

**DYNAMIC MODEL FOR RISK ANALYSIS OF PICTURE
ARCHIVING COMMUNICATION SYSTEM (PACS) AT HOSPITAL
SELAYANG**

NAZROOL BIN OMAR

UNIVERSITI TEKNOLOGI MALAYSIA

**DYNAMIC MODEL FOR RISK ANALYSIS OF PICTURE ARCHIVING
COMMUNICATION SYSTEM (PACS) AT HOSPITAL SELAYANG**

NAZROOL BIN OMAR

A project report submitted in partial fulfillment of the
requirements for the award of the degree of
Master of Computer Science (Information Security)

**Centre for Advanced Software Engineering
University Technology Malaysia**

NOVEMBER 2008

DEDICATION

To all my family members especially my mother Puan Patimah binti Ibrahim and my
youngest brother Mohammad Akmar bin Omar.
Their love and encouragement is inspiration and motivation for me.

ACKNOWLEDGEMENT

IN THE NAME OF ALLAH THE MOST GRACIOUS AND THE MOST MERCIFUL

Let my gratitude first goes to Allah Subhanahu Wata'ala for allowing and giving me the opportunity and strength to finish this project as well as this course. Secondly, thanks to my family members who always gives me the support and motivation.

I also would like to take this opportunity to thank my supervisor Dr. Rabiah binti Ahmad for and to all CASE lecturers for their guidance, support, advice and teaching. Special thanks also go to Hospital Selayang management and staffs for their cooperation and help.

Lastly but not least, I send my appreciation to my beloved friends and classmates for their encouragement and help for each other during class and outside class. May Allah bless all of us. Amen and thank you.

ABSTRACT

Risk analysis is the best method for every organization to secure their business environment from any undesired hazardous events such as malicious code attack or natural disaster that could cause a lot of losses and impairs business operation. Risk analysis is very important and necessary because the probability of a disaster occurring in an organization is highly uncertain. Hence, the prediction through analysis process is mandatory. Selecting methodology for information security risk analysis is crucial. This project analysis will follow ISO/IEC 27005 Information Security Risk Management Standard. This standard has been widely used as baseline or references by many commercial risk analysis tool developers. The risk analysis is carried out on Pictures Archiving and Communication System (PACS) of Hospital Selayang. The analysis attempts to identify and list the risks that might shut down the system operation and subsequently presented in Dynamic Fault Tree (DFT) as a dynamic model. Dynamic Fault Tree is a method that extends standard fault trees by allowing the modeling of system risks behaviors and interactions with each other over a period of time. At the end of the project risks register will be produced in the form of report. The risk report will benefit Hospital Selayang during overall risk assessment of the Pictures Archiving and Communication System (PACS).

ABSTRAK

Penganalisaan risiko merupakan satu kaedah terbaik bagi sesebuah organisasi untuk memastikan persekitaran perniagaan selamat daripada ancaman merbahaya seperti serangan pengodam atau bencana alam yang boleh menyebabkan perniagaan tergendala sekaligus menyebabkan kerugian yang besar. Penganalisaan risiko sangat penting dan perlu disebabkan oleh kebarangkalian untuk sesuatu bencana itu berlaku dalam organisasi adalah sangat tidak menentu. Justeru satu kaedah ramalan melalui proses analysis perlu dilakukan. Pemilihan kaedah untuk proses analisa risiko perlu dibuat dengan berhati-hati. Analisis dalam projek ini *adalah ISO/IEC 27005 Information Security Risk Management Standard*. Standard ini telah digunakan secara meluas sebagai penunjuk aras dan rujukan oleh ramai pembangun alatan analisa risiko komersial. Penganalisaan risiko dijalankan kepada *Pictures Archiving and Communication System (PACS)* di Hospital Selayang. Analisa cuba untuk mengenalpasti dan menyenaraikan risiko-risiko yang boleh menyebabkan sistem tergendala dan kemudian dimodelkan dalam *Dynamic Fault Tree (DFT)* model. *Dynamic Fault Tree* merupakan satu kaedah yang memperbaharui standard Fault Tree dengan menunjukkan perhubungan antara satu risiko dengan risiko yang lain dalam satu tempoh masa yang tertentu. Di akhir projek ini nanti, satu daftar risiko akan dihasilkan dalam bentuk laporan. Laporan ini akan memberi manfaat kepada Hospital Selayang semasa penilaian risiko yang menyeluruh dibuat pada *Pictures Archiving and Communication System (PACS)*.

TABLE OF CONTENTS

CHAPTER	TITLE	PAGE
	ACKNOWLEDGMENT	iv
	ABSTRACT	v
	TABLE OF CONTENTS	vii
	LIST OF TABLES	xi
	LIST OF FIGURES	xii
	LIST OF APPENDICES	xiii
	ABBREVIATIONS	xv
1.	PROJECT OVERVIEW	
1.1	Introduction	1
1.2	Background of problem	2
1.3	Problem Statement	3
1.4	Project Aim	3
1.5	Project Objectives	4
1.6	Project Scope	4
1.7	Summary	5

2.	LITERATURE REVIEW	
2.1	Introduction	6
2.2	Review of Total Hospital Information System (THIS) Background and Characteristic	7
2.3	Review of Risk Analysis	12
2.4	Review of Dynamic Fault Tree (DFT)	16
2.4.1	Functional dependency gate	17
2.4.2	Spare gate	18
2.4.3	Priority-AND gate	20
2.5	Summary	21
3.	RESEARCH METHODOLOGY	
3.1	Introduction	22
3.2	Project Development Method	22
3.2.1	Preliminary Study of Pictures Archiving and Communication System (PACS)	24
3.2.2	Study of Risk Analysis Methodology and Dynamic Fault Tree	24
3.2.3	Data Gathering	24
3.2.4	Risk Analysis	25
3.2.5	Documentation	26
3.3	Summary	26

4.	RISK ANALYSIS DESIGN	
4.1	Introduction	27
4.2	Risk Analysis Design	28
4.2.1	System Identification	30
4.2.2	Identification of assets	30
4.2.3	Valuation of assets and impact assessment	31
4.2.4	Identification of threats	32
4.2.5	Assessment of threats	32
4.2.6	Identification of vulnerabilities	33
4.2.7	Assessment of vulnerabilities	33
4.2.8	Estimation of risk	34
4.2.9	Model the Risk Using DFT	38
4.3	Summary	38
5.	IMPLEMENTATION AND RESULT	
5.1	Introduction	39
5.2	System-Related Asset Statement	39
5.3	Threat Statement	40
5.4	Vulnerability Statement	40
5.5	Risk Statement	41
5.6	Summary	43

6.	CONCLUSION	
6.1	Introduction	44
6.2	Summary of Research Finding	44
6.3	Theoretical Contributions and Implications	45
	6.3.1 Risk Analysis Technique	46
	6.3.2 Analysis Success Factor	46
6.4	Practical Contributions and Implications	48
6.5	Limitations and Suggestion for Future Work	48
6.6	Concluding Remarks	51
	REFERENCES	52

LIST OF TABLES

TABLE	TITLE	PAGE
2.1	Truth table for FDEP gate	18
2.2	Truth table for Spare gate	20
2.3	Truth table for PAND gate	21
4.1	Asset Priority	31
4.2	Asset Value and Impact	31
4.3	Threat Frequency	32
4.4	Vulnerability Assessment Level	33
4.5	Risk Likelihood of Occurrence Matrix	35
4.6	Impact Severity Rating Definitions	35
4.7	Risk Level Matrix	36
4.8	Risk Level Description	36
5.1	Risks Level of PACS	42

LIST OF FIGURES

FIGURE	TITLE	PAGE
2.1	Components of THIS	9
2.2	J2EE Architecture	11
2.3	Functional dependency gate	18
2.4	Spare gate	19
2.5	Priority-AND gate	20
3.1	Research Methodology	23
4.1	Phases in ISO/IEC 27005 Information Security Risk Management Standard	28
4.2	Risk Analysis Process Flow	29
4.3	Risk Level Determination Process Flow	37

LIST OF APPENDICES

APPENDIX	TITLE	PAGE
A	On-Site Interview Questions	54
B	Hospital Selayang Personnel	57
C	Asset Identification Worksheet	58
D	Asset Valuation Worksheet	62
	a) Asset Priority and Impact	62
	b) Priority Level for Assets	64
	c) Impact Level for Assets	64
E	Threat-source Identification Worksheet	65
	a) Threat-source Identification Description	65
	b) Threat Source Description	68
	c) Threat Motivation Description	69
	d) Targeted / Affected Asset Description	69
F	Threat Assessment Worksheet	70
	a) Threat Frequency and Impact	70
	b) Threat Frequency Description	72
G	Vulnerability Threat Pairs List	73
H	Vulnerability Assessment Worksheet	78
	a) Vulnerability Likelihood Assessment	78
	b) Vulnerability Likelihood Level Description	81
I	Risk Estimation Worksheet 1	82
	a) Risk Identification and Level	82
	b) Risk Likelihood of Occurrence Matrix	85

	c)	Likelihood Definitions	85
	d)	Impact Severity Rating Definitions	86
	e)	Risk Level Matrix	86
	f)	Risk Level Description	87
J		Risk Estimation Worksheet 2	88
	a)	DFT model for Top / Main Risk	88
	b)	DFT Model for Main Risk no. 1	89
	c)	DFT Model for Main Risk no. 2	90
	d)	DFT Model for Main Risk no. 3	91
	e)	DFT Model for Main Risk no. 4	92
	f)	DFT Model for Main Risk no. 5	93
	g)	DFT Model for Main Risk no. 6	94
K		Security Control Analysis Worksheet	95
	a)	Security Control Level and Implementation	95
	b)	Security Control Level Description	96

ABBREVIATIONS

THIS	Total Hospital Information System
DFT	Dynamic Fault Tree
PACS	Picture Archiving Communication System
NIST	National Institute of Standards and Technology

CHAPTER 1

PROJECT OVERVIEW

1.1 Introduction

The growth of e-health services such as online medical advice, online pharmacies, and online patient record; both in public and private medical sector are inevitable. The proliferation and dependency of medical online system in healthcare sector in Malaysia has fueled up the need to protect the systems from any kind of threat to ensure the continuity of the healthcare services. It is acknowledged how important for a business to implement information security management in securing their ICT assets in order to staying in business, no matter in what circumstances befall. The primary process in information security management is risk analysis; a process to identify threats and vulnerabilities, analyze them to ascertain the exposures, and highlight how the impact can be eliminated or reduced. Risk analysis will provide a basis for risk evaluation, risk treatment and risk acceptance.

This project focuses on analyzing the risk faced by ICT based health institution that runs several ICT systems to support their daily operation. Hospital Selayang is chosen as the subject because it is the first public hospital in Malaysia that fully implemented with Total Hospital Information System (THIS). Pictures Archiving and Communication System (PACS) is one of the system that runs under THIS.

This project is outlined in six chapters. The first chapter is for project overview. Chapter 2 transcribes literature review and chapter 3 provides research methodology which consists of project development method and technique. Chapter 4 describes flow of risk analysis design. Chapter 5 presents implementation and result of this project. Chapter 6 provides conclusion of this report which covers summary of research finding and contribution of this research.

In this chapter, the report is organized into seven topics. It is started by introduction of this project paper and followed by background of problem, problem statement, project aim, project objectives, and project scope. This chapter is ended by chapter summary.

1.2 Background of problem

Hospital Selayang (SH) is an ICT-based hospital. It is located in Selayang, Selangor and equipped with 960 inpatient beds and 20 clinical disciplines. It has been designed and constructed for a Total Hospital Information System (THIS) environment. It is the first hospital in Malaysia and the world to operate with THIS which covers all aspects of hospital operation. The ultimate aim of this hospital is to be paperless and filmless hospital. It is critical to ensure THIS always in continuous operation. Therefore, security is very important and plays a vital role in protecting THIS asset and information. It was obvious that risk analysis is a method in determining which countermeasures need to be implemented in fighting against wide range of potential threats.

1.3 Problem Statement

There are many questions regarding the risk analysis outcomes but for this project, it will address and answer some problems that as stated as follows:

- a. Examine what are potential threats for Pictures Archiving and Communication System (PACS) that needs to be comprehensively identified and analyzed.
- b. To identify critical asset that potentially exposure to loss as well incident that likely to happen if the asset is compromised by the threat.
- c. Proper vulnerability investigation must be conducted to search and determine for flaws and weakness exist in Pictures Archiving and Communication System (PACS) environment.
- d. To study and determine Dynamic Fault Tree (DFT) model can be used to model the information security risk in dynamic model.

1.4 Project Aim

The aim of this project is to perform risk analysis on the Pictures Archiving and Communication System (PACS) and to model the identified risks using dynamic model method called Dynamic Fault Tree (DFT) modeling technique. The analysis will be based on ISO/IEC 27005 Information Security Risk Management Standard. The analysis shall benefit Hospital Selayang in overall risk management process especially in determining what controls are needed to reduce the risks to an acceptable level.

1.5 Project Objectives

The objectives that will be specified below explain what kind of knowledge the study is expected to obtain. It also should give a clear notion of what is to be described, determined, identified and analyzed.

- a. To study existing and potential threats in Pictures Archiving and Communication System (PACS).
- b. To carry out risk analysis to Pictures Archiving and Communication System (PACS) and asset related to it based on suitable technique.
- c. To determine whether dynamic system modeling can be used in information security risks.
- d. To produce risk analysis report which consists of risk identification and risk estimation details as an input for Hospital Selayang to be used in their overall risk management process.

1.6 Project Scope

Project scope will indicate the limitation of this project in terms of its process, coverage, collaborators, participants and potential products.

- a. The unit of analysis is Hospital Selayang which is located in Gombak, Selangor, a health institution.
- b. The risk analysis is conducted on Pictures Archiving and Communication System (PACS).

1.7 Summary

This chapter has described introduction of this project report, background of problem, problem statement, project aim, project objectives and project scope. These topics have clearly stated and justify why this project is worth developed and implemented. Next chapter will discuss literature review.

CHAPTER 2

LITERATURE REVIEW

2.1 Introduction

This chapter is divided into five topics. First topic is introduction of this chapter. It follows by review of Total Hospital Information System (THIS) background and characteristic. After that, review of risk analysis and review of Dynamic Fault Tree (DFT) will be discussed. Lastly this chapter will be closed by chapter summary.

Literature review comprises three steps. Firstly is identifying the relevant sources, secondly extracting the relevant information and lastly reviewing the all the information. The sources will be acquired from library, internet and Hospital Selayang. These sources can be in many types such as books, articles, previous published journals, documentations and site interview. After that, relevant information from the review is used to construct key concepts and ideas as well as to justify the explanation or argument in the research paper.

2.2 Review of Total Hospital Information System (THIS) Background and Characteristic

Hospital Selayang is a hospital with 960 inpatient beds and 20 clinical disciplines located in Selayang in the Gombak District, Selangor. It has been designed, constructed and equipped for a Total Hospital Information System (THIS) environment with the ultimate aim of paperless and filmless hospital operation. It is the first hospital in Malaysia and the world to operate with THIS covering all aspects of its operation. In order to meet the objective of the state of the art facility, a highly qualified effective organization, operation and management has to be ensured for the success of this hospital.

The need to balance quality of care and efficiency has increasingly become a key driven for the management of healthcare institutions today. The adoption of best practices is the approach to improve operational and clinical productivity. Recognizing the importance of this issue, the emergence of THIS is come to reality. Human resources of technology experts and healthcare professionals enable THIS to provide clients with total data solutions tied to the national standards, as well as tailored to the client's specific needs. As a result, THIS is able to offer clients the most time efficient and cost effective solutions available in the market today for hospital information system.

In order to have effective hospital information, it is important to have an ideal hospital information system design focus on integration of clinical in addition to financial and administrative applications. Therefore, THIS is an extensive and wide-ranging healthcare information suite that covers a complete flow of patient processes. It allows information management across organizations. THIS is uniquely designed into modules of which new functions can easily be added on to the system providing the ability to support changes in requirements to the hospital's workflow. THIS is reduces paperwork and repetitive data entry steps, plus allows healthcare institution to take full advantage of its information systems.

THIS is a 'Made in Malaysia' product. It is developed over a period of 5 years by Kompakar eHealth Tech Sdn Bhd (eHealth), a subsidiary of Sistem Kompakar Sdn Bhd. During this period, valuable input from the specialist of Putrajaya Hospital and Putrajaya Clinic core team ensured that our THIS is fully compliance for local environment operations. THIS went through several progresses with continued forward momentum to incrementally enhance the system. THIS contains over 200 functions, which covers both administrative and clinical functions. THIS is neatly designed into several modules that cover all aspects of a patient record from clinical to administrative.

THIS automates the activities of hospital by incorporating routines such as billing, messaging, check-listing, task-listing, hot-listing, stock control, lab reporting and asset tracking, thus facilitate the encoding of the hospital's operational procedures into simple and prompt response. THIS helps as a good managerial tool to provide total, cost-effective access to complete and more accurate patient care data. In a nutshell, THIS improved healthcare delivery by providing medical personnel with better data access, faster data retrieval, higher quality data and more versatility in data display. Figure 2.1 below shows components of THIS.

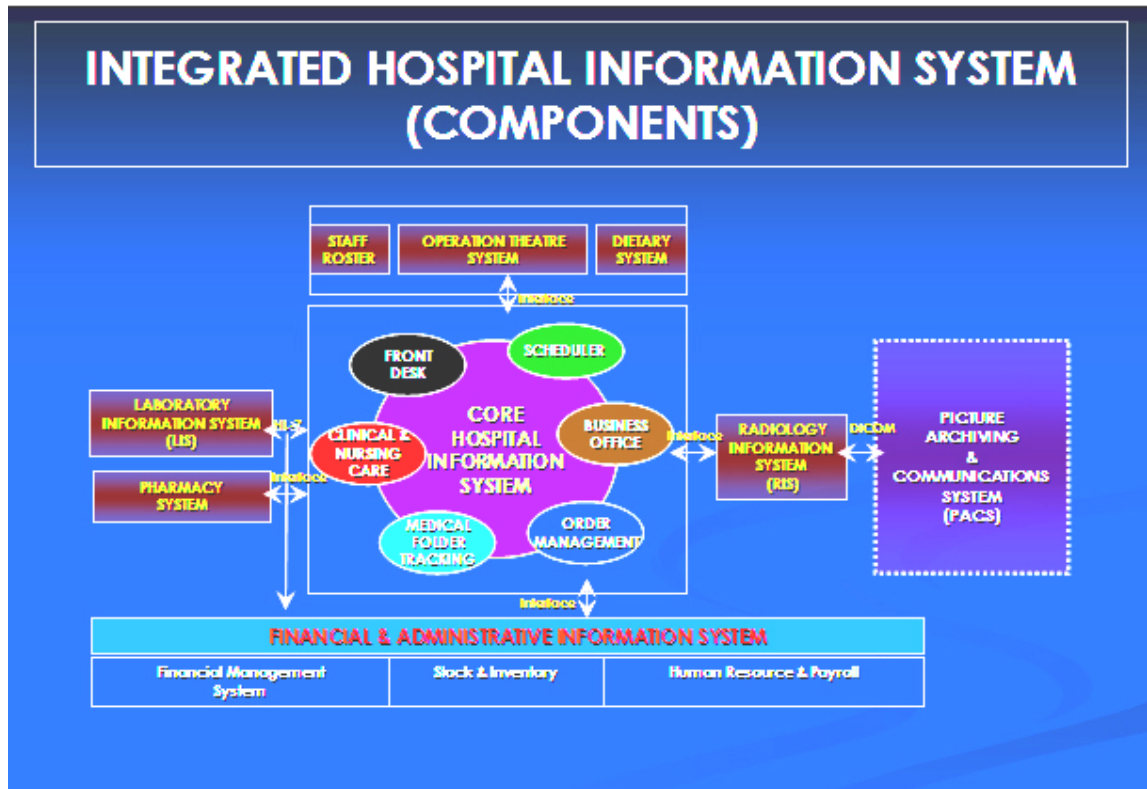


Figure 2.1: Components of THIS

The various suites of THIS can be used together to build comprehensive patient medical, financial and administrative records from the initial point till the final charge. Because of its modular nature, THIS can be implemented in totality or in parts as the need may be. The applications can be further customized to meet the specific requirement of any healthcare establishment. Its modularity provides a mechanism to enhance the scope and functionality of the package, ensuring seamless integration with new suites.

Total Hospital Information System is a comprehensive healthcare information package developed using the J2EE Framework, which ensures that the solution remains open and extensible. The bandwidth requires by the system is very minimal (256K) which can be easily accommodated by MOH who had planned to have a 1MB bandwidth. As mentioned, J2EE architecture has been deployed in the solution development, which defines the standard for developing multi-tier enterprise application. This platform emphasized on standardized, modular components capable of handling details of application behaviors automatically without complex programming.

Figure 2.2 shows J2EE architecture that consists of four architectural layers J2EE architecture standard that consists of four architectural layers. This standard includes complete specifications and compliance test to ensure portability of application across wide range of platform. Application Development Framework (ADF) is adopted in solution development, which is empowered by Oracle JDeveloper 10g. It provides a flexible and end-to-end application infrastructure. ADF is a comprehensive layer for J2EE developers that accelerate and support rapid application development for its ready-to-use J2EE Design Pattern implementations and metadata driven components. It offers drag and drop ease of use throughout the lifecycle that increases productivity in development. It simplifies building applications as a set of business services with Web, Wireless and Rich Client interfaces. Application developed on ADF framework is well-architected, high performance and portable.

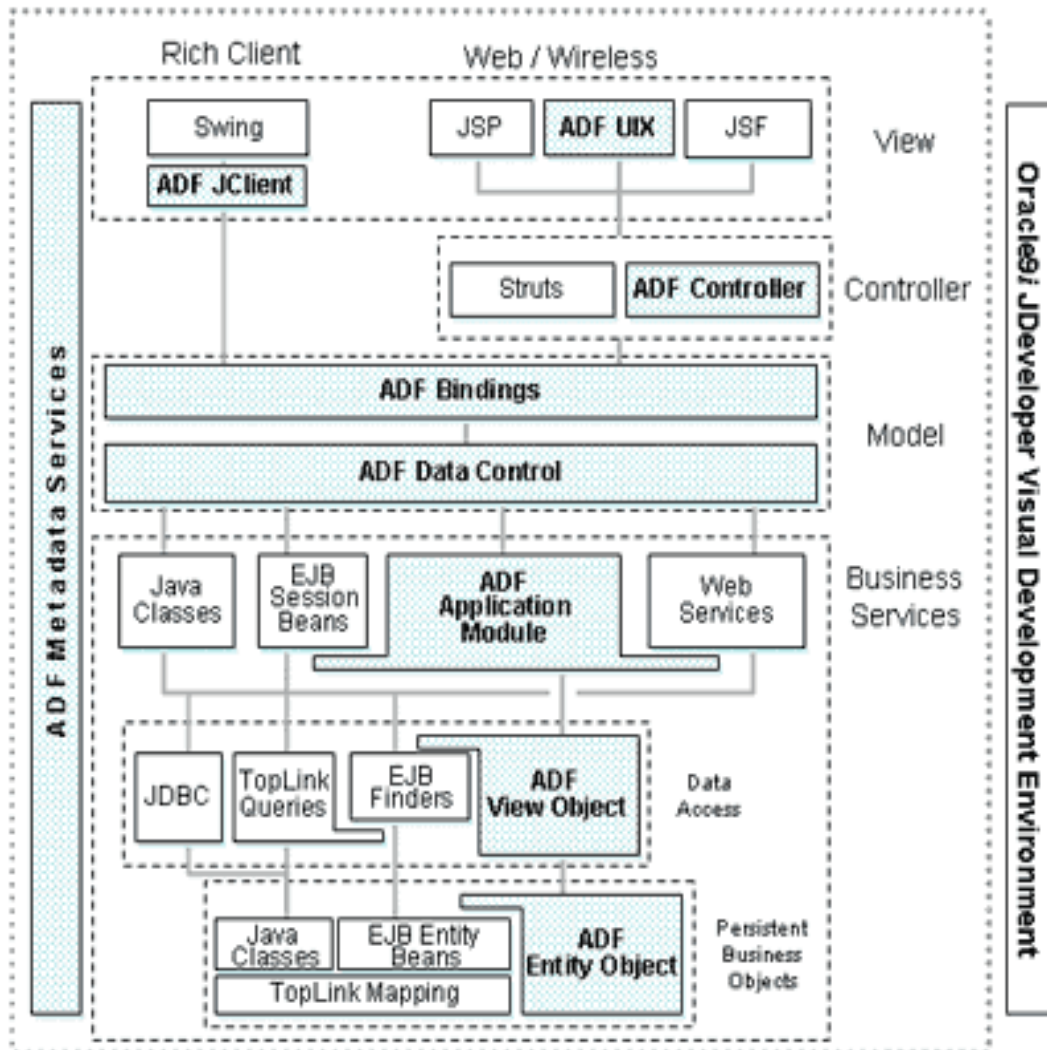


Figure 2.2: J2EE Architecture

2.3 Review of Risk Analysis

Risk Analysis can be understood as a procedure to identify and to estimate threats and vulnerabilities, analyze them to ascertain the exposures, and highlight how the impact can be eliminated or reduced by producing a report or risk model for top management attention (Baliwangi, Arima, Artana and Ishida, 2007). It also a process to determine what security is appropriate for a system or environment. It involves identifying the most probable threats to an organization and analyzing the related vulnerabilities of the organization to these threats.

Regardless of what kind of business and sector, possible threats and vulnerability that could arise inside or outside the organization need to be assessed. Although it is difficult to determine the exact nature of potential threat or their resulting consequences, but it is beneficial to perform a comprehensive risk analysis of all threats that can realistically occur to the organization. Whatever the threat and vulnerability the organization has, the goals of business recovery planning are to ensure the safety of customers, employees and computer system during and following a disaster.

The probability of disaster to occur should be determined and analyzed. The risk analysis should determine how likely the potential threat can happen and how significant the impact on various functions or departments within the organization. Therefore all locations and facilities should be included in the risk analysis. Items to consider in determining the threats should include, but not be limited to: geographic location, topography of the area, proximity to major sources of power, bodies of water and airports, degree of accessibility to facilities within the organization, history of local utility companies in providing uninterrupted services, history of the area's susceptibility to natural threats, proximity to major highways which transport hazardous waste and combustible products.

Potential exposures may be classified as natural, technical, or human threats. Natural threats for example are internal flooding, external flooding, internal fire, external fire, seismic activity, high winds, snow and ice storms, volcanic eruption, tornado, hurricane, epidemic, tidal wave and typhoon. Technical threats includes power failure/fluctuation, heating, ventilation or air conditioning failure, malfunction or failure of CPU, failure of system software, failure of application software and telecommunications failure. Human threats can be robbery, bomb threats, embezzlement, extortion, burglary, vandalism, terrorism, civil disorder, chemical spill, sabotage, explosion, war, biological contamination, radiation contamination, hazardous waste, vehicle crash, airport proximity, work stoppage (Internal/External), and popular computer crime.

Risk analysis role to measure and highlight all these threats. Risk analysis can be carried out in several ways. The most popular are quantitative risk analysis, qualitative risk analysis and hybrid risk analysis (Meritt, 2005). Every method has it own phase and steps. Choosing the right methodology for your analysis is very important and based on what your organization interest in. Risk analysis helps in the identification of the assets and resources at risk and vulnerabilities that might allow the threats to be realized. By conducting risk analysis, what safeguards already in place can be known and suggest more control which may be implemented to achieve an acceptable level of risk and increase overall awareness.

Quantitative analysis does use two elements: Probability and Likely Loss. It identifies the specific envelope in which the losses and safeguards exist. It is based substantially on objective processes and metrics (Wold and Shriver, 1997). It requires an increased degree of effort in deterring the cost values and calculations. It however, presents its results in a management-friendly form of monetary values, percentages, and probabilities. The major advantage of a quantitative impact analysis is that it provides a measurement of the impacts' magnitude, which can be used in the cost-benefit analysis of recommended controls. The Annual Loss Expectancy (ALE) is usually produces as the output. The disadvantage is that, it requires substantial time and personnel resources

to complete the quantitative process and depending on the numerical ranges used to express the measurement, the meaning of the quantitative analysis may be unclear so requiring the result to be interpreted in a qualitative manner. Others drawbacks of this analysis is no accurate probability database available so probability is usually unique to case, expected loss hard to establish not easy to accept. That why this method is in fairly limited use.

Qualitative risk analysis is simpler and widely used. This analysis uses simple calculations and uses procedure in which it is not necessary to determine the dollar value of all assets and the threat frequencies or the implementation costs of the controls. It assesses the impact and likelihood of the identified risks in a rapid and cost-effective manner for example using ranking (Blank (no effect), Low, Medium, High). By evaluating the priority of risks with consideration to impact on the project's cost, schedule, scope and quality objectives, qualitative risk analysis provides a foundation for a focused quantitative analysis or risk response plan. The inputs to the qualitative risk analysis process are organizational process assets, project scope statement, risk management plan and risk register. The output of the qualitative risk analysis process is an updated risk register that includes relative ranking or priority of project risks, risks grouped by categories, lists of risks requiring response in the near term, list of risks for additional analysis and response, watchlist of low priority risks and trends in qualitative risk analysis results. The main advantage of the qualitative analysis is that it prioritizes the risks and identifies areas for immediate improvement in addressing the vulnerabilities. The disadvantage of the qualitative analysis is that it does not provide specific quantifiable measurements of the magnitude of the impacts, therefore making a cost-benefit analysis of any recommended controls difficult.

Hybrid method is a selected combination of two methods quantitative and qualitative. It can be used to implement the components utilizing available information while minimizing the metrics to be collected and calculated. It is less numerically intensive (and less expensive) than an in-depth exhaustive analysis.

There is a risk analysis model that has the dynamic capability. It is called System Dynamics (SD) (Xu, 2004). This modeling technique is used to create a model the dynamics and behaviors of the analysis. It uses a flexible approach in representing an appropriate level of detail and variables as well as incorporating the dynamics of changing model variables. Fundamentally SD uses two connected entities: levels and rates, also known as stocks and flows. Stocks represent quantities of tangible and/or intangible entities. The symbol for a stock is a rectangle. Typical examples of stocks include people, dollars, computers, morale, attitude, and risk. Flows are equivalent to valves, that is a device setting for how much quantity may flow into or out of a stock in a given time period. Stocks and flows can flexibly take on different values in each period. Using SD, the cause-effect relationship linking among components in a system could be obtained and a better understanding of system behavior expected. It allows easy insertion of delays and non-linearity. Consequently, a better operation and maintenance management could be reached by a better understanding of system behavior. Output from an SD methodology is typically expressed by a Behavior over Time graph. This graph depicts the relationships among the variables of threats, attacks, and budget over a period of time. By viewing these relationships it can be hypothesized as to what possible modifications may be beneficial to the system.

2.4 Review of Dynamic Fault Tree Model

Dynamic fault tree (DFT) is actually extension and enhancement version of standard fault tree technique which uses static gate to depict interactions between components (Dugaan and Assaf, 2003). Fault tree is a model that used for quantitative and qualitative analysis. A fault tree becomes a dynamic fault tree whenever a dynamic gate is present. It is considered as a system dynamic modeling methodology when it becomes dynamic fault tree.

DFT is able to model complex behaviors and interactions between components or combinations of component failures that can lead to system failure in sequence manner (Boudali, Crouzen and Stoelinga, 2007). Like normal fault tree, DFT shows logical framework and logical relationship between an event (failure) and its causes but in dynamic and flexible model. A dynamic fault tree model precisely documents which failure scenarios have been considered and which have not. Dynamic fault tree analysis can be used to support engineering and management decisions, trade-off analysis as well as risk analysis.

Traditional fault tree cannot model sequence dependent failures, in which the order that events occur is important. The complex behaviors and failures sequences are best modeled by Input/Output Interactive Markov Chains (I/O-IMC) that is well-known in engineering field. But the development of a correct Markov model for a complex system can be difficult. Special purpose gates for modeling sequence dependencies are defined to solve the fault tree drawbacks and resulting the fault tree works as a Markov chain. The approach is to use the fault tree with new defined dynamic gates for model development that equivalent to the Markov chain. This approach is called dynamic fault tree model and considerably simpler than the equivalent Markov chain.

Dynamic fault tree is a graph in the form of upside-down tree. It has leaves, nodes and arrows. Leaves are used to represent basic events (BE) that correspond to failure event (usually a component failure) in the system and characterized by failure rate or failure probability. Nodes are represented by gates. Elements are combination of basic events and gates. Arrows is to show causal relations between the elements and nodes. Top-node is the “root” node that models the system failure. Failure is propagated from leaves to root.

Several special purpose gates have been added to the traditional fault tree gates (Moscardini, Loutfi and Al-Qirem, 2007). These special dynamic gates capture sequence dependencies which frequently arise when modeling computer systems. The special dynamic gates include:

- a. Functional dependency gate for modeling situations where one component’s correct operation is dependent upon the correct operation of some other component
- b. Spare gate
- c. Priority-AND gate for modeling ordered ANDing of events.

2.4.1 Functional dependency gate

The Functional Dependency (FDEP) gate is used to indicate that all dependent events are forced to occur in a particular order when the trigger event occurs. The separate occurrence of any of the dependent events has no effect on the trigger event. The FDEP gate has one trigger event and can have one or more dependent events. The FDEP gate is showed in figure 2.3.

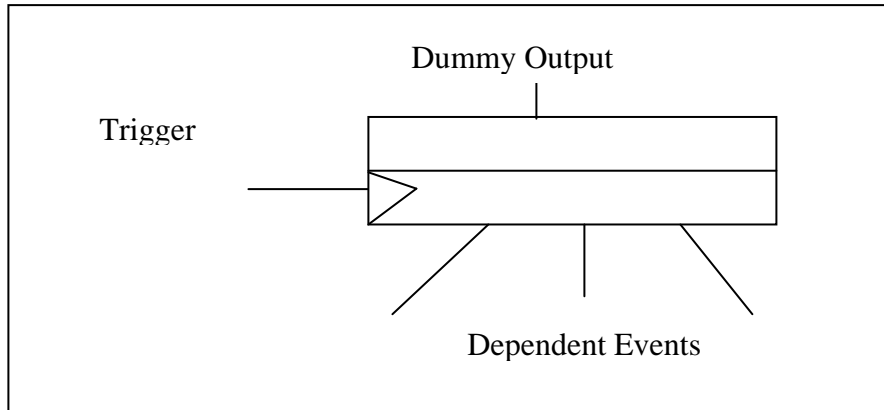


Figure 2.3: Functional dependency gate

Dependent events are repeated events that are present in other parts of the fault tree. Dependent events are either basic events or spare events. The trigger event can be a terminal event or outputs of any AND gate, OR gate, or dynamic gate (PAND, SPARE, SEQ, or FDEP). Generally, the output of an FDEP gate is not that important; however, it is equivalent to the status of its trigger event. The truth table for an FDEP gate is showed in table 2.1.

Table 2.1: Truth table for FDEP gate

Trigger	Output	Dependent Event A	Dependent Event B
T	T	T	T
T	F	T/F	T/F

2.4.2 Spare gate

The Spare gate is used to model cold, warm, and hot spares in the system. Cold event is a basic event that fires after some delay when it is activated. It cannot fire of its own accord when dormant. Warm event fires after some delay and more likely to fire when active. Hot event also fire after some delay but being dormant or active has no

influence on the likelihood of the event firing. The Spare gate is used to indicate that the output occurs if and only if all spare events (inputs) occur. Spare gate is showed in figure 2.4

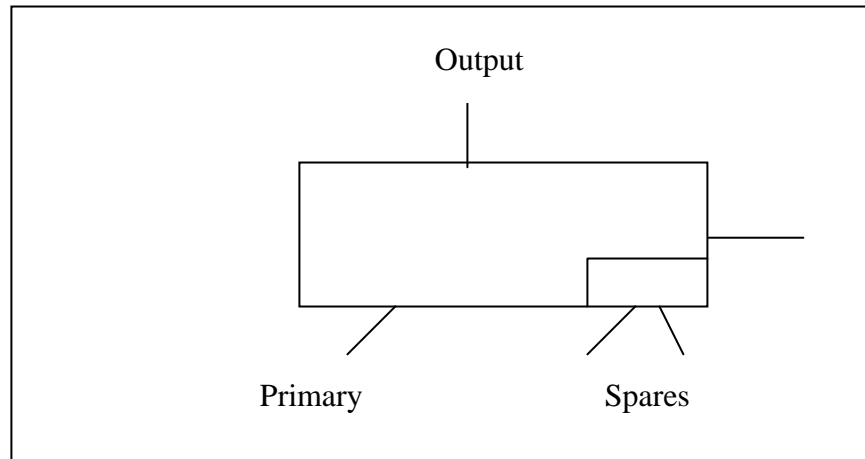


Figure 2.4: Spare gate

Spare events are a special event type used to model spare usage. A spare event can be an input to only a SPARE gate or an FDEP gate, which is described later in this article. While spare events are similar to basic events in functionality, they allow only repair rates as inputs to accurately model the temporal behavior. The dormancy factor of the spare event indicates the ratio of failure rate in the standby mode and the failure rate in the operational mode. A spare event can have a spare pool, which represents the number of identical instances of that spare component (event). For example, if a spare pool of an event is two, there are two identical spare components of that spare event. All inputs of a Spare gate are spare events. A Spare gate can have multiple inputs. The first event (left-most event) is known as the primary input, and all other inputs are known as alternative inputs. The primary event is the one that is initially active or powered on, and the alternative inputs are initially in standby mode. After a failure, the active/powered unit that is the first available spare from left to right will be made active. If all units are failed, then the spare will be considered as failed. The truth table for the Spare gate is in table 2.2.

Table 2.2: Truth table for Spare gate

A	B	Output
T	T	T
T	F	F
F	T	F
F	F	F

2.4.3 Priority-AND gate

The Priority AND gate also known as the PAND gate, is used to indicate that the output occurs if and only if all input events occur in a particular order. The order of occurrence is the order in which the input events are connected to the PAND gate from left to right. Figure 2.5 shows The PAND gate.

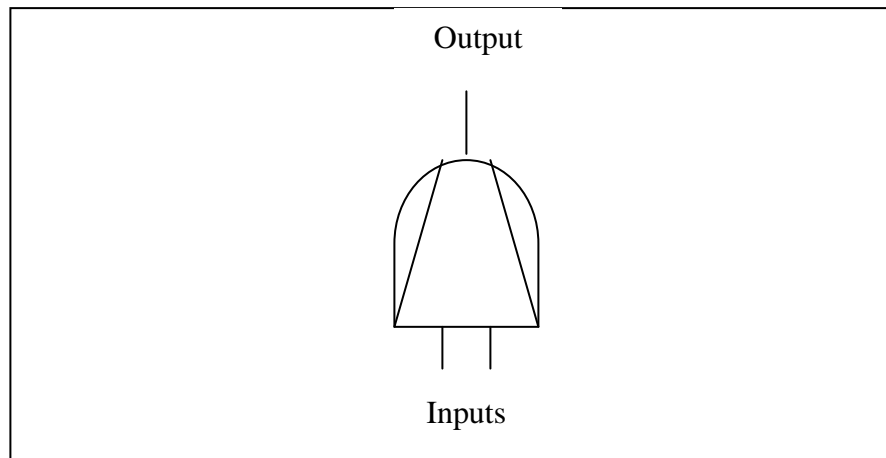


Figure 2.5: Priority-AND gate

The output of a PAND gate can be the top event or an intermediate event. The inputs can be basic events or outputs of any AND gate, OR gate, or dynamic gate (PAND, SPARE, SEQ, or FDEP). Items need to fail in temporal order from left to right to trigger the event. The PAND gate also supports a single input. When only a single input exists, then the occurrence of that input will trigger the event. The truth table for a PAND gate follows. In column A, T(1) indicates that the input event occurred first, and T(2) indicates that the input event occurred second. The Boolean equation for a PAND gate is $T = A * B$, where A occurs and then B occurs. Table 2.3 is the truth table of PAND gate.

Table 2.3: Truth table for PAND gate

A	B	Output
T(1)	T(2)	T
T(2)	T(1)	F
T	F	F
F	T	F
F	F	F

2.5 Summary

This chapter has discussed the literature review for the project. It has outlined the introduction of this chapter, review of Total Hospital Information System (THIS) background and characteristic, review of risk analysis and review of Dynamic Fault Tree (DFT). Next chapter will provided research methodology for this project.

CHAPTER 3

RESEARCH METHODOLOGY

3.1 Introduction

The methodology for the realization of this project is described in this chapter. It is defined in three topics which are introduction of this chapter, project development method and chapter summary. In project development method, research methodology for this project will be explained in five sub-topics which are preliminary study of pictures archiving and communication system (PACS), study of risk analysis methodology and dynamic fault tree, conduct data gathering, conduct risk analysis and write risk analysis report.

3.2 Project Development Method

The project methodology for risk analysis of this project is divided into five steps. The steps are showed in figure 3.1 below and will be described afterward.

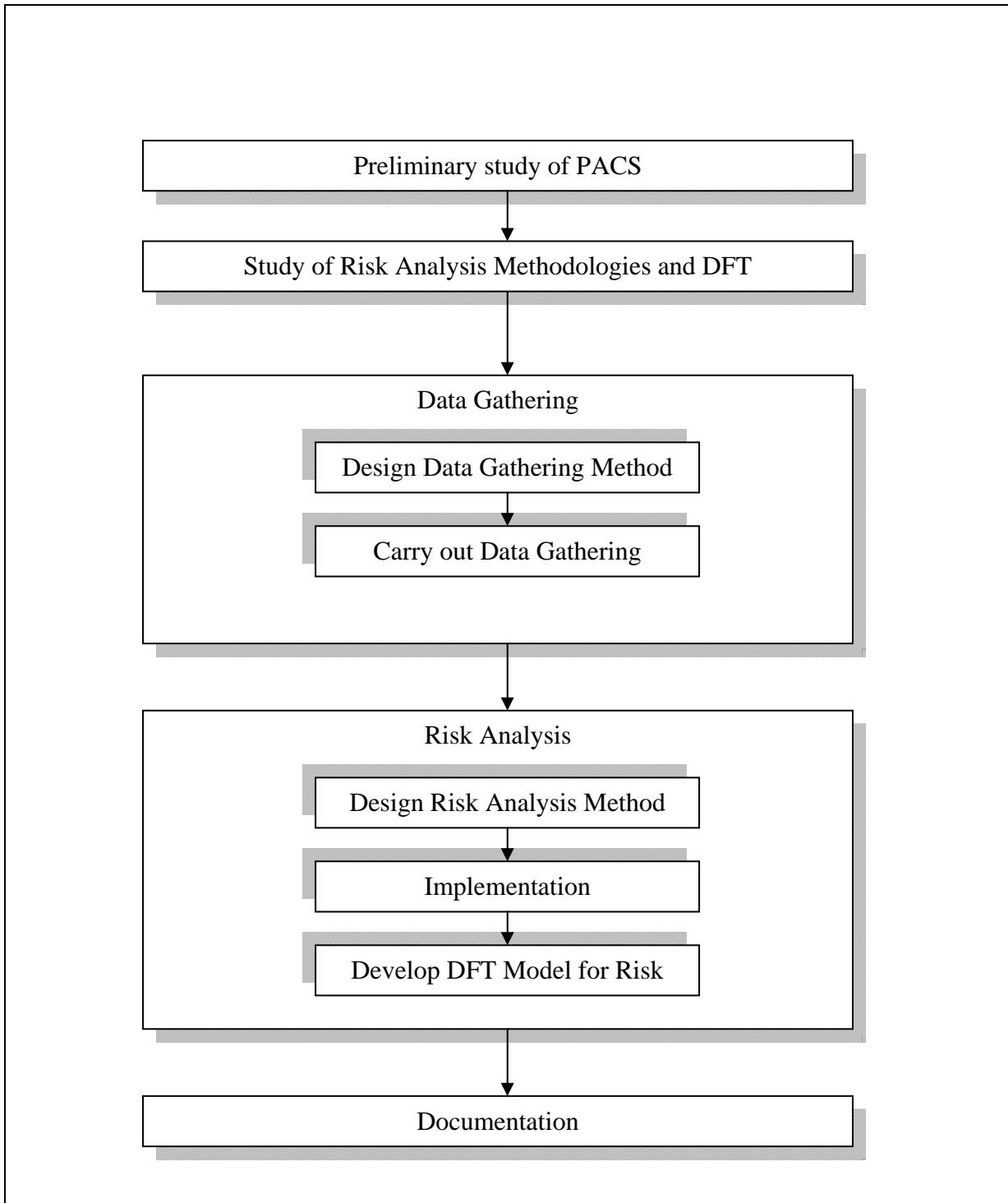


Figure 3.1: Research Methodology

3.2.1 Preliminary Study of Pictures Archiving and Communication System (PACS)

It is necessary to study the subject of the research in order to understand the real scenario and problem. In this research, Pictures Archiving and Communication System (PACS) of Selayang Hospital is the subject. All aspect of PACS needs to be explored such as user, administrator, technology, hardware, system, physical infrastructure as well as the operation. Understanding how PACS fits in the Selayang Hospital and how it operates is the key to scan for drawbacks in their implementation especially in security matters. A preliminary and unofficial visit to Selayang Hospital will be done to examine and observe how Selayang Hospital does their business. Information about the hospital also can be enquired via website and brochures. This part is the most important because here we can synchronous problems that have been foreseen with the real problems faced by the Selayang Hospital.

3.2.2 Study of Risk Analysis Methodology and Dynamic Fault Tree

A method or technique to do the risk analysis must be determined before the analysis is carried out. In order to effectively implement the chosen method of analysis, the method must be well studied and understood. In this phase, the specific and details about the risk analysis and Dynamic Fault Tree is explored by reviewing some literature from current journals, thesis, books and article.

3.2.3 Data Gathering

In this step, data gathering method will be design before conducting data gathering is conducted. For this project, the methods of data collection are:

- a. Observation - Observation will be used to study the big picture of problems or situation the PACS. Observation is done by visiting Radiology Department of Hospital Selayang to see the routine operation of PACS.
- b. On-site interview - On-site interview is used to get information about threat or vulnerability by having face to face interview with correspondent personnel. On-site interview question and answer conducted for this research is presented in **Appendix A**. Hospital Selayang personnel who involved in the on-site interview is listed in **Appendix C**.
- c. Document review - Document review is conducted to obtain more information about the Selayang Hospital ICT environment. Among the document are:
 - Current security policy
 - System documentation
 - Organization mission and vision statement
 - Client charter
 - Standard procedures

3.2.4 Risk Analysis

In this phase, risk analysis method will be designed. The design of the risk analysis is based on ISO/IEC 27005 Information Security Risk Management Standard. The design adapts risk analysis phase of the standard to come with this risk analysis method. The risk analysis method for this project will be explained in details in next chapter. Implementation of risk analysis is according to the designed method. The analysis is conducted to identify the risks of PACS based on data gathered during data

gathering phase. The found risks will be presented in a dynamic model using Dynamic Fault Tree (DFT) model

3.2.5 Documentation

Risk report will be produced in a precise report that lets Selayang Hospital management take considered decisions on how to act in response to the risk identified. The report will contain all the potential risks presented in tables and models. Every risk identified will be modeled and explained in the report.

3.3 Summary

This chapter has outlined three sub-topics which introduction, project development method and summary. In project development, all steps in conducting the whole research is explained and discussed. Next chapter will explain more details about risk analysis design for this project.

CHAPTER 4

RISK ANALYSIS DESIGN

4.1 Introduction

In this chapter the design of risk analysis will be discussed in details. This chapter outlines eight steps of the risk analysis in accordance with ISO/IEC 27005 Information Security Risk Management Standard.

This project adapts the ISO/IEC 27005 Information Security Risk Management Standard in conducting the risk analysis because it is very comprehensive and has been referred by many countries such as New Zealand and Australia for their risk assessment standards.

The structure of this chapter consists of introduction, risk analysis design and chapter summary. In risk analysis design, eight sub-topics are outlined to explain the steps of the risk analysis design.

4.2 Risk Analysis Design

The design of risk analysis in this research only adapts the second phase in ISO/IEC 27005 Information Security Risk Management Standard. The phase is risk analysis phase. Only risk analysis phase is adapted because the scope of this project is risk analysis therefore phases which related to other functions of risk assessment such as risk treatment and risk communication is not included. Figure 4.1 shows all phases in ISO/IEC 27005 Information Security Risk Management Standard.

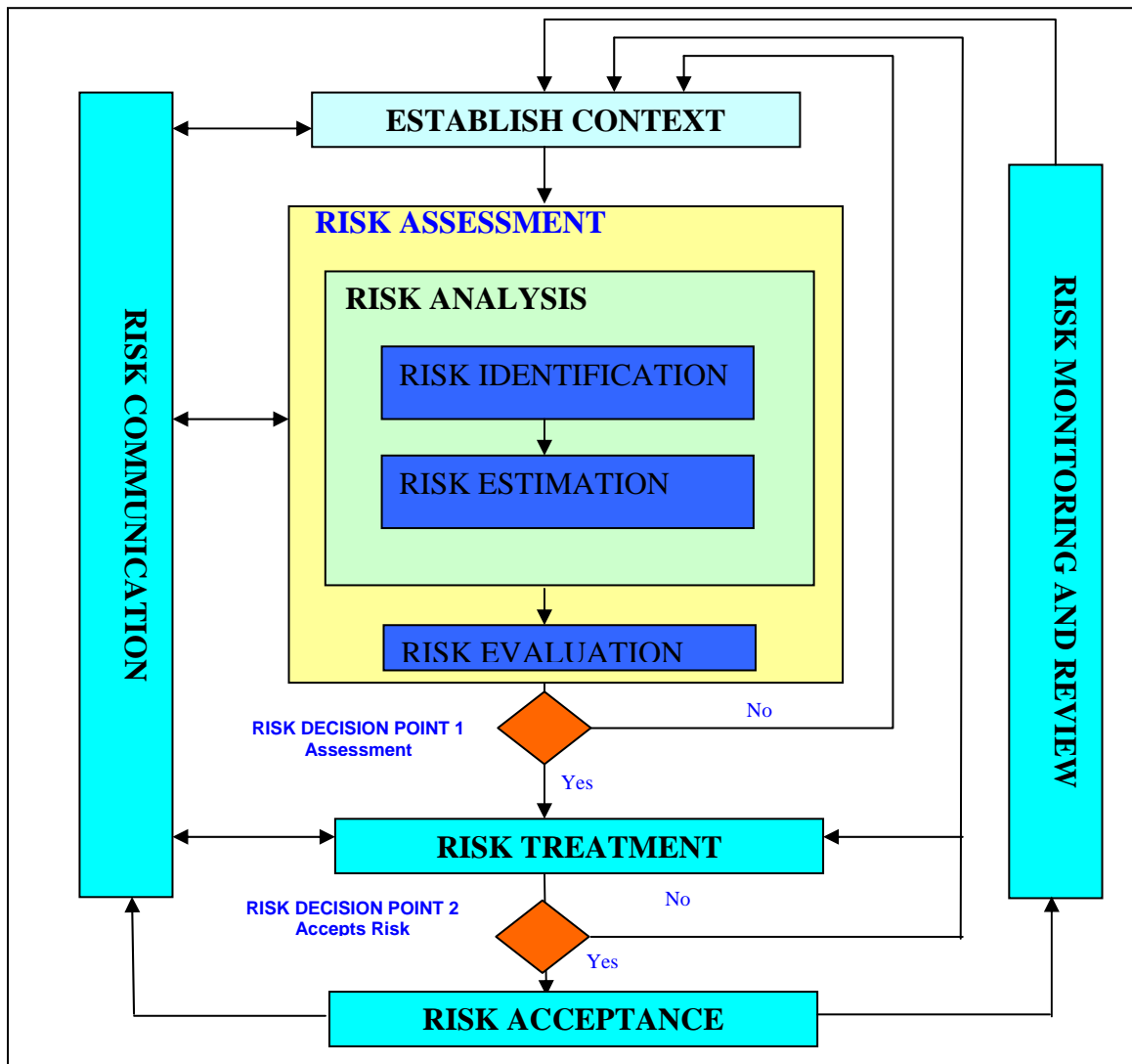


Figure 4.1: Phases in ISO/IEC 27005 Information Security Risk Management Standard

Based on the risk analysis phase, risk analysis design is developed by adapting risk identification and risk estimation processes. The analysis design follows all steps propose by ISO/IEC 27005 Information Security Risk Management Standard but it also adds up some features from other standards such as adoption of tables and worksheets from AS/NZS 4360:1999 Australian Standard Risk Management and NIST Risk Management Guide for Information Technology Systems in order to produce good and reliable design.

As the result from the adaption of the standards mention before, the risk analysis design is developed and shows in figure 4.2. The design comprises of nine steps. The design is constructed in such way to prevent the analysis from becoming too qualitative as well as too quantitative. The analysis should be combinations of all methods where necessary so that the found risks can be dynamically modeled. It is also the reason why commercial analysis tools such as CRAMM, @RISK, OCTAVE, CORAS, ISRAM AND CORA are not used for the analysis; simply because these tools are already defined as qualitative or quantitative method by their developers.

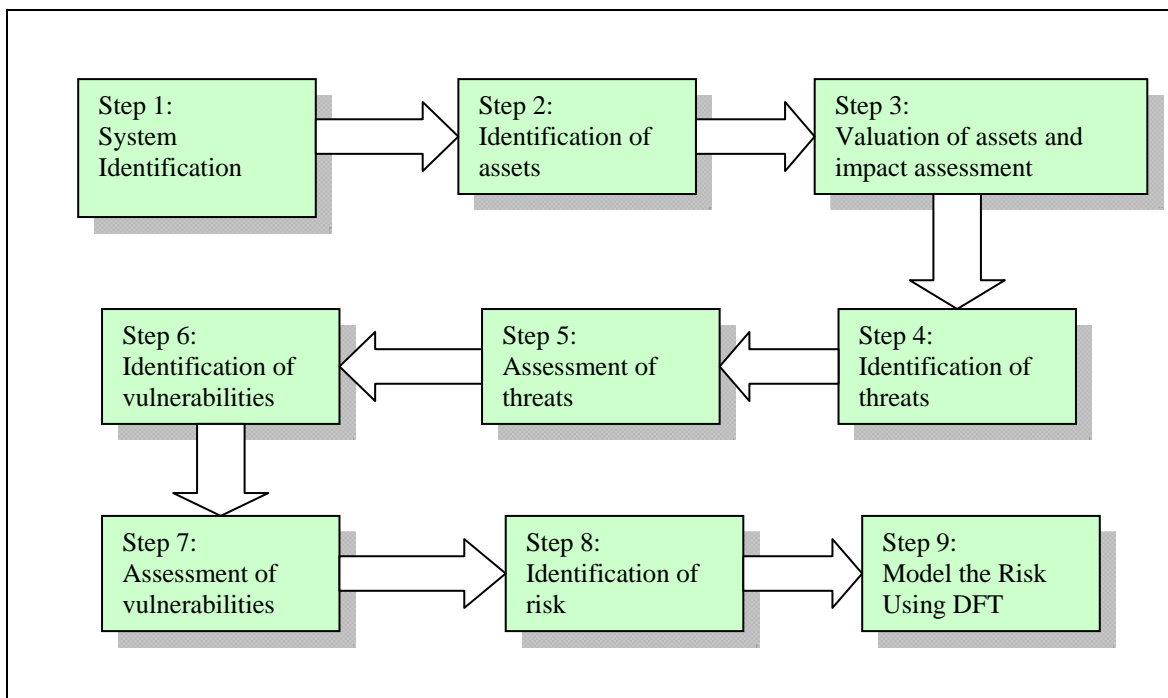


Figure 4.2: Risk Analysis Process Flow

Every step in the risk analysis design is supported with activities that must be completed to get the step deliverables. Next steps cannot be started if deliverable from previous step not in place. Activities for each step and how the deliverable is achieved are explained below in respective sub-topics.

4.2.1 System Identification

In this step the scope or boundary of the analysis is determined. The facts that risks will be similar for some systems or organizations; and sometimes varies on case-by-case basis, it is necessary to use a well-structured systematic analysis process. It is vital for researcher at this point to comprehensively identify what, why and how problems and concerns can arise as the basis for further analysis.

4.2.2 Identification of assets

This step is carried out to identify assets of the studied system. System asset identification process includes the following:

- a. Identifying and documenting the system architecture.
- b. Identifying system and subsystem assets, including all hardware, software, and ancillary equipment.
- c. Identifying system interfaces (external and internal).
- d. Identifying system boundaries

The information about the asset is gathered during on-site interview and by reviewing system documentation report and policy. Asset is divided into four categories

which are Information and ICT, People, Environment, Business Process / Activities. Asset identification worksheet is used to identify the assets and showed in **Appendix C**.

4.2.3 Valuation of assets and impact assessment

In this step, the identified assets will be assigned with values that represent the importance of the assets to the organization and asset value and impact in organization's operation using Asset Valuation Worksheet presented in **Appendix D**. Asset priority is determined using Asset Priority Table showed in table 4.1. Asset value and impact is determined using Asset Value and Impact Table showed in table 4.2 below. Both tables are adopted from Risk Management Guide for Information Technology Systems.

Table 4.1: Asset Priority

Priority	Priority Description
High	Asset is critical to business operation.
Moderate	Asset is important to business, may change to backup procedures or offline.
Low	Asset is non-vital, sometimes unnecessary for normal procedures.

Table 4.2: Asset Value and Impact

Level	Description
Sensitive	Asset is critical, loss is permanent or very time-consuming to replace, disclosed information is very sensitive, and there is intention of using it.
Moderate	Important asset may be replaced with some effort, may be a one-time loss, disclosed information is somewhat sensitive, and person receiving information does not intend to use it for malicious purposes.
Non-sensitive	Non-critical asset may be replaced easily, disclosed information is not sensitive, and person receiving confidential information has no intention of using it.

4.2.4 Identification of threats

The goal of this step is to identify the potential threats and make a list of them. Threat-source Identification Worksheet which is presented in **Appendix E** is used to identify the potential threats. The source, motivation, targeted / affected asset and description of the threats are also being taken into consideration. Threats are identified based on assets that have been identified in Asset identification worksheet.

4.2.5 Assessment of threats

This step is the process of assessing the probability of the threats. Threat Assessment Worksheet format showed in **Appendix F** is the tool used for assessing the threats. The frequency and impact of the threats is determined using Threat Frequency table showed in table 4.3. The table is adopted from NIST Risk Management Guide for Information Technology Systems.

Table 4.3: Threat Frequency

Level	Description
High	Occurs regularly or on a weekly basis.
Moderate	Occurs occasionally or a few times per year.
Low	Rarely or never occurs.

Every threat is also studied to determine if the threat can cause system denial of service, unauthorized modification, system failure, communication loss or unauthorized disclosure.

4.2.6 Identification of vulnerabilities

The aim of this step is to develop a list of system vulnerabilities that could be exploited by the potential threat. Vulnerability/Threat Pairs List format showed in **Appendix G** is used to determine and gather vulnerabilities associated with the system environment. Vulnerabilities database from NIST is used to get the list of online system vulnerabilities. Only vulnerabilities related to PACS are included in the Vulnerability/Threat Pairs List and they are determined through a vulnerabilities walkthrough session with ICT department staffs of Hospital Selayang as stated in Hospital Selayang personnel in **Appendix C**.

4.2.7 Assessment of vulnerabilities

The main purpose of this step is to assess how severe the identified vulnerabilities to occur or in other word the level of easiness of the vulnerabilities to occur. Vulnerability Assessment Worksheet is used in as a tool in assesses the vulnerabilities and presented in **Appendix H**. The level of vulnerabilities is determined using vulnerability assessment level table showed in table 4.4. This table is also adopted from NIST Risk Management Guide for Information Technology Systems.

Table 4.4: Vulnerability Assessment Level

Level	Vulnerability Assessment
High	Very easy to be exploited.
Moderate	Can be exploited with some available information.
Low	Hard to be exploited.

4.2.8 Estimation of risk

After identifying and assessing threats and vulnerability, the risks will be identified. Risks are vulnerabilities that are exploited by credible threats to create havoc and chaos to system. The risks will be identified and estimated using Risk Estimation Worksheet 1 which is presented in **Appendix J**. In the worksheet, several main risks will be identified to be the top risks so that it can become top events in Dynamic Fault Tree model. From the main risk, related risks that correlated to the main risk will be identified based on threats and vulnerabilities.

Every risk will be given risk level. Risk level will be calculated according to risk type. For main risk the level will be determined by the correlation in dynamic fault tree (DFT) model. The risk will be calculated based on the dynamic gate used to correlate the main risk with the related risks. The formula is as follows:

- a. For 'OR' Gate = $(\text{Sum of all related risks numerical values}) / (\text{count of related risks})$
- b. For 'AND' Gate = $(\text{sum (Risk N} - (\text{average of related risks}))) / (\text{count of related risks})$
- c. For 'FDEP' Gate = $(\text{Trigger Risk value} - (\text{average of all related dependent risks numerical values}))$
- d. For 'SPARE' Gate = $(\text{Spare 1} - (\text{spare 2} - (\text{spare 3} - (\text{spare 4} \dots))))$

The risk level for related risks is determined by the likelihood of occurrence and impact severity. Before the level is calculated, the likelihood of occurrence and impact severity must be determined. The likelihood of occurrence for each related risk is determined by mapping the effectiveness of existing controls with probability of threat occurrence. The effectiveness of existing controls is derived from Security Control Analysis Worksheet presented in **Appendix K** meanwhile probability of threat occurrence is derived from Threat Assessment Worksheet presented in **Appendix F**.

Risk Likelihood of Occurrence Matrix table which is adopted from NIST Risk Management Guide for Information Technology Systems showed in table 4.5 is used to determine likelihood of occurrence for each threat.

Table 4.5: Risk Likelihood of Occurrence Matrix

Effectiveness of Existing Controls	Probability of Threat Occurrence		
	Low	Moderate	High
Low	Moderate	High	High
Moderate	Low	Moderate	High
High	Low	Low	Moderate

The level of impact severity is determined using Impact Severity Rating Definitions table presented in table 4.6.

Table 4.6: Impact Severity Rating Definitions

Magnitude of Impact	Impact Definition
High (100)	Occurrence of the risk: (1) may result in human death or serious injury; (2) may result in the loss of major tangible assets, resources or sensitive data; or (3) may significantly harm, or impede the mission, reputation or interest.
Moderate (50)	Occurrence of the risk: (1) may result in human injury; (2) may result in the costly loss of tangible assets or resources; or (3) may violate, harm, or impede the mission, reputation or interest.
Low (10)	Occurrence of the risk: (1) may result in the loss of some tangible assets or resources or (2) may noticeably affect the mission, reputation or interest.

After likelihood of occurrence and impact severity are determined, the level of related risk will be determined using Risk Level Matrix showed in table 4.7.

Table 4.7: Risk Level Matrix

Risk Likelihood	Risk Impact		
	Low (10)	Moderate (50)	High (100)
High (1.0)	Low $10 \times 1.0 = 10$	Moderate $50 \times 1.0 = 50$	High $100 \times 1.0 = 100$
Moderate (0.5)	Low $10 \times 0.5 = 5$	Moderate $50 \times 0.5 = 25$	Moderate $100 \times 0.5 = 50$
Low (0.1)	Low $10 \times 0.1 = 1$	Low $50 \times 0.1 = 5$	Low $100 \times 0.1 = 10$

The risk level also can have numerical value as stated in risk level table when quantitative calculation needs to be carried out. In this analysis, quantitative value is needed when calculating the level of main risk using formula as stated before. Risk Level Description table showed in table 4.8 explain meaning of each risk value labels. The overall process flow of determining the risk level is presented in figure 4.3.

Table 4.8: Risk Level Description

Risk Level	Risk Description & Necessary Actions
High	The loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets or individuals.
Moderate	The loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets or individuals.
Low	The loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets or individuals.

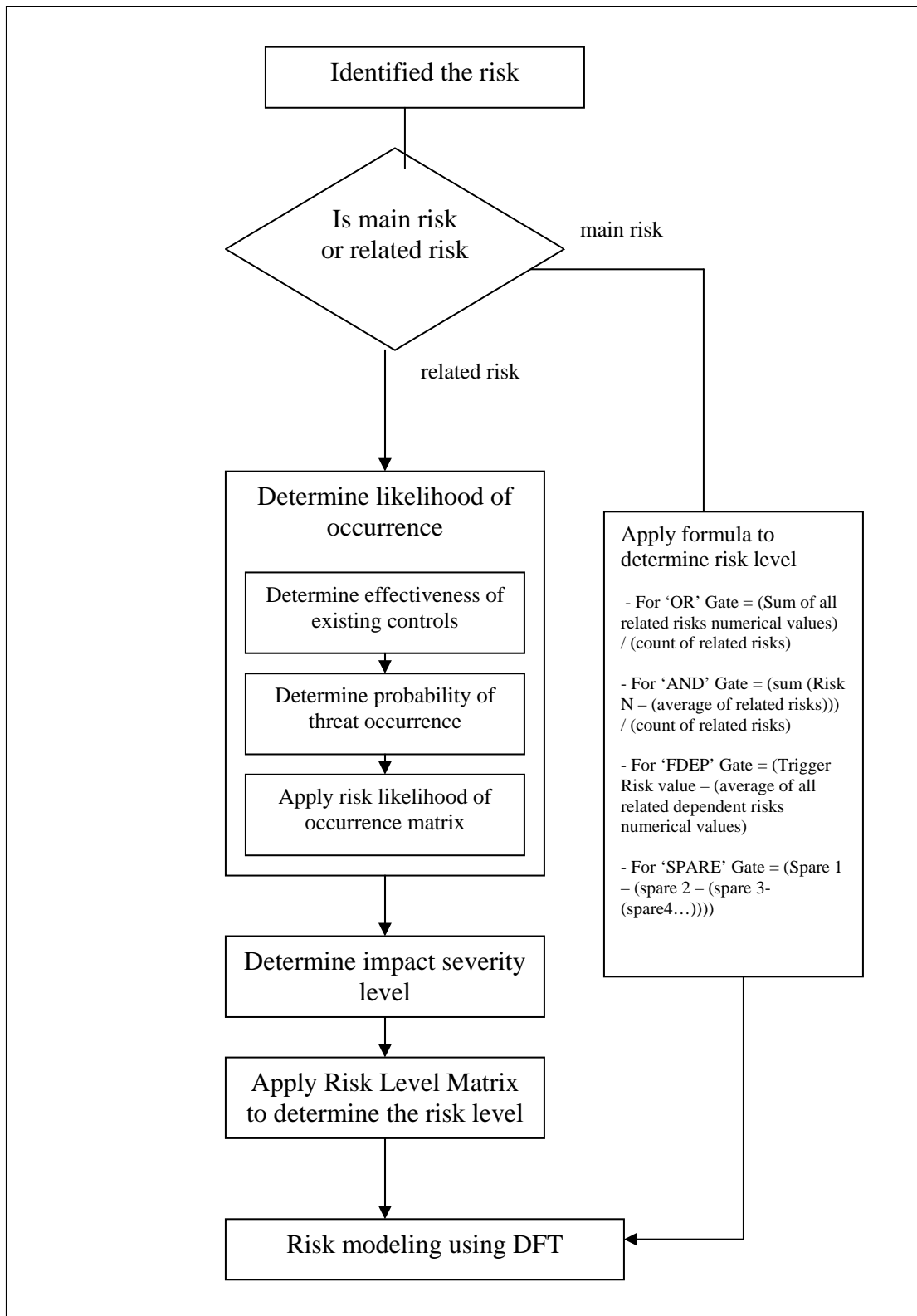


Figure 4.3: Risk Level Determination Process Flow

4.2.9 Model the Risk Using DFT

In this step the level of risk will be calculated and modeled using a good self-explanatory model so-called Dynamic Fault Tree Technique will be used. In this step, DFT model will be developed in accordance with the identified risk and show how this risks emerge and may affect the normal operation of system if the risk occurs.

DFT model helps system owners understanding and analyzing risks faced by their system in easier and more effective mode. Completed DFT model with calculated level of risk is presented Risk Estimation Worksheet which is showed in **Appendix J** and **K**.

4.3 Summary

This chapter has described all the steps that will be taken in order to conduct risk analysis for Pictures Archiving Communication System (PACS) in Hospital Selayang. There are nine steps all together. They are basically adapted from ISO/IEC 27005 Information Security Risk Management Standard and also added some feature from other standard wherever necessary and appropriate. As addition, the last step is partly based on Dynamic Fault Tree technique in order to produce a dynamic model in analyzing the risks. Next chapter will discuss the implementation and result from the risk analysis.

CHAPTER 5

IMPLEMENTATION AND RESULT

5.1 Introduction

The result of conducting risk analysis for PACS of Hospital Selayang will be explained and discussed in this chapter. The result will benefit Hospital Selayang in form of having risk register report. The risk register is well expressed in dynamic fault tree (DFT) model so that the model can be easily self-explained. Hospital Selayang could use the report as a reference and tool in conducting its overall risk assessment process especially in formulating the control to counterattack or reduce the risk.

This chapter is outlined in six topics which are introduction, system-related asset statement, threat statement, vulnerability statement and risk statement and chapter summary.

5.2 System-Related Asset Statement

System-related asset is identified using two tools which are Asset Identification Worksheet and Asset Valuation Worksheet. There are 27 assets have been identified as the system related assets. There are 14 of assets are leveled as high for priority in business, meanwhile 10 assets are moderate and another three is under low level. For

impact of losses level 19 assets are sensitive, 7 assets are moderate and only 1 is non-sensitive.

5.3 Threat Statement

In order to identify the potential threat to system, Threat-source Identification Worksheet and Threat Assessment Worksheet are used. There are 21 threats have been identified. Three threats are cause by natural source, 11 threats are under human source and seven threats are from environment / physical source. There are nine threats motivated by deliberation, five threats under accidental and seven threats are motivated by environmental.

Statistically, nine of the identified threats are happen at low frequency, 11 are moderate and only one in high frequency. There are 15 threats that can cause denial of service to PACS meanwhile 10 potential threats is identified to cause unauthorized modification and 13 threats can cause system failure. There are 13 threats can cause communication loss is 13 and 12 threats are related to unauthorized disclosure.

Getting all related threats in hand, vulnerabilities may be identified as every threat is linearly correlated to one or more vulnerabilities. The process of identifying vulnerabilities may come easy and precise with the available potential threats list.

5.4 Vulnerability Statement

Vulnerabilities are identified in the PACS system using Vulnerability Threat Pairs List and Vulnerability Assessment Worksheet. These tools are helping in matching the vulnerabilities with the potential threats. There are 65 vulnerabilities have been

identified from the given threats. Four vulnerabilities are classified under environment and infrastructure source. Vulnerabilities related to hardware source are six, for software there are 18 vulnerabilities, 10 vulnerabilities for communications, for personnel there are eight vulnerabilities and 19 vulnerabilities for documents / procedural source. From 65 vulnerabilities, 22 vulnerabilities are identified as low, 28 of them as moderate and 15 are considered as high.

Having all the information about threat and vulnerability provided, the research continued with the risk estimation task. In the risk estimation phase, risk will be identified and modeled so that a comprehensive risk report of studied system can be made for real.

5.5 Risk Statement

Risks are disastrous events that can be identified by analyzing the exploitable vulnerabilities by credential threats. Risk also can be well understood if it can be described as what can happen and how it can happen. Six main risks have been identified and given risk value. The main risks are identified based on six main sources of threats and vulnerabilities. Table 5.1 present the main risks and their related risk with risk level value.

Table 5.1: Risks Level of PACS

No.	Risk	Risk Level
1.	System down due to environment and infrastructure break down or disaster	L
1.1	System assets are stolen or destroyed because building can be broken easily	L
1.2	Power trip cause system malfunction due to burnt hardware	L
1.3	System assets ruined by flood or water due to location	L
2.	System cannot function because of poor hardware management and configuration	L
2.1	Hardware failure due to outdated and deteriorated agents	L
2.2	Hardware loss due to lack of hardware management	L
2.3	Hardware malfunction due to maintenance fault	L
3.	System compromised and malfunction due to poor software management, configuration and installation	M
3.1	System not perform the right job due to user mistake or complicated interface	L
3.2	System information is compromised by unauthorized person	M
3.3	System halting due to attack by hacker or disgruntled personnel	M
4.	System cannot perform the job properly due to communications problem or poor communication device configuration	M
4.1	Sensitive information lacking due to poor protection of communication line	M
4.2	Communication loss due to improper device maintenance	L
5.	System cannot be used or function because of personnel flaws or outsider interferences	M
5.1	Suspended system operation due to no operator or operator mistakes	M
5.2	System out of service due to personnel or outsider disruptive actions	M
6.	System cannot recover from disaster due to lack or ineffective of documents / procedural for security purposes	L
6.1	Business loss due to late response to disaster or to foresee problem	L
6.2	Reputation loss due to no procedure to secure data and business	L

Depth analysis has been done to dynamically show the correlation of main risks with the related risk. The analysis has determined that all six main risks are having 'OR' relationship with their respective related risks because each related risks are independent from each other. So only 'OR' gate is used in the DFT model as presented in Risk Estimation Worksheet 2 and attached as **Appendix K**.

5.6 Summary

Risk analysis which has been carried out throughout the research in order to produce the risk report has been outlined and presented in this chapter. The report consists of System-Related Asset Statement, Threat Statement, Vulnerability Statement and Risk Statement. The risks identified were presented in dynamic fault tree model. The risk model will be presented and suggested to Hospital Selayang as the output of the analysis which will be benefited them in risk management process. They can also use the report as reference in detailed information security risk assessment.

CHAPTER 6

CONCLUSION

6.1 Introduction

In this chapter, summary for the whole project done will be given. It covers the introduction, summary of research finding, theoretical contributions and implications, practical contributions and implications, limitations and suggestion for future work and concluding remarks.

6.2 Summary of Research Finding

Performing a risk analysis involves finding and documenting the risks in a risk registry or report. Pinpointing these risks can be a time-consuming task that will require assistances of the experts of the hardware and software as well as the risk owner. It is become more difficult if the analysis is done using a new method that has never been done before because there is no benchmark as references.

In this research, several risks are identified and presented in DFT model. The risks exist in the system is not in perturbing state as many of them are in low and medium level. This is because Hospital Selayang has already had some security countermeasures and feature implemented. But the found risks still risky and need to be

given enough attention and action. Every risk in the list is capable to trigger disastrous incident if left without any treatment.

The found risks are able to be presented in DFT model but only 'OR' gate is involved. More dynamic gate should be appears in the DFT, but given the current risks state of Hospital Selayang, other gates is unable to be included in the model. In this case, it is because all identified risks can occur on its own and have no direct effect to each other.

This analysis also suggested that Hospital Selayang should carry out overall risk assessment. The reason is to make sure the organization more realize and aware with the existence of security risks in online system. With risk assessment a comprehensive risk management can be achieved as every risk is controlled and monitored according to organization need and scope. Hospital Selayang will benefit lots from it. Concentration also needs to be given to the staff in form of comprehensive security knowledge and awareness. Information Technology staff also have to had good knowledge about every technology used in the system, hardware wise as well as software wise.

6.3 Theoretical Contributions and Implications

Risk analysis is an excellent tool that allows systematic examination of risk and uncertainty of any operational especially in healthcare. Integration of system interactions and human interactions expose medical online system to lots of explicit threat and vulnerability. Risk analysis can benefit health institution to quantify the overall level of risk for their systems and treating the risk to an acceptable level.

6.3.1 Risk Analysis Technique

Risk analysis is very beneficial for organization to some extent. It is need to be conducted in determining what level of security that organization has implemented and what security is appropriate for their system or environment. If the security level is not in the acceptable condition, risk analysis will help the security manager to make decisions on how to counterattack undesired risk to comfort level. Risk analysis also provides:-

- i) A tool for organization to know whether their system is secured or not by identifying threats and vulnerabilities exist that can deteriorate the system operation.
- ii) Risk analysis help organizations to identify all risks faced by the system. The identified risk will be prioritized to make the sure the most dangerous risk is first treated.
- iii) Risk analysis provides organization a mechanism for every member to understand and aware with security concern.
- iv) Risk analysis also the best way for security manager to communicate risk among all members of organization.

6.3.2 Analysis Success Factor

Several factors are identified as the success key in this research. These factors are important for researcher to get output from risk analysis project. Some of the factors are already well known by security expert. Attention to these factors should be paid by researchers right before begin the research because it will help them determine the path of their project. The factors are as follows:-

- a. **Top management support** - Whether can or cannot research is allowed to be done at an organization depends on the top management consensus. Getting their approval doesn't mean the research is guaranteed the result. It must be supported by their involvement in form having them in as could as possible in progress meeting so that they can see the benefit and progress of the project.
- b. **ICT and normal staff involvement** - Research cannot be continued without some input and feedback from targeted staffs from the organizations that provided all the information needed. Information from both ICT and normal user of studied system are equally important.
- c. **Clear scope of risk analysis** - Determine the scope of analysis give an idea how to carry out the research is in the desired path and ensure it can be finished as scheduled. It also helps in reaching the aim or the output. Clear scope should be determined before starting the project.
- d. **Risk analysis templates or tools** - Using template to get data and to do the analysis is very helping. There should be templates or tools used throughout the research so that it can be organized and conducted properly. The tools such as interview questionnaire, on-site questions template, data worksheet and tables, analysis and report format must be a part of the analysis.
- e. **Clear targeted output** - Researcher should know what he want from the research done. Having in mind the targeted output and how to present it, give mileage to ensure the project is come to the result.

6.4 Practical Contributions and Implications

The risk analysis technique used for this research is combination of conventional method with dynamic model to become dynamic risk analysis. The analysis is called dynamic mainly because the risks are presented in Dynamic Fault Tree (DFT) model which gives more understandable view for top managements to comprehend what risks they are facing in their organizations in relation to studied system. Dynamic risk analysis model addressed what risks can cause the system to come into malfunction state. If more than one risk associates, the model will show their connection and dependencies to each other.

The dynamic risk analysis for ICT system is new compared to qualitative and quantitative techniques. But it becomes to gain more attention from researchers because of its advantages. Besides that, this new technique is very interesting to use as it is comprised of pictures and figures in the model instead of table and numbers in conventional methods.

6.5 Limitations and Suggestion for Future Work

Although risk model developed in this research is dynamic model, the threats and vulnerabilities found using this technique are no different compared to normal analysis. The challenge is to use the dynamic fault tree (DFT) model to information security risks. DFT is previously used in engineering and financial field and currently introduced in modeling fault tolerant computer system. It is never been used to model information security risks. It is a challenge to determine whether the identified risks are related or depended on each other. If there are relations among each other, researcher also needs to identify and determine how they are related. Answer to this question is the key to answer whether DFT is capable to model information security or not.

Having the relationships of risks in hand, the next challenge is to transcribe the relationship into a model diagram using the correct notation for every type of relationship for example to use “AND” or “OR” notation. After that all modeled relationships will be combined as one model.

Other challenges exist during the analysis come from the threats and vulnerabilities identification phases at the organization. To have good co-operation from the organization is vital task. Meeting and discussion have to be done with the organization’s representatives to brief them about the objectives and framework of the analysis and research to get the approval and to be carried out.

During the data gathering, to get adequate information many interview session have been done with the staff. Getting them to understand information security from researcher point of view took some effort as some of them are not familiar with latest security jargon. Explanation also needed to be given so that they can give the desired answer.

Not having currently implemented security control documented made the job even harder as identification has to be started from the scratch. Security incident log also not well documented resulted difficulty in formulating and identifying the potential threats and vulnerabilities.

This research foresees potential related future research area that can be developed by new researchers in information security area. Listed below are some of the future researches that can be considered by new researcher to contribute in information security field.

- a. **Further extensions DFT modeling capabilities** – Dynamic Fault Tree (DFT) implemented in this project takes into considerations basic ‘or’ and ‘and’ dynamic gates to show the correlation among the risks. New research

should make use other gates to show the full capabilities of DFT in modeling more complex information security risk especially in analyzing complicated system. The research should also simplify DFT diagram and model to help the top manager to understand the risks and their impact at the same time help them making any decision about the risks effectively.

- b. **Simulation for DFT** – Dynamic Fault Tree (DFT) is widely used to analyze reliability in engineering and also well-known in financing prediction. It is still new for information security researchers and some of them not even really understand dynamic risk analysis. There should be a simulation of DFT in the sense to get the people understand and comprehend what is DFT all about and how to use it. Special research can be done just to study this method in depth and develop learning simulation for those who still new to DFT.
- c. **Using other dynamic risk analysis technique** - There are many dynamic techniques to be used in doing risk analysis dynamically. For example Go Method, Markov Modeling and Dynamic Event Tree Analysis Method. These techniques have not been used in information security risk analysis but very widely used in engineering and financial area. A research can be done to prove that these methods also applicable for information security risk analysis.
- d. **Develop fully automated dynamic risk analysis software or tools** – In this research the tasks to complete the risk analysis are done manually. All the data is collected and processed manually using spreadsheet. It is a good thing if a research could be carried out to develop software or computerized tools to help the risk analyst doing the analysis in faster and precise manner. The software or tool should be user-friendly and helpful. With the assistance of the software, risk analysis can be done easily and people will think about doing it in their organization for security purpose.

6.6 Summary

In an uncertain world, it is important to have a dynamic risk analysis methodology to account for non-normally distributed risk. Dynamic risk analysis such Dynamic Fault Tree (DFT) model enables risk management practitioners to efficiently fit many risk models simultaneously. By having the appropriate risk correlations and interaction among each other, the analyses provide the most precisely result of the portfolio risk.

What has been discussed in this chapter is summary of the analysis. The risks that have been found are explained and discussed so that the organization can foresee the benefit of having risk analysis. At the same time the method used in the analysis is also given exposure to validate that the analysis followed the standard and viable.

In the chapter, the challenges and critical success factors for the project are also included. These two parts are written as references for future work and other researcher who interested in the same topic.

This project has attempted to design and implement risk analysis of PACS in dynamic method which is conducted according to ISO/IEC 27005 Information Security Risk Management Standard. The risk report produced in form of risk register very beneficial for Hospital Selayang. The risk register can be used in the risk assessment process.

REFERENCES

- International Organization for Standardization, 2008. "ISO/IEC 27005 Information Security Risk Management Standard". ISO Publication.
- Council of Standards Australia, 1999. "AS/NZS 4360:1999 Australian Standard Risk Management". Standards Association of Australia.
- Gary Stoneburner, Alice Goguen, and Alexis Feringa, 2002. "NIST - Risk Management Guide for Information Technology Systems". NIST Special Publication 800-30.
- Joanne Bechta Dugaan, Tariq Said Assaf, 2003. "Dynamic Fault Tree Analysis of a Reconfigurable Software System". University of Virginia.
- Hong Xu, 2004. "Combining Dynamic Fault Trees and Event Trees for Probabilistic Risk Assessment". University of Virginia, Charlottesville.
- Hichem Boudali, Pepijn Crouzen, and Mariëlle Stoelinga, 2007. "Dynamic Fault Tree Analysis using Input/Output Interactive Markov Chains". University of Twente.
- Geoffrey H. Wold and Robert F. Shriver, 1997. "Risk Analysis Techniques". Disaster Recovery Journal.
- Ian P. Leistikow, Geert H. Blijham, 2005. "System-based risk analysis in healthcare". University Medical Center Utrecht.

Major Marc A. Lee, 2007. “*A Dynamic Systems Simulation Approach to Risk Mitigation for Critical Infrastructure*”. United States Military Academy.

James W. Meritt, 2005. “*A Method for Quantitative Risk Analysis*”. CISSP.

Jim Wang, 2003. “*Modeling Techniques for a Risk Analysis Methodology for Software Systems*”. Carnegie Mellon University.

Gary Leonard Cave, 2002. “*Qualitative Analysis, Methodologies in the USA*”. Entomologist, USDA-APHIS.

Dr. Doreen Watler, 2002. “*Qualitative Risk Analysis: Methodologies And Applications In Canada*”. Canadian Food Inspection Agency.

L. Baliwangi, H. Arima, K. B. Artana, K. Ishida, 2007. “*Risk Modification Through System Dynamics Simulation*”. Kobe University Japan, Kampus ITS Keputih Surabaya.

Alfredo Moscardini, Mohamed Loutfi and Raed Al-Qirem, 2007. “*The Use of System Dynamics Models to evaluate the Credit Worthiness of firms*”. University of Sunderland.

Jean-Peter Ylén, 2007. “*System Dynamic Model For E-Commerce Customer Retention Strategy*”. Technical Research Centre of Finland VTT.

Appendix A - On-site Interview Questions

No.	Question	Answer
1.	Who are valid users? (e.g., system users who provide technical support to the IT system; application users who use the IT system to perform business functions)	<ol style="list-style-type: none"> 1. Authorized Medical Officer or Paramedic who use the radiologic images 2. Maintainer and Help desk Officer (vendor- PC Soft) 3. In charge Information Technology Unit Officer 4. System Developer (vendor)
2.	What is the purpose of the system in relation to the mission?	To electronically scan, store and view medical radiology images such as X-rays, ct scan and MRI, so that doctors and other health care professionals can do their job promptly and effectively.
3.	What information is generated by, consumed by, processed on, stored in, and retrieved by the system?	X-rays image and report will be generated; the report and image will be stored in the database.
4.	What are the paths of information flow? (Flow of information pertaining to the IT system e.g., system interfaces, system input and output flowchart)	User access x-rays or CT-scan or MRI images from archive server if the images available or access directly from machine.
5.	How important is the information to the organization's mission?	Very important as this images is very crucial in diagnosis patient conditions in order to give the best treatment.
6.	What is the sensitivity (or classification) level of the information?	The radiology images and report related to them is very sensitive and cannot be exposed to unauthorized party.

7.	What information handled by or about the system should not be disclosed and to whom?	The radiology images and report related to them.
8.	Where specifically is the information processed and stored?	Basically the images is generated from the radiology machine, the images then will be used by medical officer for reporting purpose, after that the report together with the image will be stored in the archive server.
9.	What are the types of information storage?	Digital storage – server archive and backup by cassette Hard Copy – radiology film
10.	Have you organization currently implemented information storage protection that safeguards system and data availability, integrity? (Technical controls used for the IT system e.g., built-in or add-on security product that supports identification and authentication, discretionary or mandatory access control, audit, residual information protection, encryption methods)	Yes, mandatory access control, audit log and encryption are implemented at database level; only valid user is granted access to system based on their role and authority in the system and provided with their own secret user id and password.
11.	Does your organization have management controls used for the IT system? (e.g., rules of behavior, security planning)	Yes, security policy is enforced to every user and people who accesses the system.
12.	Does your organization have operational controls used for the IT system? (e.g., personnel security, backup, contingency, and resumption and recovery operations; system maintenance; off-site storage; user account establishment and deletion procedures; controls for segregation of user functions, such as	There is Business Continuity Plan.

	privileged user access versus standard user access)	
13.	Does your organization implement physical security controls for environment of the IT system? (e.g., facility security, data center policies)	Physical access control is implemented at server room using access card for authorized personnel only.
14.	Has environmental security been implemented for the IT system processing environment? (e.g., controls for humidity, water, power, pollution, temperature, and chemicals)	Yes, server room is equipped with up to date control for environmental security. Air-conditioner, power backup utilities and anti-fire floor and ceiling.
15.	What is the potential impact on the organization if the information is disclosed to unauthorized personnel?	Impact on medical treatment and legal. Disclosed information may be altered and cause mistreatment and impose organization to legal actions.
16.	What is the effect on the organization's mission if the system or information is not reliable?	Reputation as a good hospital ruins, people will go to another hospital.
17.	How much system downtime can the organization tolerate?	12 hours (1/2 day)
18.	Could a system or security malfunction or unavailability result in injury or death?	No, as hard copy backup is available for emergency cases.
19.	Does your organization have system security policies governing the IT system?	Yes, security policy regarding usage of ICT equipped is provided and implemented.

Appendix B - Hospital Selayang Personnel Involved in Interviews

No.	Name	Position and Responsibilities	No. of Years Work	Experience in PACS (years)
1.	Lee Sak Wah	Head Of Department Information Technology Department of Hospital Selayang	18	7
2.	Razlan Bin Abdul Aziz	Information Technology and Security Officer	5	5
3.	Zainal Bin Mohd Amin	Information Technology and Security Officer	20	3
4.	Dr. Hjh Zaharah bt Musa	Head of Department Imaging	21	7

Appendix C - Asset Identification Worksheet

No.	Asset	Description
1.	Information and ICT Assets	ICT asset in relation to studied system consists of hardware, software and communication elements
1.1.	Hardware	Physical ICT asset that must be available in order to operate the system.
1.1.1	X-Rays machine	Machine used to capture x-rays image from patients
1.1.2	CT-Scan machine	Machine used to capture ct-scan image of patients
1.1.3	MRI machine	Machine used to capture MRI image from patients
1.1.4	Archive Server	Server used to store radiology images for future and present uses, serves image request from users
1.1.5	Camera / Jukebox Server	Server used to store radiology image for printing purpose.
1.1.6	PC	Computer used by user to access the system
1.2	Software	Application or software to be run by hardware in order to complete the mission of the system.

1.2.1	Picture Archiving Communication System (PACS)	The application developed to handle overall business process of the system, make sure the desired output and process achieved.
1.2.2	Sun OS 5.7	Operating system for the all server in PACS environment.
1.2.3	Oracle 8 Enterprise 8.0.5.2.1	Database software used for database server.
1.2.4	Windows 2000/XP/Vista	Operating system for the computer at user workstation.
1.3	Communication Elements	Hardware that needed in order for PACS gets into network and communicates with user.
1.3.1	3COM Switch	Switch that connect all server in PACS system to Hospital Selayang network.
2.	People	Direct or indirect personnel that plays part in PACS system.
2.1	Staff	Personnel that come from inside organization.
2.1.1	Medical Officer	Doctor that uses PACS to ask for radiology images to be taken for a patient, request the radiology images to make diagnosis and write report about the images.
2.1.2	Radiologist	Person who capture and handle radiology machine and prepare images for PACS system.
2.1.3	IT Officer	ICT officer from Hospital Selayang that acts as mediator between system developer and user, and facilitated the implementation of PACS.

2.2	Vendor	Company who develop or maintain the system.
2.2.1	System Maintainer	Company that will entertain error, complaint and problem from user, solve the problem.
2.2.1	System Developer	Company who develop the system.
2.3	Other External Personnel	Those who involves indirectly to system.
2.3.1	Cleaner	Staff who hired to clean the user workstation and server room.
3.	Environment	Overall environment where the system fit in regarding the building and other facilities in the building.
3.1	Building	Place or room where system reside in.
3.1.1	Server Room	Specific room where all there server located.
3.1.2	Radiology Department	Room where the entire radiology machines is placed.
3.1.3	User workstation	User location where computer for system access located.
3.2	Facility	Add in that make the environment conducive for ICT hardware in term of security and operational.

3.2.1	Air-Condition	Used to keep the server room and radiology room temperature as low as possible in order to avoid any interference to the hardware that can malfunction if high temperature is present.
3.2.2	Fire Detection and Alarm	Tool installed in the room to avoid any fire incident by detecting and alarming if smoke or high temperature is detected.
3.2.3	Anti-Fire Construction	Floor, ceiling and wall of the room is constructed using anti-fire material so that can prevent fire or slow down burning fire from becoming more hazardous.
3.2.4	AVR	Tools that installed to every server, computer and machine to avoid total power during blackout as it act as power provider by saving power in its box.
3.2.5	Access Card Control	For security purpose authorized personnel is given access card that must be touch to access terminal to enter the server room to avoid intruder.
4.	Business Process and Activities	Document, policy or standard that must be followed by all staff in the organization or keep secret from competitor.
4.1	ICT Security Policy	Policy that outlines what must or must not be done by staff when using ICT assets.
4.2	Business Continuity Plan	Document that outline steps to be taken during incident or emergency in order to reduce loss and return to operation as quick as possible.

Appendix D - Asset Valuation Worksheet

a) Asset Priority and Impact

No	Asset	Priority in Business	Impact of Loss
1.	X-Rays machine	H	M
2.	CT-Scan machine	H	M
3.	MRI machine	H	M
4.	Archive Server	H	S
5.	Camera / Jukebox Server	H	S
6.	PC	H	S
7.	Picture Archiving Communication System (PACS)	H	S
8.	Sun OS 5.7	H	S
9.	Oracle 8 Enterprise 8.0.5.2.1	H	S
10.	Windows 2000/XP/Vista	H	S
11.	3COM Switch	H	S
12.	Medical Officer	M	S
13.	Radiologist	M	S
14.	IT Officer	M	S

No	Asset	Priority In Business	Impact of Loss
15.	System Maintainer	M	S
16.	System Developer	M	S
17.	Cleaner	L	NS
18.	Server Room	H	S
19.	Radiology Department	H	S
20.	User Workstation	H	S
21.	Air-Condition	M	M
22.	Fire Detection and Alarm	M	M
23.	Anti-Fire Construction	M	M
24.	AVR	M	M
25.	Access Card Control	M	S
26.	ICT Security Policy	L	S
27.	Business Continuity Plan	L	S

b) Priority Level for Assets

Label	Level	Description
H	High	Asset is critical to business operation.
M	Moderate	Asset is important to business, may change to backup procedures or offline.
L	Low	Asset is non-vital, sometimes unnecessary for normal procedures.

c) Impact Level for Assets

Label	Level	Description
S	Sensitive	Asset is critical, loss is permanent or very time-consuming to replace, disclosed information is very sensitive, and there is intention of using it.
M	Moderate	Important asset may be replaced with some effort, may be a one-time loss, disclosed information is somewhat sensitive, and person receiving information does not intend to use it for malicious purposes.
NS	Non-sensitive	Non-critical asset may be replaced easily, disclosed information is not sensitive, and person receiving confidential information has no intention of using it.

Appendix E - Threat-source Identification Worksheet

a) Threat-source Identification Description

No.	Source	Threat	Motivation	Targeted / Affected Asset	Description
1	N	Fire / Smoke	A	I, E	An accidental or intentional fire could damage system equipment or facility.
2	N	Acts of Nature	A	I, E	All types of natural occurrences (e.g., earthquakes, hurricanes, tornadoes) that may damage or affect the system.
3	N	Water Damage	A	I, E	Water from internal or external sources may damage system components.
4	H	Espionage / Sabotage / Terrorism / Vandalism	D	I, P	Espionage is the intentional act of or attempt to obtain confidential information. Sabotage is premeditated destruction or malicious modification of assets or data for personal or political reasons. Terrorism is the destruction or damage of resources for political reasons. Vandalism is the destruction of system resources with no clearly defined objective.

No.	Source	Threat	Motivation	Targeted / Affected Asset	Description
5	H	Theft / Pilferage	D	I, P, BP	Theft is the unauthorized removal of computer equipment or media. Pilferage is theft of property by personnel granted physical access to the property.
6	H	Hacking / Social Engineering	D	I, P	Software may be modified intentionally to bypass system security controls, manipulate data, or cause denial of service. Social engineering is the human-to-human interaction in which a hacker gathers data for use in modifying or manipulating the system.
7	H	Malicious Code	D	I	Malicious software such as viruses or worms may be introduced to the system, causing damage to the data or software.
8	H	User Errors / Omissions	A	I, P	Application and support system components may be inappropriately modified or destroyed due to unintentional administrator or user error.
9	H	Mismanagement / Waste	A	P, BP	Losses and delays caused by failure to plan, failure to adhere to plans, policies or procedures.
10	H	Eavesdropping / interception	D	I, E, BP	Intentional unauthorized access to confidential information through technical means (sniffing/interception) or by personnel having some level of system access but not having a need to know (eavesdropping)

No.	Source	Threat	Motivation	Targeted / Affected Asset	Description
11	H	Browsing / Disclosure	D	I, P	Intentional unauthorized access to confidential information by outsiders or by personnel with system access but not having a need to know (browsing)
12	H	Data Integrity Loss	D	I	Attacks on the integrity of system data by intentional alteration.
13	H	Misuse / Abuse	D	I, P	Individuals may employ system resources for unauthorized purposes.
14	H	Fraud	D	I, P	Use of the system by authorized personnel for illegal financial gain.
15	EP	Power Disruption	E	I, E	A power failure or fluctuation may occur as the result of a commercial power failure. This may cause denial of service to authorized users (failure) or a modification of data (fluctuation).
16	EP	Strike / Work Stoppage	E	P, E	Adverse impact on operations due to planned, intentional acts based on organized employee dissatisfaction.
17	EP	Hardware / Equipment Break Down	E	I, E	Failure or malfunction of hardware may cause denial of service to system users. Additionally, hardware configuration may be altered in an unauthorized manner, leading to inadequate configuration control or other situations that may impact the system.

No.	Source	Threat	Motivation	Targeted / Affected Asset	Description
18	EP	Program Errors / Software Break Down	E	I, P	Software malfunction or failure resulting from insufficient configuration controls (i.e., testing new releases, performing virus scans).
19	EP	Communication Device Malfunction	E	I	Communication links may fail during use or may not provide appropriate safeguards for data.
20	EP	Explosion / Bomb Threat	E	E	Intentional disruption of operations due to actual or threatened catastrophic explosion.
21	EP	Chemical / Electromagnetic / Biological Incident	E	E	Disruption of operations and personnel hazards due to actual or potential effects of chemicals, electromagnetic or biological agents to include infestations and illness.

b) Threat Source Description

Label	Source	Description
N	Natural	Events that happen naturally such as floods, earthquakes, tornadoes, landslides, avalanches, electrical storms, and other such events.
H	Human	Events that are either enabled by or caused by human beings, such as hacker, cracker, computer criminal, terrorist, rivalry, poorly trained and disgruntled terminated employees
EP	Environment and Physical	Events which happen without being caused by attended action directly to the system but have effect to them such as long-term power failure, chaos, picket, pollution.

c) Threat Motivation Description

Label	Motivation	Description
D	Deliberate	Done by party who has intentional interest to system.
A	Accidental	Done without intentional interest from the doer or happen without interference from human.
E	Environmental	Result from people or materials that are not directly connected to the system but can affect the overall system.

d) Targeted / Affected Asset Description

Targeted / Affected Asset Legend		
I	ICT Asset	Asset is related to ICT such as hardware, software and communication elements.
P	People	Asset that involves human resources such as system user, vendor and other external personnel that comes across with the system.
E	Environment	Asset related to building or facility that comprised the system physical architecture such as server room, workstation, air-con, fire alarm kit and so on.
BP	Business Process	Asset in form of secret documents, policy or standard that must not be disclosed to organization competitors.

Appendix F - Threat Assessment worksheet

a) Threat Frequency and Impact

No.	Threat	Frequency	Denial of Service	Unauthorized Modification	System failure	Communication Loss	Unauthorized Disclosure
1	Fire / Smoke	L	√		√	√	
2	Acts of Nature	L	√		√	√	
3	Water Damage	L	√		√	√	
4	Espionage / Sabotage / Terrorism / Vandalism	L	√	√			√
5	Theft / Pilferage	M					√
6	Hacking / Social Engineering	M					√
7	Malicious Code	M	√	√	√	√	
8	User Errors / Omissions	H		√	√	√	
9	Mismanagement / Waste	M	√	√	√	√	√

No.	Threat	Frequency	Denial of Service	Unauthorized Modification	System failure	Communication Loss	Unauthorized Disclosure
10	Eavesdropping / interception	M	√	√			√
11	Browsing / Disclosure	M					√
12	Data Integrity Loss	M		√			√
13	Misuse/Abuse	M	√	√	√	√	√
14	Fraud	L					√
15	Power Disruption	L	√		√	√	
16	Strike/Work Stoppage	L	√		√	√	
17	Hardware/Equipment Break Down	M	√		√	√	√
18	Program Errors/Software Break Down	M	√	√	√	√	√
19	Communication Device Malfunction	M	√		√	√	
20	Explosion/Bomb Threat	L	√	√	√	√	√
21	Chemical/Biological Incident	L	√	√			

b) Threat Frequency Description

Label	Level	Description
H	High	Occurs regularly or on a weekly basis.
M	Moderate	Occurs occasionally or a few times per year.
L	Low	Rarely or never occurs.

Appendix G - Vulnerability / Threat Pairs List

No.	Source	Vulnerability	Threat
1	Environment and infrastructure	Lack of physical protection of the building, doors, and windows	Theft / Pilferage
2	Environment and infrastructure	Inadequate or careless use of physical access control to buildings, rooms	Espionage / Sabotage / Terrorism / Vandalism
3	Environment and infrastructure	Unstable power grid	Power Disruption
4	Environment and infrastructure	Location in an area susceptible to flood	Water Damage
5	Hardware	Lack of periodic replacement schemes	Hardware / Equipment Failure
6	Documents / Procedural	Unprotected storage	Theft / Pilferage
7	Documents / Procedural	Lack of care at disposal	Theft / Pilferage
8	Documents / Procedural	Uncontrolled copying	Theft / Pilferage
9	Hardware	Susceptibility to voltage variations	Chemical / Electromagnetic / Biological Incident
10	Hardware	Susceptibility to humidity, dust, soiling	Hardware / Equipment Failure
11	Hardware	Sensitivity to electromagnetic radiation	Chemical / Electromagnetic / Biological Incident

No.	Source	Vulnerability	Threat
12	Hardware	Insufficient maintenance/faulty installation of storage media	User Errors / Omissions
13	Hardware	Lack of efficient configuration change control	Mismanagement / Waste
14	Software	Unclear or incomplete specifications for developers	Program Errors / Software Failure
15	Software	No or insufficient software testing	Program Errors / Software Failure
16	Software	Complicated user interface	User Errors / Omissions
17	Software	Lack of identification and authentication mechanisms like user authentication	Eavesdropping / interception
18	Software	Lack of audit trail	Misuse / Abuse, Browsing / Disclosure
19	Software	Well-known flaws in the software	Malicious Code, Hacking / Social Engineering,
20	Software	Unprotected password tables or files	Hacking / Social Engineering, Data Integrity Loss
21	Software	Poor password management easily guessable passwords, storing of passwords in clear, insufficient frequency of change	Hacking / Social Engineering, Data Integrity Loss
22	Software	Wrong allocation of access rights	Misuse / Abuse, Browsing / Disclosure
23	Software	Uncontrolled downloading and using software	Malicious Code
24	Software	No “logout” when leaving the workstation	Eavesdropping / interception
25	Software	Lack of effective change control	Mismanagement / Waste
26	Software	Lack of documentation	User Errors / Omissions

No.	Source	Vulnerability	Threat
27	Software	Lack of back-up copies	Program Errors / Software Failure
28	Software	Disposal or reuse of storage media without proper erasure	Mismanagement / Waste
29	Software	Unnecessary services enabled	Hacking / Social Engineering, Malicious Code
30	Software	Immature or new software	Malicious Code
31	Software	widely-distributed software	Malicious Code
32	Communications	Unprotected communication lines	Eavesdropping / interception
33	Communications	Poor joint cabling	Communication Device Malfunction
34	Communications	Lack of identification and authentication of sender and receiver	Eavesdropping / interception
35	Communications	Transfer of passwords in clear	Eavesdropping / interception
36	Communications	Lack of proof of sending or receiving a message	Hacking / Social Engineering
37	Communications	Dial-up lines	Eavesdropping / interception
38	Communications	Unprotected sensitive traffic	Eavesdropping / interception
39	Communications	Inadequate network management resilience of routing	Communication Device Malfunction
40	Communications	Unprotected public network connections	Hacking / Social Engineering
41	Communications	Insecure network architecture	Hacking / Social Engineering
42	Personnel	Absence of personnel	Mismanagement / Waste
43	Personnel	Unsupervised work by outside or cleaning staff	Theft / Pilferage

No.	Source	Vulnerability	Threat
44	Personnel	Insufficient security training	User Errors / Omissions
45	Personnel	Lack of security awareness	User Errors / Omissions
46	Personnel	Incorrect use of software and hardware	Program Errors / Software Failure
47	Personnel	Lack of monitoring mechanisms	Misuse / Abuse
48	Personnel	Lack of policies for the correct use of telecommunications media and messaging	Misuse / Abuse
49	Personnel	Inadequate recruitment procedures	Espionage / Sabotage / Terrorism / Vandalism
50	Documents / Procedural	Lack of information processing facilities authorization	Espionage / Sabotage / Terrorism / Vandalism
51	Documents / Procedural	Lack of formal process for authorization of public available information	Data Integrity Loss
52	Documents / Procedural	Lack of formal process for access right review supervision	Mismanagement / Waste
53	Documents / Procedural	Lack of formal policy on mobile computer usage	Theft / Pilferage
54	Documents / Procedural	Lack of formal procedure for ISMS documentation control	Data Integrity Loss
55	Documents / Procedural	Lack of formal procedure for ISMS record supervision	Data Integrity Loss
56	Documents / Procedural	Lack of formal procedure for user registration and de-registration	Hacking / Social Engineering
57	Documents / Procedural	Lack or insufficient 'clear desk and clear screen' policy	Hacking / Social Engineering

No.	Source	Vulnerability	Threat
58	Documents / Procedural	Lack of continuity plans	Mismanagement / Waste
59	Documents / Procedural	Lack of proper allocation of information security responsibilities	Mismanagement / Waste
60	Documents / Procedural	Lack of e-mail usage policy	Mismanagement / Waste
61	Documents / Procedural	Lack of procedures for classified information handling	Mismanagement / Waste
62	Documents / Procedural	Lack of procedures for reporting security weaknesses	Mismanagement / Waste
63	Documents / Procedural	Lack of regular audits supervision	Mismanagement / Waste
64	Documents / Procedural	Lack of regular management reviews	Mismanagement / Waste
65	Documents / Procedural	Lack of information security responsibilities in job descriptions	Mismanagement / Waste

Appendix H - Vulnerability Assessment Worksheet

a) Vulnerability Likelihood Assessment

No.	Vulnerability	Level
1	Lack of physical protection of the building, doors, and windows	L
2	Inadequate or careless use of physical access control to buildings, rooms	L
3	Unstable power grid	L
4	Location in an area susceptible to flood	L
5	Lack of periodic replacement schemes	M
6	Susceptibility to voltage variations	L
7	Susceptibility to humidity, dust, soiling	L
8	Sensitivity to electromagnetic radiation	L
9	Insufficient maintenance/faulty installation of storage media	M
10	Lack of efficient configuration change control	M
11	Unclear or incomplete specifications for developers	H
12	No or insufficient software testing	H
13	Complicated user interface	L
14	Lack of identification and authentication mechanisms like user authentication	L
15	Lack of audit trail	M

No.	Vulnerability	Level
16	Well-known flaws in the software	H
17	Unprotected password tables	H
18	Poor password management easily guessable passwords, storing of passwords in clear, insufficient frequency of change	H
19	Wrong allocation of access rights	M
20	Uncontrolled downloading and using software	M
21	No 'logout' when leaving the workstation	M
22	Lack of effective change control	M
23	Lack of documentation	L
24	Lack of back-up copies	L
25	Disposal or reuse of storage media without proper erasure	M
26	Unnecessary services enabled	M
27	Immature or new software	M
28	Widely-distributed software	M
29	Unprotected communication lines	H
30	Poor joint cabling	L
31	Lack of identification and authentication of sender and receiver	M
32	Transfer of passwords in clear	H
33	Lack of proof of sending or receiving a message	M
34	Dial-up lines	H
35	Unprotected sensitive traffic	H
36	Inadequate network management resilience of routing	M

No.	Vulnerability	Level
37	Unprotected public network connections	H
38	Insecure network architecture	H
39	Absence of personnel	M
40	Unsupervised work by outside or cleaning staff	M
41	Insufficient security training	M
42	Lack of security awareness	M
43	Incorrect use of software and hardware	H
44	Lack of monitoring mechanisms	H
45	Lack of policies for the correct use of telecommunications media and messaging	H
46	Inadequate recruitment procedures	M
47	Unprotected storage	H
48	Lack of care at disposal	M
49	Uncontrolled copying	M
50	Lack of information processing facilities authorization	M
51	Lack of formal process for authorization of public available information	M
52	Lack of formal process for access right review supervision	L
53	Lack of formal policy on mobile computer usage	L
54	Lack of formal procedure for ISMS documentation control	L
55	Lack of formal procedure for ISMS record supervision	L
56	Lack of formal procedure for user registration and de-registration	M
57	Lack or insufficient “clear desk and clear screen” policy	L

No.	Vulnerability	Level
58	Lack of continuity plans	L
59	Lack of proper allocation of information security responsibilities	L
60	Lack of e-mail usage policy	M
61	Lack of procedures for classified information handling	M
62	Lack of procedures for reporting security weaknesses	L
63	Lack of regular audits supervision	M
64	Lack of regular management reviews	L
65	Lack of information security responsibilities in job descriptions	L

b) Vulnerability Likelihood Level Description

Label	Level	Description
H	High	Very easy to be exploited.
M	Moderate	Can be exploited with some available information.
L	Low	Hard to be exploited.

Appendix I - Risk Estimation Worksheet 1

a) Risk Identification and Level

No.	The risk: what can happen and how it can happen	Threat Name	Probability of Threat Occurrence	Existing Controls	Likelihood Of Occurrence	Impact Severity	Risk Level
1.	System down due to environment and infrastructure break down or disaster						L (8.33)
1.1	System assets are stolen or destroyed because building can be broken easily	Theft / Pilferage, Espionage / Sabotage / Terrorism / Vandalism	M	H	L	H	L (10)
1.2	Power trip cause system malfunction due to burnt hardware	Power Disruption	L	H	L	M	L (5)
1.3	System assets ruined by flood or water due to location	Water Damage	L	H	L	H	L (10)
2.	System cannot function because of poor hardware management and configuration						L (8.33)
2.1	Hardware failure due to outdated and deteriorated agents	Hardware / Equipment Break Down, Chemical / Electromagnetic / Biological Incident	M	L	H	L	L (10)

2.2	Hardware loss due to lack of hardware management	Theft / Pilferage	M	H	L	H	L (10)
2.3	Hardware malfunction due to maintenance fault	User Errors / Omissions, Mismanagement / Waste	H	M	M	L	L (5)
3.	System compromised and malfunction due to poor software management, configuration and installation						M (17)
3.1	System not perform the right job due to user mistake or complicated interface	Program Errors / Software Break Down, User Errors / Omissions	M	H	L	L	L (1)
3.2	System information is compromised by unauthorized person	Eavesdropping / interception, Misuse / Abuse, Browsing / Disclosure, Data Integrity Loss	M	M	M	M	M (25)
3.3	System halting due to attack by hacker or disgruntled personnel	Hacking / Social Engineering, Malicious Code, Mismanagement / Waste	M	M	M	M	M (25)
4.	System cannot perform the job properly due to communications problem or poor communication device configuration						M (13)

4.1	Sensitive information lacking due to poor protection of communication line	Eavesdropping / interception, Hacking / Social Engineering	M	M	M	M	M (25)
4.2	Communication loss due to improper device maintenance	Communication Device Malfunction	M	H	L	L	L (1)
5.	System cannot be used or function because of personnel flaws or outsider interferences						M (50)
5.1	Suspended system operation due to no operator or operator mistakes	Mismanagement / Waste, User Errors / Omissions, Program Errors / Software Break Down, Misuse / Abuse	M	L	H	M	M (50)
5.2	System out of service due to personnel or outsider disruptive actions	Theft / Pilferage, Espionage / Sabotage / Terrorism / Vandalism	M	L	H	M	M (50)
6.	System cannot recover from disaster due to lack or ineffective of documents / procedural for security purposes						L (5)
6.1	Business loss due to late response to disaster or to foresee problem	Theft / Pilferage, Espionage / Sabotage / Terrorism / Vandalism	M	H	L	M	L (5)
6.2	Reputation loss due to no procedure to secure data and business	Data Integrity Loss, Mismanagement / Waste	M	H	L	M	L (5)

b) Risk Likelihood of Occurrence Matrix

Effectiveness of Existing Controls	Probability of Threat Occurrence		
	Low	Moderate	High
Low	Moderate	High	High
Moderate	Low	Moderate	High
High	Low	Low	Moderate

c) Likelihood Definitions

Likelihood Level	Likelihood Definition
High	The threat-source is highly motivated and sufficiently capable, and controls to prevent the vulnerability from being exercised are ineffective.
Moderate	The threat-source is motivated and capable, but controls are in place that may impede successful exercise of the vulnerability.
Low	The threat-source lacks motivation or capability, or controls are in place to prevent, or at least significantly impede, the vulnerability from being exercised.

d) Impact Severity Rating Definitions

Magnitude of Impact	Impact Definition
High	Occurrence of the risk: (1) may result in human death or serious injury; (2) may result in the loss of major tangible assets, resources or sensitive data; or (3) may significantly harm, or impede the mission, reputation or interest.
Moderate	Occurrence of the risk: (1) may result in human injury; (2) may result in the costly loss of tangible assets or resources; or (3) may violate, harm, or impede the mission, reputation or interest.
Low	Occurrence of the risk: (1) may result in the loss of some tangible assets or resources or (2) may noticeably affect the mission, reputation or interest.

e) Risk Level Matrix

Risk Likelihood	Risk Impact		
	Low (10)	Moderate (50)	High (100)
High (1.0)	Low $10 \times 1.0 = 10$	Moderate $50 \times 1.0 = 50$	High $100 \times 1.0 = 100$
Moderate (0.5)	Low $10 \times 0.5 = 5$	Moderate $50 \times 0.5 = 25$	Moderate $100 \times 0.5 = 50$
Low (0.1)	Low $10 \times 0.1 = 1$	Low $50 \times 0.1 = 5$	Low $100 \times 0.1 = 10$

Main Risk Calculation after DFT Modeling

Risk level for 'OR' Gate = (Sum of all related risks numerical values) / (count of related risks)

Risk level for 'AND' Gate = (sum (Risk N – (average of related risks))) / (count of related risks)

Risk level for 'FDEP' Gate = (Trigger Risk value – (average of all related dependent risks numerical values)

Risk level for 'SPARE' Gate = (Spare 1 – (spare 2 – (spare 3-(spare4...))))

Related Risk Calculation

Risk Level = Likelihood of Occurrence X Severity of Impact

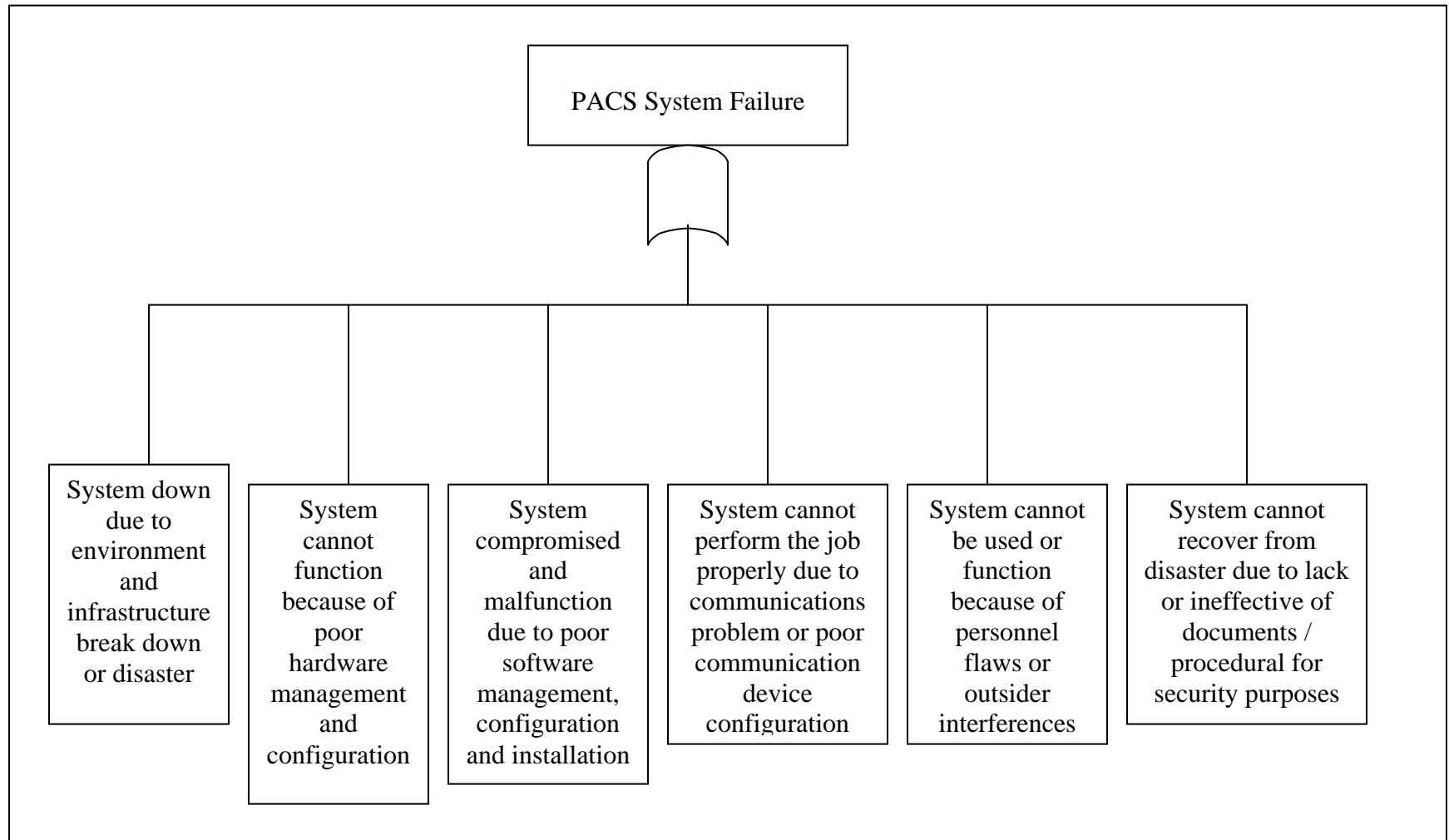
Risk Scale: Low (1 to 10); Moderate (>10 to 50); High (>50 to 100)

f) Risk Level Description

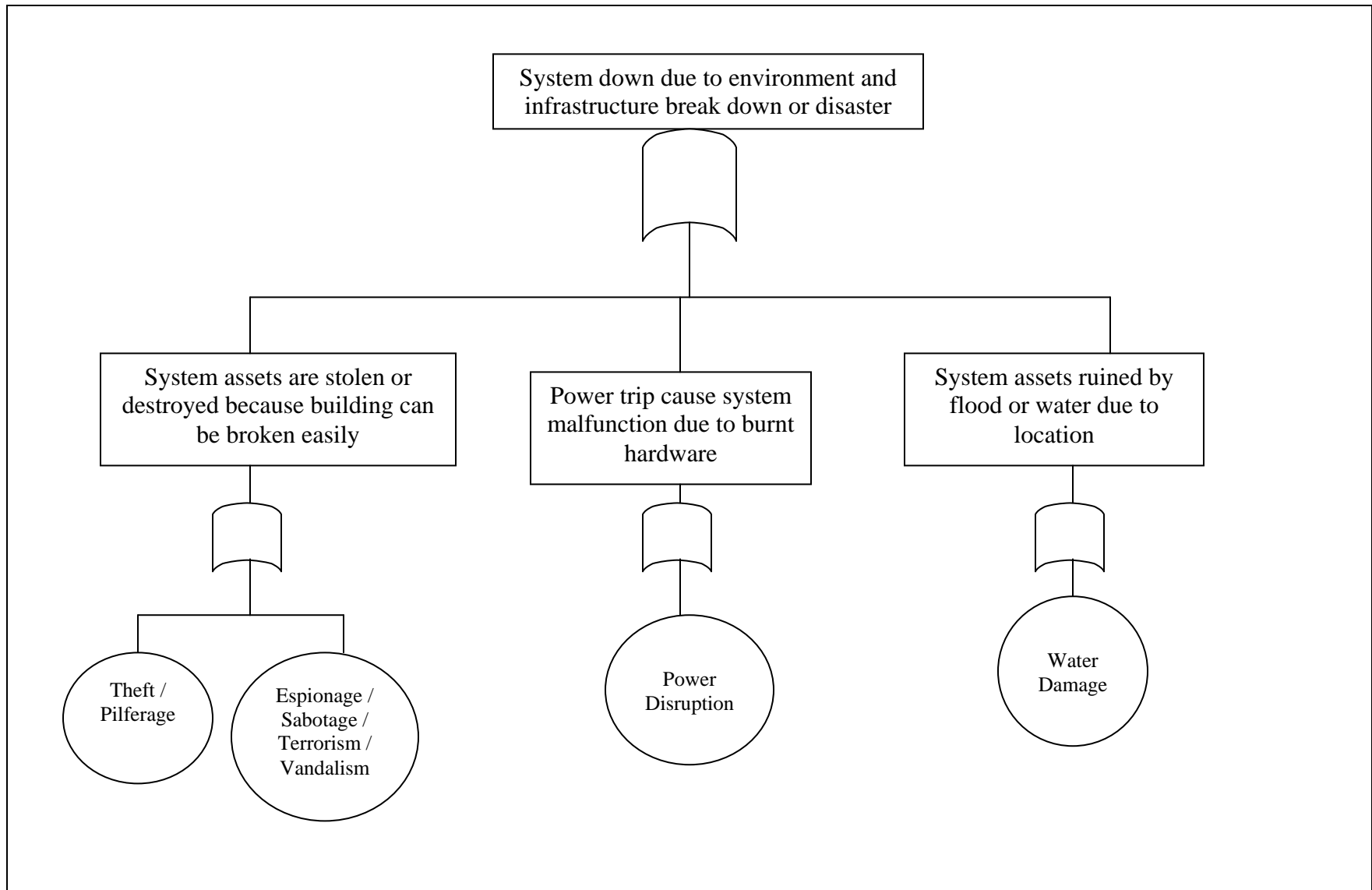
Risk Level	Risk Description & Necessary Actions
High	The loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets or individuals.
Moderate	The loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets or individuals.
Low	The loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets or individuals.

Appendix J - Risk Estimation Worksheet 2

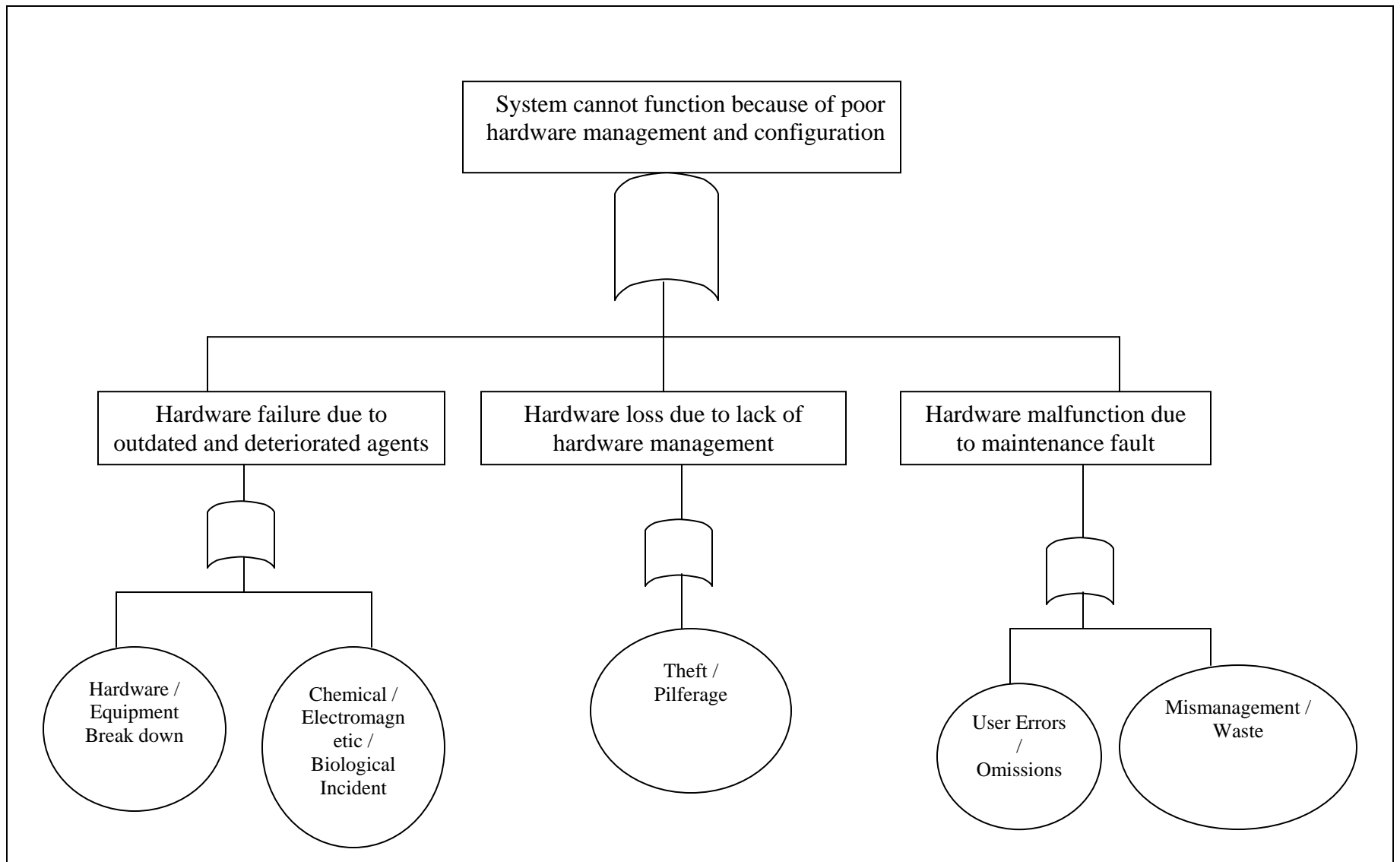
a) DFT model for Top / Main Risk



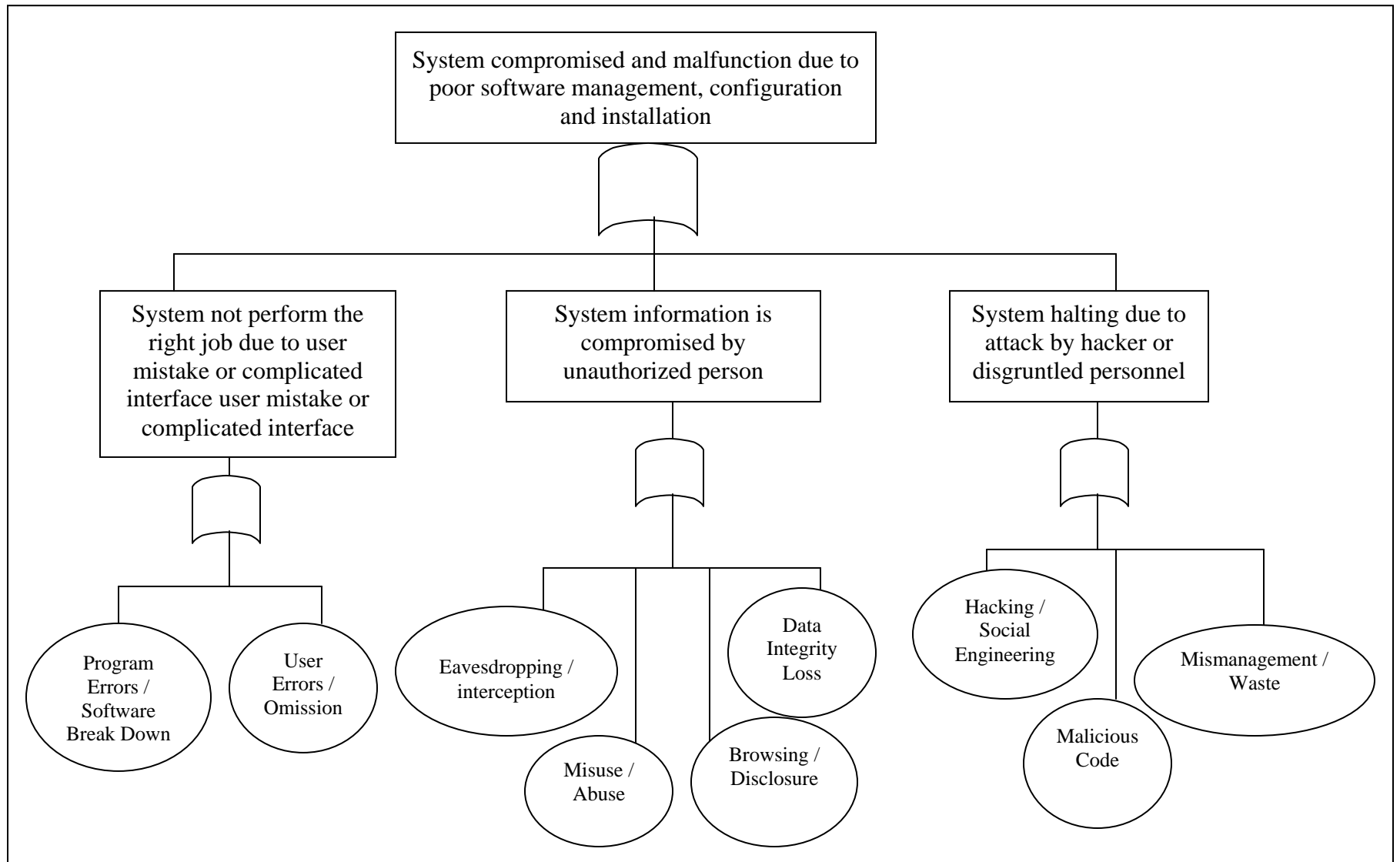
b) DFT Model for Main Risk no. 1 - System Down Due To Environment And Infrastructure Break Down Or Disaster



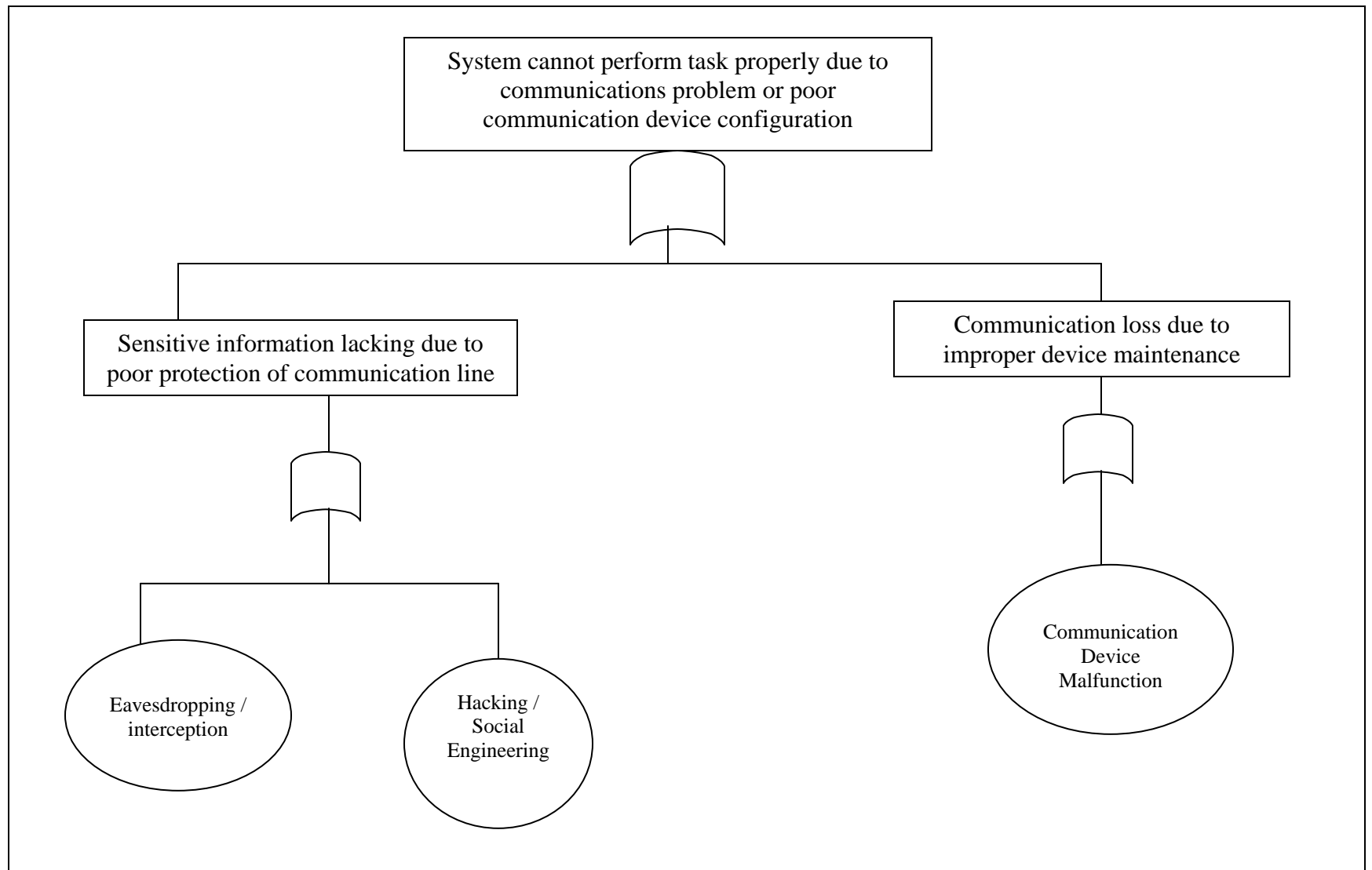
c) **DFT Model for Main Risk no. 2 - System Cannot Function Because of Poor Hardware Management and Configuration**



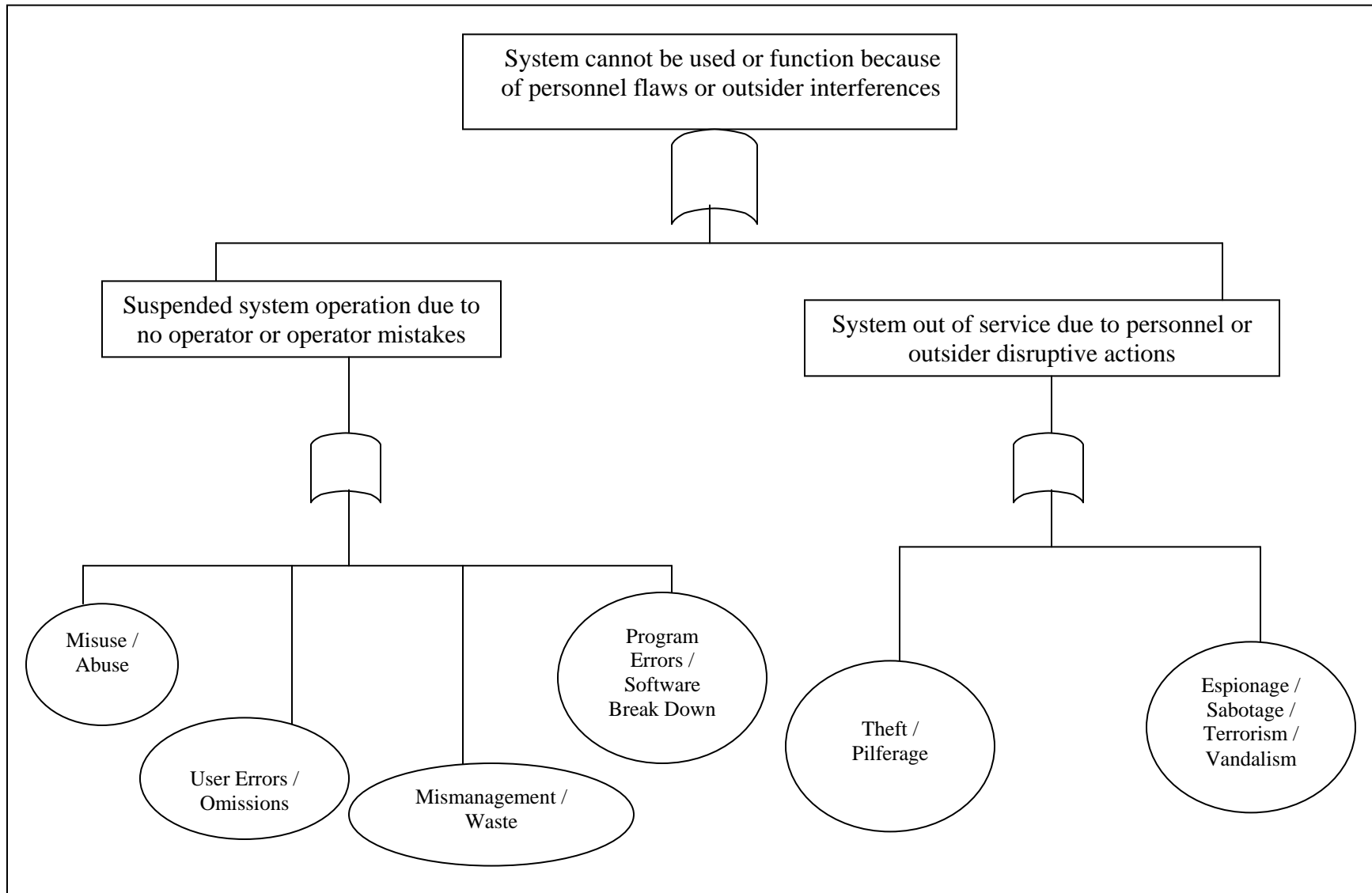
d) **DFT Model for Main Risk no. 3 - System Compromise and Malfunction Due to Poor Software Management, Configuration and Installation**



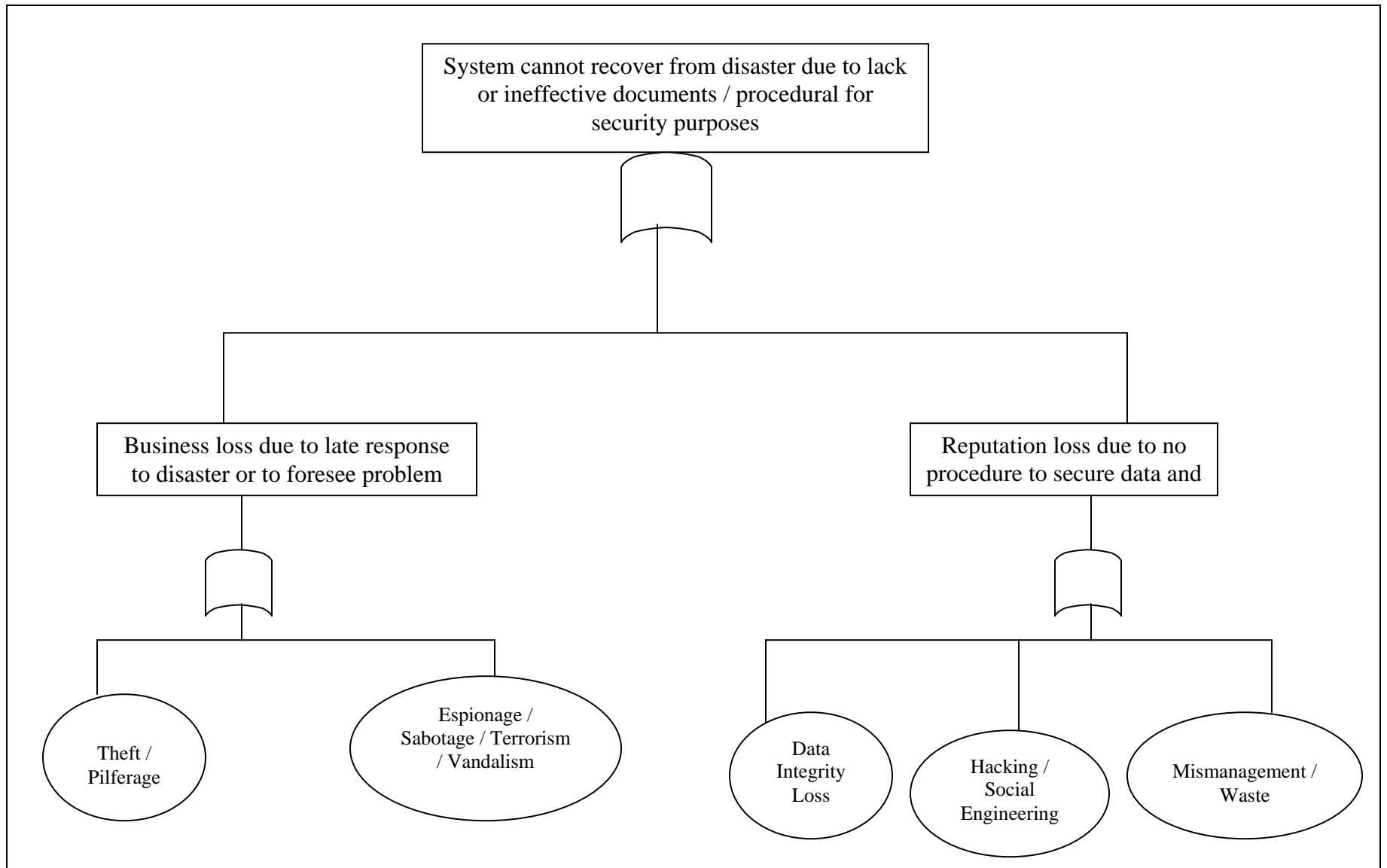
e) **DFT Model for Main Risk no. 4 - System Cannot Perform Task Properly Due to Communications Problem or Poor Communication Device Configuration**



f) **DFT Model for Main Risk no. 5 - System Cannot be Using or Functioning because of Personnel Flaws or Outsider Interferences**



g) DFT Model For Main Risk no. 6 - System Cannot Recover from Disaster Due to Lack or Ineffective Documents / Procedural for Security Purposes



Appendix K - Security Control Analysis Worksheet

a) Security Control Level and Implementation

Control Area	In-Place/ Planned	Level
1 - Risk Management		
1.1 IT Security Roles & Responsibilities	In-Place	H
1.2 Business Impact Analysis	In-Place	H
1.3 IT System & Data Sensitivity Classification	In-Place	H
1.4 IT System Inventory & Definition	In-Place	M
1.5 Risk Assessment	Planned	L
1.6 IT Security Audits	Planned	L
2 - IT Contingency Planning		
2.1 Continuity of Operations Planning	In-Place	H
2.2 IT Disaster Recovery Planning	In-Place	H
2.3 IT System & Data Backup & Restoration	In-Place	H
3 - IT Systems Security		
3.1 IT System Hardening	In-Place	H
3.2 IT Systems Interoperability Security	In-Place	M
3.3 Malicious Code Protection	In-Place	H
3.4 IT Systems Development Life Cycle Security	In-Place	L
4 - Logical Access Control		
4.1 Account Management	In-Place	M
4.2 Password Management	In-Place	M
4.3 Remote Access	In-Place	M
5 - Data Protection		
4.4 Data Storage Media Protection	In-Place	M
4.5 Encryption	In-Place	M
6 - Facilities Security		
6.1 Facilities Security	In-Place	H
7 - Personnel Security		
7.1 Access Determination & Control	In-Place	H
7.2 IT Security Awareness & Training	In-Place	L

Control Area	In-Place/ Planned	Level
7.3 Acceptable Use	In-Place	L
8 - Threat Management		
8.1 Threat Detection	Planned	L
8.2 Incident Handling	In-Place	H
8.3 Security Monitoring & Logging	Planned	L
9 - IT Asset Management		
9.1 IT Asset Control	In-Place	M
9.2 Software License Management	In-Place	H
9.3 Configuration Management & Change Control	In-Place	M

b) Security Control Level Description

Label	Level	Description
H	High	Control is fully implemented and enforced
M	Moderate	Control is implemented but not fully enforced
L	Low	Control is not fully implemented and enforced