EVALUATION OF INFORMATION SECURITY RISKS OF E-LEARNING SYSTEMS: A CASE STUDY ON UUM LEARNING ZONE

A project submitted to the Graduate School of Information Technology

College of Arts and Sciences

Universiti Utara Malaysia

In partial fulfillment of the requirement for the degree of

Master of Science in Information Technology

by

TAN WAI BENG

DECLARATION

I certify that this project contains no materials which has been accepted for the award of any other degree or diploma in any institute, college or university and that, to the best of my knowledge and belief, it contains no material previously published or written by another person, except where due reference is made in the text of the project.

PERMISION TO USE

This project presents a partial fulfillment of the requirement for a postgraduate degree from Universiti Utara Malaysia. I agree that the university library may make it freely available for inspection. I further agree that the permission for copying of this thesis in any manner, in whole or in part, for scholarly purposes may be granted by my supervisor or, in their absence by the Assistant Vice Chancellor of the College of Arts and Sciences. It is understood that any copying or publication or use of this project or parts thereof for financial gain shall not be allowed without my written permission. It is also understood that due recognition shall be given to me and to Universiti Utara Malaysia for any scholarly use which may be made of any material from my project.

Requests for permission to copy or to make other use of materials in this project, in whole or in part should be addressed to:

Dean of Research and Postgraduate Studies

College of Arts and Sciences

Universiti Utara Malaysia

06010 UUM Sintok

Kedah Darul Aman

Malaysia

ABSTRAK

Projek ini dijalankan dengan bertujuan untuk mengenal pasti keselamatan yang berisiko dalam Sistem '*E-Learning*' di UUM '*Learning Zone*' dengan menggunakan kaedah '*OCTAVE Allegro*'. Dengan itu, para kakitangan di Pusat Komputer dari Universiti Utara Malaysia(UUM) telah menjadi golongan yang penting dalam proses pengumpulan data untuk projek ini. Semua keselamatan berisiko yang berkaitan dengan Sistem '*E-Learning*' akan diramalkan dan dikelaskan berdasarkan kaedah '*OCTAVE Allegro*'. Sebenarnya, kaedah tersebut mengutamakan maklumat aset dalam konteks dengan cara-cara maklumat digunakan, tempat maklumat disimpan, diangkut dan diproses dan juga akibat daripada maklumat didedahkan dengan pelbagai ancaman, serangan dan gangguan. Selain itu, projek ini juga menunjukkan kesemua lapan langkah dalam empat peringkat dengan terperinci dalam kaedah '*OCTAVE Allegro*'. Tambahan pula, penerangan berlanjutan yang berhubungan dengan kaedah '*OTAVE Allegro*' turut serta dalam laporan ini. Selain itu, dapatan dari projek ini seperti kemungkinan ancaman yang berlaku pada masa depan dijangka akan memberi manfaat kepada pihak pengurusan di Pusat Komputer, UUM supaya mempunyai pemikiran yang mendalam terhadap keselamatan maklumat yang berisiko di '*UUM Learning Zone*'.

ABSTRACT

This project is conducted with the purpose of identifying security risks associated with E-Learning Systems in UUM Learning Zone by using OCTAVE Allegro. To narrow down the scope of the project, Computer Centre staffs from Universiti Utara Malaysia (UUM) are targeted. The information security risks of E-Learning Systems will be predicted and classified based on OCTAVE Allegro approach by focusing primarily on information assets in the context of how they are used, where they are stored, transported and processed and how they are exposed to threats, vulnerabilities and disruptions as a result. This project will show the OCTAVE Allegro approach which consists of eight steps that are organized into four phases. Detail descriptions of the OCTAVE Allegro methodology applied is also included in the report. The findings of the project such as highlighting the possible security risks are expected to provide UUM's Computer Centre management an in-depth view on the information security risks in UUM Learning Zone.

Keywords: *OCTAVE Allegro, Learning Zone, Universiti Utara Malaysia (UUM), Information Security Risk Management*

ACKNOWLEDGEMENTS

First of all, my most profound thankfulness goes to my final project supervisor Prof. Madya Nazib bin Nordin for his help, guidance and encouragement. I would also like to thank his continuous faith and support in me. Without his encouragement and guidance, it will not be easy for me to reach this extend in completion my report. Besides, I also would like to thank to my project evaluator, Mr. Mohd Samsu bin Sajat for his valuable comments and opinion to help me to keep on improving my final project report until the project report is finally accepted.

Secondly, I would like to thank all my dearest family members, especially to my parents, sisters and husband who have given me their full support in my study. Their full support remains the mainstay for me in overcoming all the difficulties in completing this study. Next I would like to thank all the lecturers who have taught me before throughout the Masters Degree course because the knowledge they imparted have allowed me to be more knowledgeable and thus in a better position to complete this research.

Thirdly, I would like to thank all the Computer Centre staff who had provided me a very clear picture as well as details about the development and implementation of UUM Learning Zone, especially thanks to Madam Nor Asiah binti Abdul Rahman (Information Technology Officer), Mr. Abdul Razak bin Ali (Senior Information Technology Officer), Mr. Shaiful Rizal bin Samad (Assistant Information Technology Officer), Mr. Khalil Kusairi bin Hisam (Chief Information Technology Officer) and Mr. Amran bin Abdullah (Information Technology Officer). There are the best team who are able to spend their

precious time to attend the interview and questionnaire survey that I have prepared for them.

Lastly, I would like to thank all my friends who had given me emotional support and taken care of me at times of difficulties, especially thanks to Mr. Tay Shu Shiang, Mr.Chau Guan Hin, Ms Khor Jia Yun, Ms. Loo Sze Phei and Ms. Ng Hooi Jin in advising and guiding me in the process of completing this report.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

ALE	Annual Loss Expectancy
CCTA	Central Computer & Telecommunications Agency
CERT/CC	CERT Coordination Centre
CMS	Course Management System
CORA	Cost-Of-Risk Analysis System
CRAMM	CCTA Risk Analysis & Management Method
ICT	Information and Communication Technology
ISM	Information Security Management
IST	Information Security Technologies
IT	Information Technology
LMS	Learning Management System
OCTAVE	Operationally Critical Threat, Asset & Vulnerability Evaluation
SCORM	Sharable Content Object Reference Model
SOL	Single Occurrence Losses
UK	United Kingdom
UML	Unified Modeling Language
UUM	Universiti Utara Malaysia
VLE	Virtual Learning Environment

CHAPTER 1

INTRODUCTION

This chapter starts with discussing the background of the study by quoting some facts obtained from the journals and local newspapers. It is followed by the problem statement, the objectives of the study and the significance of the study. The scope and the limitation of the study are also included in this chapter.

1.1 Background

In this new millennium, the global society is living in the electronic environment and age where surrounded with various of electronic transactions such as, e-learning, e-banking, e-commerce and e-mail. These transactions have become very prominent and significant.

Information security risk in E-Learning system is a topic that has become increasingly significant in the new era especially at schools, colleges, universities and other learning institutions. An information security risk is defined as any possible threats that use vulnerability in the system of an organization to cause disruption to the organizational routines and processes in some or the other form. The threats are able to lead to a loss of any form to an individual or an organization. For example, such losses can be included loss of privacy, identity theft, financial loss, negative impact on customer relations, loss or damage of confidential data or information, or a loss in profitability.

Education methods within the education environment have become a tremendous change of over the last few years. This is primarily due to the introduction of advanced and better technologies in the market, such as the Internet. As a result, there is one formulated education method that emerged from using these new technologies is Electronic Learning (E-Learning). E-Learning may is defined as technology-based learning in which learning material is delivered electronically to remote learners by using a computer network [1]. Although this learning method has brought a lot of advantages for learners, many possible threats have caused disruption within the E-Learning environment. Therefore, a great deal of study has been done in the E-Learning environment. However, one aspect that has not received much aware and attention is the important role of information security plays in the E-Learning environment.

The importance of information security in the E-Learning environment is that it is mainly dependent on information as well as communication technologies (ICT). However, the use of ICT could rise many possible information security risks that could damage and compromise many valuable information. Moreover, these information security risks are not necessary significant in E-Learning environment but it also can appear at anywhere. Therefore, all necessary and precaution steps should be taken by educational institutions in order to ensure information is properly and highly secured within the E-Learning environment.

1.2 Problem Statement

Nowadays, people are getting the benefits of accessing vast information quickly with consideration to ICT. The information may exist in many forms such as it can be printed or written on paper, stored electronically and transmitted by post or by electronic means. However, the information should be always being appropriately protected in whatever forms the information takes by which it is shared.

Information deriving from useful data has become the main asset in an organization. Nevertheless, when it is always easy for everyone to access, it will also be easy and useful for everyone to gain access. As a result of this increasing intention, it has exposed to a growing number and wider variety of threats and vulnerabilities. Therefore, it must be protected in order to avoid the loss of its confidentiality, integrity and availability. Some of the most serious threats are listed as below.

1. Deliberate software attacks (virus, worms, macros, denial of service)
2. Technical software failures and errors (bugs, coding problems, unknown loopholes)
3. Acts of human error or failure (accidents, employee mistakes)
4. Deliberate acts of espionage or trespass (unauthorized access and/or data collection)

5. Deliberate acts of sabotage or vandalism (destruction of information or system)
6. Technical hardware failures or errors (equipment failure)
7. Deliberate acts of theft (illegal confiscation of equipment or information)
8. Compromises to intellectual property (piracy, copyright, infringement)
9. Quality of Service deviations from service providers (power and WAN service issues)
10. Technological obsolescence (antiquated or out-dated technologies)
11. Deliberate acts of information extortion (blackmail for information disclosure)

According to [3], problem arises with regard to the IT infrastructure. The UUM campus LAN occasionally does not support the increasing traffic. Many students reported slow access even in the campus. To date, teaching materials developed by the lecturers for the system were limited to small size documents in various formats. However, bigger files in audio/video format are not supported at the moment.

Based on the threats mentioned above, this project has to identify the security risks associated with E-Learning systems.

1.3 Project's Objectives

The main goal of this research is to identify and consolidate the security risks associated with E-learning system using OCTAVE Allegro. To achieve the goal, several specific objectives are defined:

- To develop qualitative risk evaluation criteria that describes UUM Learning Zone's operational risk tolerances. The purpose is to evaluate a risk's effect on UUM Learning Zone's mission and business objectives. The risk criteria concerned are such as financial, reputation and customer confidence, productivity, technology and specific institutional policy.
- To identify assets that is important to the mission of UUM Learning Zone. In this project, I used the information asset called "Teaching and Learning materials" as this asset is of value to the UUM Learning Zone.
- To identify threats and vulnerabilities to those assets. To date, the possible risks are the weakness in IT infrastructure and teaching and learning materials are disclosure to unauthorized individuals.
- To determine and evaluate the potential consequences to UUM Learning Zone if threats are realized such as significant labor charges will be required to re-create the teaching courses and the lecturers' overall perception of the UUM Learning Zone's quality could be negatively affected if the teaching materials are publicized.

1.4 Scope and Limitation

To narrow down the scope of the project, only Computer Centre staffs from Universiti Utara Malaysia (UUM) are targeted. A sample size of 5 staffs will be invited to participate in this facts finding. Questionnaires survey and interview section will be used in this project to collect the required dataset.

The limitation of this project is based on a single case study rather than a multiple case study was selected. The case study is conducted on UUM E-Learning System: Learning Zone. A deep level of access information can be obtained from the single case study only [6].

1.5 Significance of the Study

These findings of the study will provide UUM's Computer Centre management an in-depth view on maintaining reliability and integrity of the security system in UUM Learning Zone and hence help the Computer Centre in better planning on its ICT facilities and services in order to provide a more secured and protected academic technologies to lecturers as well as students. Besides that, it is hoped that the results and suggestions of this research will be adopted and used by the related authorities as part of their reference when making strategy planning for E-Learning development process. Last but not least, the findings of this project are also expected to give the UUM's Computer Centre management a good guidance in planning their future services in the E-Learning systems by highlighting them the possible security risks might happen in UUM Learning Zone in future use and hence create awareness among the Computer Centre management staffs.

CHAPTER 2

LITERATURE REVIEW

This chapter presents the literature review which touch touches on three areas. The first area discusses about security of E-Learning. The second area discusses on possible risks regarding E-Learning while the third area discusses on comparing different information security risk analysis methodologies.

2.1 Security of E-Learning

Securing the E-Learning environment requires according the four types of threats, which are fabrication, modification, interruption and interception [38]. The author has mentioned that research has been done to secure the e-learning environment. Researches in security mainly focus on three main areas such as policy, identity (also known as access management) and intellectual property.

Controlling access has played an important role in order to avoid all attacks in the E-Learning environment. Therefore, one of the best ways is to implement authentication and authorization process. In authentication process, it can identify who he claims to be. In other words, it is a process to identify and verify a legal user to the E-Learning environment. However, a system which is fully secured will be difficult to be accessed by user too. [26] suggested to provide a single sign to user on authentication and authorization services to all

authorized web applications and web resources. [22] recommended an approach to protect intellectual property by extending the control of the copyright holder on the entire lifetime of the digital data. Moreover, he also suggested a method called CIPRESS, which is able to control the access to the material. [27] discussed another technical aspect concerning how to secure E-Learning by digital identity design and privacy preservation.

However, it is considered insufficient if we are only using certain technology devices for controlling access purpose since the attack can be come from outsiders as well as insiders. Therefore, appropriate supervision of handling of information security issues is important in order to ensure threats and vulnerabilities free. Furthermore, information security risks management is important to ensure a success in securing the implementation in e-learning system.

2.2 Possible risks regarding E-Learning

[2] focused on e-learning system and also emphasized on how important it is in order to ensure that proper information security measures have been played the roles to ensure that all information within E-Learning environment is properly secured and protected. Besides, the author also highlighted four information security pillars that should be implemented to enhance the whole information security as regards to E-Learning. Each of these pillars and its actions should be individually addressed and implemented.

According to [3], the implementation of E-Learning system in UUM Learning Zone did not fully meet and fulfill the E-Learning definition. Most of the lecturers and students are highly aware of the implementation. Therefore, the further effort has to be implemented to improve the implementation on E-Learning system.

Based on [40], accountability and learning effectiveness apply in E-Learning. Major types of risk involving with operations of E-Learning courses are from preparation of the courseware (content risk), Internet speed (technological risk), facilitating instructors (people risk) and E-Learning course administration (process risk).

Besides, there is an average of 10 – 20 viruses released every day. Viruses are designed to take advantage of security flaws in software or operating systems. These flaws can attack Microsoft Windows NetBIOS using buffer overflows. Buffer flows happen when an attacker sends responses to a program longer than what is expected. If the victim software is not designed well, then the attacker can overwrite the memory allocated to the software and execute malicious code.

Viruses and worms are the examples of malicious code designed to spread and cause a system to perform a function that it was not originally designed to do [32]. Viruses are programs that need to be activated or run before

they are dangerous or spread. The computer system only becomes infected once the program is run and the payload has been deployed. There are four ways a virus can spread such as through email, network, downloading or installing software and inserting infected media.

The following are the description for threats:

2.2.1 Virus

A program or piece of code that is loaded on to computer without the user's knowledge and runs against user's wishes. It can also replicate themselves, that means it can make a copy of itself and relatively easy to produce. Besides, virus is dangerous because it will quickly use all memory available and halt the system. Furthermore, it also capable of transmitting itself across network and bypassing security systems.

2.2.2 Worm

A worm is a special type of virus that can replicates itself over a computer network and usually performs malicious actions, such as fully utilize the computer's resources and shutting the system down. However, it is unable to attach itself to other programs.

2.2.3 Trojan horses

Trojan horses are destructive program that do not replicate themselves but they just play a role as destructive. It is able to introduce viruses onto the computer.

2.3 Comparing Different Information Security Risks Analysis Methodologies

According to [5], there are numerous risk analysis methodologies available today such as come are qualitative and others quantitative. However, a major task for an organization is to determine which one is the best to use. The best way to choose between methodologies is to compare them by using objective and quantifiable criteria. Therefore, we need a framework for comparison.

The author described five different information security risk analysis methodologies during his research. The five methodologies were analyzed into two categories such as qualitative methodologies and quantitative methodologies. The qualitative methodologies are OCTAVE, CORAS and CRAMM while ISRAM and CORA are the quantitative methodologies. A brief overview is given of each in order to analyze mutual aspects of the different methodologies.

2.3.1 OCATVE

OCTAVE (Operationally Critical Threat, Asset and Vulnerability Evaluation) was developed at the CERT Coordination Center (CERT/CC). This approach concentrates on assets, threats and vulnerabilities. The major concept of OCTAVE is self-direction. That means the people in the organization must lead the information security risk evaluation [33]. The staff from the organization's business unit and IT department can become an analysis team for leading the evaluation and recording result.

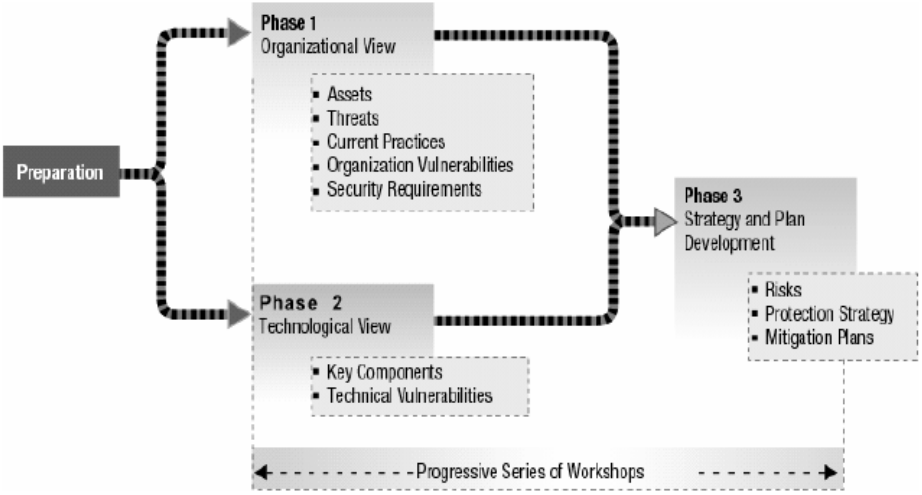


Figure 2.1: Three OCTAVE Method Phases

Based on Figure 2.1, the OCTAVE approach has three phases, with each broken down into processes. Each process has certain activities that must be completed. Within each of these activities, different steps must be taken in order to achieve the desired outputs [34]. The final result that risk decisions can be based on is the threat profile of

different assets. Each threat profile contains information on which mitigation decisions can be based.

2.3.2 CORAS

CORAS was developed under the Information Society Technologies (IST) program. One of the main objectives of CORAS is to "develop a framework that exploits methods for risk analysis, semi-formal methods for object-oriented modeling and computerized tools for a precise, unambiguous and efficient risk assessment of security critical systems" [35]. The methodology is based on UML (Unified Modeling Language), a language that uses diagrams to illustrate relationships and dependencies between users and the environment where they work.

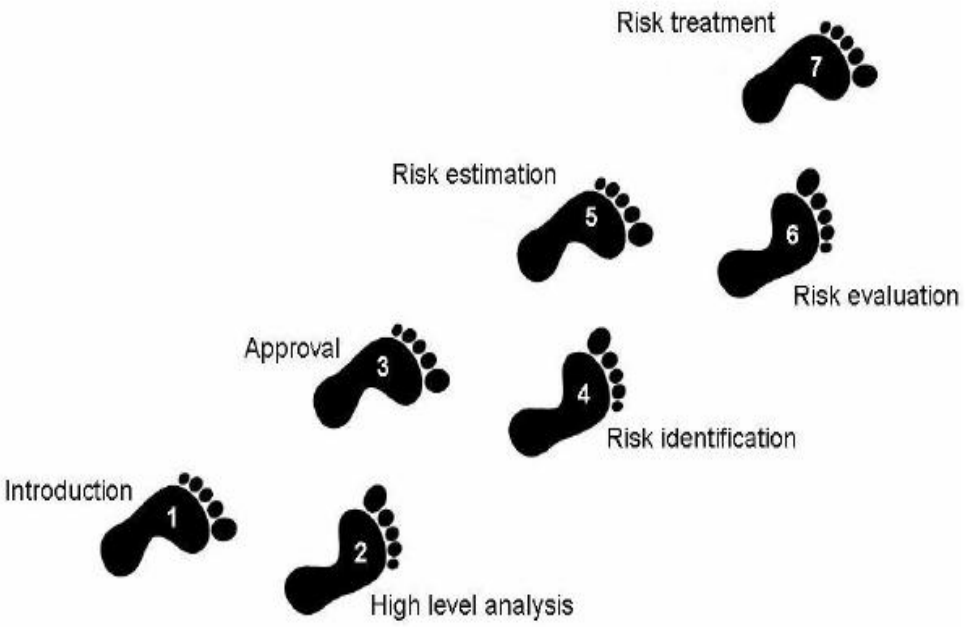


Figure 2.2: The CORAS Method

During an information security risk analysis, information is brainstormed from discussions with different people from different

expertise and fields who give their opinions and share information. By using this way, all participants can communicate efficiently and understand each other and finally come out a UML profile. In CORAS the final result on which decisions can be based is the UML class diagrams of each asset.

2.3.3 CRAMM

CRAMM (CCTA Risk Analysis and Management Method) was developed by the CCTA (Central Computer and Telecommunication Agency) in 1985. The CCTA was tasked by the UK Government Cabinet's Office to investigate the risk analysis and management methods within the central government for IT.

CRAMM provides steps to determine the likelihood and the impact of a threat on an asset. Subsequently, these determined values are used to calculate the risk value for each threat to all the assets. CRAMM also provides a "fast-track" method by logically grouping assets.

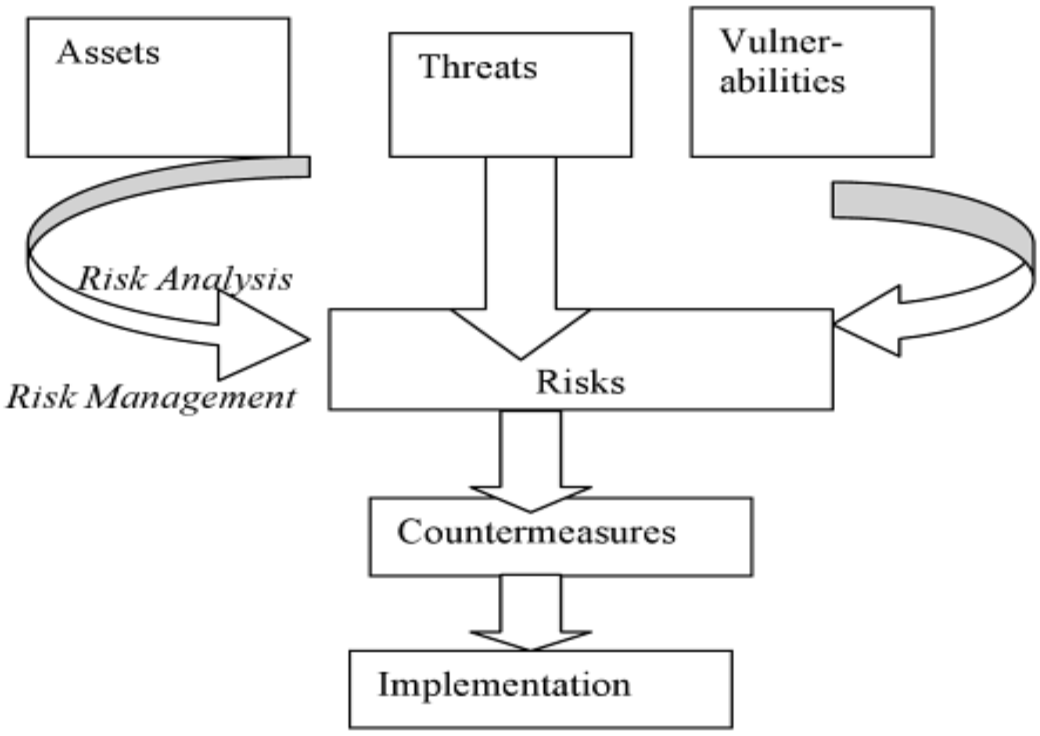


Figure 2.3: Conceptual diagram of CRAMM

2.3.4 ISRAM

The ISRAM methodology was developed in December 2003 at the National Research Institute of Electronics and Cryptology and the Gebze institute of Technology in Turkey [36]. It is marketed as a quantitative approach to risk analysis. It allows the manager and staff of the organization for the participation. ISRAM is a survey-based model. Two separate and independent surveys are conducted for the two attributes of risk such as probability and consequence. The risk factor for ISRAM is a numerical value between 1 and 25. This numerical value corresponds to a qualitative, high, medium or low value and it is this qualitative value on which risk management decisions are based. The ISRAM methodology has seven steps.

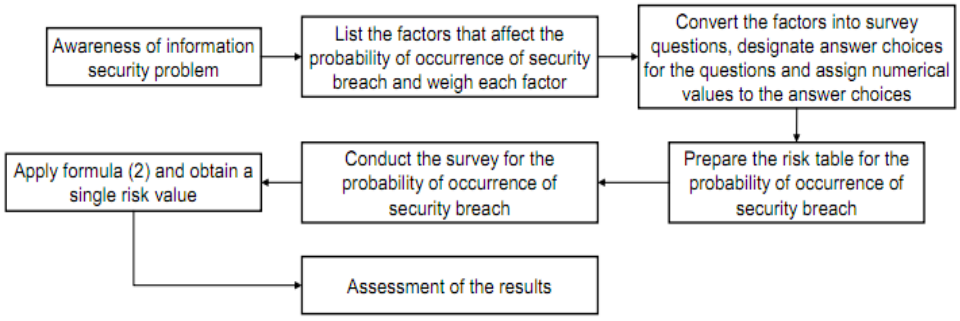


Figure 2.4: Basic flow diagram of ISRAM

2.3.5 CORA

CORA (Cost-Of-Risk Analysis system) was developed by International security Technology, Inc. (IST) [37]. The CORA risk model uses data collected about threats, functions and assets and the vulnerabilities of the functions and assets to the threats to calculate the consequences which is the losses due to the occurrences of the threats. It is a methodology where the risk parameters are expressed quantitatively and where losses are expressed in quantitative monetary terms.

CORA uses a two-step process to support risk management. Parameters for threats, functions and assets are validated and refined until the best values are determined. Then, CORA calculates Single Occurrence Losses (SOL) and Annual Loss Expectancy (ALE) for each of the threats identified. It estimates a single loss value for a threat to an organization and then multiplies this value by the frequency of the threat occurrence.

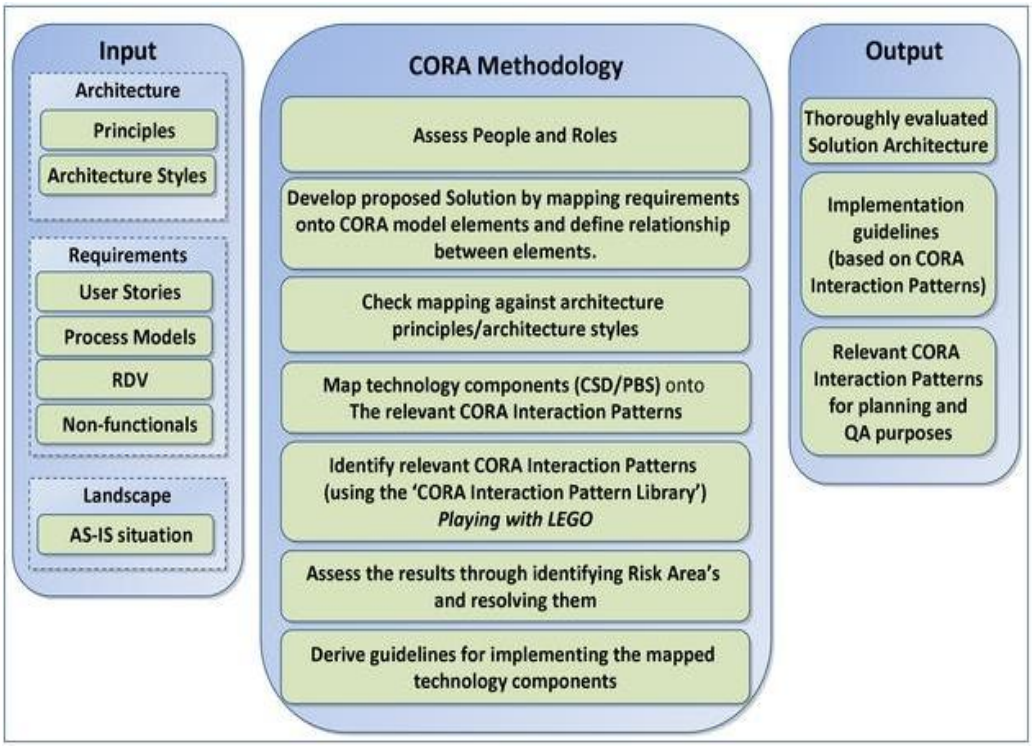


Figure 2.5: Overview of the CORA Methodology

CHAPTER 3

RESEARCH METHODOLOGY

In order to achieve this study's objective, a few methods have been assessed. After a thorough discussion, the method called OCTAVE Allegro is finally selected. The decision is made because the method concentrates on assets, threats and vulnerabilities.

This chapter presents in details the methodology used in the study. The OCTAVE Allegro approach is to allow road assessment of an organization's operational risk environment with the goal of producing more robust results without the need for extensive risk assessment knowledge. This approach is not only focusing on information assets in the context of how they are used but it also can be stored, transported and processed and also how they are exposed to threats, vulnerability and disruptions as a result. Besides, OCTAVE Allegro can be performed in a workshop-style, collaborative setting and is supported with guidance, worksheets and questionnaires. However, it is suitable for individual who is able to perform risk assessment without the organizational involvement.

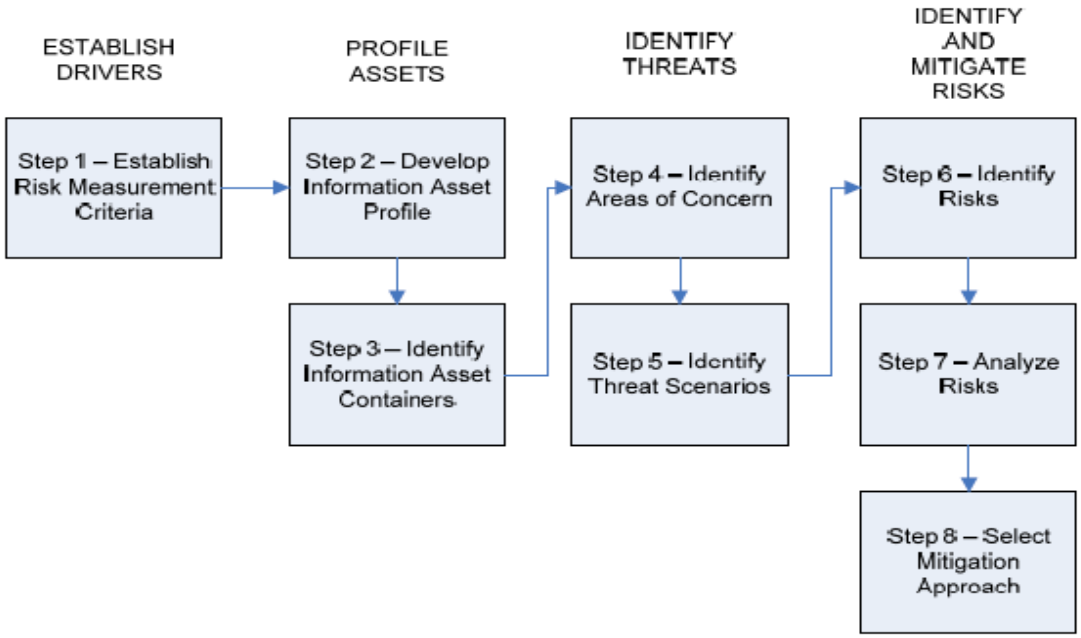


Figure 3.1: OCTAVE Allegro RoadMap in evaluating Information Security Risks in UUM Learning Zone

The OCTAVE Allegro approach consists of eight steps that are organized into four phases as in Figure 3.1. In phase 1, UUM has to develop risk measurement criteria consistent with organizational drivers. During the second phase, information assets that are determined to be critical are profiled. The profiling process establishes clear boundaries for the asset, identifies its security requirements and identifies all of the locations where the asset is stored, transported or processed. In phase 3, threats to the information asset are identified in the context of the locations where the asset is stored, transported or processed. In the final phase, risks to information assets are identified and analyzed and the development of mitigation approaches is commenced.

This project consisted research activities which included questionnaires and semi structured interviews. The semi-structured interviews conducted amongst a sample of UUM Learning Zone content developers within the university.

The main task was to interview other people involved in the provision of UUM Learning Zone support at the University especially the developers of the UUM Learning Zone packages. These developers of the UUM Learning Zone support environment were the staff involved in the development of the UUM Learning Zone who maintained the in-house E-Learning environment at UUM. It is called Learning Management System (LMS). Learning Zone is UUM's learning management system (LMS) based on Moodle. It provided a virtual environment to deliver online courses and training for the university staff, lecturers and students.

Each of the interviewees was given a set of questions a week before the interviews were conducted to familiarize them with the overall aim of the interview. The Laddering technique was utilized within the interviews in order to tap into and get an in-depth understanding something about the interviewee and the way he/she expressed themselves.

CHAPTER 4

INFORMATION SECURITY RISKS MANAGEMENT IN E-LEARNING

Nowadays, many information security technology, hardware and software have been used to secure the e-learning environment. [25] has suggested the obligation of having effective mechanisms for security and privacy control and management is significant. In order to reduce the threats in e-learning, an appropriate planning concerning how to manage the control is needed. In fact, there is only authorized user are allowed to access to the e-learning system. Unfortunately, the process has not been handled properly and as a result, the unauthorized user is able to get permission to access to the system. Therefore, security management has played an important role to ensure the success of the security controls and solution implementation.

Besides, information security can be achieved by a suitable set of controls called Information Security Management (ISM). It includes policies, process, procedures, organizational structures and software and hardware functions. [2] has suggested four main elements of information security within e-learning environments, including ensuring e-learning information security governance, creating e-learning information security policy and procedures, implementing e-learning information security countermeasures and monitoring the e-learning information security countermeasures. The elements mentioned above include the management aspect to ensure that the security implementation achieve its objective.

ISM in e-learning can be justified as similar as to other e-services. However, there are some minor different elements based on the services being offered. For E-Learning, it offers flexibility to the user as a learner and at the same time, it is ensuring availability, integrity and confidentiality of information. Besides, the behaviours of users in e-learning are also different from the users in other e-services. In conclusion, ISM is needed for e-learning system.

CHAPTER 5

INFORMATION SECURITY IN E-LEARNING

5.1 Overview

E-Learning is mainly dependent on information and communication technologies. According to [21], e-learning is based on three fundamental criteria such as network-capable updating, storage/retrieval, distribution and sharing of information, delivery to the end user via computer using standard Internet technology and focus on the broadest view of e-learning.

The first and second criteria expose the e-learning institutions to the threats. It is because the use of ICT could lead to many possible information security risks which could compromise information such as loss of confidentiality, availability, exposure of critical data and vandalism of public information services [22]. However, no efforts have been done to rectify this situation. More efforts have been focused to enhance the content and technology due to address content and technology have become the challenges in securing a successful e-learning environment.

Security is needed within e-learning environment. It is because knowledge has become an important element for personal success. In e-learning system, information deriving from useful data has become main asset of the organization. The important security issues in e-learning are protection against student manipulation, use authentication and confidentiality [22]. However, information should be protected when

the functionality of e-learning is expanding. The purpose is to avoid the loss of its confidentiality, integrity and availability. As we know that *"knowledge has to be shared with everyone"*. However, the flow of sensitive information should be restricted to only well-defined groups. For example, the specific learning materials are only available for certain authorized groups. Furthermore, it is very difficult to verify whether an assignment has been completed and sent by valid student. As a result, we are facing problems in maintaining the identity and the secure content.

E-learning has the same characteristics with other e-services. There are three main characteristics of every e-service are the service is accessible via the Internet, the service is consumed by a person via the Internet and lastly there might be a fee which the consumer pays the provider for using the e-services. That means, the functionality, security threats and the management approaches to e-learning have common features with other e-services. In other words, if an organization would like to protect and maximize the return of investment in learning technology, content and services, the systems that have been used in the organization have to be more interoperable, manageable and usable [23]. According to [17], there are a lot of problems in adoption of online education. The problems occurred are not mainly on the high costs and a number of tasks that need to be carried out, but it is rather to the security aspect.

5.2 Information Security Elements in E-Learning

Information security means the protection of information from threats. The aim of e-learning is to provide teaching and learning services to everyone. Furthermore, the main goal for e-learning security is to ensure availability and integrity of information.

According to [38], *availability* in e-learning is the assurance that the e-learning environment is accessible by only authorized users whenever needed. There are two elements of availability such as denial of service and secondly the loss of data processing capabilities. As we know, the e-learning users are dependent on the information on the Internet. Therefore, the availability of materials and information to be accessed at any time and any places is very difficult. As a result, there is a problem occurred on e-learning users and e-learning provider.

According to [25], some features which affect e-learning are privacy and security for e-delivery and collaborative education. The availability of materials and information is insufficient. In fact, it is important to ensure the reliability of the materials and the information is published. This issue relates to another security element which is called integrity. *Integrity* in e-learning is the protection of data form intentional or accidental unauthorized changes. Actually, integrity depends on access control. Therefore, it is necessary to uniquely identify all people who attempt access. Besides, integrity can be compromised by hackers, masqueraders unauthorized user activity, unprotected downloaded files, LANs and unauthorized programs such as Trojan horses, viruses and worms. Each of these threats can make the unauthorized changes to data or programs.

Although availability and integrity are the main security requirements within e-learning environment, *confidentiality* also has played an important role in the environment. Confidentiality is the protection of information in the system in order to avoid unauthorized person to gain access. Some of the most commonly threats to information confidentiality are hackers, masqueraders, unauthorized user activity, unprotected downloaded files, local area networks (LANs) and Trojan horses.

5.3 Importance of User Login and Secured Logging System in E-Learning

Nowadays, users have expected instant and effortless accessing to information. Therefore, it is importance to provide a useful and accurate access to users, especially in online e-learning environments.

User login is the way for providing identity and access services. User has to provide the user ID and password. There are three crucial identity and access services from the user login, such as identification, authentication and authorization. Identification is the recognition of the user as a genuine member of a user community. Besides, authentication means the verification of the user's identity and authorization is the permission to access specific resources.

Besides that, according to [39], the secured logging system provides three security abilities, such as auditing, accountability and non-repudiation. Auditing is the process of examining user online transaction activities while accountability is the association of user

actions. Non-repudiation can be defined as a process of eliminating an incorrect or mistaken activity performed by a user.

The two methods mentioned above have contributed a sense of security for the users. There have played an important role in building confidence and trust in an e-learning environment. In conclusion, user login is used to restrict access to authenticated users to access resources and systems while the logging systems is to keep track all users' activities once in the system.

CHAPTER 6

CASE STUDY: UUM LEARNING ZONE

This chapter presents the overview of UUM Learning Zone. It also describes the limitations faced in the E-learning system and hints how further works can be continued in the future.

6.1 Overview

The implementation of e-learning in the teaching and learning at UUM was started in 2000 with the selection and development of an integrated system that consists of both academic and administrative components of higher education. According to [3], the E-learning system comprises twelve modules that provide UUM's academic community with arrays of innovative strategies and activities to enhance the conventional face-to-face instruction. It is developed jointly by a local IT company and UUM. Recently, the system is being used as a supplementary component to instruction. Furthermore, the system provides capabilities for synchronous and asynchronous threaded discussion forum, online assessment and tracking of students' access to the

modules. As a result, the e-learning system has become a major component in UUM Community Portal in supporting the university community's needs based on academic, research and administrative requirements. Based on the paper, so far there are a total of 1900 academic staffs have undergone the training and 75% have been using the system in their courses since 2002. The feedbacks form both academic staff and students have shown that the system has merit for teaching and learning. However, there are major issues that have been frequently raised concern the infra and info structure. Besides that, the university policy of incremental implementation has been the major factor in the integration of the system in the teaching and learning process. In order to support these services, a good strategic planning for the university's vision and mission has to be developed and at the same time, a well-organized e-learning management needs to be implemented in the organization.

6.2 Introduction

Moodle is an open source Course Management System (CMS) which is also known as a Learning Management System (LMS) or a Virtual Learning Environment (VLE). Nowadays, this system has become very popular among educators, lecturers and teachers around the world as a teaching tool for creating online dynamic web sites for their students. Learning Zone is UUM's learning management system (LMS) based on Moodle, which is developed from a learning-centric perspective rather than a technical administrative perspective. In fact, Learning Zone has successfully allowed lecturers to enhance UUM

students' learning by providing an online environment to distribute learning materials. Besides, it also encourages collaboration and interaction within and outside the classroom among UUM lecturers and students. Furthermore, it has a range of functionality to allow for content creation and delivery, communication, collaboration and assessment. The features which available in Learning Zone are Assignment module, Chat module, Choice module, Database module, Forum module, Glossary module, SCORM module, Survey module, Wiki module, Web Meeting module and Turnitin module.

6.3 Network

UUM network is high-speed and extends to all university buildings, including student residences via ISLAN. UUM staffs on campus are automatically connected to the network. Furthermore, they can also able to connect to the network at home. It means, everyone including staff, students or even visitors can use the wireless network. Besides, departmental supporters are managing and supporting the staff PCs by using Active Directory. The network is protected by the firewall (will be discussed in 6.5). In terms of internet bandwidth, UUM also has invested much money to supply internet access around the university compound. All staff and students are able to access internet with spend 155MB.

6.4 Wireless

In UUM, Wireless Local Area Network (WLAN) infrastructure consists of a wired backbone network, an air controller and a plurality of wireless access points (WAPs). Then, each WAP has a processor, a wired backbone interface, a first radio, a directional antenna, a second radio and an antenna. In order to use wireless facility in university, staff and students must connect through Access Point which is called “uumzone” together with the valid login ID and password. Besides, it provides 90pcs Cisco Access Point device to support around academic building and administrative building while 12pcs Aruba Access Point device is provided to support “Dewan Penginapan Pelajar Yayasan Al-Bukhari” and the other areas. Besides, 95% Access Point radio using B/G 802.11G and normally all access point can cover 100mradius in open space.

6.5 Firewall

DMZ (Demilitarized Zone) is a commonly-touted feature of home broadband routers. UUM has implemented their networking firewall using DMZ device. In a DMZ configuration, many computers on the LAN run outside the firewall connected to a public network as similar as the Internet. Those computers have the ability to intercept traffic and broker requests for the rest of the LAN, adding an extra layer of protection for computers behind the firewall. Nowadays, computers in DMZ are able to respond, forward or re-issue requests out to the Internet or other public network, as what the proxy servers do. Besides, the LAN firewall is to prevent computers in the DMZ from initiating

inbound requests. It means, the incoming requests must first pass through a DMZ computer before reaching the firewall.

6.6 UUM Learning Zone Architecture

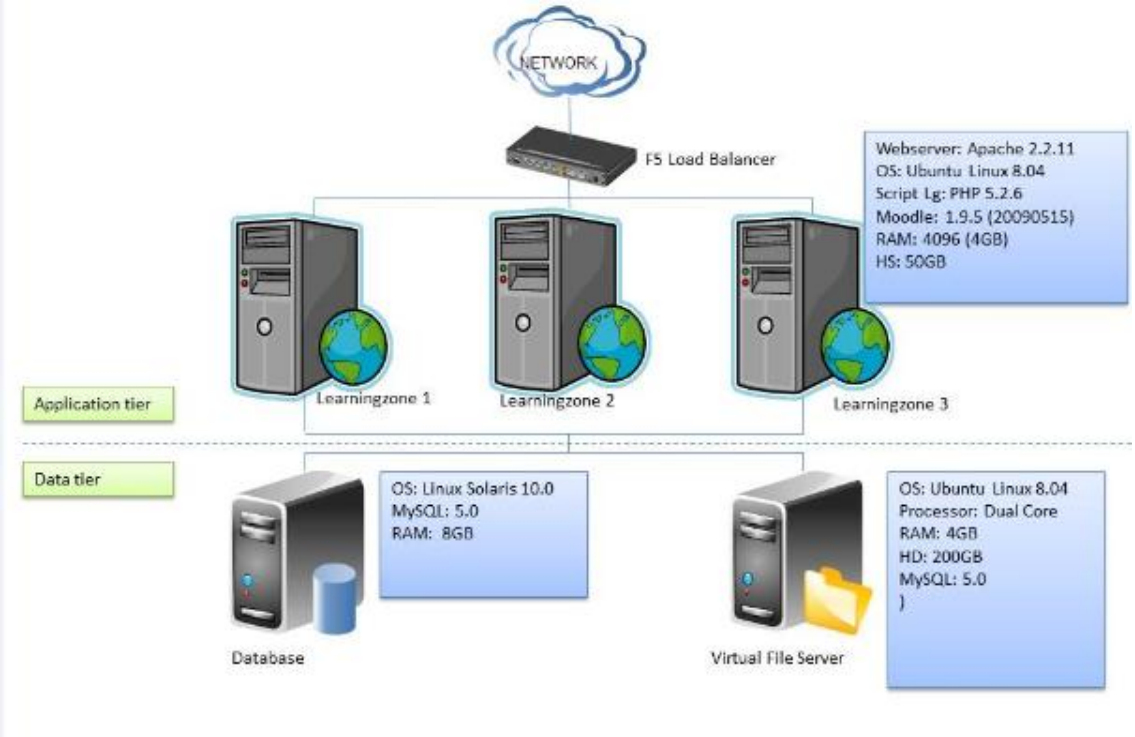


Figure 6.1: Learning Zone UUM Architecture

The Figure 6.1 shows the complete UUM Learning Zone Architecture. There are 4 databases for each semester. There are also 3 main servers. The virtual file server is used to store the teaching and learning materials of each semester. This server is mainly storing metadata which is the reference or directory of the data.

For every term and semester ends, all the data has to be backup and moved to archive folder. Then, a new moodle has to be built for the coming new semester. The new moodle is developed in the development server and then it will be transferred to the production server. However, the crucial scenario and problem is most probably occurred. It is system failure.

Besides, the teaching materials developed by the lecturers for the LMS do conform to SCORM, which is a collection of standards and specifications for web-based e-learning. It has communications between client side content and a host system called the run-time environment, which is commonly supported by a learning management system (LMS).

CHAPTER 7

METHODOLOGY ANALYSIS

This chapter presents in details the methodology used in the study. It starts with the process of data selection and collection, followed by various data preprocessing processes. Once the data is processed, it is trained and validated through the methodology. An optimized mitigation is created at the end of the experiment.

Figure 3.1 shows the complete steps of the methodology used in this research. The major steps involved in the methodology will start with the process of data collection from the target UUM Computer Centre staff, followed by the subsequent analysis processes of existing OCTAVE method.

In order to collect data, an interview with Computer Centre staff has been carried out on 21 April 2011, at 1pm, Conference room. There were 5 staffs that were really spending time to attend the interview. There were Madam Nor Asiah binti Abdul Rahman (Information Technology Officer), Mr. Abdul Razak bin Ali (Senior Information Technology Officer), Mr. Shaiful Rizal bin Samad (Assistant Information Technology Officer), Mr. Khalil Kusairi bin Hisam (Chief Information Technology Officer) and Mr. Amran bin Abdullah (Information Technology Officer). Besides, I also prepared questionnaires for them to answer.

There are four distinct area of activity that are carried out through eight steps in the OCTAVE Allegro methodology. The activity areas are shown in the Table 7.1.

Activity Area	Description
Establish drivers	Develop risk measurement criteria that are consistent with UUM Computer Centre drivers.
Profile assets	Identify the assets of the risk assessment and profile the assets containers that are identified.
Identify threats	Identify and document the threats in the context of their containers through a structured process.
Identify and mitigate risks	Identify and analyze the risks based on threat information and mitigation strategies are developed to address those risks.

Table 7.1: Description for the activity areas

The individual steps of the methodology are described in more details below.

7.1 Step 1 – Establish Risk Measurement Criteria

The first step in the OCTAVE Allegro process establishes the organizational drivers that will be used to evaluate the effect of a risk to an organization's mission and business objective. These drivers are reflected in a set of risk measurement criteria that is created and captured as part of this initial step. Risk measurement criteria are a set of qualitative measures against which the effects of a realized risk can be evaluated and form the foundation of an information asset risk assessment. Using consistent risk measurement criteria that accurately reflect an organizational view ensures that decisions

about how to mitigate risk will be consistent across multiple information assets and operating or departmental units.

In addition to evaluate the extent of an impact in a specific area, an organizational must recognize which impact areas are the most significant to its mission and business objectives. For example, an impact in technical access may be more significant than an impact on its physical access in UUM Learning Zone. This prioritization of impact areas is also performed in this initial step.

7.2 Step 2 – Develop an Information Asset Profile

The methodology focuses on the information assets of the organizational and begins the process of creating a profile for those assets. A profile is a representation of an information asset describing its unique features, characteristics and value. This process is to ensure that an asset is clearly and consistently described, there is free of ambiguous definition of the asset's boundaries and the security requirements for the asset are adequately defined. The profile for each asset is captured on a single worksheet that forms the basis for the identification of threats and risks in subsequent steps.

7.3 Step 3 – Identify Information Asset Containers

Container is the place where information assets are stored, transported and processed. In this step, all of the containers in which an asset is stored, transported and processed, whether internal or external are identified. Furthermore, an information asset

has to be mapped to all of the containers in which it lives. Therefore, defining the boundaries and unique circumstances must be examined for risk.

7.4 Step 4 – Identify Areas of Concern

It begins the risk identification process by brainstorming about possible conditions or situations that can threaten an organization's information asset. Area of concern may characterize a threat that is unique to an organization and its operating conditions. The purpose of this step is to quickly capture a complete list of all possible threat scenarios for an information asset.

7.5 Step 5 – Identify Threat Scenarios

In the first half of Step 5, the areas of concern captured in Step 4 are expanded into threat scenarios that further detail the properties of a threat. However, the collection of threats developed from these areas of concern does not necessarily provide a robust consideration of possible threats to an organization's information asset. Therefore, in the second half of Step 5, a broad range of additional threats is considered by examining threat scenarios.

A range of threat scenarios can be represented visually in a tree structure or it is also known as a threat tree. The details about threat tree are as follows:

Threat Tree	Definition
Human actors using technical means	Threats to the information asset via the organization's technical infrastructure or by direct access to a container (technical asset)

	that hosts an information asset. They require direct action by a person and can be deliberate or accidental in nature.
Human actors using physical access	Threats to the information asset that result from physical access to the asset or a container (technical asset) that hosts an information asset. They require direct action by a person and can be deliberate or accidental in nature.
Technical problems	Problems with an organization's information technology and systems. For example, hardware defects, software defects, malicious code and other system-related problems.
Other problems	Problems or situations that are outside the control of an organization. For example, natural disasters and unavailability of critica infrastructures.

Table 7.2: Description for the threat three

The threat scenarios derived from the areas of concern correspond to a branch on one or more of these threat trees. Each branch of the threat tree is also considered for each information asset in order to ensure a more robust consideration of threats.

Besides, this step also provides an opportunity for consideration of probability in the description of threat scenarios. Probability helps an organization determine which of the scenarios are more likely given its unique operating environment. This is useful in

later steps when an organization begins the process of prioritizing its risk mitigation activities. However, because it is often difficult to accurately quantify probability, especially with respect to security vulnerabilities and events, probability is expressed in this methodology qualitatively as high, medium or low.

7.6 Step 6 – Identify Risks

In Step 6, the consequences to an organization if a threat is realized are captured and completing the risk picture. A threat can have multiple potential impacts on an organization. For example, the disruption in UUM Learning Zone system can affect UUM's reputation with its lecturers and students as well as its productivity. The activities involved in this step ensure that the various consequences of risk are captured.

7.7 Step 7 – Analyze Risks

In Step 7, a simple quantitative measure of the extent to which the organization is impacted by a threat is computed. This relative risk score is derived by considering the extent to which the consequence of a risk impacts the organization against the relative importance of the various impact areas and possibly the probability. For example, if reputation is most important to an organization, risks that have an impact on the organization's reputation will generate higher scores than risks with same impacts and probabilities in another area. By prioritizing these impact criteria, an organization ensures that risks are prioritized in the context of its organizational drivers.

7.8 Step 8 – Select Mitigation Approach

In Step 7, the final step of the OCTAVE Allegro process, organizations determine which of the risks they have identified require mitigation and develop a mitigation strategy for those risks. This is accomplished by first prioritizing risks based on their relative risk score. Once risks have been prioritized, mitigation strategies are developed that consider the value of the asset and its security requirements, the containers in which it lives as well as the organization's unique operating environment.

CHAPTER 8

RESULT ANALYSIS

This chapter presents the results of the eight steps of the OCTAVE Allegro methodology. The outputs obtained from each step in the process are captured on a series of worksheets which are then used as inputs to the next step in the process.

8.1 Step 1 – Establish Risk Measurement Criteria

A qualitative set of measures (risk measurement criteria) is defined in order to evaluate a risk's effect on UUM Learning Zone's mission and goals. It defines ranges of high, medium and low impacts for UUM Learning Zone. The criteria are documented on the *Risk Measurement Criteria Worksheets*. The impact areas are Reputation or Customer Confidence, Financial, Productivity, Specific institutional policy.

After that, the impact areas are prioritized from most important to least important using the *Impact Area Ranking Worksheet*. The most important category should receive the highest score and the least important the lowest. All impact areas that will be used for risk measurement must be ranked. This prioritization is used in the risk assessment to develop a relative risk score that can help UUM Computer Centre to determine how to address risks that have been identified in the assessment.

Table 8.1 : RISK MEASUREMENT CRITERIA – REPUTATION AND CUSTOMER CONFIDENCE

Allegro Worksheet 1	RISK MEASUREMENT CRITERIA – REPUTATION AND CUSTOMER CONFIDENCE		
Impact Area	**Low**	**Moderate**	**High**
Reputation (Computer Centre Staff)	Reputation among Computer Centre staff is minimally affected; little or no effort or expense is required to recover.	Reputation among Computer Centre staff is damaged. No more than $100K in time and effort required to recover.	Reputation among Computer Centre staff is severely damaged. More than $100K in time and effort required to recover. Relationship with Computer Centre staff is affecting reputation with lecturers and students. Poor relationship affecting UUM learning Zone efficiency and having noticeable effect reliability rate.
Reputation (Lecturers)	Reputation among lecturers is minimally affected; little or no effort or expense is required to recover. Little or no change in	Reputation among lecturers is damaged, causing lecturers population to reconsider encouraging students to use	Reputation among lecturers is severely damaged. Academic lecturers are considering leaving. Occupancy changes of

	Computer Centre occupancy rate.	UUM Learning Zone. Occupancy rate changes of between one and five percent directly attributable to reputation problem. More than $100K in time and effort required to recover.	more than five percent are directly attributable to reputation problems. More than $500K in time and effort required to recover.
Reputation (Students)	Reputation among students from which UUM Learning Zone draws students is minimally affected; little or no effort or expense is required to recover.	Reputation among students is damaged, causing potential students to balk at lecturers' recommendations to use the UUM Learning Zone. More than $100K in time and effort required to recover.	Reputation among students is severely damaged, causing potential students to refuse lecturers' recommendations to use the UUM Learning Zone. More than $500K in time and effort required to recover.
Other: Occupancy Rates	A reduction of the UUM occupancy rate of less than 2%	A reduction of the UUM occupancy rate of between 2% and 5%.	A reduction of the UUM occupancy rate of more than 5%

Table 8.2: RISK MEASUREMENT CRITERIA – FINANCIAL

Allegro Worksheet 2	RISK MEASUREMENT CRITERIA – FINANCIAL		
Impact Area	**Low**	**Moderate**	**High**
Cost of Equipment and Access	Increase of less than 2.5% in annual equipment costs.	Increase of between 2.5% and 5% in annual equipment costs.	Increase of more than 5% in annual equipment costs.
Maintenance Costs and Infrastructure	Less than $100K reduction in yearly maintenance loss	Between $100K and $1M in yearly maintenance loss	More than $1M in yearly maintenance loss
Direct Cost	Less than $100K reduction in yearly direct costs	Between $100K and $1M in yearly direct costs	More than $1M in yearly direct costs
Conversion Costs	Less than $100K reduction in yearly conversion costs	Between $100K and $1M in yearly conversion costs	More than $1M in yearly conversion costs
Other:			

Table 8.3: RISK MEASUREMENT CRITERIA – PRODUCTIVITY

Allegro Worksheet 3	RISK MEASUREMENT CRITERIA – PRODUCTIVITY		
Impact Area	**Low**	**Moderate**	**High**
Staff Hours	Staff work hours increase labor costs by less than $100K.	Staff work hours increase labor costs between $100K and $1M.	Staff work hours increase labor costs by more than $1M.
Other: Maintenance Rate	Maintenance rate for UUM Learning Zone decreases less than 2%.	Maintenance rate for UUM Learning Zone decreases between 2% and 5%.	Maintenance rate for UUM Learning Zone decreases by more than 5%.
Other:			

Table 8.4: RISK MEASUREMENT CRITERIA – TECHNOLOGY

Allegro Worksheet 4	RISK MEASUREMENT CRITERIA - TECHNOLOGY		
Impact Area	**Low**	**Moderate**	**High**
Reliability	No occasional breakdowns and interruptions to Computer Centre staff, lecturers and students.	Temporary occurrences on breakdowns and interruptions. Only minimal affects on motivation and concentration from loss of time.	Permanent occurrences on breakdowns and interruptions. Loss of time that seriously affects motivation and concentration.
Stability	Minimal rapid evolution of the technology for Computer Centre staff and lecturers.	Temporary rapid evolution of the technology for Computer Centre staff and lecturers.	Tremendous rapid evolution has caused instability of the technology in hardware, software and delivering bandwidth. It radically affects the attraction and reliability of UUM Learning Zone among lecturers and students.
Other:			

Table 8.5: RISK MEASUREMENT CRITERIA – SPECIFIC INSTITUTIONAL POLICY

Allegro Worksheet 5	RISK MEASUREMENT CRITERIA – SPECIFIC INSTITUTIONAL POLICY		
Impact Area	**Low**	**Moderate**	**High**
University Policy	No University fears of mischief and viruses has to the deployment of UUM Learning Zone	Minimal University fears of mischief and viruses to the deployment of UUM Learning Zone	Tremendous University fears of mischief and viruses has proved highly inhibiting to the deployment of UUM Learning Zone
Other:			

Table 8.6: RISK MEASUREMENT CRITERIA – USER DEFINED

Allegro Worksheet 6	RISK MEASUREMENT CRITERIA – USER DEFINED		
Impact Area	**Low**	**Moderate**	**High**

Table 8.7: IMPACT AREA PRIORITIZATION

Allegro Worksheet 7	IMPACT AREA PRIORITIZATION WORKSHEET
PRIORITY	**IMPACT AREAS**
5	**Technology**
4	**Financial**
3	**Productivity**
2	**Reputation and Customer Confidence**
1	**Specific Institutional Policy**
n/a	**User Defined**

8.2 Step 2 – Develop an Information Asset Profile

In this step, it is a process of defining the information asset. After that, the containers are identified which the information asset "live". This can fully identify all of the points at which the information assets might be vulnerable to disclosure, modification, loss/destruction or interruption.

A profile is created to form the basis for the identification of threats and risks in subsequent steps. Information asset profiling is important for ensuring that an asset is clearly and consistently described, that there is an unambiguous definition of the asset's boundaries and that the security requirements for the asset are adequately defined.

Table 8.8: CRITICAL INFORMATION ASSET PROFILE

Allegro Worksheet 8	CRITICAL INFORMATION ASSET PROFILE	
(1) Critical Asset *What is the critical information asset?*	**(2) Rationale for Selection** *Why is this information asset important to the organization?*	**(3) Description** *What is the agreed-upon description of this information asset?*
Teaching and Learning Materials	**Keeping the teaching materials is important to complement lecturers' lectures and tutorials. Besides, keeping the learning materials is essential for students to access supplementary learning materials, browse through related web resources, attempt quizzes and discuss topics related to their subjects.**	**This information asset contains all of the information necessary to help students to have better learning experience and acquire critical lifelong learning skills. This includes forums, chat room, messages, courses, latest news and associated materials codes and histories.**

(4) Owner(s) *Who owns this information asset?*		
The owner of the information asset is the Madam Nor Asia bent Abdul Raman (Information Technology Officer)		
(5) Security Requirements *What are the security requirements for this information asset?*		
□ **Confidentiality**	Only authorized personnel can view this information asset, as follows:	**Staff of the UUM Computer Centre responsible for arranging and uploading teaching materials should have "read" access to the online course created. Lecturers also can have access to the units that have been created. Students have their own "read" access to their own registered courses.**
□ **Integrity**	Only authorized personnel can modify this information asset, as follows:	**Only authorized lecturers may update or change the teaching materials. The teaching materials should only be updated with the actual teaching contents provided to the students.**
□ **Availability**	This asset must be available for these personnel to do their jobs, as follows:	**The teaching and learning materials must be available to Computer Centre staff for updates to the system and for maintenance purpose.**
	This asset must be available for **24** hours, **7** days/week, **and 52**	**The teaching and learning materials information asset should be available 24 x 7 as lecturer and students are able to access to the**

	weeks/year.	**UUM Learning Zone for learning purpose. It also must be available to the Computer Centre staff, especially the UUM Learning Zone Staff during regular office hours.**
□ **Other**	This asset has special regulatory compliance protection requirements, as follows:	

(6) Most Important Security Requirement

What is the most important security requirement for this information asset?

□ Confidentiality	□ Integrity	□ **Availability** √	□ Other

8.3 Step 3 – Identify Information Asset Containers

The places where an information asset is stored, transported or processed can become points of vulnerability and threats that put the information asset at risk. In other word, they can also become places where controls can be implemented to ensure that information assets are protected from harm so that they can be used as intended.

Containers are most typically identified as some type of technical asset such as hardware, software of system, application system, servers and networks. Besides, a container can also be a physical object such as piece of paper or a person that is important to UUM Learning Zone. People containers are particularly important with respect to intellectual property or information that is generally sensitive or confidential.

Table 8.9: INFORMATION ASSET RISK ENVIRONMENT MAP (TECHNICAL)

Allegro Worksheet 9a	INFORMATION ASSET RISK ENVIRONMENT MAP (TECHNICAL)
INTERNAL	
CONTAINER DESCRIPTION	**OWNER(S)**
1. The teaching and learning materials primarily resides on the UUM Learning Zone which consists of four database servers and three main application/ web servers. It provides a web interface for authorized personnel to access or manipulate the data entries. The underlying operating system is Ubuntu Linux	**Managed by UUM Computer Centre**
2. UUM internal network. All transactions to and from the UUM Learning Zone travel on the network.	**Managed by UUM Computer Centre**
3.	
4.	

EXTERNAL	
CONTAINER DESCRIPTION	**OWNER(S)**
1. The internet. Once UUM lecturer has requested to create an online unit on UUM Learning Zone, the request will be approved by the chair executives. All the approval requests are electronically sent to all the respective lecturers.	**Managed by UUM Computer Centre**
2.	
3.	
4.	

Table 8.10: INFORMATION ASSET RISK ENVIRONMENT MAP (PHYSICAL)

Allegro Worksheet 9b	INFORMATION ASSET RISK ENVIRONMENT MAP (PHYSICAL)
INTERNAL	
CONTAINER DESCRIPTION	**OWNER(S)**
1. Backup tapes of teaching and learning materials are created in the end of each semester.	**Managed by UUM Computer Centre**
2.	
3.	
EXTERNAL	
CONTAINER DESCRIPTION	**OWNER(S)**
1.	
2.	

Table 8.11: INFORMATION ASSET RISK ENVIRONMENT MAP (PEOPLE)

Allegro Worksheet 9c	INFORMATION ASSET RISK ENVIRONMENT MAP (PEOPLE)
INTERNAL PERSONNEL	
NAME OR ROLE/RESPONSIBILITY	**DEPARTMENT OR UNIT**
1. Computer Centre Staff	**UUM Computer Centre**
2.	
3.	
EXTERNAL PEERSONNEL	
CONTRACTOR, VENDOR,ETC	**ORGANIZATION**
1. Third-party vendor manages the integration Implementation from Sybase to the UUM Learning Zone system. Relationship is managed via the UUM Computer Centre.	**SRNS Technology (IT company)**
2.	

8.4 Step 4 – Identify Areas of Concern

In step 4, it is a process of developing information asset risk profiles. Risk is the combination of a threat and the resulting impact of the threat if acted upon. Here, it begins to address the threat component of the risk equation by brainstorming about possible conditions or situations that can threaten your information asset. These real world scenarios are referred to as areas of concern and may represent threats and their corresponding undesirable outcomes. The areas of concern are captured and used to seed the development of risk profiles in Step 5. The following are examples of areas of concern:

Areas of concern
Power failure at UUM Computer Centre
Backup tapes lost and unable to recover teaching materials.

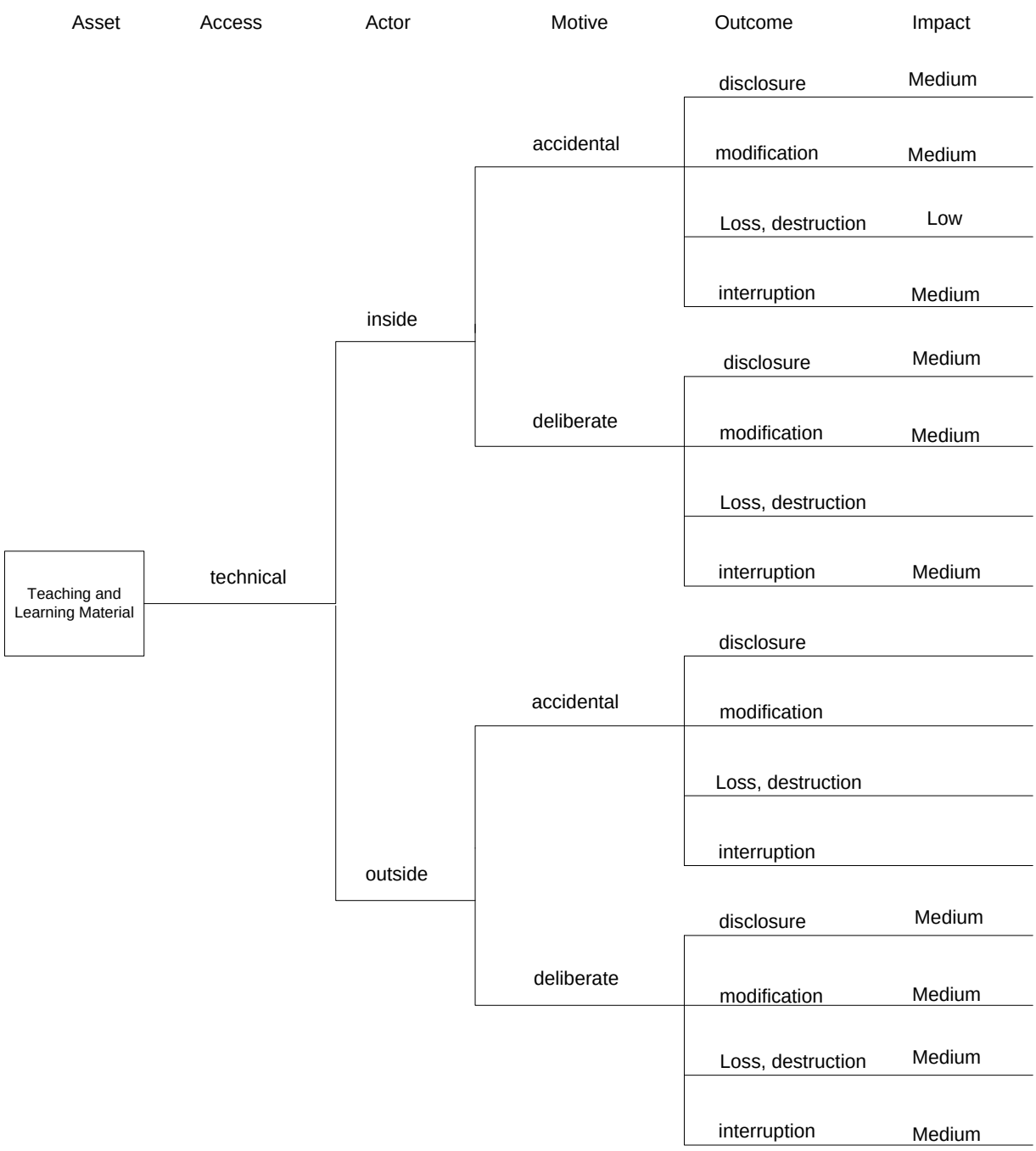
8.5 Step 5 – Identify Threat Scenarios

In step 5, areas of concern are expanded into threat scenarios that further detail the properties of a threat. A threat has the following properties:

- Asset – something of value to the enterprise
- Access/means – how the asset is accessed by an actor (technical means, physical access). Access applies only to human actors.
- Actor – who or what may violate the security requirement (confidentiality, integrity, availability) of an asset.
- Motive – the intent of an actor. For example: deliberate or accidental). Motive applies only to human actors.
- Outcome – the immediate result (disclosure, modification, destruction, interruption) of violating the security requirements of an asset.

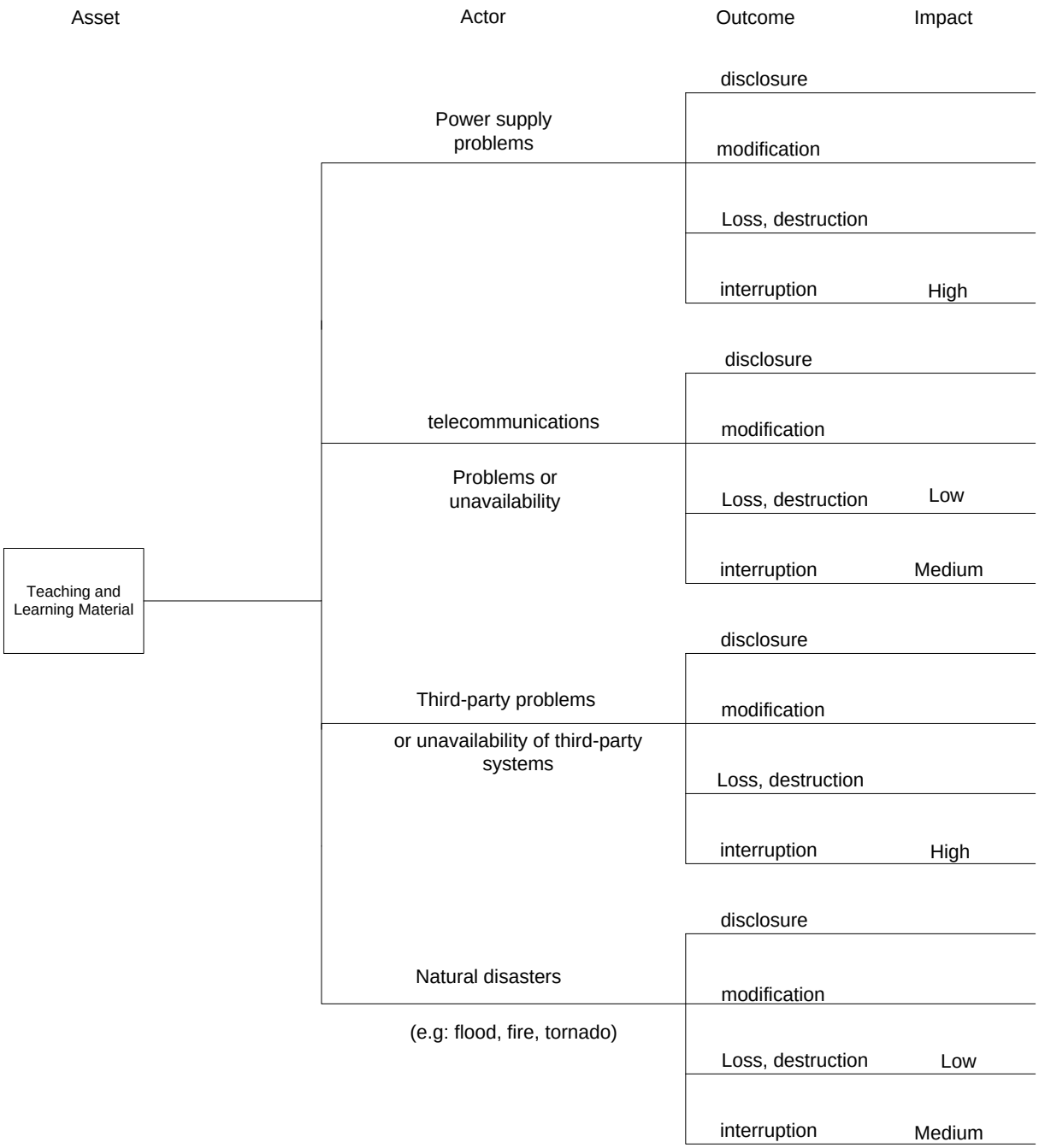
In the Allegro risk assessment, four threat trees are considered. These trees are described in the Table 7.2 and graphically represented below.

Figure 8.1 - Human Actors Using Technical Access



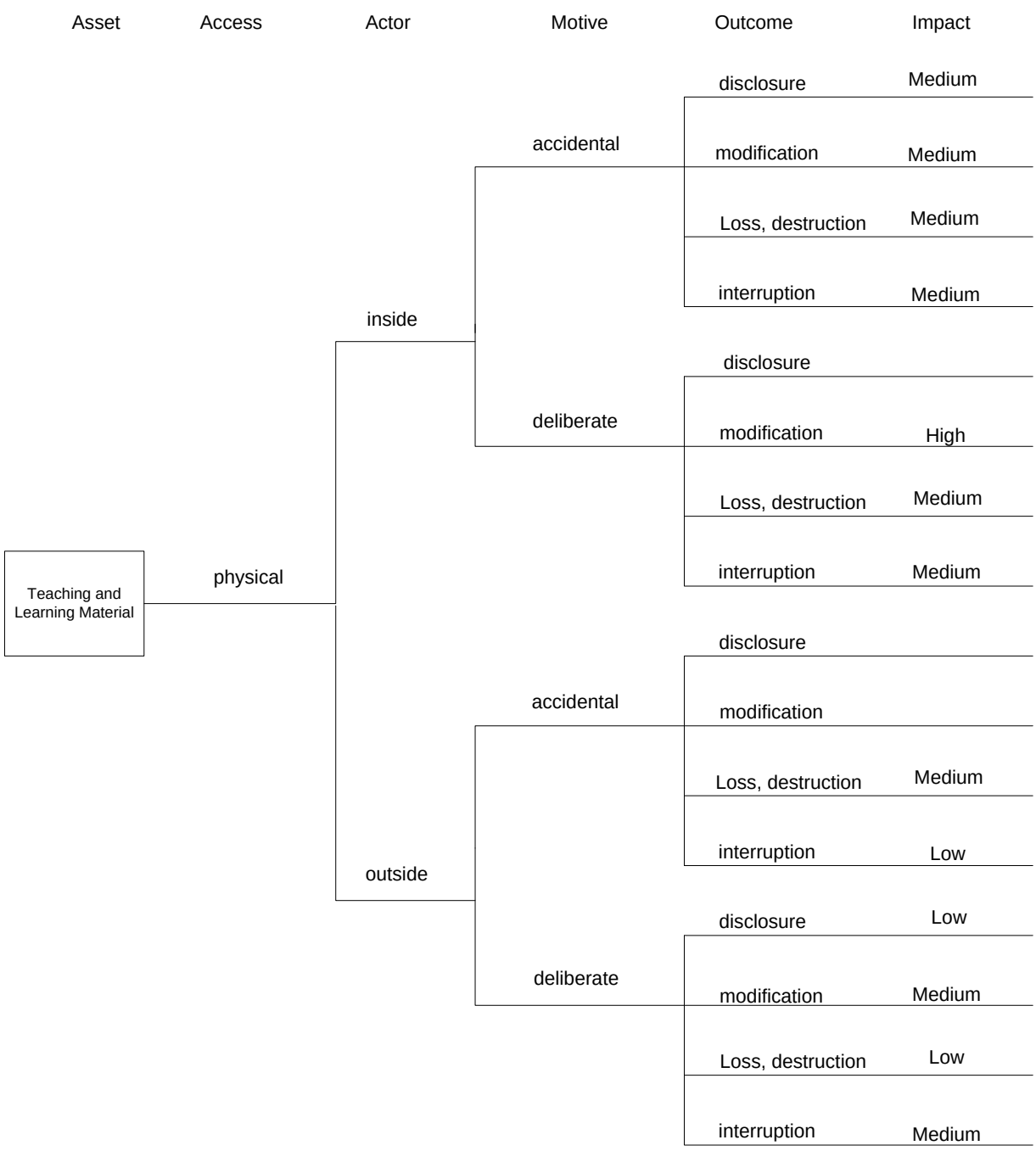
Based on the tree above, the UUM Computer Centre staffs have the potential in disclosure, modification and interruption teaching and learning materials in accidentally or deliberately by using networks. Besides, outsiders such as part-time registered students and part-time lecturers have the chance to deliberate the teaching and learning materials in the result of disclosure, modification, interruption and loss or destruction through Internet.

Figure 8.2 - Other Problems Using Technical Access



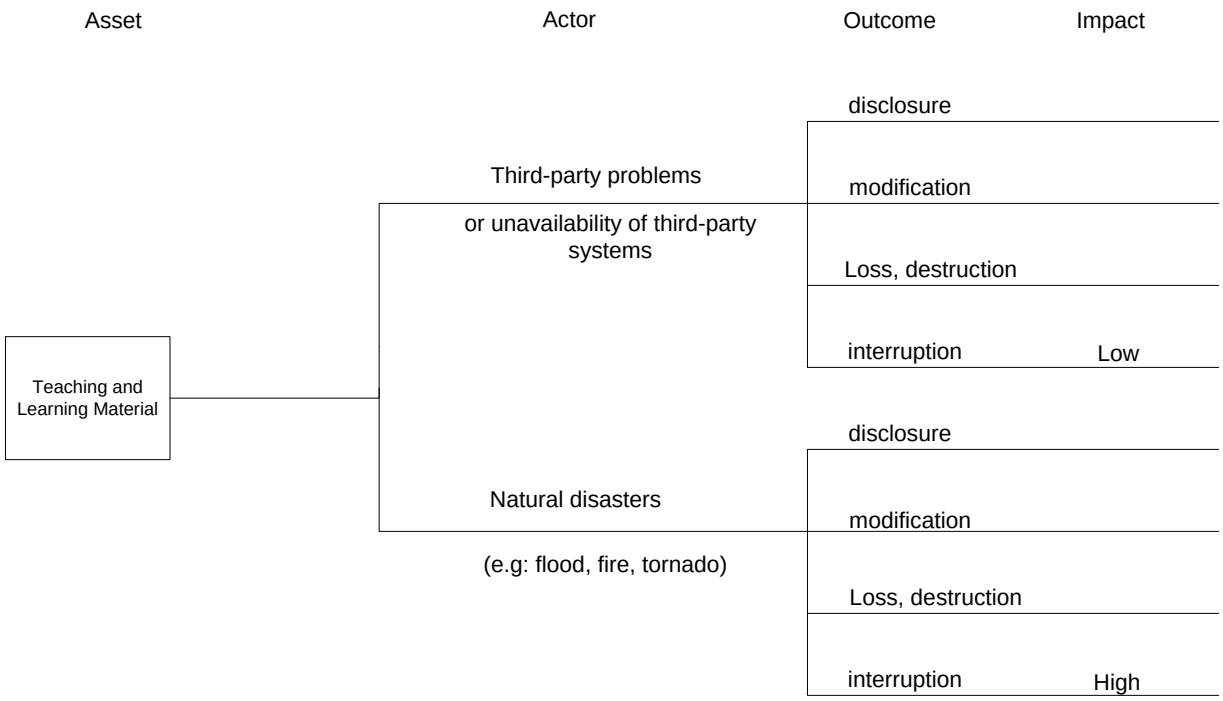
From the tree above, mostly the problems are occurred in power supply and unavailability of third party systems. These two problems have caused a tremendous interruption for teaching and learning materials in UUM Learning Zone.

Figure 8.3 - Human Actors Using Physical Access



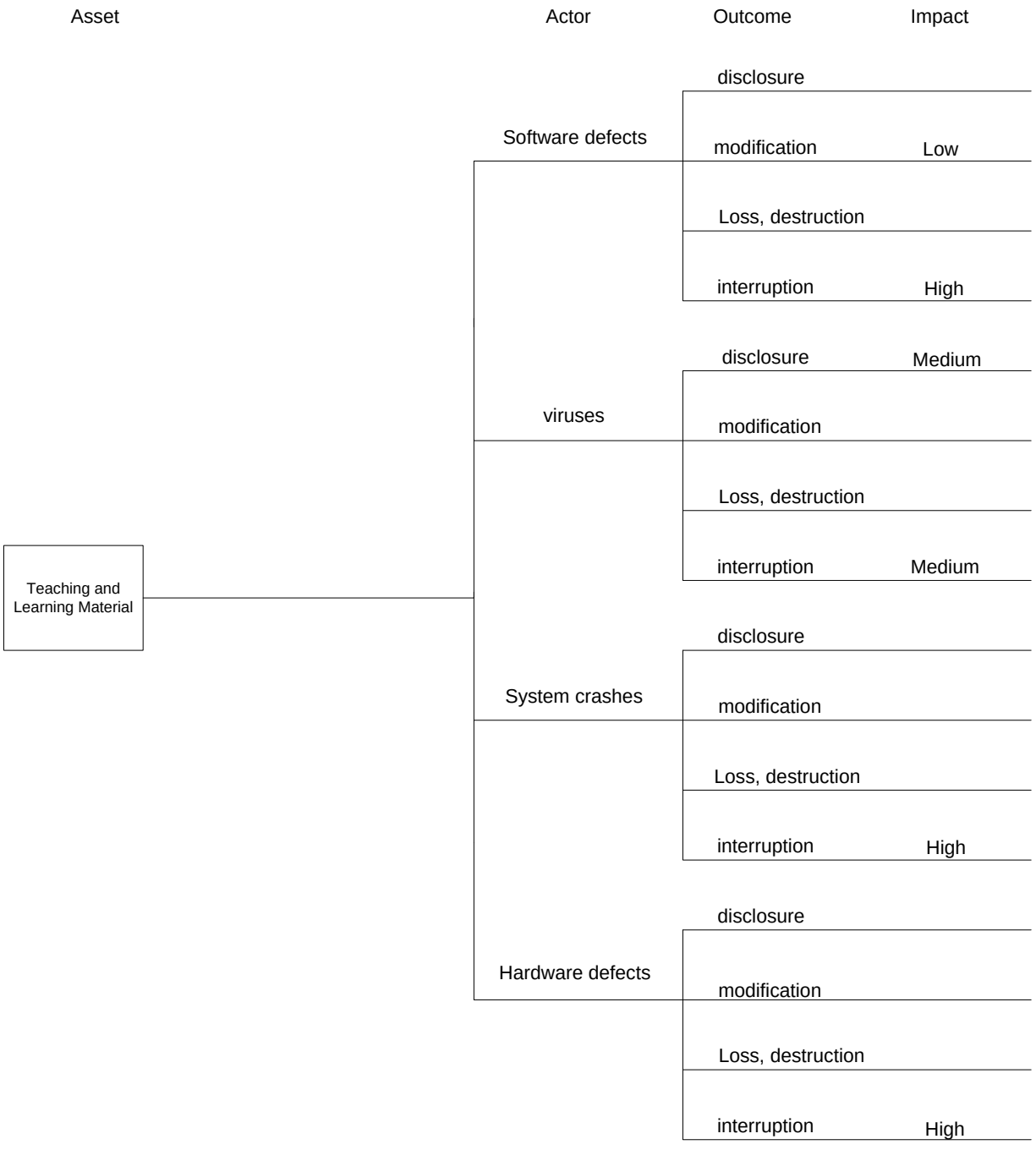
Based on the tree above, the UUM Computer Centre staffs have the potential in disclosure, modification, loss and interruption teaching and learning materials in accidentally.

Figure 8.4 - Other Problems Using Physical Access



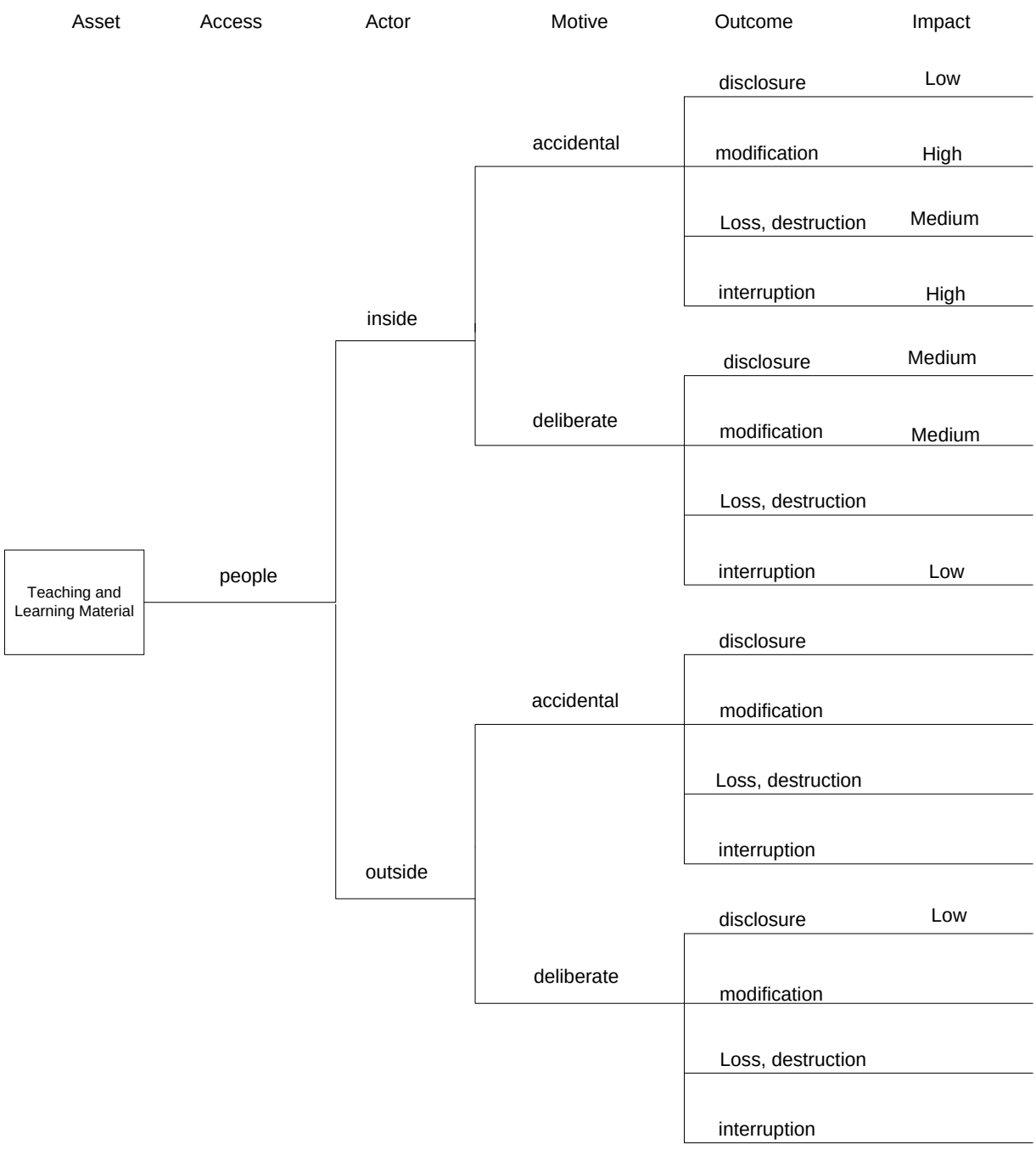
Natural disaster is the main source to lead the teaching and learning materials have a high chance to be interrupted.

Figure 8.5 - System Problems



Based on the tree above, software defects, hardware defects and system crashes are the main problems to give high interruption on the teaching and learning materials in UUM Learning Zone.

Figure 8.6 - Human Actors Using People Access



Based on the tree above, the UUM Computer Centre staffs are accidentally modifying and interrupting the teaching and learning materials in most of the time.

8.6 Step 6 – Identify Risks

By identifying how the organization is impacted, we can complete the risk equation. This can be illustrated as follows:

Threat (condition) + Impact (consequence) = Risk

[Step 4 and Step 5] + [Step 6] = Risk

The following table provides a few examples.

Threat Scenario	Consequence
Power failure at UUM Computer Centre	Significant labor charges will be required to re-create the teaching courses.
Backup tapes lost and unable to recover transactions.	The lecturers' overall perception of the UUM Learning Zone's quality could be negatively affected if the teaching materials are publicized.

8.7 Step 7 – Analyze Risks

In Step 7, I qualitatively measure the extent to which the UUM Learning Zone is impacted by a threat by computing a risk score for each risk to each information asset. This scoring information is used for determining which risks have to be mitigated immediately and for prioritizing mitigation actions for the remainder of risks in Step 8.

Besides, a relative risk score will be generated. The relative risk score is derived by considering the extent to which the consequence of a risk affects UUM Learning Zone as compared to the relative importance of the various impact areas. That means, if the area of "reputation" is most important in UUM Learning Zone and the consequence of a risk causes an extensive impact to reputation, and then action has to be taken to ensure that this risk is mitigated. By using these criteria, it is to ensure that risks are scored in the context of the organizational drivers.

Consider the following example:

Threat Scenario	Consequence
Backup tapes lost and unable to recover transactions. (Only one set of backup tapes is currently being created and store off site.)	If there is a system crash and UUM Computer Centre is unable to recall backup tapes to restore teaching and learning materials, then all materials will need to be restored from the respective lecturers.
	There would be significant financial and productivity impacts to restore materials.
	Likely that during the restoration process many changes would be overlooked or incorrectly added.

This consequence indicates direct effects on the UUM Learning Zone's financial and productivity. By using the *Risk Measurement Criteria* in Step 1, the following values were assigned.

Impact Area	**Impact Value**
Reputation & Customer Confidence	Moderate
Financial	High
Productivity	High
Technology	Low
Specific Institutional Policy	Low

The value of "high" in financial and productivity are assigned because UUM Learning Zone has to restore all transactions. The consequence has little or no effect on specific institutional policy, so a value of "low" has been assigned.

Impact values are assigned quantitative values as follows: High – 3, Moderate – 2 and Low – 1.

Consider the following example. UUM Learning Zone ranked its impact areas as shown below. The technology area is considered to be the most important impact area and the specific institutional policy the least important. The impact values were assigned as the consequences were considered. The following table shows the way to calculate the total score for Table 8.13.

Impact Area	**Ranking**	**Impact Value**	**Score**
Reputation	2	Moderate (2)	4
Financial	4	High (3)	12
Productivity	3	High (3)	9
Technology	5	Low (1)	5
Specific Institutional Policy	1	Low(1)	1
		Total Score	**31**

8.7 Step 8 – Select Mitigation Approach

In Step 8, risks have to be considered on which mitigate is needed and how. This is done by prioritizing risks, deciding on an approach to mitigate important risk based on a number of organizational factors and developing a mitigation strategy that considers the value of the asset and the places where it lives.

Besides, it is simply to sort each of the risks that have identified by their risk score. Then, the risks are categorized in an orderly way that will help to begin to make decision on the mitigation status. In fact, there are many ways for UUM Learning Zone to categorize its risks. One of the ways is to develop a risk matrix to categorize the risks identified. The Relative Risk Matrix table below shows an example of how to do this.

RELATIVE RISK MATRIX			
PROBABILITY	**RISK SCORE**		
	30 TO 45	**16 TO 29**	**0 TO 15**
HIGH	POOL 1	POOL 2	POOL 2
MEDIUM	POOL 2	POOL 2	POOL 3
LOW	POOL 3	POOL 3	POOL 4

A mitigation approach is assigned to each risk. The following table can be used as a guide to make decision in mitigation. However, a decision about a mitigation approach is highly dependent on UUM Learning Zone's unique operating circumstances.

Pool	Mitigation Approach
Pool 1	Mitigate
Pool 2	Mitigate or Defer
Pool 3	Defer or Accept
Pool 4	Accept

By referring to Table 8.13, it shows the risk score is 31 and the probability is medium. Therefore, these two indications show that the risk is in Pool 2. That means the risk can be mitigated or deferred. Based on the risk score, there is a mitigation approach.

Besides that, according to Table 8.12, the total risk score is calculated as follows.

Impact Area	**Ranking**	**Impact Value**	**Score**
Reputation	2	Moderate (2)	4
Financial	4	High (3)	12
Productivity	3	High (3)	9
Technology	5	Moderate (1)	10
Specific Institutional Policy	1	Low(1)	1
		Total Score	**36**

By referring to Table 8.12, it shows the risk score is 36 and the probability is medium. Therefore, these two indications show that the risk is in Pool 2. That means the risk can be mitigated or deferred. Based on the risk score, there is a mitigation approach.

Table 8.12 - INFORMATION ASSET RISK

Allegro – Worksheet 10		INFORMATION ASSET RISK WORKSHEET	
Information Asset Risk	Threat	**Information Asset**	Teaching and Learning Materials
		Area of Concern	Insufficient electrical power supply at UUM Computer Centre and lead to UUM Learning Zone system and equipments failure
		(1) Actor *Who would exploit the area of concern or threat?*	System which is overloaded and the power supply has been fully utilized in server room and the technical equipments at other department units in UUM Computer Centre
		(2) Means *How would the actor do it? What would they do?*	-
		(3) Motive *What is the actor's reason for doing it?*	-
		(4) Outcome *What would be the resulting effect on the information asset?*	□ **Disclosure** □ **Modification** □ **Destruction** □ **Interruption** √
		(5) Security Requirements *How would the information asset's security requirements be breached?*	UUM Learning Zone must be available for daily learning activities such as creating units and uploading teaching materials.
		(6) Probability	□ **High**

		What is the likelihood that this threat scenario could occur?	☐ **Medium**√ ☐ **Low**		
	(7) Consequences *What are the consequences to the organization or the information asset owner as a result of the outcome and breach of security requirements?*		**(8) Severity** *How severe are these consequences to the organization or asset owner by impact area?*		
			Impact Area	**Value**	**Score**
	Significant labor charges will be required to overcome the system failure as the Computer Centre staffs have to work in shifts.		Reputation & Customer Confidence	**Medium**	**4**
			Financial	**High**	**12**
	The lecturers' overall perception of the UUM Learning Zone's quality could be negatively affected if the users are unable to access to the system to complete their tasks at anytime.		Productivity	**High**	**9**
			Technology	**Medium**	**10**
	Significant financial and productivity impacts.		Specific Institutional Policy	**Low**	**1**
			User defined Impact Area		
				Relative Risk Score	**36**
(9) Risk Mitigation					

Based on the total score for this risk, what action will you take?			
□ **Accept**	□ **Defer**	□ **Mitigate √**	□ **Transfer**
For the risks that you decide to mitigate, perform the following:			
On what container would you apply controls?	*What administrative, technical and physical controls would you apply on this container? What residual risk would still be accepted by the organization?*		
UUM Computer Centre Staffs	• The UUM Computer Centre staffs have to be on duty at anytime to ensure the UUM Learning Zone is operating smoothly everyday without any failures.		
UUM Computer Centre	• Establish an electrical power generator at the UUM Computer Centre area in order to support daily high usage for computer system such as UUM Learning Zone.		

Table 8.13 - INFORMATION ASSET RISK

Allegro – Worksheet 10		INFORMATION ASSET RISK WORKSHEET	
Information Asset Risk	Information Asset	Teaching and Learning Materials	
	Area of Concern	Backup tapes lost and unable to recover teaching and learning materials. (Only one set of backup tapes is currently being created and store off site.)	
	Threat	**(1) Actor** *Who would exploit the area of concern or threat?*	UUM Computer Centre Staffs
		(2) Means *How would the actor do it? What would they do?*	Shipment of backup tapes is lost in storage.
		(3) Motive *What is the actor's reason for doing it?*	Accidental
		(4) Outcome *What would be the resulting effect on the information asset?*	□ **Disclosure** □ **Modification** □ **Destruction** √ □ **Interruption**
		(5) Security Requirements *How would the information asset's security requirements be breached?*	Only authorized personnel can view this information asset.

	(6) Probability *What is the likelihood that this threat scenario could occur?*	□ **High** □ **Medium**√ □ **Low**		
	(7) Consequences *What are the consequences to the organization or the information asset owner as a result of the outcome and breach of security requirements?*	**(8) Severity** *How severe are these consequences to the organization or asset owner by impact area?*		
		Impact Area	**Value**	**Score**
	If there is a system crash and UUM Computer Centre is unable to recall backup tapes to restore materials, then all materials will need to be restored from the respective lecturers.	Reputation & Customer Confidence	**Moderate**	**4**
		Financial	**High**	**12**
	There would be significant financial and productivity impacts to restore all materials.	Productivity	**High**	**9**
		Technology	**Low**	**5**
	Likely that during the restoration process many changes would be overlooked or incorrectly added.	Specific Institutional Policy	**Low**	**1**
		User defined		

		Impact Area		
			Relative Risk Score	**31**

(9) Risk Mitigation

Based on the total score for this risk, what action will you take?

☐ **Accept**	☐ **Defer**	☐ **Mitigate**√	☐ **Transfer**

For the risks that you decide to mitigate, perform the following:

On what container would you apply controls?	*What administrative, technical and physical controls would you apply on this container? What residual risk would still be accepted by the organization?*
Backup tapes	• Simply add a backup run and keep second copy of the backup tapes stored on site. Keeping a second copy of recent tapes on site will provide some redundancy but will not completely remove risk of being able to restore old materials.

CHAPTER 9

CONCLUSIONS

This chapter presents the major contributions of the study. It also describes the limitations faced in the methodology and hints how further works can be continued in the future.

9.1 Research Contributions

The findings of this research are to identify the information security risks occurred in UUM Learning Zone based on information asset risk from OCTAVE Allegro.

These findings of the study will provide UUM's Computer Centre management an in-depth view on maintaining reliability and integrity of the security system in UUM Learning Zone. By exploring the root of the problems and the relationship between/among the criteria, UUM Computer Centre is able to better plan its ICT facilities and services in order to provide a more secured and protected academic technologies to lecturers as well as students. By radically improving the UUM Learning Zone facilities and services, it is expected the new batch of the students or even new lecturers will be more adaptive and reliable to the E-Learning system.

It is anticipated that the results and suggestions of this project can be adopted and used by the related authorities as part of their reference when making strategy planning for E-Learning development process. In fact, UUM's lecturers and students are the main users for the UUM Learning Zone. However, the actuality of the information security risks happened in UUM Learning Zone is somehow stunning and worrying. Necessary corrective actions should be taken to prevent this situation form worsening. The high number of information security risks in UUM Learning Zone should be able to be reduced if the roots of the problems are highly valued and explored thoroughly.

The findings of this project are also expected to give the UUM's Computer Centre management a good guidance in planning their future services in the E-Learning system. This project is expected to highlight to them the possible security risks might happen in UUM Learning Zone in future use and create awareness among the Computer Centre management staffs.

9.2 Future Works

Due to the time constraint, it is regret that this project is not able to collect significant amount of data from UUM lecturers and students. The result obtained in this project may not be that perfect in evaluating the information security risks in UUM Learning Zone. Future works can be extended from this research by gathering more data from the UUM lecturer and students in order to achieve favorable result. Besides that, the factors that affect the information

security risks can be also be analyzed from more perspectives and dimensions rather that the methodology mentioned in this report.

REFERENCES

[1] Zhang, J., Zhao, L. & Nunamaker, J. F. (2004), "*Can e-learning replace classroom learning?"*, Communications of the ACM, 47(5): 75-79.

[2] Kritzinger, E. & H von Solms, S.H. (2006), *"E-learning: Incorporating Information Security Governance"*, Issues in Informing Science and Information Technology Institute, Volume 3, 2006, 319-325.

[3] Ahmad Jelani Shaari, Azman Ta'a & Muhamad Shahbani Abu Bakar (2004), *"Development and Implementation of an LMS : Universiti Utara Malaysia's Experience"*, 1-14.

[4] Caralli, R.A., Stevens, J., Young, L.R. & Wilson, W.R. (2007), *"Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process"*, Software Engineering Institute, Carnegie Mellon Unversity, 2007

[5] Vorster, A. & Labuschagne, L. (2005), *"A Framework for Comparing Different Information Security Risk Analysis Methodologies",* Proceedings of SAICSIT 2005, University of Johannesburg, 95-103

[6] Yin, R.K. 1993, *"Application of case study research Newbury Park",* Sage Publications.

[7] Kwok, L. & Longley, D. (1997), *"Code of practice: A standard for information security management"*, In Proceedings of IFIP TCII, 13th International Conference on Information Security.

[8] Von Solms, S. H. & Eloff, J. H. P. (2004), "*Information Security"*, Johannesburg, South-Africa.

[9] Von Solms, S. H. (2001a), "*Information security – A multidimensional discipline",* Computer & Security, 20(6): 504-508.

[10] Alberts, C., Dorofee, A., Stevens, J. & Woody, C. (2004) *"OCTAVE-S Implementation Guide, Version 1"*, Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 2004.

[11] Woody, C. (2006), *"Applying OCTAVE: Practitioners Report".* Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 2006.

[12] Mason, R. and Rennie. F. (2006), "*E-learning: the key concepts",* Routlege, Abingdon Great Britain.

[13]Eklund, J., Kay, M. and Lynch, H.M. (2003), *"E-learning: emerging issues and keytrends: A discussion paper"*, Australian National Training Authority, Australia.

[14]Conole, G., Smith, J. and White, S. (2007), *"A critique of the impact of policy and funding", in Conole, G. and Oliver, M. (eds). Contemporary perspectives in E-learning Research themes, methods and impact on practice*", Routledge, London, New York, pp. 38-54

[15]Dietinger, T. (2003), *"Aspects of E-Learning Environments (unpublished Doctor of Technical Sciences thesis)"*, Institute for Information Processing and Computer Supported New Media (IICM), Graz University of Technology, Austria.

[16]Morrison, D. (2003), *"E-learning strategies",* Wiley Chichester.

[17]Allen, E. and Seaman, J. (2007), *"Online Nation Five Years of Growth in Online Learning"*, I. Sloan Consortium, United States.

[18]Jain, K. K. and Ngoh, L. B. (2003), *"Motivating Factors in e-learning - Case Study of UNITAR, Student Affairs Online"*, [Online], vol. 4, no. 1, pp. 21, June, 2008 available at: http://www.studentaffairs.com/ejournal/Winter_2003/e-learning.html

[19]A. Aziz, S.H., M.Yunus, A.S., A. Bakar, K. and B. Meseran, H. (2006), *"Design and development of learning management system at Universiti Putra Malaysia : A case study of e-SPRINT. I"*, WWW 06: Proceedings of the 15th international Conference on World Wide Web, May 23-26, 2006, Edinburgh, Scotland, ACM, New York, pp.979-980

[20]Raitman, R., Ngo, L. and Augar, N. (2005), *"Security in the Online E-Learning environment"*, Advanced Learning Technologies, 2005. ICALTv2005. Fifth IEEE International Conference on Advanced Learning technologies, pp. 702-706.

[21]Rosenberg, M.J. (2001), *"E-learning strategies for delivering knowledge in digital age"*, McGraw-Hill, New York.

[22]Graf, F. (2002), *"Providing security for elearning"*, Computers & Graphics, vol. 26, no. 2, pp.355-365.

[23]Norman, S. and Da Costa, M. (2003), *"Overview of e-learning Specifications and Standards"*, Open Learning Agency, and Eduspecs Technical Liaison Office.

[24]Furnell, S.M. and Karweni, T. (2001), *"Security issues in Online Distance Learning"*, VINE: The Journal of Information and Knowledge Management Systems, vol.31, no.2.

[25]Yang, C., Lin, F.O. and Lin, H. (2002), *"policy-based Privacy and Security Management for Collaborative E-education Systems"*, Proceedings of the 5th

IASTED International Multi-Conference Computers and Advanced Technology in Education (CATE 2002), pp. 501-505.

[26]Saxena, R. (2004), *"Security and online content management: balancing access and security"*, Breaking boundaries: integration and interoperability, 12th Biennial VALA Conference and Exhibition Victorian Association for Library Automation.

[27]Yong, J. (2007), *"Digital Identity Design and Privacy Preservation for e-Learning"*, Proceeding of the 2007 11th International Conference on Computer Supported Cooperative Work in Design, pp.858-863.

[28]Treek, D. (2003), *"An integral framework for information systems security management"*, Computer & Security, vol.22, no. 4, pp.337-360.

[29]Abrams, M.D., Jajodia, S. and Podell, H.J. (1995), *"Information Security: An Integrated Collection of Essays"*, in IEEE Computer Society Press, Los Alamitos, CA, USA, pp.98-99.

[30]Whitson, G.(2003), *"Computer security: theory, process and management"*, J. Comput. Small Coll, vol.18, no. 6, pp. 57-66.

[31]Bornjman, M.G., and Labuschagne L.(2006), *" A Comparative Framework for Evaluating Information Security Risk Management Methods"*, Standard Bank Academy for Information technology, Rand Afrikaans University, South Africa.

[32]Martin, J (2003), *"Information Systems Security Training Virus and Worms"*, InfoSec Professionals, 2003.

[33]Bornman, G. and Labuschagne, L. (2004), *"A Comparative framework for evaluating information security risk management methods"*, In proceedings of the Information Security South Africa Conference, 2004.

[34]Alberts, C. and Dorofee, A. (2002), *"Managing information security risks, The OCTAVE approach"*, Addison Wesley, 2002.

[35]Fredriksen, R., Kristiansen, M., Gran, B., and Stolen, K. (2001), *"The CORAS framework for a model-based risk management process"*, 2001.

[36]Karabacak, B. and Sogukpinar, I. (2005), *"ISRAM: Information security risk analysis method"*, Computer & Security, vol.24, no. 2, pp.147-159.

[37]INTERNATIONAL SECURITY TECHNOLOGY Inc (IST Inc). 2000, *"Managing risks using CORA"*, PowerPoint presentation.

[38] Najwa Hayaati Mohd Alwi and Ip-Shing, F. (2010), *"E-Learning and Information Security Management"*, Infonomics Society, 2010.

[39]Raitman, R., Ngo, L., Augar, N. and Zhou, WL., (2005), *"Security in the Online E-learning Environment"*, Proceedings of the Fifth IEEE International Conference on Advanced Learning Technologies (ICALT '05), 2005.

[40]Patomviriyavong, S., Samphanwattanachai, B. and Suwannoi, T., (2006), "*eLearning Operational Risk Assessment and Management: A Case Study of the M.Sc. in management Program*", Third International Conference on eLearning for Knowledge-Based Society, August 3-4, 2006, Bangkok, Thailand.

Appendix A

OCTAVE Allegro Worksheets v1.0

The following shows all of the worksheets necessary for completing the OCTAVE Allegro assessment for **one information asset**.

Allegro Worksheet 1	RISK MEASUREMENT CRITERIA – REPUTATION AND CUSTOMER CONFIDENCE		
Impact Area	**Low**	**Moderate**	**High**
Reputation	Reputation is minimally affected; little or no effort or expense is required to recover.	Reputation is damaged, and some effort and expense is required to recover.	Reputation is irrevocably destroyed or damaged.
Customer Loss	Less than _____% reduction in customers due to loss of confidence	_____to _____% reduction in customers due to loss of confidence	More than _____% reduction in customers due to loss of confidence
Other:			

Allegro Worksheet 2	RISK MEASUREMENT CRITERIA – FINANCIAL		
Impact Area	**Low**	**Moderate**	**High**
Operating Costs	Increase of less than _____% in yearly operating costs	Yearly operating costs increase by _____to _____%.	Yearly operating costs increase by more than _____%.
Revenue Loss	Less than _____% yearly revenue loss	_____to _____% yearly revenue loss	Greater than _____% yearly revenue loss
One-Time Financial Loss	One-time financial cost of less than $_____	One-time financial cost of $_____ to $_____	One-time financial cost greater than $_____
Other:			

Allegro Worksheet 3	RISK MEASUREMENT CRITERIA – PRODUCTIVITY		
Impact Area	**Low**	**Moderate**	**High**
Staff Hours	Staff work hours are increased by less than _____% for _____to _____ day(s).	Staff work hours are increased between _____% and _____% for _____to _____ day(s).	Staff work hours are increased by greater than _____% for _____to _____ day(s).
Other:			
Other:			
Other:			

Allegro Worksheet 4	RISK MEASUREMENT CRITERIA – SAFETY AND HEALTH		
Impact Area	**Low**	**Moderate**	**High**
Life	No loss or significant threat to customers' or staff members' lives	Customers' or staff members' lives are threatened, but they will recover after receiving medical treatment.	Loss of customers' or staff members' lives
Health	Minimal, immediately treatable degradation in customers' or staff members' health with recovery within four days	Temporary or recoverable impairment of customers' or staff members' health	Permanent impairment of significant aspects of customers' or staff members' health
Safety	Safety questioned	Safety affected	Safety violated
Other:			

Allegro Worksheet 5	RISK MEASUREMENT CRITERIA – FINES AND LEGAL PENALTIES		
Impact Area	**Low**	**Moderate**	**High**
Fines	Fines less than $_____ are levied.	Fines between $_____ and $_____ are levied.	Fines greater than $_____ are levied.
Lawsuits	Non-frivolous lawsuit or lawsuits less than $_____ are filed against the organization, or frivolous lawsuit(s) are filed against the organization.	Non-frivolous lawsuit or lawsuits between $_____ and $_____ are filed against the organization.	Non-frivolous lawsuit or lawsuits greater than $_____ are filed against the organization.
Investigations	No queries from government or other investigative organizations	Government or other investigative organization requests information or records (low profile).	Government or other investigative organization initiates a high-profile, in-depth investigation into organizational practices.
Other:			

Allegro Worksheet 6	RISK MEASUREMENT CRITERIA – USER DEFINED		
Impact Area	**Low**	**Moderate**	**High**

Allegro Worksheet 7	IMPACT AREA PRIORITIZATION WORKSHEET
PRIORITY	IMPACT AREAS
	Reputation and Customer Confidence
	Financial
	Productivity
	Safety and Health
	Fines and Legal Penalties
	User Defined

Allegro Worksheet 8	CRITICAL INFORMATION ASSET PROFILE	
(1) Critical Asset *What is the critical information asset?*	**(2) Rationale for Selection** *Why is this information asset important to the organization?*	**(3) Description** *What is the agreed-upon description of this information asset?*
(4) Owner(s) *Who owns this information asset?*		
(5) Security Requirements *What are the security requirements for this information asset?*		
❑ **Confidentiality**	Only authorized personnel can view this information asset, as follows:	
❑ **Integrity**	Only authorized personnel can modify this information asset, as follows:	
❑ **Availability**	This asset must be available for these personnel to do their jobs, as follows:	
	This asset must be available for _____ hours, _____ days/week, _____ weeks/year.	
❑ **Other**	This asset has special regulatory compliance protection requirements, as follows:	
(6) Most Important Security Requirement *What is the most important security requirement for this information asset?*		
❑ Confidentiality	❑ Integrity	❑ Availability ❑ Other

Allegro Worksheet 9a	INFORMATION ASSET RISK ENVIRONMENT MAP (TECHNICAL)
INTERNAL	
CONTAINER DESCRIPTION	OWNER(S)
1.	
2.	
3.	
4.	
EXTERNAL	
CONTAINER DESCRIPTION	OWNER(S)
1.	
2.	
3.	
4.	

Allegro Worksheet 9b	INFORMATION ASSET RISK ENVIRONMENT MAP (PHYSICAL)
INTERNAL	
CONTAINER DESCRIPTION	OWNER(S)
1.	
2.	
3.	
4.	
EXTERNAL	
CONTAINER DESCRIPTION	OWNER(S)
1.	
2.	
3.	
4.	

Allegro Worksheet 9c	INFORMATION ASSET RISK ENVIRONMENT MAP (PEOPLE)
INTERNAL PERSONNEL	
NAME OR ROLE/RESPONSIBILITY	DEPARTMENT OR UNIT
1.	
2.	
3.	
4.	
EXTERNAL PERSONNEL	
CONTRACTOR, VENDOR, ETC.	ORGANIZATION
1.	
2.	
3.	
4.	

Allegro - Worksheet 10	INFORMATION ASSET RISK WORKSHEET			
Information Asset Risk	Information Asset			
	Area of Concern			
Threat	(1) Actor *Who would exploit the area of concern or threat?*			
	(2) Means *How would the actor do it? What would they do?*			
	(3) Motive *What is the actor's reason for doing it?*			
	(4) Outcome *What would be the resulting effect on the information asset?*	❑ **Disclosure** ❑ **Modification**	❑ **Destruction** ❑ **Interruption**	
	(5) Security Requirements *How would the information asset's security requirements be breached?*			
	(6) Probability *What is the likelihood that this threat scenario could occur?*	❑ **High**	❑ **Medium**	❑ **Low**

(7) Consequences *What are the consequences to the organization or the information asset owner as a result of the outcome and breach of security requirements?*	(8) Severity *How severe are these consequences to the organization or asset owner by impact area?*		
	Impact Area	**Value**	**Score**
	Reputation & Customer Confidence		
	Financial		
	Productivity		
	Safety & Health		
	Fines & Legal Penalties		
	User Defined Impact Area		
	Relative Risk Score		

(9) Risk Mitigation

Based on the total score for this risk, what action will you take?

❑ Accept	❑ Defer	❑ Mitigate	❑ Transfer

For the risks that you decide to mitigate, perform the following:

On what container would you apply controls?	*What administrative, technical, and physical controls would you apply on this container? What residual risk would still be accepted by the organization?*

Appendix B

OCTAVE Allegro Questionnaires v1.0

The following shows the three scenario questionnaires, one for each of the container types in which an information asset can be stored, transported or processed (technical, physical and people). These questionnaires are used in Step 5 of the OCTAVE Allegro process to help ensure a robust consideration of threats in the assessment process.

Threat Scenario Questionnaire 1	**Technical Containers**		
This worksheet will help you to think about scenarios that could affect your information asset on the technical containers where it resides. These scenarios may pose risks that you will need to address. Consider each scenario and circle an appropriate response. If your answer is "yes" consider whether the scenario could occur accidentally or intentionally or both.			
Scenario 1: Think about the people who work in your organization. Is there a situation in which an employee could access one or more technical containers, *accidentally* or *intentionally*, causing your information asset to be:			
Disclosed to unauthorized individuals?	**No**	**Yes (accidentally)**	**Yes (intentionally)**
Modified so that it is not usable for intended purposes?	**No**	**Yes (accidentally)**	**Yes (intentionally)**
Interrupted so that it cannot be accessed for intended purposes?	**No**	**Yes (accidentally)**	**Yes (intentionally)**
Permanently destroyed or temporarily lost so that it cannot be used for intended purposes?	**No**	**Yes (accidentally)**	**Yes (intentionally)**
Scenario 2: Think about the people who are external to your organization. This could include people who may have a legitimate business relationship with your organization or not. Is there a situation where an outsider could access one or more technical containers, *accidentally* or *intentionally*, causing your information asset to be:			
Disclosed to unauthorized individuals?	**No**	**Yes (accidentally)**	**Yes (intentionally)**
Modified so that it is not usable for intended purposes?	**No**	**Yes (accidentally)**	**Yes (intentionally)**
Interrupted so that it cannot be accessed for intended purposes?	**No**	**Yes (accidentally)**	**Yes (intentionally)**
Permanently destroyed or temporarily lost so that it cannot be used for intended purposes?	**No**	**Yes (accidentally)**	**Yes (intentionally)**

Threat Scenario Questionnaire – 1 (cont)	**Technical Containers**

Scenario 3:

In this scenario, consider situations that could affect your information asset on any technical containers you identified. Determine whether any of the following could occur, and if yes, determine whether these situations would cause one or more of the following outcomes:

- Unintended disclosure of your information asset
- Unintended modification of your information asset
- Unintended interruption of the availability of your information asset
- Unintended permanent destruction or temporary loss of your information asset

A software defect occurs	**No**	**Yes (disclosure)**	**Yes (modification)**	**Yes (interruption)**	**Yes (loss)**
A system crash of known or unknown origin occurs	**No**	**Yes (disclosure)**	**Yes (modification)**	**Ye (interruption)**	**Yes (loss)**
A hardware defect occurs	**No**	**Yes (disclosure)**	**Yes (modification)**	**Yes (interruption)**	**Yes (loss)**
Malicious code (such as a virus, worm, Trojan horse, or back door) is executed	**No**	**Yes (disclosure)**	**Yes (modification)**	**Yes (interruption)**	**Yes (loss)**
Power supply to technical containers is interrupted	**No**	**Yes (disclosure)**	**Yes (modification)**	**Yes (interruption)**	**Yes (loss)**
Problems with telecommunications occur	**No**	**Yes (disclosure)**	**Yes (modification)**	**Yes (interruption)**	**Yes (loss)**
Other third-party problems or systems	**No**	**Yes (disclosure)**	**Yes (modification)**	**Yes (interruption)**	**Yes (loss)**
Natural or man-made disasters (flood, fire, tornado, explosion, or hurricane) occur	**No**	**Yes (disclosure)**	**Yes (modification)**	**Yes (interruption)**	**Yes (loss)**

Threat Scenario Questionnaire – 2	**Physical Containers**		
This worksheet will help you to think about scenarios that could affect your information asset on the physical containers where it resides. These scenarios may pose risks that you will need to address. Consider each scenario and circle an appropriate response. If your answer is "yes" consider whether the scenario could occur accidentally or intentionally or both.			
Scenario 1: Think about the people who work in your organization. Is there a situation in which an employee could access one or more physical containers, *accidentally* or *intentionally*, causing your information asset to be:			
Disclosed to unauthorized individuals?	**No**	**Yes (accidentally)**	**Yes (intentionally)**
Modified so that it is not usable for intended purposes?	**No**	**Yes (accidentally)**	**Yes (intentionally)**
Interrupted so that it cannot be accessed for intended purposes?	**No**	**Yes (accidentally)**	**Yes (intentionally)**
Permanently destroyed or temporarily lost so that it cannot be used for intended purposes?	**No**	**Yes (accidentally)**	**Yes (intentionally)**
Scenario 2: Think about the people who are external to your organization. This could include people who may have a legitimate business relationship with your organization or not. Is there a situation in which an outsider could access one or more physical containers, *accidentally* or *intentionally*, causing your information asset to be:			
Disclosed to unauthorized individuals?	**No**	**Yes (accidentally)**	**Yes (intentionally)**
Modified so that it is not usable for intended purposes?	**No**	**Yes (accidentally)**	**Yes (intentionally)**
Interrupted so that it cannot be accessed for intended purposes?	**No**	**Yes (accidentally)**	**Yes (intentionally)**
Permanently destroyed or temporarily lost so that it cannot be used for intended purposes?	**No**	**Yes (accidentally)**	**Yes (intentionally)**

Threat Scenario Questionnaire -2 (cont)	**Physical Containers**				
Scenario 3: In this scenario, consider situations that could affect your physical containers and, by default, affect your information asset. Determine whether any of the following could occur, and if yes, determine whether these situations would cause one or more of the following outcomes: • Unintended disclosure of your information asset • Unintended modification of your information asset • Unintended interruption of the availability of your information asset • Unintended permanent destruction or temporary loss of your information asset					
Other third-party problems occur	**No**	**Yes (disclosure)**	**Yes (modification)**	**Yes (interruption)**	**Yes (loss)**
Natural or man-made disasters (flood, fire, tornado, explosion, or hurricane) occur	**No**	**Yes (disclosure)**	**Yes (modification)**	**Yes (interruption)**	**Yes (loss)**

Threat Scenario Questionnaire – 3	**People**		
This worksheet will help you to think about scenarios that could affect your information asset because it is known by key personnel in the organization. These scenarios may pose risks that you will need to address. Consider each scenario and circle an appropriate response. If your answer is "yes" consider whether the scenario could occur accidentally or intentionally or both.			
Scenario 1: Think about the people who work in your organization. Is there a situation in which an employee has detailed knowledge of your information asset and could, *accidentally* or *intentionally*, cause the information asset to be:			
Disclosed to unauthorized individuals?	**No**	**Yes (accidentally)**	**Yes (intentionally)**
Modified so that it is not usable for intended purposes?[9]	**No**	**Yes (accidentally)**	**Yes (intentionally)**
Interrupted so that it cannot be accessed for intended purposes?[10]	**No**	**Yes (accidentally)**	**Yes (intentionally)**
Permanently destroyed or temporarily lost so that it cannot be used for intended purposes?[11]	**No**	**Yes (accidentally)**	**Yes (intentionally)**
Scenario 2: Think about the people who are external to your organization. This could include people who may have a legitimate business relationship with your organization or not. Is there a situation in which an outsider could, *accidentally* or *intentionally*, cause your information asset to be:			
Disclosed to unauthorized individuals?	**No**	**Yes (accidentally)**	**Yes (intentionally)**