2.2.3I	1.000	.855
O&PRA2.2.4I	1.000	.538

Extraction Method: Principal Component Analysis.

Total Variance Explained

	Initial Eigenvalues			Extraction Sums of Squared Loadings		
Component	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	2.758	68.956	68.956	2.758	68.956	68.956
2	.705	17.628	86.584			
3	.408	10.195	96.779			
4	.129	3.221	100.000			

Extraction Method: Principal Component Analysis.

Component Matrix[a]

	Component
	1
O&PRA2.2.1I	.824
O&PRA2.2.2I	.829
O&PRA2.2.3I	.925
O&PRA2.2.4I	.734

Extraction Method: Principal Component Analysis.

a. 1 components extracted.

Reliability Test

Case Processing Summary

		N	%
Cases	Valid	27	100.0
	Excluded[a]	0	.0
	Total	27	100.0

a. Listwise deletion based on all variables in the procedure.

Reliability Statistics

Cronbach's Alpha	N of Items
.841	4

C.2.3 Category

Validity Test

Correlation Matrix[a]

		O&PRA2.2K	O&PRA2.2.1K	O&PRA2.2.2K	O&PRA2.2.3K	O&PRA2.2.4K
Correlation	O&PRA2.2K	1.000	.748	.622	.672	.585
	O&PRA2.2.1K	.748	1.000	.636	.738	.591
	O&PRA2.2.2K	.622	.636	1.000	.949	.341
	O&PRA2.2.3K	.672	.738	.949	1.000	.400
	O&PRA2.2.4K	.585	.591	.341	.400	1.000
Sig. (1-tailed)	O&PRA2.2K		.000	.000	.000	.001
	O&PRA2.2.1K	.000		.000	.000	.001
	O&PRA2.2.2K	.000	.000		.000	.041
	O&PRA2.2.3K	.000	.000	.000		.019
	O&PRA2.2.4K	.001	.001	.041	.019	

a. Determinant = .010

KMO and Bartlett's Test

Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		.743
Bartlett's Test of Sphericity	Approx. Chi-Square	108.509
	df	10
	Sig.	.000

Anti-image Matrices

		O&PRA2.2K	O&PRA2.2.1K	O&PRA2.2.2K	O&PRA2.2.3K	O&PRA2.2.4K
Anti-image Covariance	O&PRA2.2K	.369	-.120	-.018	-.005	-.139
	O&PRA2.2.1K	-.120	.280	.046	-.064	-.122
	O&PRA2.2.2K	-.018	.046	.090	-.072	.004
	O&PRA2.2.3K	-.005	-.064	-.072	.069	.009
	O&PRA2.2.4K	-.139	-.122	.004	.009	.590
Anti-image Correlation	O&PRA2.2K	.880[a]	-.372	-.101	-.029	-.297
	O&PRA2.2.1K	-.372	.780[a]	.289	-.458	-.301
	O&PRA2.2.2K	-.101	.289	.661[a]	-.912	.018
	O&PRA2.2.3K	-.029	-.458	-.912	.663[a]	.045
	O&PRA2.2.4K	-.297	-.301	.018	.045	.842[a]

a. Measures of Sampling Adequacy(MSA)

Communalities

	Initial	Extraction
O&PRA2.2K	1.000	.747
O&PRA2.2.1K	1.000	.787
O&PRA2.2.2K	1.000	.742
O&PRA2.2.3K	1.000	.829
O&PRA2.2.4K	1.000	.440

Extraction Method: Principal Component Analysis.

Total Variance Explained

Component	Initial Eigenvalues			Extraction Sums of Squared Loadings		
	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	3.545	70.897	70.897	3.545	70.897	70.897
2	.828	16.559	87.455			
3	.335	6.701	94.156			
4	.252	5.048	99.204			
5	.040	.796	100.000			

Extraction Method: Principal Component Analysis.

Component Matrix[a]

	Component
	1
O&PRA2.2K	.864
O&PRA2.2.1K	.887
O&PRA2.2.2K	.861
O&PRA2.2.3K	.911
O&PRA2.2.4K	.663

Extraction Method: Principal Component Analysis.

a. 1 components extracted.

Reliability Test

Case Processing Summary

		N	%
Cases	Valid	27	100.0
	Excluded[a]	0	.0
	Total	27	100.0

a. Listwise deletion based on all variables in the procedure.

Reliability Statistics

Cronbach's Alpha	N of Items
.893	5

C.3 Risk Assessment Investment

C.3.1 Likelihood

Validity

Correlation Matrix[a]

		InvRA2.3L	InvRA2.3.1L	InvRA2.3.2L	InvRA2.3.3L
Correlation	InvRA2.3L	1.000	.867	.878	.841
	InvRA2.3.1L	.867	1.000	.931	.952
	InvRA2.3.2L	.878	.931	1.000	.922
	InvRA2.3.3L	.841	.952	.922	1.000
Sig. (1-tailed)	InvRA2.3L		.000	.000	.000
	InvRA2.3.1L	.000		.000	.000
	InvRA2.3.2L	.000	.000		.000
	InvRA2.3.3L	.000	.000	.000	

a. Determinant = .002

KMO and Bartlett's Test

Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		.856
Bartlett's Test of Sphericity	Approx. Chi-Square	138.209
	df	6
	Sig.	.000

Anti-image Matrices

		InvRA2.3L	InvRA2.3.1L	InvRA2.3.2L	InvRA2.3.3L
Anti-image Covariance	InvRA2.3L	.210	-.028	-.056	.004
	InvRA2.3.1L	-.028	.070	-.027	-.050
	InvRA2.3.2L	-.056	-.027	.103	-.028
	InvRA2.3.3L	.004	-.050	-.028	.084
Anti-image Correlation	InvRA2.3L	.918[a]	-.231	-.381	.027
	InvRA2.3.1L	-.231	.813[a]	-.316	-.653
	InvRA2.3.2L	-.381	-.316	.881[a]	-.303
	InvRA2.3.3L	.027	-.653	-.303	.826[a]

a. Measures of Sampling Adequacy(MSA)

Communalities

	Initial	Extraction
InvRA2.3L	1.000	.867
InvRA2.3.1L	1.000	.952
InvRA2.3.2L	1.000	.942
InvRA2.3.3L	1.000	.935

Extraction Method: Principal Component Analysis.

Total Variance Explained

	Initial Eigenvalues			Extraction Sums of Squared Loadings		
Component	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	3.697	92.414	92.414	3.697	92.414	92.414
2	.181	4.522	96.936			
3	.077	1.920	98.855			
4	.046	1.145	100.000			

Extraction Method: Principal Component Analysis.

Component Matrix[a]

	Component
	1
InvRA2.3L	.931
InvRA2.3.1L	.976
InvRA2.3.2L	.971
InvRA2.3.3L	.967

Extraction Method: Principal Component Analysis.

a. 1 components extracted.

Reliability Test

Case Processing Summary

		N	%
Cases	Valid	26	100.0
	Excluded[a]	0	.0
	Total	26	100.0

a. Listwise deletion based on all variables in the procedure.

Reliability Statistics

Cronbach's Alpha	N of Items
.971	4

C.3.2 Impact

Validity Test

Correlation Matrix[a]

		InvRA2.3I	InvRA2.3.1I	InvRA2.3.2I	InvRA2.3.3I
Correlation	InvRA2.3I	1.000	.510	.508	.527
	InvRA2.3.1I	.510	1.000	.954	.780
	InvRA2.3.2I	.508	.954	1.000	.776
	InvRA2.3.3I	.527	.780	.776	1.000
Sig. (1-tailed)	InvRA2.3I		.004	.004	.003
	InvRA2.3.1I	.004		.000	.000
	InvRA2.3.2I	.004	.000		.000
	InvRA2.3.3I	.003	.000	.000	

a. Determinant = .024

KMO and Bartlett's Test

Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		.766
Bartlett's Test of Sphericity	Approx. Chi-Square	85.563
	df	6
	Sig.	.000

Anti-image Matrices

		InvRA2.3I	InvRA2.3.1I	InvRA2.3.2I	InvRA2.3.3I
Anti-image Covariance	InvRA2.3I	.696	-.013	-.010	-.115
	InvRA2.3.1I	-.013	.085	-.076	-.033
	InvRA2.3.2I	-.010	-.076	.087	-.027
	InvRA2.3.3I	-.115	-.033	-.027	.360
Anti-image Correlation	InvRA2.3I	.933[a]	-.052	-.041	-.231
	InvRA2.3.1I	-.052	.686[a]	-.880	-.191
	InvRA2.3.2I	-.041	-.880	.689[a]	-.155
	InvRA2.3.3I	-.231	-.191	-.155	.929[a]

a. Measures of Sampling Adequacy(MSA)

Communalities

	Initial	Extraction
InvRA2.3I	1.000	.482
InvRA2.3.1I	1.000	.895
InvRA2.3.2I	1.000	.891
InvRA2.3.3I	1.000	.794

Extraction Method: Principal Component Analysis.

Total Variance Explained

	Initial Eigenvalues			Extraction Sums of Squared Loadings		
Component	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	3.062	76.555	76.555	3.062	76.555	76.555
2	.620	15.497	92.052			
3	.272	6.807	98.859			
4	.046	1.141	100.000			

Extraction Method: Principal Component Analysis.

Component Matrix[a]

	Component
	1
InvRA2.3I	.694
InvRA2.3.1I	.946
InvRA2.3.2I	.944
InvRA2.3.3I	.891

Extraction Method: Principal Component Analysis.

a. 1 components extracted.

Reliability Test

Case Processing Summary

		N	%
Cases	Valid	26	100.0
	Excluded[a]	0	.0
	Total	26	100.0

a. Listwise deletion based on all variables in the procedure.

Reliability Statistics

Cronbach's Alpha	N of Items
.893	4

C.3.3 Category

Validity Test

Correlation Matrix[a]

		InvRA2.3K	InvRA2.3.1K	InvRA2.3.2K	InvRA2.3.3K
Correlation	InvRA2.3K	1.000	.568	.721	.569
	InvRA2.3.1K	.568	1.000	.894	.857
	InvRA2.3.2K	.721	.894	1.000	.863
	InvRA2.3.3K	.569	.857	.863	1.000
Sig. (1-tailed)	InvRA2.3K		.001	.000	.001
	InvRA2.3.1K	.001		.000	.000
	InvRA2.3.2K	.000	.000		.000
	InvRA2.3.3K	.001	.000	.000	

a. Determinant = .020

KMO and Bartlett's Test

Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		.777
Bartlett's Test of Sphericity	Approx. Chi-Square	89.709
	df	6
	Sig.	.000

Anti-image Matrices

		InvRA2.3K	InvRA2.3.1K	InvRA2.3.2K	InvRA2.3.3K
Anti-image Covariance	InvRA2.3K	.449	.056	-.126	.020
	InvRA2.3.1K	.056	.164	-.082	-.067
	InvRA2.3.2K	-.126	-.082	.114	-.060
	InvRA2.3.3K	.020	-.067	-.060	.218
Anti-image Correlation	InvRA2.3K	.764[a]	.208	-.559	.065
	InvRA2.3.1K	.208	.779[a]	-.598	-.356
	InvRA2.3.2K	-.559	-.598	.717[a]	-.382
	InvRA2.3.3K	.065	-.356	-.382	.867[a]

a. Measures of Sampling Adequacy(MSA)

Anti-image Matrices

		InvRA2.3K	InvRA2.3.1K	InvRA2.3.2K	InvRA2.3.3K
Anti-image Covariance	InvRA2.3K	.449	.056	-.126	.020
	InvRA2.3.1K	.056	.164	-.082	-.067
	InvRA2.3.2K	-.126	-.082	.114	-.060
	InvRA2.3.3K	.020	-.067	-.060	.218
Anti-image Correlation	InvRA2.3K	.764[a]	.208	-.559	.065
	InvRA2.3.1K	.208	.779[a]	-.598	-.356
	InvRA2.3.2K	-.559	-.598	.717[a]	-.382
	InvRA2.3.3K	.065	-.356	-.382	.867[a]

a. Measures of Sampling Adequacy(MSA)

Total Variance Explained

	Initial Eigenvalues			Extraction Sums of Squared Loadings		
Component	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	3.255	81.365	81.365	3.255	81.365	81.365
2	.519	12.966	94.331			
3	.148	3.702	98.033			
4	.079	1.967	100.000			

Extraction Method: Principal Component Analysis.

Component Matrix[a]

	Component
	1
InvRA2.3K	.776
InvRA2.3.1K	.930
InvRA2.3.2K	.969
InvRA2.3.3K	.921

Extraction Method: Principal Component Analysis.

a. 1 components extracted.

Reliability Test

Case Processing Summary

		N	%
Cases	Valid	26	100.0
	Excluded[a]	0	.0
	Total	26	100.0

a. Listwise deletion based on all variables in the procedure.

Reliability Statistics

Cronbach's Alpha	N of Items
.920	4

C.4 Risk Assessment Finance

C.4.1 Likelihood

Validity Test

Correlation Matrix[a]

		KeuRA2.5L	KeuRA2.5.1L
Correlation	KeuRA2.5L	1.000	.942
	KeuRA2.5.1L	.942	1.000
Sig. (1-tailed)	KeuRA2.5L		.000
	KeuRA2.5.1L	.000	

a. Determinant = .113

KMO and Bartlett's Test

Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		.500
Bartlett's Test of Sphericity	Approx. Chi-Square	42.596
	df	1
	Sig.	.000

Anti-image Matrices

		KeuRA2.5L	KeuRA2.5.1L
Anti-image Covariance	KeuRA2.5L	.113	-.106
	KeuRA2.5.1L	-.106	.113
Anti-image Correlation	KeuRA2.5L	.500[a]	-.942
	KeuRA2.5.1L	-.942	.500[a]

a. Measures of Sampling Adequacy(MSA)

Communalities

	Initial	Extraction
KeuRA2.5L	1.000	.971
KeuRA2.5.1L	1.000	.971

Extraction Method: Principal Component Analysis.

Total Variance Explained

Component	Initial Eigenvalues			Extraction Sums of Squared Loadings		
	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	1.942	97.102	97.102	1.942	97.102	97.102
2	.058	2.898	100.000			

Extraction Method: Principal Component Analysis.

Component Matrix[a]

	Component
	1
KeuRA2.5L	.985
KeuRA2.5.1L	.985

Extraction Method: Principal Component Analysis.

a. 1 components extracted.

Reliability Test

Case Processing Summary

		N	%
Cases	Valid	22	100.0
	Excluded[a]	0	.0
	Total	22	100.0

a. Listwise deletion based on all variables in the procedure.

Reliability Statistics

Cronbach's Alpha	N of Items
.968	2

C.4.2 Impact

Validity

Correlation Matrix[a]

		KeuRA2.5I	KeuRA2.5.1I
Correlation	KeuRA2.5I	1.000	.940
	KeuRA2.5.1I	.940	1.000
Sig. (1-tailed)	KeuRA2.5I		.000
	KeuRA2.5.1I	.000	

a. Determinant = .116

KMO and Bartlett's Test

Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		.500
Bartlett's Test of Sphericity	Approx. Chi-Square	41.990
	df	1
	Sig.	.000

Anti-image Matrices

		KeuRA2.5I	KeuRA2.5.1I
Anti-image Covariance	KeuRA2.5I	.116	-.109
	KeuRA2.5.1I	-.109	.116
Anti-image Correlation	KeuRA2.5I	.500[a]	-.940
	KeuRA2.5.1I	-.940	.500[a]

a. Measures of Sampling Adequacy(MSA)

Communalities

	Initial	Extraction
KeuRA2.5I	1.000	.970
KeuRA2.5.1I	1.000	.970

Extraction Method: Principal Component Analysis.

Total Variance Explained

Component	Initial Eigenvalues			Extraction Sums of Squared Loadings		
	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	1.940	97.008	97.008	1.940	97.008	97.008
2	.060	2.992	100.000			

Extraction Method: Principal Component Analysis.

Component Matrix[a]

	Component
	1
KeuRA2.5I	.985
KeuRA2.5.1I	.985

Extraction Method: Principal Component Analysis.

a. 1 components extracted.

Reliability

Case Processing Summary

		N	%
Cases	Valid	22	100.0
	Excluded[a]	0	.0
	Total	22	100.0

a. Listwise deletion based on all variables in the procedure.

Reliability Statistics

Cronbach's Alpha	N of Items
.969	2

C.4.3 Category

Validity Test

Correlation Matrix[a]

		KeuRA2.5K	KeuRA2.5.1K
Correlation	KeuRA2.5K	1.000	.925
	KeuRA2.5.1K	.925	1.000
Sig. (1-tailed)	KeuRA2.5K		.000
	KeuRA2.5.1K	.000	

a. Determinant = .145

KMO and Bartlett's Test

Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		.500
Bartlett's Test of Sphericity	Approx. Chi-Square	37.710
	df	1
	Sig.	.000

Anti-image Matrices

		KeuRA2.5K	KeuRA2.5.1K
Anti-image Covariance	KeuRA2.5K	.145	-.134
	KeuRA2.5.1K	-.134	.145
Anti-image Correlation	KeuRA2.5K	.500[a]	-.925
	KeuRA2.5.1K	-.925	.500[a]

a. Measures of Sampling Adequacy(MSA)

Communalities

	Initial	Extraction
KeuRA2.5K	1.000	.962
KeuRA2.5.1K	1.000	.962

Extraction Method: Principal Component Analysis.

Total Variance Explained

Component	Initial Eigenvalues			Extraction Sums of Squared Loadings		
	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	1.925	96.244	96.244	1.925	96.244	96.244
2	.075	3.756	100.000			

Extraction Method: Principal Component Analysis.

Component Matrix[a]

	Component
	1
KeuRA2.5K	.981
KeuRA2.5.1K	.981

Extraction Method: Principal Component Analysis.

a. 1 components extracted.

Reliability Test

Case Processing Summary

		N	%
Cases	Valid	22	100.0
	Excluded[a]	0	.0
	Total	22	100.0

a. Listwise deletion based on all variables in the procedure.

Reliability Statistics

Cronbach's Alpha	N of Items
.960	2

C.5 Risk Assessment Information Technology

C.5.1 Likelihood

Validity Test

Correlation Matrix[a]

		Gen. ITRA2.4L	Gen. ITRA2.7L	Gen. ITRA2.7.1L
Correlation	Gen. ITRA2.4L	1.000	.459	.481
	Gen. ITRA2.7L	.459	1.000	.818
	Gen. ITRA2.7.1L	.481	.818	1.000
Sig. (1-tailed)	Gen. ITRA2.4L		.004	.003
	Gen. ITRA2.7L	.004		.000
	Gen. ITRA2.7.1L	.003	.000	

a. Determinant = .250

e

KMO and Bartlett's Test

Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		.632
Bartlett's Test of Sphericity	Approx. Chi-Square	40.447
	df	3
	Sig.	.000

Anti-image Matrices

		Gen. ITRA2.4L	Gen. ITRA2.7L	Gen. ITRA2.7.1L
Anti-image Covariance	Gen. ITRA2.4L	.755	-.065	-.101
	Gen. ITRA2.7L	-.065	.325	-.246
	Gen. ITRA2.7.1L	-.101	-.246	.317
Anti-image Correlation	Gen. ITRA2.4L	.881[a]	-.130	-.206
	Gen. ITRA2.7L	-.130	.593[a]	-.767
	Gen. ITRA2.7.1L	-.206	-.767	.588[a]

a. Measures of Sampling Adequacy(MSA)

Communalities

	Initial	Extraction
Gen. ITRA2.4L	1.000	.522
Gen. ITRA2.7L	1.000	.827
Gen. ITRA2.7.1L	1.000	.841

Extraction Method: Principal Component Analysis.

Total Variance Explained

Component	Initial Eigenvalues			Extraction Sums of Squared Loadings		
	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	2.190	72.998	72.998	2.190	72.998	72.998
2	.629	20.950	93.948			
3	.182	6.052	100.000			

Extraction Method: Principal Component Analysis.

Component Matrix[a]

	Component
	1
Gen. ITRA2.4L	.722
Gen. ITRA2.7L	.909
Gen. ITRA2.7.1L	.917

Extraction Method: Principal Component Analysis.

a. 1 components extracted.

Reliability Test

Case Processing Summary

		N	%
Cases	Valid	32	100.0
	Excluded[a]	0	.0
	Total	32	100.0

a. Listwise deletion based on all variables in the procedure.

Reliability Statistics

Cronbach's Alpha	N of Items
.807	3

C.5.2 Impact

Validity Test

Correlation Matrix[a]

		Gen. ITRA2.4I	Gen. ITRA2.7I	Gen. ITRA2.7.1I
Correlation	Gen. ITRA2.4I	1.000	.537	.521
	Gen. ITRA2.7I	.537	1.000	.896
	Gen. ITRA2.7.1I	.521	.896	1.000
Sig. (1-tailed)	Gen. ITRA2.4I		.001	.001
	Gen. ITRA2.7I	.001		.000
	Gen. ITRA2.7.1I	.001	.000	

a. Determinant = .139

KMO and Bartlett's Test

Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		.637
Bartlett's Test of Sphericity	Approx. Chi-Square	57.509
	df	3
	Sig.	.000

Anti-image Matrices

		Gen. ITRA2.4I	Gen. ITRA2.7I	Gen. ITRA2.7.1I
Anti-image Covariance	Gen. ITRA2.4I	.704	-.068	-.040
	Gen. ITRA2.7I	-.068	.191	-.165
	Gen. ITRA2.7.1I	-.040	-.165	.196
Anti-image Correlation	Gen. ITRA2.4I	.925[a]	-.185	-.107
	Gen. ITRA2.7I	-.185	.587[a]	-.855
	Gen. ITRA2.7.1I	-.107	-.855	.591[a]

a. Measures of Sampling Adequacy(MSA)

Communalities

	Initial	Extraction
Gen. ITRA2.4I	1.000	.564
Gen. ITRA2.7I	1.000	.883
Gen. ITRA2.7.1I	1.000	.873

Extraction Method: Principal Component Analysis.

Total Variance Explained

Component	Initial Eigenvalues			Extraction Sums of Squared Loadings		
	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	2.319	77.311	77.311	2.319	77.311	77.311
2	.577	19.219	96.530			
3	.104	3.470	100.000			

Extraction Method: Principal Component Analysis.

Component Matrix[a]

	Component
	1
Gen. ITRA2.4I	.751
Gen. ITRA2.7I	.940
Gen. ITRA2.7.1I	.934

Extraction Method: Principal Component Analysis.

a. 1 components extracted.

Reliability Test

Case Processing Summary

		N	%
Cases	Valid	32	100.0
	Excluded[a]	0	.0
	Total	32	100.0

a. Listwise deletion based on all variables in the procedure.

Reliability Statistics

Cronbach's Alpha	N of Items
.852	3

C.5.3 Category

Validity Test

Correlation Matrix[a]

		Gen. ITRA2. 4K	Gen. ITRA2. 7K	Gen. ITRA2. 7.1K
Correlation	Gen. ITRA2.4K	1.000	.442	.443
	Gen. ITRA2.7K	.442	1.000	.800
	Gen. ITRA2.7.1K	.443	.800	1.000
Sig. (1-tailed)	Gen. ITRA2.4K		.006	.006
	Gen. ITRA2.7K	.006		.000
	Gen. ITRA2.7.1K	.006	.000	

a. Determinant = .282

KMO and Bartlett's Test

Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		.625
Bartlett's Test of Sphericity	Approx. Chi-Square	36.966
	df	3
	Sig.	.000

Anti-image Matrices

		Gen. ITRA2.4K	Gen. ITRA2.7K	Gen. ITRA2.7.1K
Anti-image Covariance	Gen. ITRA2.4K	.782	-.086	-.087
	Gen. ITRA2.7K	-.086	.350	-.263
	Gen. ITRA2.7.1K	-.087	-.263	.350
Anti-image Correlation	Gen. ITRA2.4K	.879[a]	-.163	-.166
	Gen. ITRA2.7K	-.163	.586[a]	-.751
	Gen. ITRA2.7.1K	-.166	-.751	.586[a]

a. Measures of Sampling Adequacy(MSA)

Communalities

	Initial	Extraction
Gen. ITRA2.4K	1.000	.495
Gen. ITRA2.7K	1.000	.824
Gen. ITRA2.7.1K	1.000	.824

Extraction Method: Principal Component Analysis.

Total Variance Explained

	Initial Eigenvalues			Extraction Sums of Squared Loadings		
Component	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	2.143	71.436	71.436	2.143	71.436	71.436
2	.657	21.898	93.334			
3	.200	6.666	100.000			

Extraction Method: Principal Component Analysis.

Component Matrix[a]

	Component
	1
Gen. ITRA2.4K	.703
Gen. ITRA2.7K	.908
Gen. ITRA2.7.1K	.908

Extraction Method: Principal Component Analysis.

a. 1 components extracted.

Reliability Test

Case Processing Summary

		N	%
Cases	Valid	32	100.0
	Excluded[a]	0	.0
	Total	32	100.0

a. Listwise deletion based on all variables in the procedure.

Reliability Statistics

Cronbach's Alpha	N of Items
.800	3

C.6 Risk Assessment General

C.6.1 Likelihood

Validity Test

Correlation Matrix[a]

		GenRA2.6L	GenRA2.6.1L	GenRA2.6.2L
Correlation	GenRA2.6L	1.000	.965	.781
	GenRA2.6.1L	.965	1.000	.878
	GenRA2.6.2L	.781	.878	1.000
Sig. (1-tailed)	GenRA2.6L		.000	.000
	GenRA2.6.1L	.000		.000
	GenRA2.6.2L	.000	.000	

a. Determinant = .012

KMO and Bartlett's Test

Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		.573
Bartlett's Test of Sphericity	Approx. Chi-Square	130.164
	df	3
	Sig.	.000

Anti-image Matrices

		GenRA2.6L	GenRA2.6.1L	GenRA2.6.2L
Anti-image Covariance	GenRA2.6L	.050	-.036	.048
	GenRA2.6.1L	-.036	.030	-.053
	GenRA2.6.2L	.048	-.053	.165
Anti-image Correlation	GenRA2.6L	.573[a]	-.933	.526
	GenRA2.6.1L	-.933	.540[a]	-.759
	GenRA2.6.2L	.526	-.759	.618[a]

a. Measures of Sampling Adequacy(MSA)

Communalities

	Initial	Extraction
GenRA2.6L	1.000	.917
GenRA2.6.1L	1.000	.981
GenRA2.6.2L	1.000	.853

Extraction Method: Principal Component Analysis.

Total Variance Explained

	Initial Eigenvalues			Extraction Sums of Squared Loadings		
Component	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	2.751	91.702	91.702	2.751	91.702	91.702
2	.231	7.693	99.395			
3	.018	.605	100.000			

Extraction Method: Principal Component Analysis.

Component Matrix[a]

	Component
	1
GenRA2.6L	.957
GenRA2.6.1L	.991
GenRA2.6.2L	.924

Extraction Method: Principal Component Analysis.

a. 1 components extracted.

Reliability Test

Case Processing Summary

		N	%
Cases	Valid	32	100.0
	Excluded[a]	0	.0
	Total	32	100.0

a. Listwise deletion based on all variables in the procedure.

Reliability Statistics

Cronbach's Alpha	N of Items
.954	3

C.6.2 Impact

Validity Test

Correlation Matrix[a]

		GenRA2.6I	GenRA2.6.1I	GenRA2.6.2I
Correlation	GenRA2.6I	1.000	.899	.826
	GenRA2.6.1I	.899	1.000	.929
	GenRA2.6.2I	.826	.929	1.000
Sig. (1-tailed)	GenRA2.6I		.000	.000
	GenRA2.6.1I	.000		.000
	GenRA2.6.2I	.000	.000	

a. Determinant = .026

KMO and Bartlett's Test

Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		.709
Bartlett's Test of Sphericity	Approx. Chi-Square	106.114
	df	3
	Sig.	.000

Anti-image Matrices

		GenRA2.6I	GenRA2.6.1I	GenRA2.6.2I
Anti-image Covariance	GenRA2.6I	.192	-.079	.008
	GenRA2.6.1I	-.079	.083	-.080
	GenRA2.6.2I	.008	-.080	.137
Anti-image Correlation	GenRA2.6I	.790[a]	-.628	.051
	GenRA2.6.1I	-.628	.634[a]	-.754
	GenRA2.6.2I	.051	-.754	.730[a]

a. Measures of Sampling Adequacy(MSA)

Communalities

	Initial	Extraction
GenRA2.6I	1.000	.893
GenRA2.6.1I	1.000	.963
GenRA2.6.2I	1.000	.914

Extraction Method: Principal Component Analysis.

Total Variance Explained

Component	Initial Eigenvalues			Extraction Sums of Squared Loadings		
	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	2.770	92.335	92.335	2.770	92.335	92.335
2	.176	5.866	98.202			
3	.054	1.798	100.000			

Extraction Method: Principal Component Analysis.

Component Matrix[a]

	Component
	1
GenRA2.6I	.945
GenRA2.6.1I	.981
GenRA2.6.2I	.956

Extraction Method: Principal Component Analysis.

a. 1 components extracted.

Reliability Test

Case Processing Summary

		N	%
Cases	Valid	32	100.0
	Excluded[a]	0	.0
	Total	32	100.0

a. Listwise deletion based on all variables in the procedure.

Reliability Statistics

Cronbach's Alpha	N of Items
.953	3

C.6.3 Category

Validity Test

Correlation Matrix[a]

		GenRA2.6K	GenRA2.6.1K	GenRA2.6.2K
Correlation	GenRA2.6K	1.000	.861	.856
	GenRA2.6.1K	.861	1.000	.954
	GenRA2.6.2K	.856	.954	1.000
Sig. (1-tailed)	GenRA2.6K		.000	.000
	GenRA2.6.1K	.000		.000
	GenRA2.6.2K	.000	.000	

a. Determinant = .022

KMO and Bartlett's Test

Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		.745
Bartlett's Test of Sphericity	Approx. Chi-Square	111.105
	df	3
	Sig.	.000

Anti-image Matrices

		GenRA2.6K	GenRA2.6.1K	GenRA2.6.2K
Anti-image Covariance	GenRA2.6K	.246	-.041	-.033
	GenRA2.6.1K	-.041	.083	-.069
	GenRA2.6.2K	-.033	-.069	.085
Anti-image Correlation	GenRA2.6K	.917[a]	-.284	-.229
	GenRA2.6.1K	-.284	.684[a]	-.825
	GenRA2.6.2K	-.229	-.825	.691[a]

a. Measures of Sampling Adequacy(MSA)

Communalities

	Initial	Extraction
GenRA2.6K	1.000	.882
GenRA2.6.1K	1.000	.951
GenRA2.6.2K	1.000	.948

Extraction Method: Principal Component Analysis.

Total Variance Explained

Component	Initial Eigenvalues			Extraction Sums of Squared Loadings		
	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	2.781	92.703	92.703	2.781	92.703	92.703
2	.173	5.760	98.463			
3	.046	1.537	100.000			

Extraction Method: Principal Component Analysis.

Component Matrix[a]

	Component
	1
GenRA2.6K	.939
GenRA2.6.1K	.975
GenRA2.6.2K	.974

Extraction Method: Principal Component Analysis.

a. 1 components extracted.

Reliability Test

Case Processing Summary

		N	%
Cases	Valid	32	100.0
	Excluded[a]	0	.0
	Total	32	100.0

a. Listwise deletion based on all variables in the procedure.

Reliability Statistics

Cronbach's Alpha	N of Items
.957	3

C.7 Risk Response

Validity Test

Correlation Matrix[a]

		RR2.9	RR2.10	RR2.11
Correlation	RR2.9	1.000	.692	.598
	RR2.10	.692	1.000	.708
	RR2.11	.598	.708	1.000
Sig. (1-tailed)	RR2.9		.000	.000
	RR2.10	.000		.000
	RR2.11	.000	.000	

a. Determinant = .248

KMO and Bartlett's Test

Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		.717
Bartlett's Test of Sphericity	Approx. Chi-Square	42.080
	df	3
	Sig.	.000

Anti-image Matrices

		RR2.9	RR2.10	RR2.11
Anti-image Covariance	RR2.9	.497	-.208	-.103
	RR2.10	-.208	.386	-.218
	RR2.11	-.103	-.218	.476
Anti-image Correlation	RR2.9	.756[a]	-.475	-.212
	RR2.10	-.475	.670[a]	-.508
	RR2.11	-.212	-.508	.739[a]

a. Measures of Sampling Adequacy(MSA)

Communalities

	Initial	Extraction
RR2.9	1.000	.746
RR2.10	1.000	.829
RR2.11	1.000	.759

Extraction Method: Principal Component Analysis.

Total Variance Explained

Component	Initial Eigenvalues			Extraction Sums of Squared Loadings		
	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	2.334	77.792	77.792	2.334	77.792	77.792
2	.402	13.406	91.197			
3	.264	8.803	100.000			

Extraction Method: Principal Component Analysis.

Component Matrix[a]

	Component
	1
RR2.9	.864
RR2.10	.911
RR2.11	.871

Extraction Method: Principal Component Analysis.

a. 1 components extracted.

Reliability Test

Case Processing Summary

		N	%
Cases	Valid	33	100.0
	Excluded[a]	0	.0
	Total	33	100.0

a. Listwise deletion based on all variables in the procedure.

Reliability Statistics

Cronbach's Alpha	N of Items
.851	3

C.8 Control Activities

Validity Test

Correlation Matrix[a]

		CA3.2	CA3.2.1	CA3.2.2	CA3.3.2	CA3.3.3	CA3.3.4
Correlation	CA3.2	1.000	.712	.483	.621	.407	.514
	CA3.2.1	.712	1.000	.671	.452	.481	.366
	CA3.2.2	.483	.671	1.000	.339	.704	.619
	CA3.3.2	.621	.452	.339	1.000	.568	.659
	CA3.3.3	.407	.481	.704	.568	1.000	.761
	CA3.3.4	.514	.366	.619	.659	.761	1.000
Sig. (1-tailed)	CA3.2		.000	.002	.000	.009	.001
	CA3.2.1	.000		.000	.004	.002	.018
	CA3.2.2	.002	.000		.027	.000	.000
	CA3.3.2	.000	.004	.027		.000	.000
	CA3.3.3	.009	.002	.000	.000		.000
	CA3.3.4	.001	.018	.000	.000	.000	

a. Determinant = .016

KMO and Bartlett's Test

Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		.714
Bartlett's Test of Sphericity	Approx. Chi-Square	121.231
	df	15
	Sig.	.000

Anti-image Matrices

		CA3.2	CA3.2.1	CA3.2.2	CA3.3.2	CA3.3.3	CA3.3.4
Anti-image Covariance	CA3.2	.339	-.177	.010	-.112	.084	-.087
	CA3.2.1	-.177	.287	-.153	-.061	-.038	.118
	CA3.2.2	.010	-.153	.278	.130	-.104	-.104
	CA3.3.2	-.112	-.061	.130	.375	-.089	-.123
	CA3.3.3	.084	-.038	-.104	-.089	.294	-.119
	CA3.3.4	-.087	.118	-.104	-.123	-.119	.262
Anti-image Correlation	CA3.2	.729[a]	-.568	.032	-.314	.268	-.292
	CA3.2.1	-.568	.641[a]	-.541	-.187	-.132	.430
	CA3.2.2	.032	-.541	.694[a]	.404	-.365	-.386
	CA3.3.2	-.314	-.187	.404	.736[a]	-.268	-.394
	CA3.3.3	.268	-.132	-.365	-.268	.790[a]	-.427
	CA3.3.4	-.292	.430	-.386	-.394	-.427	.703[a]

a. Measures of Sampling Adequacy(MSA)

Communalities

	Initial	Extraction
CA3.2	1.000	.604
CA3.2.1	1.000	.587
CA3.2.2	1.000	.647
CA3.3.2	1.000	.577
CA3.3.3	1.000	.688
CA3.3.4	1.000	.686

Extraction Method: Principal Component Analysis.

Total Variance Explained

Component	Initial Eigenvalues			Extraction Sums of Squared Loadings		
	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	3.789	63.157	63.157	3.789	63.157	63.157
2	.861	14.355	77.512			
3	.762	12.696	90.209			
4	.287	4.787	94.996			
5	.175	2.912	97.908			
6	.126	2.092	100.000			

Extraction Method: Principal Component Analysis.

Component Matrix[a]

	Component
	1
CA3.2	.777
CA3.2.1	.766
CA3.2.2	.804
CA3.3.2	.760
CA3.3.3	.829
CA3.3.4	.828

Extraction Method: Principal Component Analysis.

a. 1 components extracted.

Reliability Test

Case Processing Summary

		N	%
Cases	Valid	33	100.0
	Excluded[a]	0	.0
	Total	33	100.0

a. Listwise deletion based on all variables in the procedure.

Reliability Statistics

Cronbach's Alpha	N of Items
.876	6

C.9 Information and Communication

Validity Test

Correlation Matrix[a]

		IC4.4.3	IC4.4.5	IC4.4.6	IC4.4.7	IC5.1.5
Correlation	IC4.4.3	1.000	.377	.422	.478	.793
	IC4.4.5	.377	1.000	.883	.680	.639
	IC4.4.6	.422	.883	1.000	.737	.654
	IC4.4.7	.478	.680	.737	1.000	.676
	IC5.1.5	.793	.639	.654	.676	1.000
Sig. (1-tailed)	IC4.4.3		.015	.007	.002	.000
	IC4.4.5	.015		.000	.000	.000
	IC4.4.6	.007	.000		.000	.000
	IC4.4.7	.002	.000	.000		.000
	IC5.1.5	.000	.000	.000	.000	

a. Determinant = .016

KMO and Bartlett's Test

Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		.757
Bartlett's Test of Sphericity	Approx. Chi-Square	121.397
	df	10
	Sig.	.000

Anti-image Matrices

		IC4.4.3	IC4.4.5	IC4.4.6	IC4.4.7	IC5.1.5
Anti-image Covariance	IC4.4.3	.342	.049	-.006	.006	-.201
	IC4.4.5	.049	.206	-.143	-.007	-.050
	IC4.4.6	-.006	-.143	.183	-.089	-.009
	IC4.4.7	.006	-.007	-.089	.391	-.076
	IC5.1.5	-.201	-.050	-.009	-.076	.215
Anti-image Correlation	IC4.4.3	.668[a]	.184	-.023	.016	-.742
	IC4.4.5	.184	.739[a]	-.736	-.025	-.235
	IC4.4.6	-.023	-.736	.747[a]	-.331	-.047
	IC4.4.7	.016	-.025	-.331	.905[a]	-.260
	IC5.1.5	-.742	-.235	-.047	-.260	.740[a]

a. Measures of Sampling Adequacy(MSA)

Communalities

	Initial	Extraction
IC4.4.3	1.000	.504
IC4.4.5	1.000	.742
IC4.4.6	1.000	.790
IC4.4.7	1.000	.728
IC5.1.5	1.000	.790

Extraction Method: Principal Component Analysis.

Total Variance Explained

	Initial Eigenvalues			Extraction Sums of Squared Loadings		
Component	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	3.555	71.095	71.095	3.555	71.095	71.095
2	.854	17.086	88.181			
3	.333	6.660	94.841			
4	.151	3.025	97.865			
5	.107	2.135	100.000			

Extraction Method: Principal Component Analysis.

Component Matrix[a]

	Component
	1
IC4.4.3	.710
IC4.4.5	.862
IC4.4.6	.889
IC4.4.7	.853
IC5.1.5	.889

Extraction Method: Principal Component Analysis.

a. 1 components extracted.

Reliability Test

Case Processing Summary

		N	%
Cases	Valid	33	100.0
	Excluded[a]	0	.0
	Total	33	100.0

a. Listwise deletion based on all variables in the procedure.

Reliability Statistics

Cronbach's Alpha	N of Items
.888	5

C.10 Monitoring

Validity Test

Correlation Matrix[a]

		M6.1	M7.1	M7.1.1	M7.1.2
Correlation	M6.1	1.000	.563	.598	.332
	M7.1	.563	1.000	.665	.315
	M7.1.1	.598	.665	1.000	.696
	M7.1.2	.332	.315	.696	1.000
Sig. (1-tailed)	M6.1		.000	.000	.030
	M7.1	.000		.000	.037
	M7.1.1	.000	.000		.000
	M7.1.2	.030	.037	.000	

a. Determinant = .157

KMO and Bartlett's Test

Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		.655
Bartlett's Test of Sphericity	Approx. Chi-Square	55.242
	df	6
	Sig.	.000

Anti-image Matrices

		M6.1	M7.1	M7.1.1	M7.1.2
Anti-image Covariance	M6.1	.590	-.132	-.126	.041
	M7.1	-.132	.484	-.187	.118
	M7.1.1	-.126	-.187	.265	-.239
	M7.1.2	.041	.118	-.239	.474
Anti-image Correlation	M6.1	.823[a]	-.248	-.319	.077
	M7.1	-.248	.685[a]	-.521	.247
	M7.1.1	-.319	-.521	.608[a]	-.673
	M7.1.2	.077	.247	-.673	.572[a]

a. Measures of Sampling Adequacy(MSA)

Communalities

	Initial	Extraction
M6.1	1.000	.597
M7.1	1.000	.633
M7.1.1	1.000	.861
M7.1.2	1.000	.515

Extraction Method: Principal Component Analysis.

Total Variance Explained

Component	Initial Eigenvalues			Extraction Sums of Squared Loadings		
	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	2.606	65.149	65.149	2.606	65.149	65.149
2	.775	19.369	84.518			
3	.444	11.107	95.625			
4	.175	4.375	100.000			

Extraction Method: Principal Component Analysis.

Component Matrix[a]

	Component
	1
M6.1	.772
M7.1	.796
M7.1.1	.928
M7.1.2	.718

Extraction Method: Principal Component Analysis.

a. 1 components extracted.

Reliability Test

Case Processing Summary

		N	%
Cases	Valid	33	100.0
	Excluded[a]	0	.0
	Total	33	100.0

a. Listwise deletion based on all variables in the procedure.

Reliability Statistics

Cronbach's Alpha	N of Items
.820	4