

**AN INFORMATION SECURITY REFERENCE FRAMEWORK  
FOR  
E-LEARNING MANAGEMENT SYSTEMS**

**By**

**SORENE ASSEFA**

**DISSERTATION**

Submitted in the fulfilment  
of the requirements for the degree



**MASTER OF SCIENCE**

in

**COMPUTER SCIENCE**

in the

**FACULTY OF SCIENCE**

at the

**UNIVERSITY OF JOHANNESBURG**

**SUPERVISOR: PROF. S.H. (BASIE) VON SOLMS**

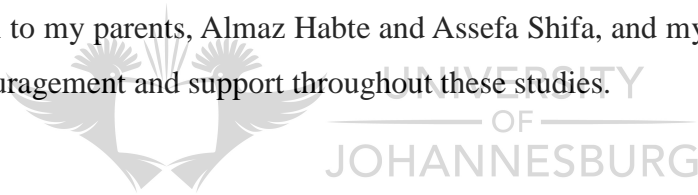
**MAY 2009**

## ACKNOWLEDGEMENTS

I wish to express my sincere appreciation to my mentor, Professor S.H. (Basie) von Solms, for his continuous guidance and support throughout my dissertation. I am so overwhelmed and honoured to be the recipient of the National Research Foundation (NRF) bursary, which I dedicate to his unflinching support. I know this would not have been possible without his intervention, and I thank him immensely for his generous support, confidence in my work and his conspicuously empowering role in my life.

In addition, I would like to give my sincere thanks to the University of Johannesburg for giving me the merit based bursaries that facilitated the pursuit of my education.

I am also grateful to my parents, Almaz Habte and Assefa Shifa, and my siblings for their motivation, encouragement and support throughout these studies.





## **NOTE**

Due to the nature of this research, most of the cited materials are primarily electronic literature.

This dissertation is strictly focused on creating and enhancing the information security aspects of e-LMSs through the creation of an Information Security Reference Framework, which is based on the International Organization for Standardization (ISO) 27002. The ISO 27002 standard is a widely accepted international best practice for Information Security Management.



**TITLE:** An Information Security Reference Framework for e-Learning  
Management Systems.

**AUTHOR:** Sorene Assefa

**PROMOTER:** Prof. S.H. (Basie) von Solms

**COURSE:** MSc (Computer Science)

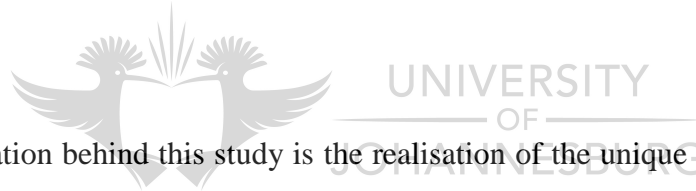
**DEPARTMENT:** Academy for Information Technology

**LANGUAGE:** English



## ABSTRACT

Knowledge sharing technique has been revolutionized over the past years, and the use of Information and Communication Technologies (ICTs) is one of the main contributors to this revolution. One of the knowledge sharing means that emerged from the use of ICTs is the electronic Learning (e-Learning) system. An e-Learning Management System (e-LMS) is a software application that utilises ICTs to manage and deliver e-Learning to users. One of the main advantages of the e-LMS is unlimited access to information, including shared knowledge regardless of geographic location and time, which is the basis for its widespread popularity of e-LMSs in the academic and corporate environment.



The main motivation behind this study is the realisation of the unique nature of e-LMSs, and its dependency on ICTs that makes it more vulnerable to information security risks; if these information security risks are not mitigated or put to an acceptable level, the overall integrity of the entire e-Learning process will be compromised. Moreover, in spite of the abundance of literature in e-Learning systems, the security aspect of e-LMS has been given very little consideration.

This dissertation will investigate the possible information security risks facing e-LMSs from each user's (i.e. Lecturers, Learners and Administrator) perspective. For the identified risks, as a possible information security counter measure, the author has created an information security reference framework, called 'An Information Security Reference Framework for e-Learning Management Systems' (ISRFe-LMS), which is based on the

International Organization for Standardization's (ISO) 27002. The ISO 27002 Standard is internationally accepted best practice for Information Security Management. Thus, the purpose of this dissertation is strictly focused on creating and enhancing the security of e-LMSs through the creation of the ISRFe-LMS.

The Moodle e-LMS has been studied from its information security capabilities and mapped to the ISRFe-LMS, to validate how well it conforms to the security standards and criteria set by the ISRFe-LMS.

The study consists of four parts. Part One serves as an introduction to the research topic, and provides the motivation for the need of the research as well as its scope. Chapter One provides insight into the motivation behind the need for studying and creating an information security reference framework for the security of e-LMSs.

Part Two identifies the components for the ISRFe-LMS. It consists of Chapters Two to Six. Chapter Two provides the background to the e-LMSs by defining the concepts and terminology related to the environment. Chapter Three provides a brief investigation and analysis of the Moodle e-LMS in terms of its functional features, system architecture and, most importantly, its information security mechanism implementations. Chapter Four identifies the common information security risks facing e-LMSs from each user's (i.e. Learner, Lecturer and Administrator) perspective. Chapter Five identifies and discusses the information security dimensions needed to ensure security in an e-LMS environment. Chapter Six proposes the use of the six information security services as one of the

information security counter measures for the information security risks as identified in Chapter Four.

Part Three deals with the actual development of the ISRFe-LMS as well as mapping the Moodle e-LMS against the ISRFe-LMS to determine its security conformance. This part consists of Chapters Seven and Eight. Chapter Seven creates the Information Security Reference Framework for e-Learning Management Systems (i.e. ISRFe-LMS) by consolidating all deliverables from Part Two, while Chapter Eight deals with the actual mapping of the Moodle e-LMS against the ISRFe-LMS.

Part Four consists of the dissertation's results and recommendations. This part consists of Chapter Nine, which provides the research findings, discusses whether or not the objective(s) of the research have been met, and identifies and recommends further research areas.

Two papers, based on this dissertation, have also been accepted for presentation at well known international conferences. These papers will be published in the official proceeding of the conferences. These papers are:

- Information Security Drivers for e-Learning Management Systems (e-LMS). eLearning Africa 2009 - 4<sup>TH</sup> International Conference on ICT for Development, Education and Training, 27 - 29 May, 2009, Dakar, Senegal.
- An Information Security Reference Framework for e-Learning Management Systems (ISRFe-LMS). IFIP World Conference on Computers in Education (WCCE), 27 - 31 July, 2009, Brazil.

# TABLE OF CONTENTS

<b>PART ONE: ESTABLISHING THE NEED FOR AN INFORMATION SECURITY REFERENCE FRAMEWORK FOR e-LEARNING MANAGEMENT SYSTEMS (ISRFe-LMS)</b>	<b>1</b>
<b>1. Introduction</b>	<b>2</b>
1.1. Preview	2
1.2. Background	2
1.2.1. Literature Review	5
1.3. Research Problem	9
1.4. Research Objectives	11
1.5. Research Questions	13
1.6. Research Hypothesis	15
1.7. Research Methodologies	15
1.8. Research Justification	16
1.9. Anticipated Deliverables and Dissemination of the Research	17
1.10. Research Structure	18
1.11. International Exposé of the Research Performed in this Dissertation	22
<b>PART ONE: CONCLUSION</b>	<b>23</b>
<b>PART TWO: IDENTIFYING THE COMPONENTS FOR THE ISRFe-LMS</b>	<b>24</b>
<b>2. Overview of e-Learning Management Systems (e-LMSs)</b>	<b>27</b>
2.1. Preview	27
2.2. Background	28
2.3. Definitions of the Most Frequently Used Terminology	30
2.3.1. e-Learning	30
2.3.2. e-Learning Systems	31
2.3.2.1. Course Management Systems (CMS)	32
2.3.2.2. e-Learning Management Systems (e-LMS)	32
2.3.2.3. e-Learning Content Management Systems (e-LCMS)	33
2.4. The Architecture of an e-LMS	34
2.5. Components of an e-LMS	36
2.6. Advantages and Disadvantages of the e-LMSs	38
2.6.1. Advantages	38
2.6.2. Disadvantages	40
2.7. e-LMS Functional Features	42
2.8. Conclusion	44

<b>3. Review of the Moodle e-Learning Management System (e-LMS)</b>	<b>46</b>
3.1. Preview	46
3.2. Moodle e-LMS Background	47
3.3. Moodle's Functional Features	50
3.4. The Architecture of Moodle	52
3.5. The Information Security Feature of Moodle	54
3.5.1. Identification and Authentication	54
3.5.1.1. Information Security Mechanisms	55
3.5.1.2. Information Security Policies	56
3.5.2. Authorization	57
3.5.2.1. Information Security Mechanisms	57
3.5.3. Confidentiality	58
3.5.3.1. Information Security Mechanisms	58
3.5.4. Integrity	58
3.5.4.1. Information Security Mechanisms	58
3.5.5. Non-Denial	59
3.5.5.1. Information Security Mechanisms	59
3.5.6. Availability	59
3.5.6.1. Information Security Mechanisms	59
3.6. Conclusion	60
<b>4. Common e-LMSs Information Security Risks</b>	<b>62</b>
4.1. Preview	62
4.2. Background	63
4.3. Users and their Roles in e-LMS	65
4.3.1. Lecturer	66
4.3.2. Learner	67
4.3.3. Administrator	67
4.4. Investigation of the Information Security Risks of Using an e-LMS	69
4.4.1. Lecturer	69
4.4.2. Learner	72
4.4.3. Administrator	74
4.5. Conclusion	75
<b>5. Information Security Drivers for an e-LMS</b>	<b>78</b>
5.1. Preview	78
5.2. Background	79
5.3. Information Security	80
5.3.1. The Five Information Security Dimensions	81





6.2.3.2. Activity: Set Up Roles and Privileges .....	130
6.2.3.3. Activity: Assign Roles and Privileges .....	130
6.2.3.4. Activity: Assign Lecturers to a Course(s) .....	132
6.3. Conclusion .....	133
<b>PART TWO: CONCLUSION</b>	<b>135</b>
<b>PART THREE: CREATING ISRFe-LMS AND MAPPING MOODLE AGAINST THE ISRFe-LMS</b>	<b>136</b>
<b>7. ISRFe-LMS</b>	<b>138</b>
7.1. Preview .....	138
7.2. Background .....	139
7.2.1. The Development Phases of the ISRFe-LMS .....	140
7.3. ISRFe-LMS .....	141
7.4. Conclusion .....	143
<b>8. Mapping the Moodle e-LMS Against the ISRFe-LMS</b>	<b>145</b>
8.1. Preview .....	145
8.2. Background .....	145
8.3. Scope .....	146
8.4. Methodology .....	146
8.5. Evaluation Reports .....	146
8.6. Conclusion .....	149
<b>PART THREE: CONCLUSION</b>	<b>150</b>
<b>PART FOUR: DISSERTATION RESULTS AND RECOMMENDATIONS</b>	<b>151</b>
<b>9. Conclusion and Recommendations</b>	<b>153</b>
9.1. Preview .....	153
9.2. Dissertation Summary .....	153
9.3. Further Research .....	155
<b>Appendix A: Implementation Guideline for the ISRFe-LMS</b> .....	<b>156</b>
<b>Appendix B.1.: Password Policy for XYZ e-LMS</b> .....	<b>162</b>

<b>Appendix B.2.:</b>	Information Security User Awareness Program for XYZ e-LMS .....	164
<b>Appendix C:</b>	Information Security Reference Framework for e-LMS, Paper Presented at IFIP World Conference on Computers in Education (WCCE), 27 - 31 July, 2009, Brazil. ....	167
<b>Appendix D:</b>	Information Security Drivers for e-LMS, Paper Presented at eLearning Africa 2009 - 4 <sup>TH</sup> International Conference on ICT for Development, Education and Training, 27 - 29 May, 2009, Dakar, Senegal .....	180
<b>Appendix E:</b>	Symbol and Abbreviations .....	185
<b>BIBLIOGRAPHY</b>	.....	186



## LIST OF FIGURES

Figure 1.1.:	Graphic Presentation of the Research Objectives .....	12
Figure 1.2.:	Graphic Presentation of the Research Road map.....	21
Figure 2.1.:	Graphic Presentation of the Relationships between e-Learning, e-Learning System and e-Learning Systems .....	33
Figure 2.2.:	System Architecture of an e-LMS .....	35
Figure 2.3.:	Graphic Presentation of the Basic Components of an e-LMS .....	37
Figure 3.1.:	Moodle e-LMS Concise Information Chart [15].....	49
Figure 5.1.:	The Five Information Security Dimensions for e-LMS .....	83
Figure 5.2.:	Elements of e-LMS ISG [14].....	85
Figure 5.3.:	The Relationships between the Six Information Security Services and the Five Information Security Dimensions .....	89
Figure 5.4.:	The Six Information Security Services and Mechanisms .....	91
Figure 6.1.:	The Risk to the Six Information Security Services Mapping Framework .....	107
Figure 6.2.:	Example of the Risk to the Information Security Services Mapping Framework .....	108
Figure 7.1.:	The Development Phases of the ISRFe-LMS .....	140
Figure 7.2.:	The Graphic Representation of the ISRFe-LMS .....	142

## LIST OF TABLES

Table 2.1.: A Summarized List of the Minimal Functional Features Expected From e-LMS [4].....	43
Table 3.1.: A Summarized List of Built-in Modules/Features of Moodle's e-LMS [22].....	52
Table 6.1.: The Mapping of Risk 1 of Activity 6.2.1.1. With the Six Information Security Services.....	110
Table 6.2.: The Mapping of Risk 1 of Activities 6.2.1.2. and 6.2.1.3. With the Six Information Security Services.....	111
Table 6.3.: The Mapping of Risks 2, 3 and 4 of Activities 6.2.1.2. and 6.2.1.3. With the Six Information Security Services.....	112
Table 6.4.: The Mapping of Risk 1 of Activities 6.2.1.4. and 6.2.1.5. With the Six Information Security Services.....	113
Table 6.5.: The Mapping of Risk 2 of Activities 6.2.1.4. and 6.2.1.5. With the Six Information Security Services.....	113
Table 6.6.: The Mapping of Risks 3 and 4 of Activities 6.2.1.4. and 6.2.1.5. With the Six Information Security Services.....	114
Table 6.7.: The Mapping of Risk 5 of Activities 6.2.1.4. and 6.2.1.5. With the Six Information Security Services.....	114
Table 6.8.: The Mapping of Risks 1 and 2 of Activities 6.2.1.6. and 6.2.1.7. With the Six Information Security Services.....	115

Table 6.9.: The Mapping of Risks 3, 4 and 5 of Activities 6.2.1.6. and 6.2.1.7. With the Six Information Security Services .....	116
Table 6.10.: The Mapping of Risk 1 of Activity 6.2.1.8. With the Six Information Security Services .....	117
Table 6.11.: The Mapping of Risk 2 of Activity 6.2.1.8. With the Six Information Security Services .....	117
Table 6.12.: The Mapping of Risk 1 of Activity 6.2.1.9. With the Six Information Security Services .....	118
Table 6.13.: The Mapping of Risk 2 of Activity 6.2.1.9. With the Six Information Security Services .....	119
Table 6.14.: The Mapping of Risk 1 of Activity 6.2.2.1. With the Six Information Security Services .....	120
Table 6.15.: The Mapping of Risk 1 of Activity 6.2.2.2. With the Six Information Security Services .....	121
Table 6.16.: The Mapping of Risk 2 of Activity 6.2.2.2. With the Six Information Security Services .....	121
Table 6.17.: The Mapping of Risk 1 of Activity 6.2.2.3. With the Six Information Security Services .....	123
Table 6.18.: The Mapping of Risk 2 of Activity 6.2.2.3. With the Six Information Security Services .....	123
Table 6.19.: The Mapping of Risk 3 of Activity 6.2.2.3. With the Six Information Security Services .....	124

Table 6.20.: The Mapping of Risks 4 and 5 of Activity 6.2.2.3. With the Six Information Security Services .....	124
Table 6.21.: The Mapping of Risk 6 of Activity 6.2.2.3. With the Six Information Security Services .....	125
Table 6.22.: The Mapping of Risk 1 of Activity 6.2.2.4. With the Six Information Security Services .....	126
Table 6.23.: The Mapping of Risk 2 of Activity 6.2.2.4. With the Six Information Security Services .....	126
Table 6.24.: The Mapping of Risk 3 of Activity 6.2.2.4. With the Six Information Security Services .....	127
Table 6.25.: The Mapping of Risk 1 of Activity 6.2.2.5, With the Six Information Security Services .....	128
Table 6.26.: The Mapping of Risk 1 of Activity 6.2.2.6. With the Six Information Security Services .....	129
Table 6.27.: The Mapping of Risk 2 of Activity 6.2.2.6. With the Six Information Security Services .....	129
Table 6.28.: The Mapping of Risk 1 of Activity 6.2.3.1. With the Six Information Security Services .....	130
Table 6.29.: The Mapping of Risk 1 of Activity 6.2.3.2. and 6.2.3.3. With the Six Information Security Services .....	131
Table 6.30.: The Mapping of Risk 2 of Activity 6.2.3.2. and 6.2.3.3. With the Six Information Security Services .....	132
Table 6.31.: The Mapping of Risk 1 of Activity 6.2.3.4. With the Six Information Security Services .....	133

# **ESTABLISHING THE NEED FOR AN INFORMATION SECURITY REFERENCE FRAMEWORK FOR e-LEARNING MANAGEMENT SYSTEMS (ISRFe-LMS)**

This dissertation is divided into four distinct parts.

Part One attempts to establish the motivation behind the need for this dissertation by investigating and analyzing relevant literature related to the concepts and theories of electronic Learning (e-Learning) systems focusing on the specifics of e-Learning Management Systems (e-LMS). Part One comprises the first chapter of the dissertation.

Chapter One provides background information for the study and formulates the motivation for this study. This chapter also provides the overall organization of the dissertation.

# CHAPTER ONE

## INTRODUCTION

### 1.1. PREVIEW

The objective of this chapter is to motivate the need for an information security reference framework for creating a secure e-Learning Management System (e-LMS), to give an overview of this dissertation, and to serve as a general introduction of the direction that this study will be take. The following section will provide the background to the problem addressed in this dissertation. Moreover, it provides a concise report on the review of the literature around the security of e-Learning systems.

### 1.2. BACKGROUND

It is traditionally accepted that there are two major knowledge sharing systems: the traditional system and the Information and Communication Technologies (ICTs) based system. Each system is independent and should not be taken as a replacement of the other. Instead, they complement each other.



The traditional system uses a specific geographic place, where lecturers and students meet to share knowledge and write assessment tests. Having a traditional system increases the intimate relationship between lecturers and their learner(s). However, as it is bound to a specific time and place, it cannot accommodate everyone.

There is a need for widening access to learning. “Social, technological and economical changes as well as the changing demands of the market make it necessary for individuals to continuously develop and advance themselves and their competencies through learning” [18]. One solution to this problem is the use of Information and Communication Technologies (ICTs) as a medium to achieve the learning/teaching goals. Email, forums, blogs and chat rooms are some of these ICT tools. One of the knowledge sharing systems that emerged from the use of ICTs is electronic Learning (e-Learning).

The need for unlimited access to information, skills and knowledge is the driving force for the adoption of e-Learning. e-Learning can be defined as a technology based learning in which learning materials are delivered electronically to remote learners via computer networks [35]. One of the main advantages of using e-Learning is the ability to access and share information regardless of geographic location and time. As seen in the definition, e-Learning is technology based learning; in this case the technology is referred

to as an e-Learning system. e-Learning systems cover a wide range of systems such as e-Learning Management Systems (e-LMS) and e-Learning Content Management Systems (e-LCMS). For the purpose of this dissertation, only e-LMSs will be discussed.

As identified by [45], one of the success factors of e-LMSs is the deployment of the ICTs, such as the Internet, as transportation media. That said, the fact that e-LMSs rely on ICT make them vulnerable to further information security risks. Although most of the current e-LMSs have some sort of information security mechanisms, such as password based Identification and Authentication and access control, in place, information security still remains a crucial issue for most institutions. The author recommends that one possible solution for providing adequate security in an e-LMS is through the development and implementation of a comprehensive Information Security Reference Framework.

This dissertation attempts to develop a comprehensive Information Security Reference Framework for e-Learning Management Systems (ISRFe-LMS). It will be used to map and evaluate the security of the Moodle e-LMS to examine how it conforms to the ISRFe-LMS.

This research project takes both a theoretical and a practical approach. The theoretical aspect deals with utilizing relevant literature related to the theories and concepts of e-LMSs with emphasis on the information security aspect; which provides an overview of the knowledge and ideas that have been established around e-LMSs and serves as a background to the motivation behind the research project. In contrast, the practical aspect deals with the actual creation of the ISRFe-LMS as well as the mapping of the Moodle e-LMS to the ISRFe-LMS. Some of the literature reviewed in order to formulate the research problems are presented in the following section.

### 1.2.1. LITERATURE REVIEW



UNIVERSITY  
OF  
JOHANNESBURG

This literature review attempts to analyze the literature relevant to the study of e-Learning systems. It has two aims: the first is to identify the ideas that have been established by researchers around e-LMSs; the second is to show that it is necessary to do further research around creating security guidelines that can be used by any e-Learning system with an emphasis on e-LMSs. To achieve both aims, relevant literature that have shaped the current theory, specifically on security issues of e-LMSs, are investigated.

Most of the current literature focuses on the general theory behind e-Learning systems, mostly highlighting how e-Learning systems can be used to overcome some of the challenges facing traditional learning systems, its pros and cons, the conceptual view of e-Learning systems, and the various uses of ICT in higher education. [22 and 43] are examples of such literature which has been reviewed.

In spite of the abundance of varied literature on e-Learning, security aspects related to the system have been given little consideration. Despite the widespread acceptance of e-Learning systems, there is no consensus on a standard framework for the evaluation of the quality of such a system [31]. [15, 17, 35 and 38] note that security serves as the most important element to ensure that all information within e-Learning systems is protected and the overall integrity of the system is maintained. The article presented by [17] shows that most of the e-Learning innovations have focused on content development and delivery with little consideration to privacy and security requirements. Similarly, [15, 55 and 38] mention that, due to their nature and inherently complex architecture, e-Learning systems are exposed to information security risks that could compromise the credibility and the comparative competence of user institutions.

To enhance the security of e-Learning systems, all of the researchers [15, 17, 35 and 38] have used different approaches. To improve the privacy and security of e-Learning systems, the current e-Learning standards were analyzed and some technologies were proposed as possible solutions in [17]. The proposed technologies are Onion Routing for network privacy, developing policies for privacy and security management and designing trust mechanisms to ensure that e-Learning satisfies the privacy principles/policies defined in [17].

As discussed in [38], one way of approaching the security problem of e-LMSs is from the perspective of “secure from what?”. The authors of [38] developed a conceptual framework, known as the Availability, Integrity, Confidentiality and Authentication (AICA) Threat Model, which can be used by developers of e-LMSs as guidelines to decrease the number of overlooked security vulnerabilities at the design stage. Other valuable approaches are those presented by [15 and 35]. A mathematical evaluation framework to evaluate the security of an e-Learning system is proposed in [15]. The use of information security pillars to enhance the security of an e-Learning system is discussed in [35].

As seen in [15, 17, 35 and 38], the security of e-Learning systems requires more attention and further research. The solution proposed by [17 and 38] fails to include the non-technical part of security, which makes it non-comprehensive. As identified by [48], adequate security can only be achieved through the combination of technical and non-technical aspects of information security. The use of the International Organization for Standardization's (ISO) 27002 code of practice for Information Security Management Standard can be a useful tool in creating a comprehensive Information Security Reference Framework for IT Systems [31]. ISO 27002 is a widely accepted security standard for Information Security Management, which takes a very broad approach in its coverage of information security basic requirements that need to be addressed to implement appropriate information security [16, 31 and 50]. Therefore, ISO 27002 could be used as a guideline for creating comprehensive information security countermeasures for e-Learning systems. Taking all of these models into account, the author proposes an Information Security Reference Framework for e-LMSs, which is based on the ISO 27002 standard, as a more comprehensive measure for creating a secure e-LMS environment.

In the following sections, the motivation for this research, its objectives and methodologies used to achieve those objectives, and the deliverables of the research will be discussed.

### 1.3. RESEARCH PROBLEM

E-Learning Management Systems (e-LMSs) are mainly dependent on ICTs. All ICTs have inherent security risks, and if these risks are not properly addressed and mitigated, the e-LMS will remain vulnerable to security threats. As mentioned above, several investigations in e-LMSs have been undertaken, mostly focusing on the functionality and benefits that they can provide. However, information security, trust and dependability issues in such systems have not been addressed in the same depth and detail [17].

Moreover, due to the diversity of functionalities provided by the current e-LMSs, it remains difficult to adequately define effective security measures for e-LMSs. Based on the literature reviews conducted, no comprehensive Information Security Reference Framework could be found to date. The author proposes that one of the possibilities for providing pertinent security to an e-LMS is by developing an information security reference framework, which can be used as a standard for the mapping and evaluation of existing e-LMS packages within the context of security conformance.

### *Statement of problem*

---

- ✎ *e-LMSs are mainly dependent on ICTs. All ICTs have inherent information security risks, and if these risks are not properly addressed and mitigated, the e-LMS will remain vulnerable to the information security threats.*
- ✎ *Several investigations have been undertaken on e-LMSs. However, information security, trust and dependability issues have, to date, not been addressed in the same depth and detail.*
- ✎ *Based on the literature review conducted, there is currently no comprehensive Information Security Reference Framework to be found which could be used as a standard for the mapping and evaluation of existing e-LMS packages within the context of security conformance.*

This section identifies the research problem, which is the driver of this dissertation.

Based on the statement of the problem, the author defines a set of objectives, which will be discussed in the following section.



## 1.4. RESEARCH OBJECTIVES

The main objective of this dissertation is to develop an Information Security Reference Framework for e-Learning Management Systems (ISRFe-LMS), which can be used as a standard for mapping and evaluating the information security functionalities of an e-LMS. To achieve this objective, the following sub-objectives are developed:

1. To gain an understanding of an e-LMS;
2. To gain an understanding of the information security risks involved in using an e-LMS;
3. To identify the information security pillar(s) that must be enforced for a learning activity to run in a secure environment and ultimately result in a secure running e-LMS;
4. To develop general security requirements for e-LMSs, where e-LMS users function in a secure environment;
5. To determine how to combine the above four elements in order to create a proper information security reference framework which will be called An Information Security Reference Framework for e-Learning Management Systems (ISRFe-LMS ); and
6. To map and evaluate the Moodle e-LMS against the ISRFe-LMS. These objectives are represented diagrammatically in Figure 1.1..

### *Statement of Objective*

To develop the ISRFe-LMS which will be used to map and evaluate the information security functionalities of an e-LMS.

### **SUB OBJECTIVES**

To gain an understanding of an e-LMS;

1

To gain an understanding of the information security risks involved in using an e-LMS;

2

To identify the information security pillar(s) that must be enforced for a learning activity to run in a secure environment and ultimately result in a secure running e-LMS;

3

To develop scenarios for e-LMSs users;

4

To determine the components of the ISRFe-LMS; and

5

To map and evaluate the Moodle e-LMS against the ISRFe-LMS.

6

*Source: Author's own composition*

**Figure 1.1.: Graphic Presentation of the Research Objectives**

To address the problem statement and achieve the above objectives, a set of research questions are formulated, which will be discussed in the following section.

## 1.5. RESEARCH QUESTIONS

This research is guided by a set of research questions. The main research question is the following:

### *Main question*

---

What are the components of the ISRFe-LMS?

In order to answer this main research question, which is aimed at developing the ISRFe-LMS, the following sub-questions are formulated and addressed in different sections of the study.

### *Sub-question 1:*

---

What are the basic functional features expected from e-Learning Management Systems (e-LMSs)?

### *Sub-question 2:*

---

What are the most common activities that users (i.e. Administrator, Lecturers and Learners) can do on e-LMSs?

*Sub-question 3:*

---

What are the main information security risks specifically related to the activities identified in sub-question 2?

*Sub-question 4:*

---

Which information security dimensions are most relevant in creating a secure e-LMS environment?

*Sub-question 5:*

---

What role should the six information security services, as identified in [16], play in the dimensions identified in sub-question 4?

In order to develop the ISRFe-LMS, this dissertation addresses each of the research questions individually and sequentially in different sections in the study and finally reflects on the outcome of each question within the context of creating the ISRFe-LMS.

## 1.6. RESEARCH HYPOTHESIS

As already briefly discussed in section 1.3., an e-LMS is mainly dependent on ICTs. All ICTs have inherent security risks. Therefore, the study builds on an already reached solid conclusion that e-LMSs have been suffering from various security vulnerabilities of ICTs. Thus, the study has taken the position that developing an appropriate comprehensive information security reference framework, ISRFe-LMS, is an optimal alternative that would help the e-LMSs overcome their security challenges.

To identify, propose and realise solutions for the research problem (section 1.3.) and research questions (section 1.5.), as well as to achieve the research objective(s) (section 1.4.), the methods and procedures used in this research are discussed in the following section.

## 1.7. RESEARCH APPROACH

To achieve the main objective, the research takes both a theoretical and a practical approach.

- The theoretical approach comprises the first three chapters of the dissertation, which rely on literature as sources of pertinent information.

- The practical approach comprises Chapters Four to Nine, which deal with the design and implementation of the ISRFe-LMS, as well as actual mapping of the Moodle e-LMS against the ISRFe-LMS.

The above two approaches will be used to achieve the ultimate objectives discussed in the previous section. The justification for the need for this research will be presented in the following section.

## 1.8. RESEARCH JUSTIFICATION



The primary reason for attaching key importance to information security in the e-LMS environment is due to the fact that the e-LMS is mainly dependent on ICTs. These technologies all have inherent security risks; if these risks are not properly addressed and mitigated in the e-LMS, the integrity of the whole e-Learning process may be compromised. One glaring example is that the risks involved in an online assessment application of an e-LMS, if not properly secured, can compromise the entire e-LMS environment. If, in such systems, the basic information security services of identification and authentication, access control, confidentiality, integrity, availability and non-denial are not enforced, severe trust problems will arise.

## 1.9. ANTICIPATED DELIVERABLES AND DISSEMINATION OF THE RESEARCH

The deliverables planned are precisely those which will provide answers or reactions to the problem statement as discussed in section 1.3..

The two deliverables are:

1. A comprehensive information security reference framework for an e-LMS, ISRFe-LMS, based on internationally accepted best practices. Many security reference frameworks base their security policies on internationally recognized standards such as ISO 27002 [16, 31 and 33].
2. A mapping of the information security functionalities of Moodle e-LMS against the ISRFe-LMS and an evaluation report.

The study findings are intended to be disseminated through posters, seminars, reports and journal articles (See also section 1.11.).

## 1.10. RESEARCH STRUCTURE

This dissertation consists of nine chapters, which incorporate both the research organization and the project aspects of the study. The direction and organization of the study presented below provide a brief overview of each of the chapters. To get an idea of the research processes, see Figure 1.2., which presents a graphical presentation of the research road map.

### Chapter One: Introduction

This chapter provides insight into the motivation behind the need for this study, which is the need for creating an Information Security Reference Framework for e-Learning Management Systems (ISRFe-LMS).

### Chapter Two: Overview of e-LMSs

This chapter provides an overall insight into e-LMSs in general and their information security vulnerabilities.



**Chapter Three: Review of the Moodle e-LMS**

This chapter provides a brief investigation and analysis of the Moodle e-LMS in terms of its functional features, system architecture and most importantly its information security mechanism implementations.

**Chapter Four: Common e-LMSs Information Security Risks**

This chapter identifies common information security risks facing e-LMSs from the different user (i.e. Learner, Lecturer and Administrator) perspectives.

**Chapter Five: Information Security Drivers for an e-LMS**

This chapter identifies the most significant information security dimensions that need to be considered in creating a secure e-LMS environment.

**Chapter Six: Recommended Solutions**

This chapter identifies and proposes the use of information security services as one of the countermeasures for the information security risks identified in Chapter Four.

**Chapter Seven: ISRFe-LMS**

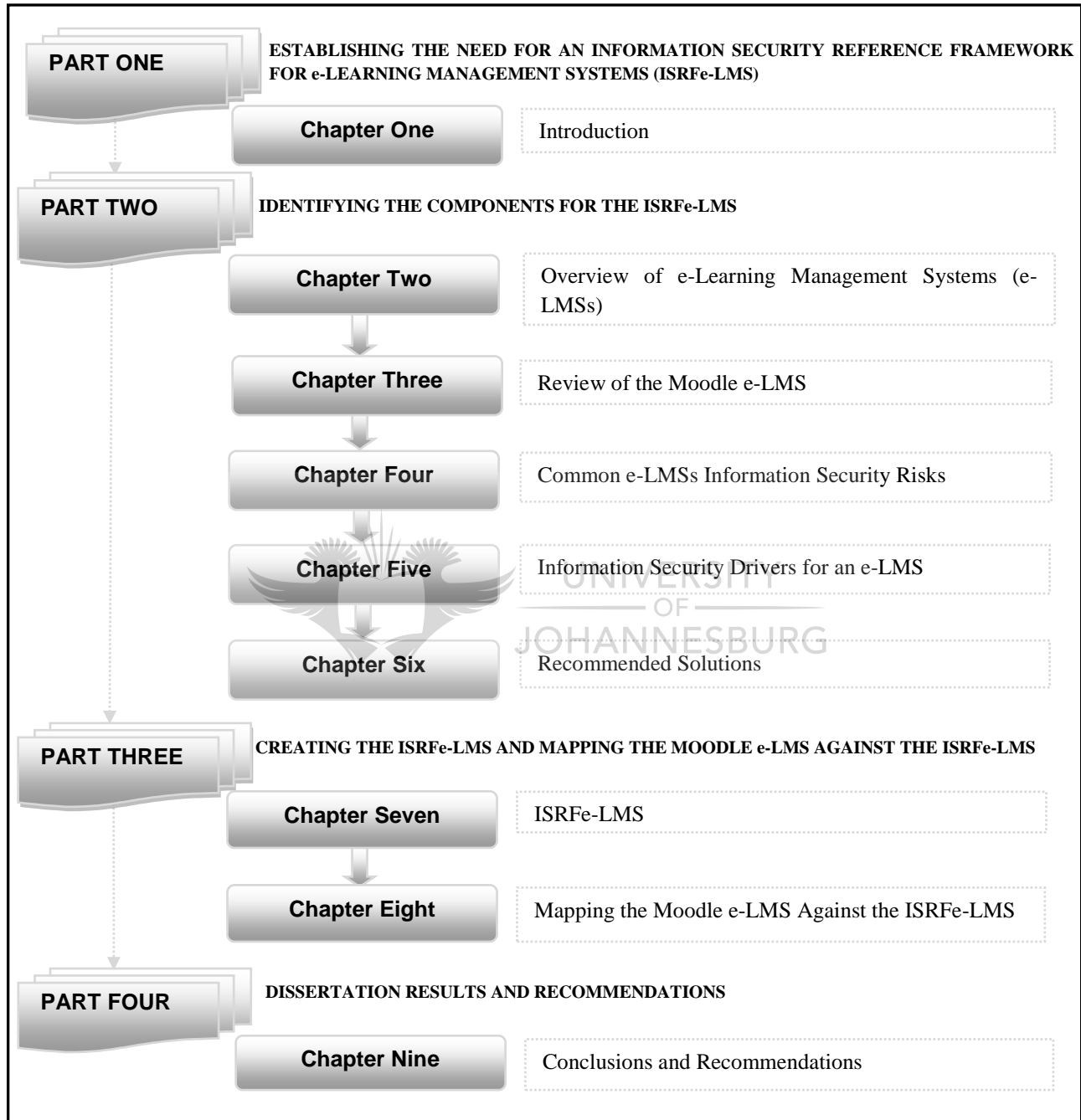
This chapter determines and defines the components of the ISRFe-LMS.

**Chapter Eight: Mapping the Moodle e-LMS against the ISRFe-LMS**

This chapter carries out the actual mapping of the Moodle e-LMS against the ISRFe-LMS to determine its information security conformance.

**Chapter Nine: Conclusions and Recommendations**

This chapter provides the summary of findings and recommendations for further studies.



*Source: Author's own composition*

**Figure 1.2.: Graphic Presentation of the Research Roadmap**

## 1.11. INTERNATIONAL EXPOSÉ OF THE RESEARCH PERFORMED IN THIS DISSERTATION

Two papers, based on this dissertation, have been accepted for presentation at well known international conferences. These papers will be published in the official proceeding of the conferences. These papers are:

- An Information Security Reference Framework for e-Learning Management Systems (ISRFe-LMS). IFIP World Conference on Computers in Education (WCCE), 27 - 31 July, 2009, Brazil. (See also Appendix C)
- Information Security Drivers for e-Learning Management Systems (e-LMS). eLearning Africa 2009 - 4<sup>TH</sup> International Conference on ICT for Development, Education and Training, 27 - 29 May, 2009, Dakar, Senegal. (See also Appendix D)

Chapter One critically analyzes and investigates recent and relevant literature to formulate the motivation behind the need for this study, which is the creation of an Information Security Reference Framework for e-Learning Management Systems (ISRFe-LMS). In this chapter, the problem statement has been identified, the objectives of the research have been established and the methodologies and approaches that will be used to achieve those objectives were addressed. Moreover, a brief overview of the direction and structure the dissertation will take has been given.



Part One (Chapter One) identifies the fact that security issues related to e-Learning Management Systems (e-LMSs) have been given little consideration. One way of addressing the security issue is through the creation of a comprehensive Information Security Reference Framework. Part One (Chapter One) has also established the need for an Information Security Reference Framework for e-Learning Management Systems (ISRFe-LMS). Part Two attempts to identify the components of the ISRFe-LMS.

As shown in Part One, information security is one of the main concerns for e-Learning Management Systems (e-LMSs). Part Two aims to understand e-LMSs from an information security perspective. This will be done by investigating the information security vulnerabilities of e-LMSs as well as identifying the possible information security countermeasures that will be used to mitigate or reduce the identified information security risks to an acceptable level. The information gathered will be used to identify the necessary components for the ISRFe-LMS.

Part Two consists of Chapters Two to Six, which are briefly reviewed as follows:

Chapter Two provides an overview of e-LMSs.

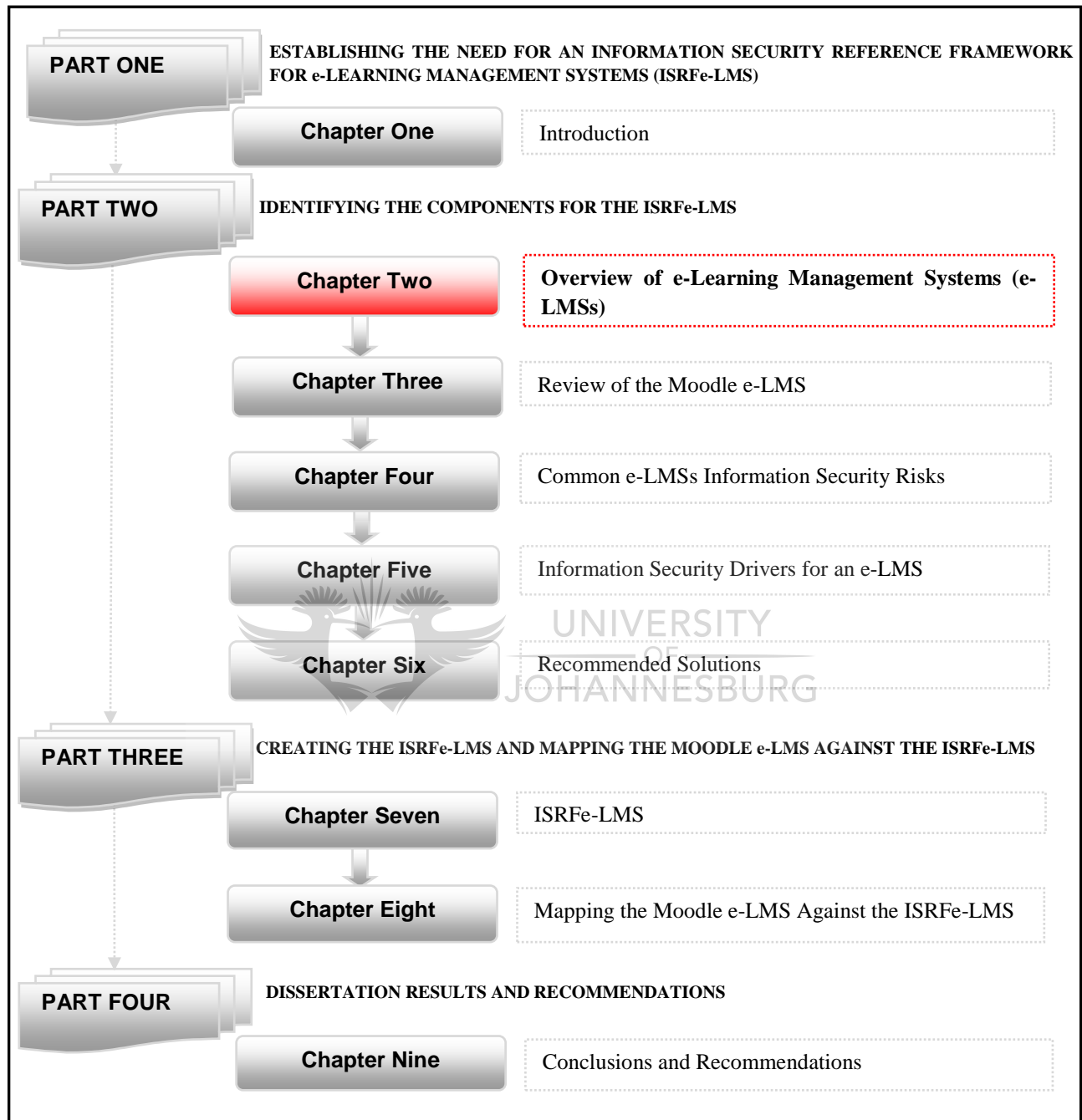
Chapter Three provides a brief review of the Moodle e-LMS.

Chapter Four identifies the common information security risks from the user's perspective.

Chapter Five identifies the most important information security dimensions that need to be considered in creating a secure e-LMS environment.

Chapter Six discusses how the technical dimension (i.e. the six Information Security Services) could be used as a possible information security countermeasure for the information security risks identified in Chapter Four.







## CHAPTER TWO

# OVERVIEW OF e-LEARNING MANAGEMENT SYSTEMS (e-LMSs)

### 2.1. PREVIEW

The purpose of this dissertation is to create a secure e-LMS environment by mitigating or reducing the information security vulnerabilities of e-LMSs through the creation of the Information Security Reference Framework for e-Learning Management Systems (ISRFe-LMS). Before delving into the core issue, it is necessary to have a basic understanding of the concepts and terminologies related to an e-LMS environment. Therefore, this chapter is designed to discuss the three most frequently used concepts: e-Learning, e-Learning Systems, and e-Learning Management Systems (e-LMSs). Moreover, this chapter discusses the common architectural design of e-LMSs and most frequently cited advantages and disadvantages of using e-LMSs. This chapter is guided by sub-question 1 of Chapter One, section 1.5.:

#### *Sub-question 1:*

---

What are the basic functional features expected from e-LMSs?

In the following section, the evolution of education methods from an historical perspective is presented.

## 2.2. BACKGROUND

Knowledge sharing methods have evolved over the years and can probably be described in many ways. One way of representing the evolution of education is to divide the evolution of knowledge sharing methods into the following three phases.

Phase One can be identified with the periods before the existence and/or acceptance of computers. Computers were not widely available, and education and training were classroom based. This can be seen as an instructor led education method, where the lecturer is in full control of the education system. Phase One is characterized mainly by the place and time of learning, where social interaction mattered most.



Phase Two emerged in the 1980s with the arrival and increasing popularity of personal computers [44]. The invention and social acceptance of computers have led to computer based training, which can be identified as the start of Phase Two, and can also be seen as the Computer Based Learning (CBL) era. CBL is learning via the means of CD-ROMs, where learning materials are multimedia based audio, video, animation, and so on [44]. CBL allows learners to access information, independent of time and place.

Phase Three is identified with the advent of the Internet and the web at the end of the 1990s, which marked a new beginning for the ICT based learning experiences [44]. The need for unlimited access to information, intellectual skills and knowledge is the driving force for the creation and the enhancement of ICT based education. The introduction of ICT based education led to Phase Three, which is also known as the electronic Learning (e-Learning) era. During this period, e-Learning, education and training are delivered via networks such as the Internet, intranet, extranet, and so on [7 and 34].

The technological innovation is consistently enabling social advancement (i.e. competition for high skilled workers), altering the way in which work and education are undertaken, which in turn requires that learning occurs on a just-in-time basis [20]. Due to the integrated nature of e-Learning, users can access the system from any location at any time; learners are allowed to take self-paced education, which is independent of place and time.

This background information provides a concise overview of the historical evolution of knowledge sharing/education systems. All three phases can be used in support of each other to create a comprehensive education system. To understand e-Learning, it is necessary to have an understanding of the terms related to e-Learning, which will be discussed in the following section.

## 2.3. DEFINITIONS OF THE MOST FREQUENTLY USED TERMINOLOGY

In this dissertation, e-Learning, e-Learning Systems and e-Learning Management Systems (e-LMSs) are some of the most frequently used terms. The definitions, explanations and relationships between these terms are discussed below (see Figure 2.1. for a Graphical Presentation of the Relationships Between e-Learning, e-Learning Systems and e-LMSs).

### 2.3.1. e-LEARNING

e-Learning can be defined as a technology based learning in which learning materials are delivered electronically to remote learners via computer networks [35]. e-Learning may cover a wide set of applications, systems and processes, such as e-Learning Systems, web-based learning, virtual classrooms and digital collaboration [7]. An e-Learning system will be discussed briefly in the following section.

### 2.3.2. e-LEARNING SYSTEMS

Much of the literature has tried to uncover the meaning of an e-Learning System. The most concise definition is given by [7], which defines it as a technology that makes use of network technologies such as the Internet, intranet, extranet and more to deliver contents to individuals. An e-Learning System has features to design, deliver and administer online learning [48].

e-Learning systems can be applicable in both corporate and academic environments. In corporate environments, e-Learning systems can be used as an efficient way of sharing information between co-workers. As supported by [20], e-Learning is becoming a norm for corporate training. In academic environments, e-Learning systems can be used in primary, secondary, tertiary and special training centres to enhance the traditional learning system or to create a complete online learning system.

e-Learning systems cover a wide range of systems. Some of these e-Learning Systems will be discussed below.

### 2.3.2.1. COURSE MANAGEMENT SYSTEMS (CMS)

A CMS is a software package designed to help educators create effective online learning systems, referred to as e-Learning systems. An example is Dokeos CMS [37].

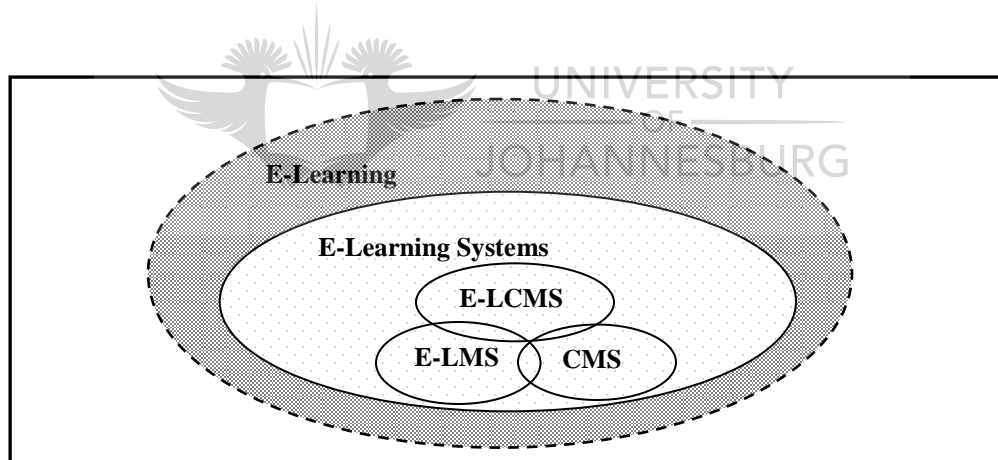
### 2.3.2.2. e-LEARNING MANAGEMENT SYSTEMS (e-LMS)

An e-LMS is defined as “a software package that enables the management and the delivery of online content to learners” [48]. As seen in the definition, an e-LMS is a complete software package with various features that enables the management and delivery of online content to remote learners via ICTs. For instance, the management and administrative feature which allows the administrator to undertake administrative roles over the activities of users and the functioning of the learning contents, is a feature of an e-LMS. An e-LMS may also be seen as an interface between its users (i.e. Learners, Lecturers and Administrator) and contents such as course material. Some examples of e-LMSs are WebCT, Claroline, Moodle and ILIAS [48].

**2.3.2.3. e-LEARNING CONTENT MANAGEMENT SYSTEMS (e-LCMS)**

An e-LCMS is more detailed or involved than e-LMSs and CMSs, and not only creates, manages and delivers course content but also allows the editing and reuse of materials. Some examples of e-LCMS are ATutor, Out Start, and Eedo [49].

Each of the e-Learning systems (CMS, e-LMS and e-LCMS) discussed above are designed to provide a unique solution for improving the education experience. However, they all overlap in their capabilities and the functional features they provide. Figure 2.1. below provides a pictorial representation of the relationships between the terminology discussed on section 2.3..



*Source: Author's own composition*

**Figure 2.1.: Graphic Presentation of the Relationships Between e-Learning, e-Learning System and e-Learning Systems (e-LMS, e-LCMS and CMS).**

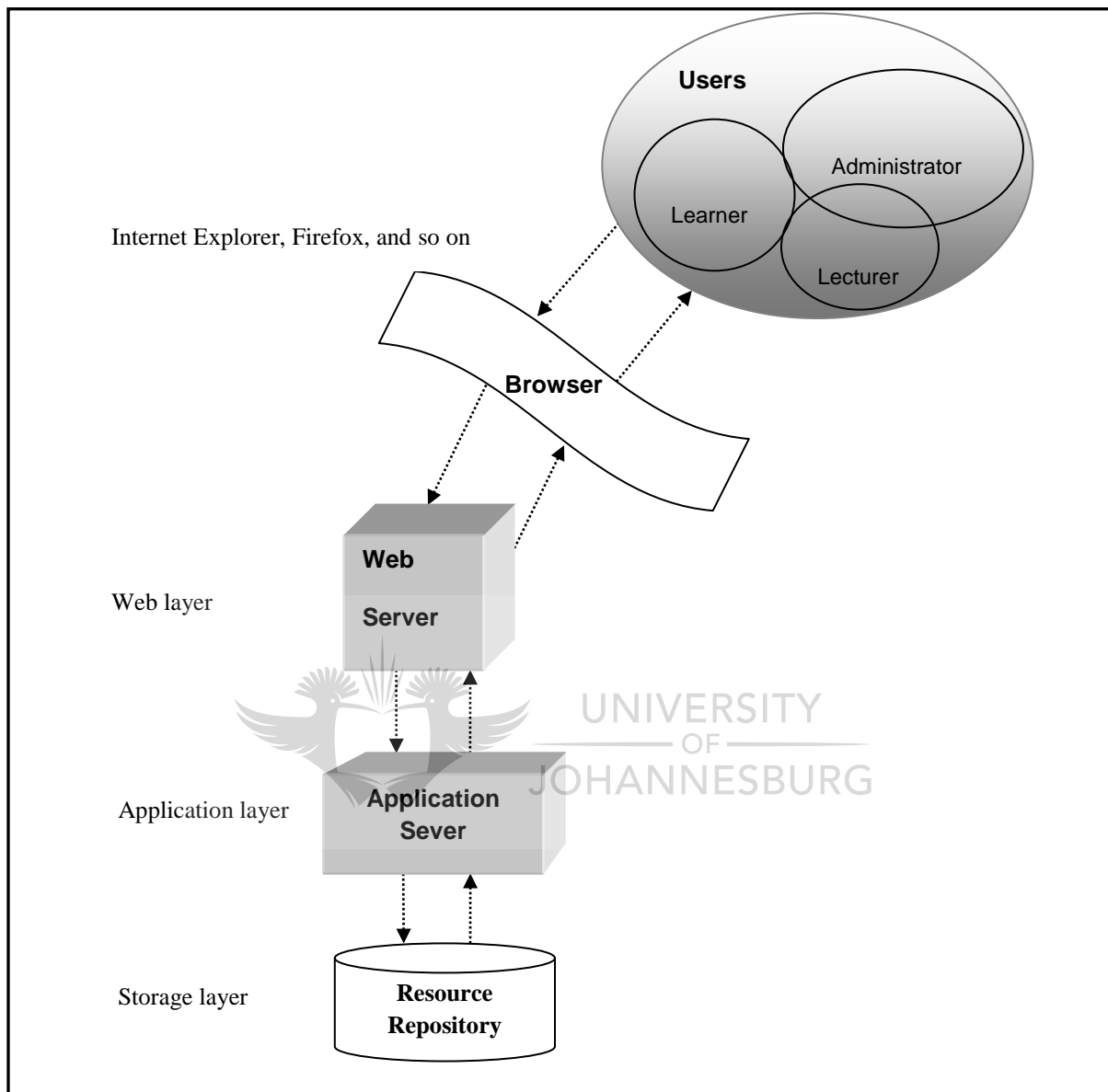
To provide further insight, the architecture and its core components of an e-LMS will be discussed in the following section.

## 2.4. THE ARCHITECTURE OF AN e-LMS

Various vendors provide different e-LMSs. However, most of the current e-LMSs share core architectural design features, such as a centralized repository, to store all the necessary information and an organized design approach to facilitate easy navigation throughout. As identified by [21], most of e-LMSs share the three layers architecture, namely: a storage layer, an application layer, and a web layer (See Figure 2.2. for the graphic presentation of the system architecture of an e- LMS):

- **Storage layer:** A resource repository, which stores all of the required data of the e-LMS.
- **Application layer:** This acts as the bridge between the web layer and the storage layer. The requests sent from the web layer are received and processed and then the results are sent back to the web layer.
- **Web layer:** This is the front end of the e-LMS, which is designed to provide a simple, efficient and uniform graphical user interface. The web layer allows users to utilize the functionalities provided by the e-LMS. These functionalities can be coded/developed using different programming/scripting languages.





*Source: Author's own composition*

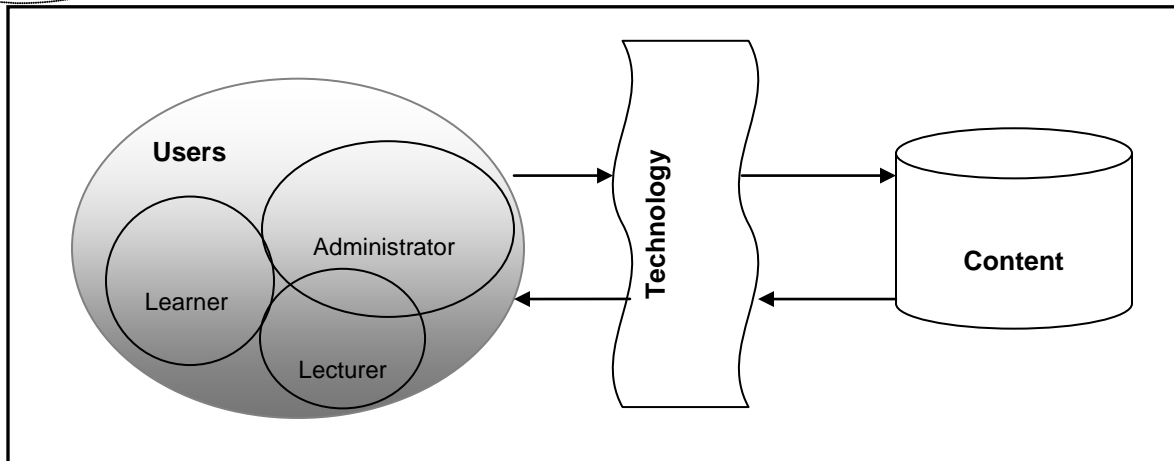
### Figure 2.2.: System Architecture of an e-LMS

Figure 2.2. illustrates the e-LMS's architectural design that highlights the core building blocks required to implement an e-LMS. In the next section, a high level explanation of the e-LMSs components will be discussed. A typical e-LMS has three core components: users, contents and technology [11 and 18].

## 2.5. COMPONENTS OF AN e-LMS

Each e-LMS is unique, though most have common basic components. According to [11 and 18], the basic components of e-LMSs are users, contents and technology. The concise clarifications of these components are discussed as follows (see Figure 2.3. for more clarification about connections between these basic components):

1. **Users:** An e-LMS has three kinds of users.
  - **An Administrator:** The person who controls and manages the overall access to e-LMSs;
  - **A Learner:** The person who tries to achieve a specific learning goal through e-LMSs; and
  - **A Lecturer:** The person who monitors the progress of learners' activities and helps learners by providing all the necessary course materials and feedbacks.
2. **Contents:** Information resources such as course material, assessment feedbacks, and informative guidelines, which help e-LMS users to achieve their goals. These contents can be in multimedia format and/or interactive such as in films, pictures, diagrams, text, music, games, etc.
3. **Technology:** An interface between the user(s) and the content. The users may use the technology to access the content.



*Source: Author's own composition*

**Figure 2.3.: Graphic Presentations of Basic Components of an e-LMS**

The most common system's architecture shared by most of e-LMSs as well as the components (i.e. role players) required to create an e-learning environment using e-LMSs were discussed in the previous sections. In the next section, the most frequently cited advantages and disadvantages of using e-LMSs in creating a complete e-learning environment or a support system for a traditional learning system will be discussed.

## 2.6. ADVANTAGES AND DISADVANTAGES OF e-LMSs

In this section, the most frequently cited advantages and disadvantages associated with the use of e-LMSs are discussed briefly.

### 2.6.1. ADVANTAGES

Some of the advantages associated with the use of e-LMSs are:

1. **Flexibility:** e-LMSs provide flexibility. Learners' time and speed preference is respected [18].
2. **Independence of Place and Time:** e-LMSs allow learners and lecturers to achieve their learning objectives regardless of their geographic location and time [18].
3. **Cost Reduction:** e-LMSs allow learners to share knowledge online, which reduces learners' and lecturers' expenses such as transportation cost, paper and so on [18].
4. **Just-in-Time Learning:** Unlike traditional learning systems, most e-LMSs are designed for just-in-time learning. Since there is a high competition for skilled employees, many companies use e-LMSs for efficient transfer and management of knowledge [11].



5. **Adaptive Learning:** e-LMSs are designed in a way to fit a learner's requirements instead of being content oriented [18].
6. **Content Consistency:** The organizational and centralised repository approach of e-LMSs allows all learners to receive equal access to their training materials and lecturers [22].
7. **Rapid Dissemination of Information:** As indicated by [22], any updates and changes in the course curriculum and content can easily and immediately be made available to the learners. A bulletin board is one of the e-LMS features that allows lecturers to announce any information in a most effective way.
8. **Provides Unique Features:** An e-LMS allows lecturers and learners to share knowledge using multimedia features such as videos, interactive quizzes, games, chat rooms and forums, which were not always possible in traditional learning systems [22].
9. **Increased Learner Participation:** e-LMSs provide synchronous communication media such as a discussion forum. As supported by [22], these media are less confrontational, which increases learner participation.

10. **Motivation:** The use of multimedia, such as video, games, and interactivity, does motivate learners [18].

11. **Learners' Progress:** The lecturer can easily track the learners' progress by utilising the progress report functional feature of an e-LMS [11 and 18].

Despite the above benefits, if an e-LMS is not implemented properly and all the necessary infrastructures are not in place, the system can have some disadvantages. Some of these disadvantages will be discussed in the next section.



### 2.6.2. DISADVANTAGES

Some of the disadvantages associated with the use of e-LMSs are:

1. **Limited Contact:** e-LMSs may limit learners' interaction with their lecturers [11]. e-LMSs allows learners to learn by themselves in their own time and space; however, if they get stuck or make any mistakes, there is no one to whom they can turn (i.e. no tutors and workshops).

2. **Requires Infrastructure:** In order to use e-LMSs, learners need to have access to a PC, internet and software, to name the minimum requirements. In addition, multimedia requires high bandwidth [18].
3. **e-LMSs are Expensive:** Commercial e-LMSs are mostly expensive. However, freeware e-LMSs do exist to provide the same kind of functionality.
4. **PC Learning may be Unpleasant or Unhealthy:** Since e-LMSs operate on computers, some users may find it difficult to access and perform their work on screen [11].
5. **Requires Prerequisite Knowledge:** e-LMS users must have minimum background knowledge in order to understand and use e-LMSs [11 and 18]. For instance, installation and use of the e-LMSs can be complex for computer illiterate people.
6. **Security:** Security is currently a serious challenge and concern facing e-LMSs.
7. **Requires High Motivation:** e-LMS is a self paced system which allows learners to learn and train anytime anywhere. Learners could be less committed due to the flexible nature of e-LMSs, which could result in only a few online learners finishing a course [18].

Many more advantages and disadvantages can be listed. However, it is not the purpose of this section to identify and list all of the possible pros and cons of using e-LMSs as a learning mechanism. In the following section, the common functional features of e-LMSs will be discussed.

## 2.7. e-LMS FUNCTIONAL FEATURES

The functional requirements of an e-LMS define some of the minimal core features expected from ideal e-LMSs, which allow efficient, user-friendly and uniform interface for e-LMS users. Five major functional feature categories are listed [14]. They are:

1. The portal;
2. The search;
3. The course catalogue;
4. The assessment;
5. The progress report; and
6. The communication tool.

As identified by [14], a summarized list of functional requirements is presented in Table 2.1.



<b>PORTAL</b>	
<b>Learner</b>	<ul style="list-style-type: none"> <li>▪ Add his/her personal information such as contact address;</li> <li>▪ Create/modify account information; and</li> <li>▪ Display list of enrolled courses and their related information.</li> </ul>
<b>Lecturer</b>	<ul style="list-style-type: none"> <li>▪ Add his/her personal information such as contact address;</li> <li>▪ Create/modify account information; and</li> <li>▪ Display the courses currently responsible for.</li> </ul>
<b>Administrator</b>	<ul style="list-style-type: none"> <li>▪ Allow administration of users, groups, courses and the system itself.</li> </ul>
<b>SEARCH</b>	
<b>Search</b>	<ul style="list-style-type: none"> <li>▪ Allows authorized users (Learner(s), Lecture(s) or Administrator) to locate documents and contents on the site.</li> </ul>
<b>COURSE CATALOGUE</b>	
<b>Course</b>	<ul style="list-style-type: none"> <li>▪ Deals with the categorization of courses; courses are mostly organized based on their topics or duration.</li> <li>▪ Provides information on the course offers, register information (i.e. date, pre-requisites), lecturers and tutors teaching the course, rules and regulation (i.e. drop policies), notifications and schedules.</li> </ul>
<b>ASSESSMENT</b>	
<b>Assignment</b>	<ul style="list-style-type: none"> <li>▪ This pertains to how assignments are handled, allowing students to submit assignments and teachers to evaluate.</li> </ul>
<b>Quiz</b>	<ul style="list-style-type: none"> <li>▪ This feature allows a teacher to create online assessments, which can be in the form of true/false, multiple choice, essay writing.</li> </ul>
<b>PROGRESS REPORT</b>	
<b>Result</b>	<ul style="list-style-type: none"> <li>▪ This feature provides the results of each student's activities and performance, which is integrated with the course catalogue and assessment.</li> </ul>
<b>COMMUNICATION TOOLS</b>	
<b>Synchronous</b>	<ul style="list-style-type: none"> <li>▪ To maintain communication between the users, chat rooms can be used.</li> </ul>
<b>Asynchronous</b>	<ul style="list-style-type: none"> <li>▪ May provide a means of communication between users. Examples are emails, bulletin boards and discussion forums.</li> </ul>

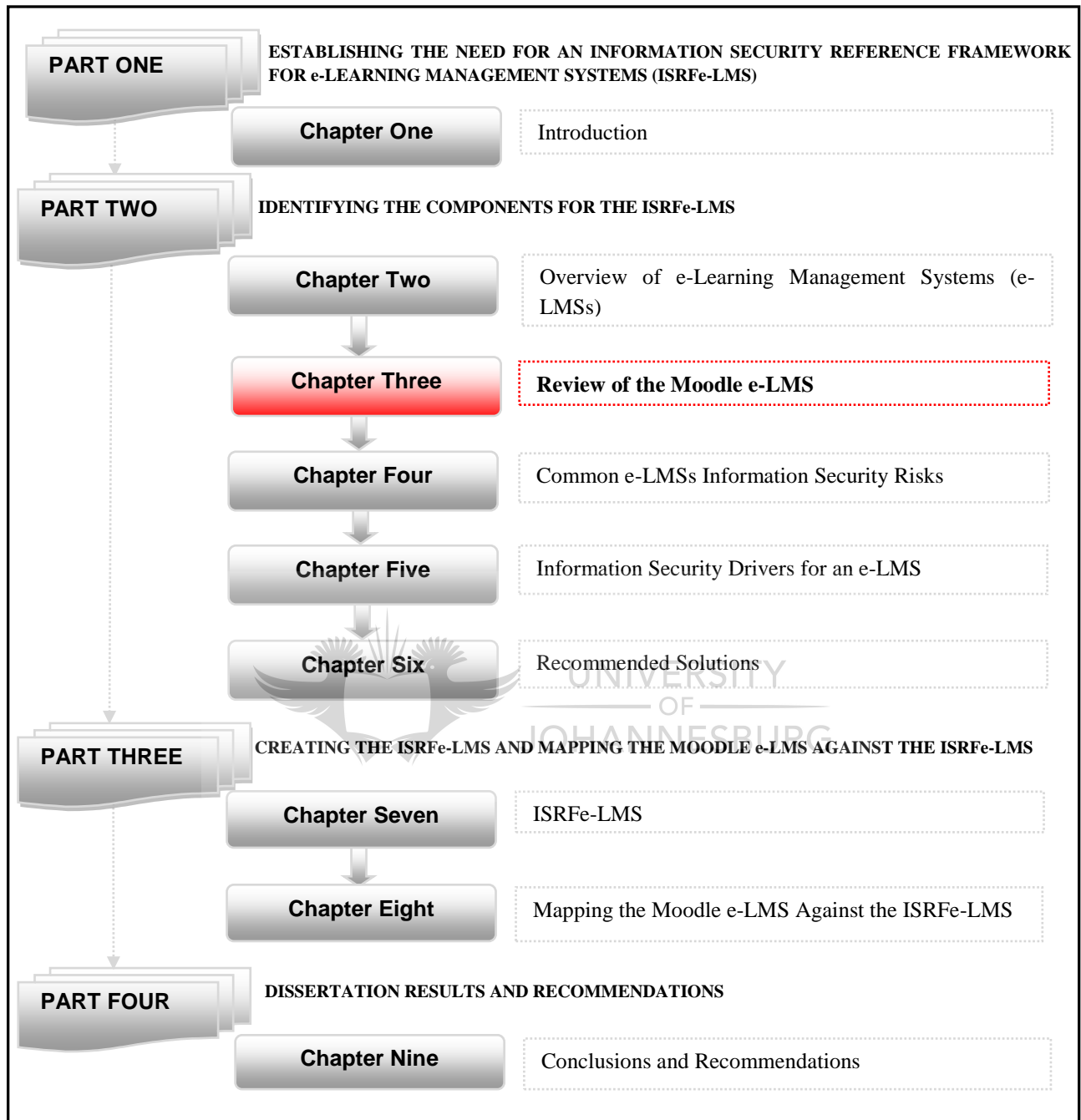
**Table 2.1.: A Summarized List of the Minimal Functional Features Expected From an e-LMS [14]**

Table 2.1. presents a summary of the basic functional features expected from ideal e-LMSs.

## 2.8. CONCLUSION

The purpose of this chapter was to provide a basic insight into the e-LMS environment. The terminology related to the concepts was defined, the functional features expected from ideal e-LMSs were highlighted, and the architectural design and the components of the e-LMSs were discussed.

In Chapter Three, the Moodle e-LMS will be reviewed to understand its basic architectural design, functional features and its prevailing security sub systems.

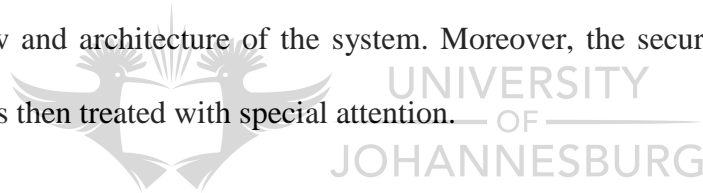


## CHAPTER THREE

### REVIEW OF THE MOODLE e-LEARNING MANAGEMENT SYSTEM (e-LMS)

#### 3.1. PREVIEW

A general overview of e-LMSs was provided in the previous chapter. This chapter intends to focus on the Modular Object Oriented Dynamic Learning Environment (Moodle) e-LMS, which will be analyzed briefly. Moodle will be analysed by providing a product overview and architecture of the system. Moreover, the security sub-system of Moodle e-LMS is then treated with special attention.



In the next section, an overview of the Moodle e-LMS will be provided, where the historical background and the philosophy behind the design as well as the features available to end-users will be discussed.

### 3.2. MOODLE e-LMS BACKGROUND

One of the most popular open source e-LMSs is Moodle. Moodle was created by Martin Dougiamas, while he was a PhD researcher at the Curtin University of Technology [12]. As noted from the official Moodle documentation [37], the term Moodle originates from the acronym for Modular Object Oriented Dynamic Learning Environment. Martin created the Moodle e-LMS from the realization of the need for an effective, easy to use and intuitive online learning system for academic environments. Moodle version 1.0 was released on August 20, 2002. Since then, the product has made much advancement in terms of features and performance. Currently, Moodle is on version 1.9 [37].

Different e-LMSs have different approaches in their design and implementation; an instructor-oriented approach is the most common approach shared by most of the e-LMSs. An instructor-oriented e-LMS is an e-LMS where lecturers pre-define the overall layout and course content of the system. Moodle follows a different approach or philosophy in its design and implementation, known as Social Constructionist Pedagogy [9]. Unlike an instructor-oriented e-LMS, in Social Constructionist Pedagogy, users (i.e. Administrators, Lecturers and Learners) are involved in constructing their own knowledge. Moodle's Social Constructionist Pedagogy philosophy is reflected in its design and functional features. For instance, the built-in Glossary feature of Moodle e-LMS is designed in a way that both learners and lecturers can add/maintain the glossary lists as they progress through the course.

The Moodle e-LMS has been written using the Hypertext Preprocessor (PHP) scripting language. PHP is an open source scripting language, which makes it freely and easily accessible. One of the most attractive features of the Moodle e-LMS is that it is able to run on any platform where PHP, Apache and MySQL/PostgreSQL databases are installed. All PHP, Apache and MySQL/PostgreSQL databases are available freely. To make use of the Moodle e-LMS features, users are only required to install the freely available Moodle e-LMS application, browser and the Internet connection. Figure 3.1. depicts the summarized profile of Moodle e-LMS as identified on the official Moodle site [37].



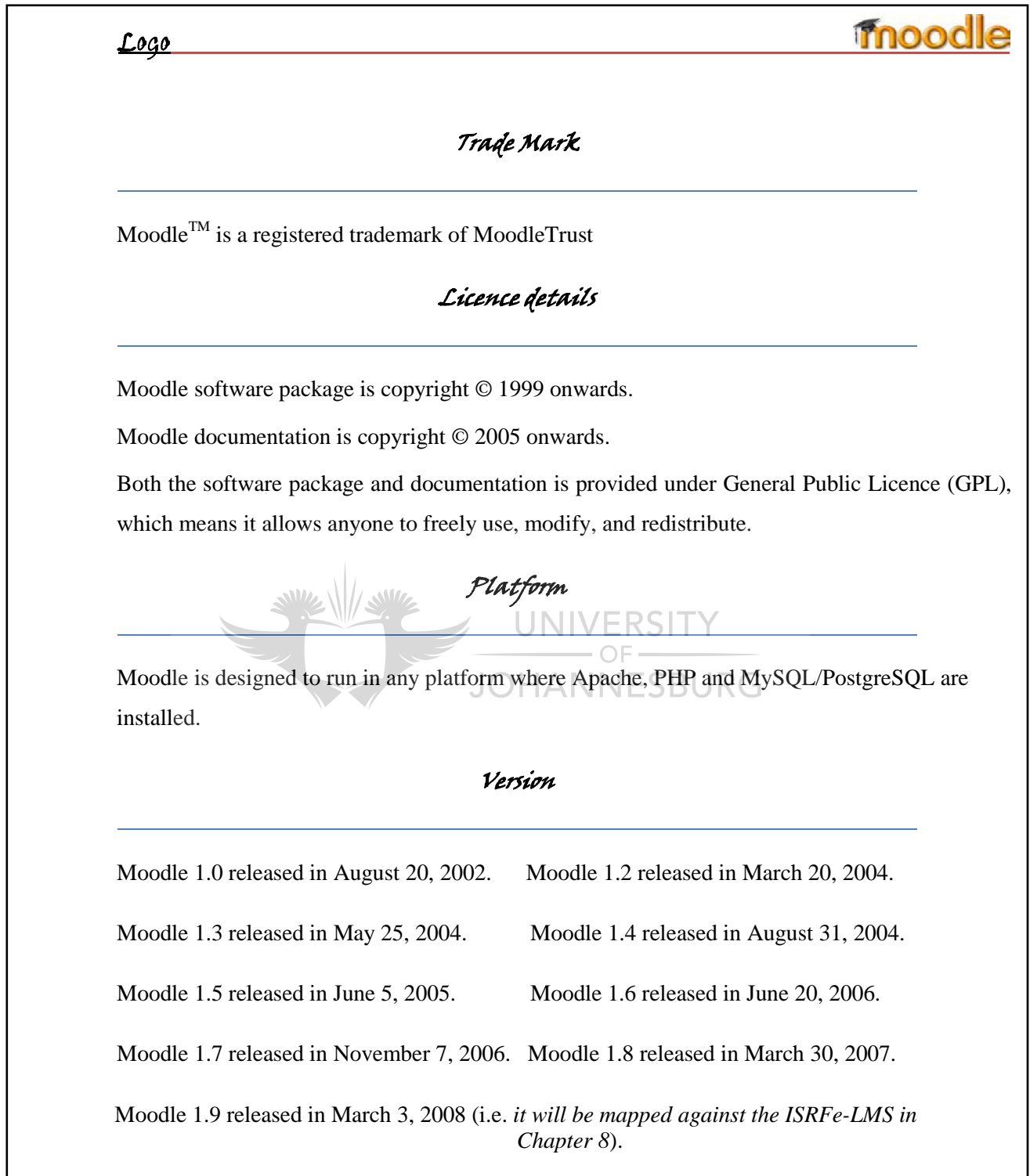


Figure 3.1.: Moodle e-LMS Concise Information Chart [37]

As shown in Figure 3.1., the Moodle e-LMS has recently released its latest version, Moodle 1.9. Since the release of the first version, the Moodle e-LMS has made tremendous improvements in its functional features and performance. In the next section, the most common functional features of the Moodle e-LMS will be discussed.

### 3.3. MOODLE'S FUNCTIONAL FEATURES

Every e-LMS has an approach that guides the user experiences. The Moodle e-LMS follows a modular approach in the design and implementation of its features. For instance, in Moodle, almost everything is organized in terms of a course and every course belongs to a category [37]. One of the advantages of its modular approach is easy addition, update and customization of features.

The Moodle e-LMS supports two kinds of modules or features: the built-in module and the add-on module. Both built-in and add-on modules are used to create flexible, easy to use, effective and interactive online learning systems. Built-in modules are features that will be available when the Moodle e-LMS is installed. An example of a built-in module is the assignment module which allows students to submit their assessments to be reviewed by their lecturers. See Table 3.1. for further information on built-in modules of Moodle's e-LMS. Add-on modules, however, require separate installation procedures in order to make use of the added functionalities. Add-on modules have specific features that allow



the customization of Moodle in order to meet specific needs. The Appointment Module is an example of an add-on module [40]. Moodle's three major built-in module categories are listed below. They are:

1. The Communication Modules;
2. The Assessment Modules; and
3. The Other Modules.

COMMUNICATION BUILT-IN MODULES	
<b>Chat</b>	A Synchronous discussion platform which allows e-LMS users to have discussions and share knowledge on the chosen topic.
<b>Forums</b>	An Asynchronous discussion platform, which allows e-LMS users to think about the topic and contribute in their own time.
<b>Wiki</b>	Allows e-LMS users to add/edit information on a specific topic; which is used as collaborative learning.
ASSESSMENT BUILT-IN MODULES	
<b>Assignments</b>	Allows lecturers to grade electronically submitted materials or paper based assignments or other class activities. Uploaded files to be reviewed by lectures.
<b>Quizzes</b>	Allows lecturers to set up and upload quizzes.
<b>Workshop</b>	Graded effort among students.
<b>Hotpot</b>	Allows lectures to create different types of quizzes such as multiple choices, short answer and so on.
OTHER BUILT-IN MODULES	
<b>Glossaries</b>	Allows e-LMS users to create and maintain a list of glossaries from their course, which can be browsed and searched.
<b>Choices</b>	Allows a lecturer to set and ask a multiple choice question; the outcome helps to decide on the course content.
<b>Survey</b>	Allows assessment of the learning activity.
<b>SCORM</b>	A package that enables interoperability, accessibility and reusability of web based learning content.
<b>Site</b>	Allows an administrator to manage access to the system; which defines roles and

<b>Management</b>	privileges of lecturers and learners.
<b>User Management</b>	Allows lecturers and learners to create their profiles.
<b>Course Management</b>	Allows lecturers to create a course category and organize the course category; create a course, and then finally categorize the course by type. For instance, some of the course material can be files, text pages or links.

**Table 3.1.: Summarized List of Built-in Module/Features of Moodle's e-LMS [40]**

Table 3.1. Summarizes the most common functional features of the Moodle e-LMS. The architectural structure of Moodle will be discussed in the next section.

### 3.4. THE ARCHITECTURE OF MOODLE



The system architectural design of the Moodle e-LMS is comprised of three layers: the application directory, data directory and database, which work together in order to create an effective and interactive online learning system [40]. The three components of Moodle's system architecture will be discussed below.

- **Application directory**

Each application occupies one directory, with many sub-directories for various modules. Some of these directories are: Admin and Lang directory, which hold the PHP code that creates the administrative pages and holds the translation of the Moodle interface, respectively.

- **Data directory**

Data directories are secure data storages where all files uploaded by users (i.e. Learners, Lecturers or Administrators) will be stored. For instance, assignments that are submitted by learners for evaluation by their lecturers will be stored in the data directory.

- **Database**

Objects created by Moodle systems, such as quizzes, grades, user logins, settings and contents of forums will be stored in the database. The most common databases used by Moodle are MySQL and PostgreSQL.

The next section attempts to review the security sub-system of Moodle. The review does not include the security of the operating system and the web, on which Moodle runs. For the purpose of this research, only the security sub-system of Moodle, within the context of how Moodle adapts security in order to provide effective and reliable e-Learning environments will be investigated.

### 3.5. THE INFORMATION SECURITY FEATURE OF MOODLE

This section carries out an investigation on the information security functionality of the Moodle e-LMS. To do so, the author will be using the six Information Security Services as a guideline [31]. The six Information Security Services are: Identification and Authentication, Authorization, Confidentiality, Integrity, Non-Denial/Non-Repudiation and Availability Information Security Services. How each of these information security services are enforced in the Moodle e-LMS will be discussed in the next section. Please note that due to the fact that available Moodle e-LMS documentations are limited, practical tests on the information security functionalities of the system has been conducted.



#### 3.5.1. IDENTIFICATION AND AUTHENTICATION

Moodle allows users to have access to the system as anonymous users, guests or registered users [37].

- **Anonymous Users** are users who are allowed to use the Moodle e-LMS environment without any identification information. Anonymous users usually have limited privileges.
- **Guest Users** are users with certain levels of access rights to the resources available. Guest users do not require prior registration.

- **Registered Users** are users who have pre-registered and are known by the Moodle e-LMS. Each registered user has a unique user id and password that will be used by users to access the Moodle e-LMS environment.

In the Moodle e-LMS environment, Identification and Authentication information security services are used to verify the accounts of registered users (i.e. users known to the system before any access).

Moodle e-LMS uses a password based mechanism to enforce the Identification and Authentication Information Security Service that will be discussed in detail in the next section.



#### 3.5.1.1. INFORMATION SECURITY MECHANISMS

Moodle uses the Password Based Information Security Mechanism to enforce the Identification and Authentication information security service. According to [37], the Moodle e-LMS has three ways of managing the authentication process, which are:

- **Email Based Self-Registration:** This allows users to choose their own username and password and the confirmation email is sent to the user's email address. In this way, the system confirms the user's account. When the user logs in, his/her username and password are checked against the stored values in the Moodle database.

- **Manual Accounts:** All accounts will be created manually by the administrator.
- **No Login:** Used by administrator to restrict accounts.

Moodle uses two authentication options: through an external database (MySQL or PostgreSQL) or with a server (LDAP, IMAP). Depending on which authentication option is used, there are two ways of granting access to users:

1. When users are authenticated with an external database (MySQL or PostgreSQL), Moodle copies over the username and password from the external database into Moodle's internal database. From then on, whenever the user logs on, it uses Moodle's internal database to verify authenticity of the username and password.
2. When users authenticate with a server (LDAP, IMAP), Moodle checks the username and password against the server every time the user signs in [40].

### 3.5.1.2. INFORMATION SECURITY POLICIES

In addition to the Identification and Authentication information security service, Moodle uses additional security features in order to strengthen the security and keep away unauthorized users from accessing the system or specific content. Some of the security features are:

- Having Moodle information security policies and procedures in place. For instance, a user will be automatically logged out once it has been idle for a set period of time;

The purpose of the Identification and Authentication Information Security Service is to ensure only authorized users are allowed access to the system, which makes it the heart of information security in any e-LMSs and must be enforced effectively. The second Information Security Service that is important in creating a secure e-LMS environment is Authorization, which will be discussed in the next section.

### 3.5.2. AUTHORIZATION

Authorization Information Security Service ensures only legitimate users can have access to their respective information resources.

#### 3.5.2.1. INFORMATION SECURITY MECHANISMS

The Moodle e-LMS supports Role Based Access Control (RBAC) mechanisms for controlling access to the information resources. To strengthen Authorization, the Moodle e-LMSs categorize courses into groups and assign users to the group, whereby information security controls, policies and procedures are assigned to each group [37].

### 3.5.3. CONFIDENTIALITY

The Confidentiality Information Security Service ensures that only authorized user may view the content of the information resource.

#### 3.5.3.1. INFORMATION SECURITY MECHANISMS

Moodle enforces confidentiality through the implementation of effective Identification and Authentication as well as authorization information security service. Moodle also uses a unique key called an enrolment key that is assigned to each resource such as course material. Anyone who knows this key is able to access the resource. The use of an enrolment key adds extra layer of security and also enforces the confidentiality information security service.

### 3.5.4. INTEGRITY

The Integrity Information Security Service ensures that only authorized users may alter the content of the information resource.

#### 3.5.4.1. INFORMATION SECURITY MECHANISMS

Moodle enforces the integrity Information Security Service through the use of strong Identification and Authentication as well as Authorization Information Security Service.



### 3.5.5. NON-DENIAL

The Non-Denial Information Security Service ensures that actions performed by users may not be denied later.

#### 3.5.5.1. INFORMATION SECURITY MECHANISMS

Moodle enforces the Non-Denial Information Security Service through the implementation of an effective Identification and Authentication service. Moodle supports the activity log feature which provides users' activity histories.

### 3.5.6. AVAILABILITY



UNIVERSITY  
OF  
JOHANNESBURG

The Availability Information Security Service ensures the system is reliable and available at all times.

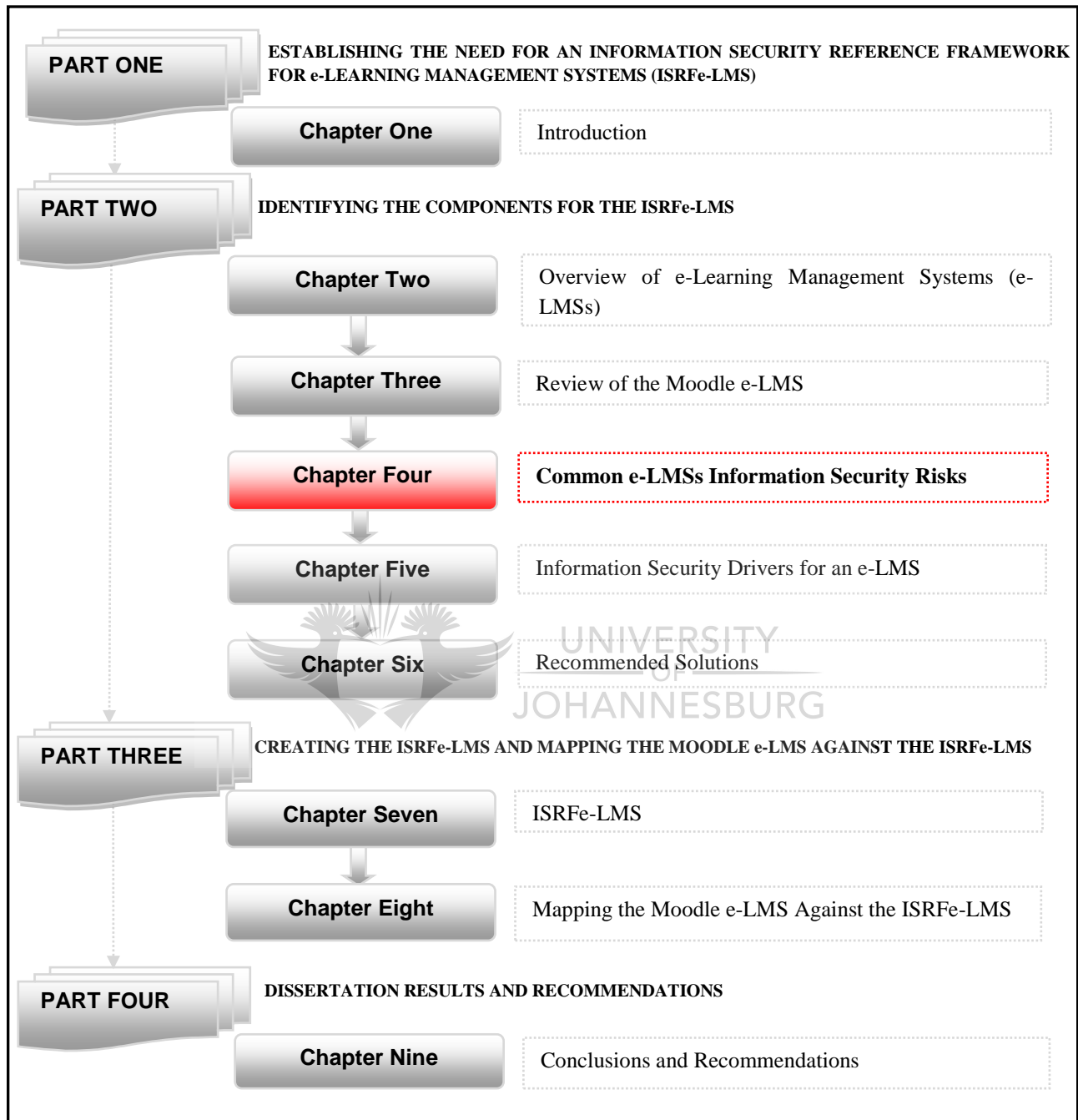
#### 3.5.6.1. INFORMATION SECURITY MECHANISMS

Moodle ensures the availability of the system through the use of backup facilities, which allow the system to stay stable and maintain its data integrity.

### 3.6. CONCLUSION

Moodle is a free, interoperable, open source e-LMS which allows users to create flexible, reliable and interactive online learning environments. The Moodle e-LMS has adopted different information security policies and procedures, as well as information security mechanisms to ensure the six Information Security Services are enforced. This chapter has put a great emphasise on the security sub-system of Moodle e-LMS by examining the information security mechanisms adopted by the system in order to enforce the six Information Security Services throughout the environment.





## CHAPTER FOUR COMMON e-LMSs INFORMATION SECURITY RISKS

### 4.1. PREVIEW

The Moodle e-LMSs were analyzed and examined in the previous chapter. The motivation for the need for a comprehensive Information Security Reference Framework for e-LMS (ISRFe-LMS) will continue in this chapter. To attain a reasonable level of security in an e-LMS environment, it is necessary to have a good understanding of the information security risks involved in using the e-LMS. The two research questions that will be addressed and act as a guideline for this chapter are:

#### *Sub-question 2:*

---

What kind of activities can users (i.e. Administrators, Lecturers and Students) do in e-LMSs?

#### *Sub-question 3:*

---

What are the main information security risks specifically related to the activities identified in sub-question 2?

This chapter attempts to identify the common information security risks related to the e-LMS's environment from the perspective of each user's activities. Please note that the information security vulnerabilities presented in the next section do not refer to Moodle e-LMS but to e-LMSs in general. To accomplish this, the author first identifies the most common activities performed by each user and then develops scenarios to illustrate some of the potential information security risks related to each activity.

## 4.2. BACKGROUND

An e-LMS is highly dependent on the information it holds; the architectural design and integrated nature of the system makes it vulnerable to information security risks. An information security risk can be defined as a change from a known state to an unknown state, thereby creating a period of uncertainty [25]. Risk involves only the possibility of suffering harm or loss which will have an impact on the objective of the system [6]. A clearer and more concise definition of an information security risk is provided by [6], which is a function of the likelihood of a threat exploiting a particular potential vulnerability of system. Therefore, an information security risk exists only when a threat exploits a vulnerability of an asset [6]. Assets, threats and vulnerabilities are the three important terms in the definition of the information security risk. The definitions and the relations between these terms are given below.

- **Assets** are resources - e-LMSs deal particularly with intangible assets such as information and data. For example, some of an e-LMS's assets are learners' personal information and course materials.
- **Vulnerabilities** are information security weaknesses that may be accidentally or intentionally exploited to cause potential harm or loss of assets [25]. For example, some of an e-LMS's vulnerabilities are caused by weak password choices by users or weak authentication methods.
- **A Threat** is any act aimed at exploiting a vulnerability [6 and 25]. For example, some of the possible threats that e-LMSs are exposed to are unauthorised interception, interruption, deletion, modification and fabrication.

All of the above definitions highlight the negative impact of the information security risks, which need to be addressed by applying information security measures. Although there is a major growth in e-LMSs usages, unethical conduct such as unauthorised interception, interruption, plagiarism and deception of users have been major challenges [36]. As highlighted by [15, 35 and 38], the nature and inherently complex architecture of e-LMSs are exposed to information security risks. In addition, e-LMSs centralised repository approaches make e-LMSs more vulnerable to information security threats; the centralised database may contain critical personal and business information which needs to be protected from unauthorized access.

Before discussing any of the information security risks and countermeasures, it is necessary to have a good understanding of the overall environment of an e-LMS. For the purpose of this dissertation, an e-LMS will be investigated from each user's (i.e. Learners, Lecturers and Administrators) perspective to understand the types of activities each user will be performing in order to achieve the overall knowledge sharing goals. In the following section, the most common activities performed by each user will be discussed.

### 4.3. USERS AND THEIR ROLES IN e-LMS

An e-LMS is usually made up of various sub-systems or modules, which deal with specific aspects of the overall objectives of the system. For instance, e-Exam (e-Assessment) allows learners to take online quizzes set up by their lecturers and e-Assignment allows learners to upload their assignments for evaluation. Each user has roles and responsibilities on the e-LMS modules.

### 4.3.1. LECTURER

A Lecturer is one of the user components of an e-LMS who is responsible for coaching as well as tracking the performances of his/her respective learner(s). The lecturer can:

1. Manage his/her profile: for instance, create his/her account, change his/her password or contact details;
2. Create course materials and identify and attach all information to the course; for instance, register information (i.e. dates, pre-requisites), rules and regulation (i.e. drop policies);
3. Upload the course material created;
4. Create and upload online assessment materials such as quizzes in the form of true or false, multiple choice, matching and so on;
5. Set up and post assignment(s);
6. Set up grading scales;
7. Evaluate the assignments submitted by learners and then upload the results for learners;
8. Use communication means such as synchronous (i.e. chat) and asynchronous (i.e. forums) communication media to keep in touch with their learners and subordinates; and
9. Assign learners to a course.



### 4.3.2. LEARNER

The learner is another user of the e-LMS who uses the e-LMS in order to achieve learning objectives. Learners can:

1. Manage their profiles: for instance, create an account, change a password or contact details;
2. Access course materials;
3. Take online assessment exams or quizzes, which are set by the lecturer;
4. Complete posted assignment(s) offline and submit it online for feedback;
5. Access their assessment results; and
6. Use communication means such as synchronous (i.e. chat) and asynchronous (i.e. forums) communication media to keep in touch with their lecturers and fellow classmates.

### 4.3.3. ADMINISTRATOR

An administrator is the person who oversees and moderates the activities carried out on the e-LMS. Moreover, the administrator defines and assigns privileges to the rest of the e-LMS users. The administrator can:

1. Manage their profiles: for instance, create an account, change a password or contact details.

2. Set up roles and privileges;
3. Assign roles and privileges to learners and lecturers; and
4. Assign lecturers to a course(s).

e-LMSs sub-systems are faced with information security vulnerabilities. Any security breach on sub-systems can compromise the reliability and dependability of the entire system. For instance, one of the information security vulnerabilities of e-Exam (e-Assessment) is the inability to authenticate exam takers. One of the scenarios given by [36] addresses the issue of deceivers (i.e. logging in with someone's identity). Sometimes, users give away their authentication information (i.e. username and password) intentionally so that another person can do exams on their behalf (see scenario 1 for a detailed explanation).

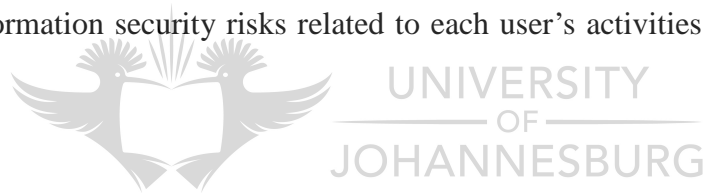
- **Scenario 1:** Learner ( $L_1$ ) gives his secret information (i.e. identification and authentication) to his friend ( $L_2$ ) willingly so that  $L_2$  can write the exam on the behalf of  $L_1$ . If this issue is not addressed, it opens a door for dishonesty, where one can easily claim that someone else has stolen his/her password.

The author tried to identify the most common information security vulnerabilities of e-LMSs from each user's perspective and this will be discussed in the next section. Each of the information security risks identified in this section corresponds to the e-LMS user's activities identified in section 4.3.1., 4.3.2. and 4.3.3..

## 4.4. INVESTIGATING THE INFORMATION SECURITY RISKS OF USING AN e-LMS

The main aim of this section is to identify the growing information security challenges of the e-LMSs from each user's perspective.

These vulnerabilities could lead to possible information security risks that could compromise the integrity of the system, and which could compromise the reputation of the institution. In the following sections, scenarios will be formulated and discussed to illustrate the information security risks related to each user's activities (i.e. as discussed in section 4.3.).



### 4.4.1. LECTURER

Without proper information security, an e-LMS could be exposed to the following most common information security risks, which arise from the lecturers' activities discussed in section 4.3.1.:

- **Activity 1:** Manage his/her profile: for instance, create his/her account, change his/her password or contact details. One of the risks related to this activity is :

1. An unauthorized person can change the profile of the lecturer.

- **Activity 2:** Create course materials and identify and attach all information to the course; for instance, register information (i.e. dates, pre-requisites), rules and regulation (i.e. drop policies).
  
- **Activity 3:** Upload the course material created. Some of the risks related to activity 2 and 3 are:
  1. Fake course material can be created and uploaded by unauthorized users;
  2. Course material may be viewed by an unauthorized person;
  3. Course material may be altered by an unauthorized person; and
  4. Course material may be deleted by an unauthorized person.
  
- **Activity 4:** Create and upload online assessment materials such as quizzes in the form of true or false, multiple choices, matching and so on.
  
- **Activity 5:** Set up and post assignment(s).Some of the risks related to activity 4 and 5 are:
  1. Fake assignments can be uploaded;
  2. The exam set up by the lecturer can be viewed before the due date;
  3. The assessment material can be altered by an authorized person; and
  4. The exam can be deleted when a student knows that he/she is not ready.

- **Activity 6:** Set up grading scales. One risk related to this activity is:
  1. Fake grading scales can be uploaded by an unauthorized person.
- **Activity 7:** Evaluate the assignments submitted by learners and then upload the results for learners. Some of the risks related to this activity are:
  1. Fake assessment results can be uploaded;
  2. Assessment results may be viewed by an authorized person;
  3. Assessment results may be changed by an authorized person;and
  4. Assessment results may be deleted by an authorized person.
- **Activity 8:** Use communication means such as synchronous (i.e. chat) and asynchronous (i.e. forums) communication media to keep in touch with their learners and subordinates. One of the risks related to this activity is:
  1. An unauthorized person may act as an authorized lecturer during discussion.
- **Activity 9:** Assign learners to a course. One of the risks related to this activity is:
  1. An unauthorised person may act as an authorized lecturer and register learners to a course.

In the next section, the possible information security risks related to the learners' activities will be discussed in detail.

#### 4.4.2. LEARNER

Without proper information security an e-LMS could be exposed to the following most common information security risks, which arise from the learners' activities discussed in section 4.3.2.:

- **Activity 1:** Manage their profiles, for instance create an account, change a password or contact details. One risk related to this activity is:
  1. An unauthorized person may alter/delete the profile of the learner.
- **Activity 2:** Access course materials. One of the risks related to this activity is:
  1. Someone can access a course material pretending to be the learner.
- **Activity 3:** Take online assessment exams or quizzes which are set by the lecturer. Some of the risks related to this activity are:
  1. The learner can pass his/her personal Identification and Authentication information to his/her friend so that the friend can write the exam on his/her behalf; and

2. When a learner finds out he/she cannot pass the test, he/she can create a Denial of Service attack (DOS) to sabotage the exam.

- **Activity 4:** Complete posted assignment(s) offline and submit it online for feedback.

1. Someone can submit a fake assignment pretending to be the learner;
2. The student can deny submitting the assignment when he/she thinks that he/she will not pass; and
3. Submitted assignments can be viewed, copied, changed or deleted.

- **Activity 5:** Access their assessment result.

1. The grade report may also be viewed by unauthorized persons.

- **Activity 6:** Use communication means such as synchronous (i.e. chat) and asynchronous (i.e. forums) communication media to keep in touch with their lecturers and fellow classmates.

1. Cheating during exams, which includes getting unauthorized help from someone, through the use of a synchronous (i.e. chat) and asynchronous (i.e. forum) collaboration during exam or devices such as calculators, cell phones and so on [36].

In the next section, the possible information security risks related to the administrators' activities will be discussed in detail.

#### 4.4.3. ADMINISTRATOR

Without proper information security an e-LMS could be exposed to the following most common information security risks, which arise from the administrator's activities discussed on section 4.3.3:

- **Activity 1:** Manage their profiles: for instance, create an account, change a password or contact details. One risk related to this activity is:
  1. An unauthorized person may alter/delete the profile of the administrator.
  
- **Activity 2:** Set up roles and privileges.
  
- **Activity 3:** Assign roles and privileges to learners and lecturers. Some of the risks related to activity 2 and 3 are:
  1. Fake roles and privileges could be set by an unauthorized user;  
and
  2. The roles and privileges could be altered by an unauthorized user.



- **Activity 4:** Assign lecturers to a course(s). One of the risks related to this activity is:

1. An unauthorized person may act as an authorized administrator and assign lecturers to a course.

The scenarios investigated above (section 4.4.1., 4.4.2. and 4.4.3.) clearly illustrate some of the potential information security risks. Unless countermeasures are identified and implemented, the system integrity will be compromised. One of the recommended solutions will be discussed in Chapter Seven.

## **4.5. CONCLUSION**



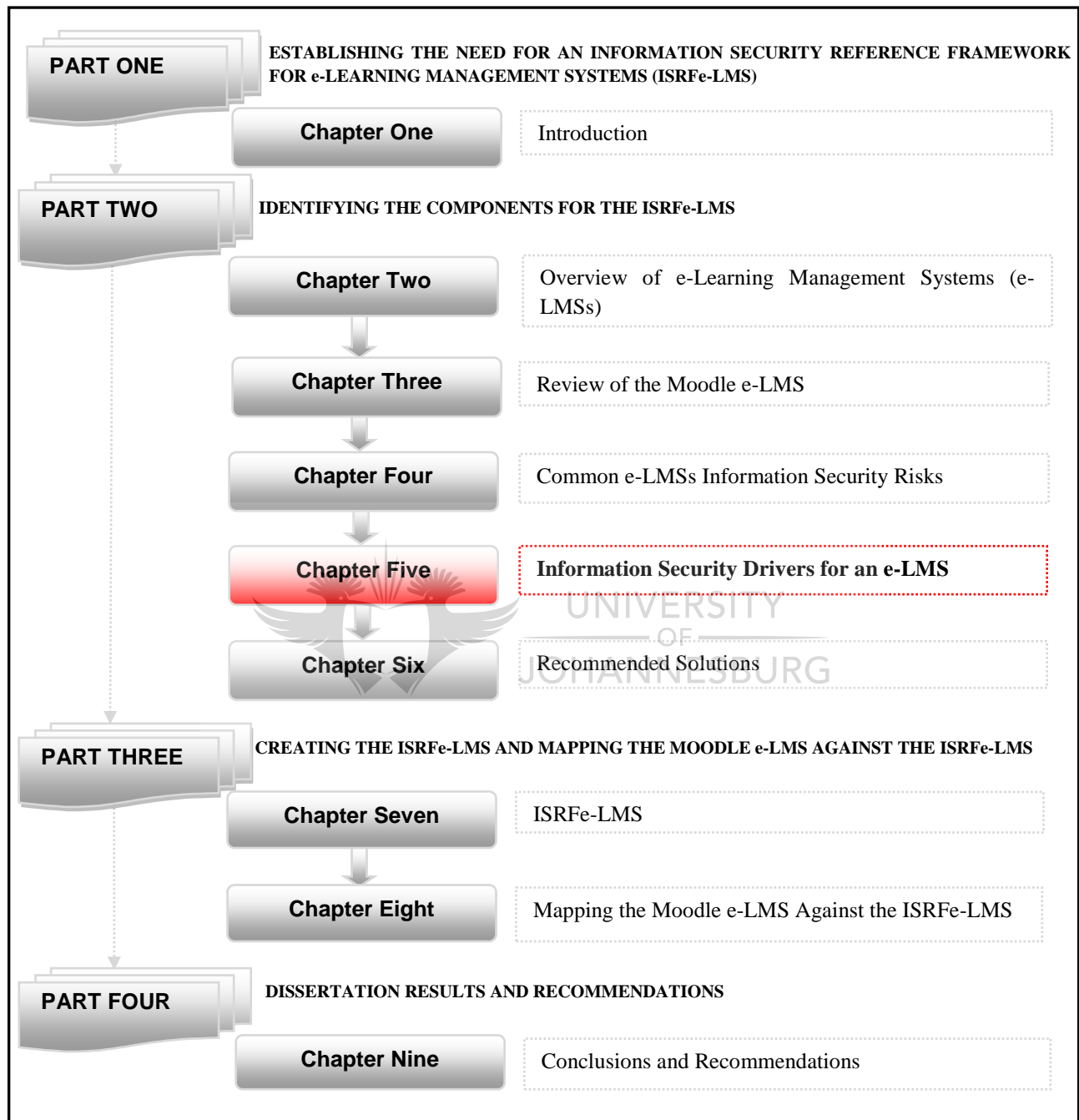
UNIVERSITY  
OF  
JOHANNESBURG

This chapter highlighted how important it is to ensure that the security of an e-LMS environment is maintained at all times. The scenarios investigated above clearly illustrate some of the potential information security risks, and confirm that unless countermeasures are identified and implemented, the integrity of the system will be compromised. Non-technical information security issues (i.e. users not acting accordingly with the information security policies and procedure) are the major cause of most of the information security breaches that have been discussed in this chapter. For instance, users may deliberately pass on their identity (username and password) to another party. In this case, even if the e-LMS has technical information security mechanisms in place, such as

forcing each user to be verified before access is allowed, without non-technical

Information Security countermeasures (i.e. user awareness and support), the system is still vulnerable. “Technology can only assist and cannot replace the expertise of human” [19]. Therefore, it is necessary to understand information security as a multi-dimensional discipline. How the combination of information security dimensions could be used to create a secure e-LMS will be discussed in the next chapter.





## CHAPTER FIVE

### INFORMATION SECURITY DRIVERS FOR AN e-LMS

#### 5.1. PREVIEW

The previous chapter identified the most generic information security vulnerabilities facing e-LMSs. The scenarios presented in section 4.4. show that there are potential information security vulnerabilities facing e-LMSs, which means that information security measures need to be in place in order to mitigate the risks. Most of the current e-LMSs do provide some form of technical mechanism, like password based authentication, to protect the valuable assets. As explained in the previous chapter, having only technical information security measures in place do not necessarily ensure that the security of an e-LMS environment is maintained at all times.

This chapter originated from the realisation that the information security is a multi-dimensional discipline, but the dynamic nature of information security makes it impossible to define a fixed list of information security dimensions [47]. For the purpose of this dissertation, the author has identified the five most important information security dimensions for the e-LMS environment. The aim of this chapter is to briefly discuss each dimension and show how these dimensions contribute to the Information Security Reference Framework for e-Learning Management Systems (ISRF-e-LMS) that will be created later in this dissertation.

The following research question will be addressed and used as guideline for this chapter.

*Sub-question 4:*

---

Which information security dimensions are most relevant in creating a secure e-LMS environment?

The next section provides background information on the multi-dimensional concept of information security.

## 5.2. BACKGROUND



The integrated and dynamic nature of e-LMSs should make it clear that information security is one of the most important aspects to be considered during the implementation and usage of an e-LMS. Before discussing how the five identified dimensions of information security could be used as countermeasures, it is important to understand the multi-dimensional concept behind information security.

### 5.3. INFORMATION SECURITY

Information security can be defined as the process of protecting information and information assets from a wide range of threats [24]. Installing anti-virus software or setting up firewalls are examples of information security countermeasures that could be used to protect a system's assets such as personal information and data. The information security measures implemented by most e-LMSs only deal with the security of the network or database. As noted in section 4.4., securing only the network and database does not ensure the overall security of an e-LMS environment. As highlighted in [47], information security should not be seen as only a technical issue but as a multi-dimensional discipline, where each dimension needs to be taken into account in order to create a comprehensively secure environment. The author identified five dimensions of information security that should be put in place to enhance the overall information security of an e-LMS environment. In the next section, the five information security dimensions will be introduced, and the relationship between these dimensions will be discussed.

### 5.3.1. THE FIVE INFORMATION SECURITY DIMENSIONS

As identified by [47], the dynamic nature of information security makes it impossible to have a fixed list of dimensions. For the purpose of this dissertation, the author proposes that the following five essential information security dimensions should be put in place for a proper information security within e-LMS environments:

- The e-LMS Information Security Governance (ISG) Dimension;
- The e-LMS Information Security Policies and Procedures Dimension;
- The e-LMS User Awareness Dimension;
- The e-LMS Monitoring Dimension; and
- The e-LMS Technical Dimension.

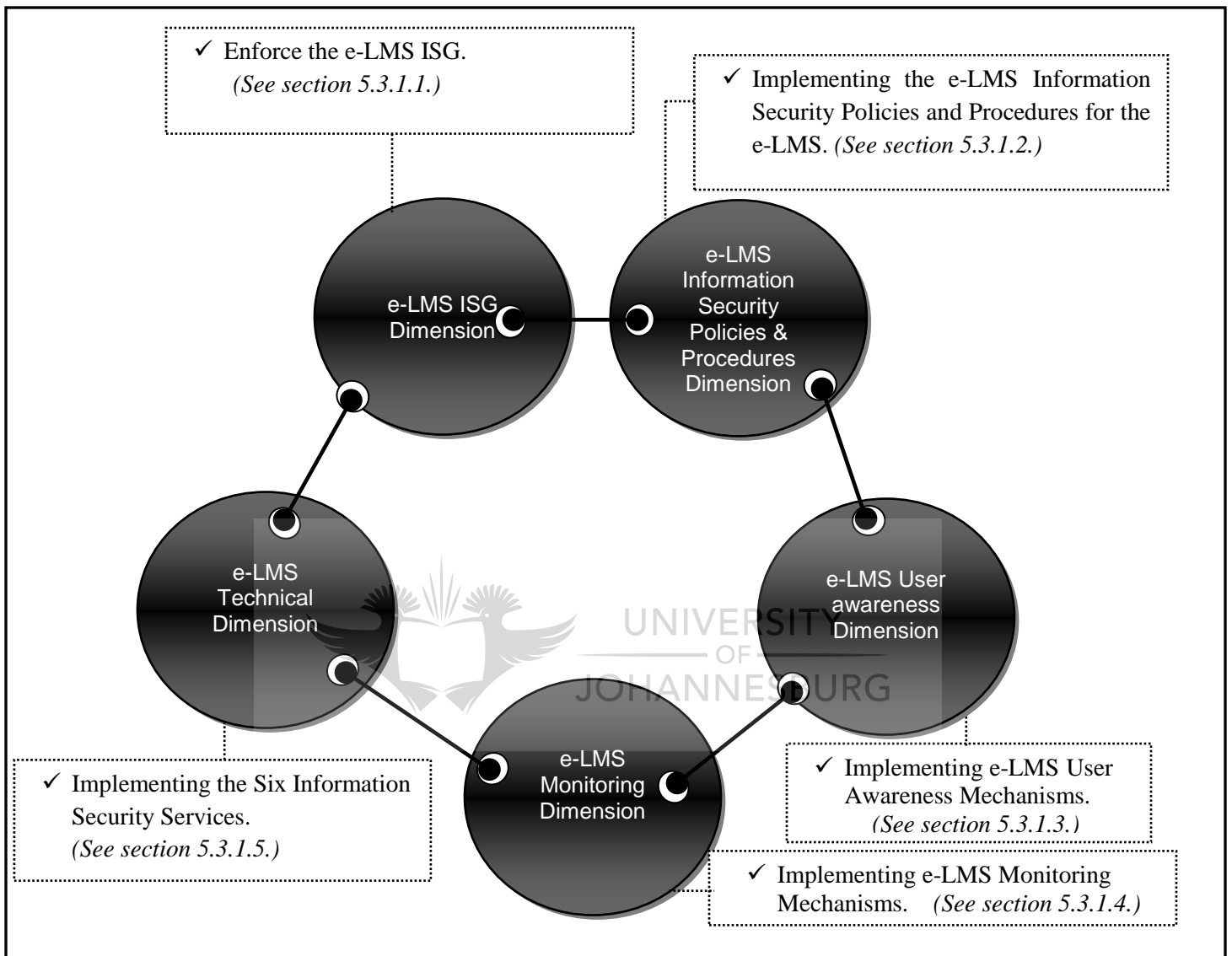
There is no fixed boundary between these dimensions and they should be treated in a coordinated way. The scenario below illustrates how necessary the five information security dimensions are to enforce an effective Identification and Authentication Information Security Service in an e-LMS environment.

- **Scenario:** 'Bob', the system administrator, has decided to use a password based mechanism (i.e. the e-LMS Technical Dimension). To create a strong Identification and Authentication, Bob creates a password policy and procedure that needs to be followed by users during the creation of identity (username/password) as well as utilizing the mechanism (i.e. the e-LMS Policy and Procedure Dimension). Bob decides to create an

information security awareness program so that end users are aware of the information security policies and procedures and act in a way that does not compromise the technical measures (i.e. the e-LMS User Awareness Dimension). Bob wants to make sure that the information security mechanism implemented has served its objectives (i.e. the e-LMS Monitoring Dimension). Bob agrees to ensure the e-LMS Information Security Governance (ISG) is implemented throughout the e-LMS environment.

As noted from the scenario above, to create and maintain a secure e-LMS environment, it is necessary to take all five information security dimensions into account. Each of these five information security dimensions and their respective action(s) that need to be executed are illustrated on Figure 5.1.:





Source: Author's own composition

**Figure 5.1.: The Five Information Security Dimensions for e-LMSs.**

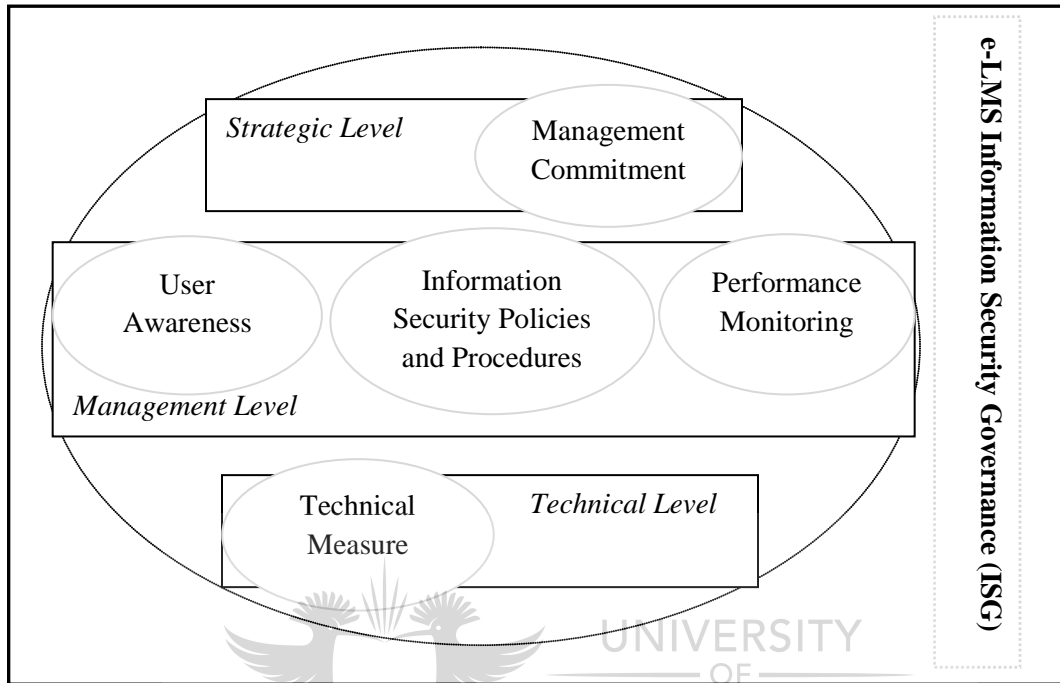
Each dimension depicted in Figure 5.1. has one or more action that needs to be executed.

In the next section, each dimension and its respective actions will be discussed further.

**5.3.1.1. e-LMS INFORMATION SECURITY GOVERNANCE (ISG) DIMENSION**

The ISO 27002 standard for information security management suggests that enforcing an effective ISG is one of the critical elements for the successful implementation and maintenance of information security within systems [28 and 31]. According to [16 and 31], ISG is an information security strategy for the implementation and maintenance of a comprehensive information security program in any IT System. Therefore, some of the basic elements that e-LMS ISG should consist of are discussed below. (See Figure 5.2 for graphical presentation of the e-LMS ISG elements)

1. Management Commitment and Leadership for information security;
2. Information Security Policies and Procedures that guide the e-LMS users;
3. Ensuring the implementation of the technical measures efficiently and effectively;
4. A complete set of user awareness programs for each information security policy in order to ensure that e-LMS users comply with policy; and
5. An effective performance monitoring to ensure compliance of the information security policies and the effectiveness of the technical measures [16 and 31].



**Figure 5.2: Elements of e-LMS ISG [16]**

Figure 5.2. depicts the elements of the e-LMS ISG that need be considered in order to enforce effective ISG for e-LMSs.

### **5.3.1.2. e-LMS INFORMATION SECURITY POLICIES AND PROCEDURES DIMENSION**

Based on ISO 27002, implementing an effective Information Security Policy and Procedure is one of the critical elements for the successful implementation of information security within any system [28]. An e-LMS Information Security Policy and Procedure

Dimension serves as a guideline which deals solely with the policies and procedures that must be in place in order to manage and enforce information security in an e-LMS [35 and 47]. For instance, a password policy provides end users with guidelines to follow during the creation and usage of passwords (i.e. for sample password policies see Appendix B.1.).

### 5.3.1.3. e-LMS USER AWARENESS DIMENSION

According to ISO 27002, an appropriate training on the Information Security Policies and Procedures should be provided for all system users [28 and 50]. The User Awareness Dimension deals with creating an information security awareness program for end users [13 and 47]. Therefore, to create an acceptable level of awareness about the e-LMS information security policies and procedures and users' roles in maintaining the information security objectives of the e-LMS, appropriate training should be provided for all e-LMS users. Having technical information security measures by itself does not fully ensure information security; it is necessary that end users are aware of it and act accordingly in a way that does not compromise the technical measures. For instance, if the e-LMS uses password-based information security mechanisms to implement Identification and Authentication services and the user gives out his/her password intentionally or unintentionally, the whole information security measure is compromised. Therefore, an information security awareness program is vital in controlling and securing the e-LMS environment [13].

#### 5.3.1.4. e-LMS MONITORING DIMENSION

As per the ISO 27002 standard, performance evaluation of the implementation of information security control is suggested to be one of the critical elements for the successful implementation of information security in any system [28]. The major goal of the monitoring dimension is to define a monitoring mechanism that will be used to evaluate the performance of the information security mechanisms adopted and implemented in mitigating and reducing the information security risks to an acceptable level, and also verify compliance to the e-LMS information security Policies and Procedures.

#### 5.3.1.5. e-LMS TECHNICAL DIMENSIONS



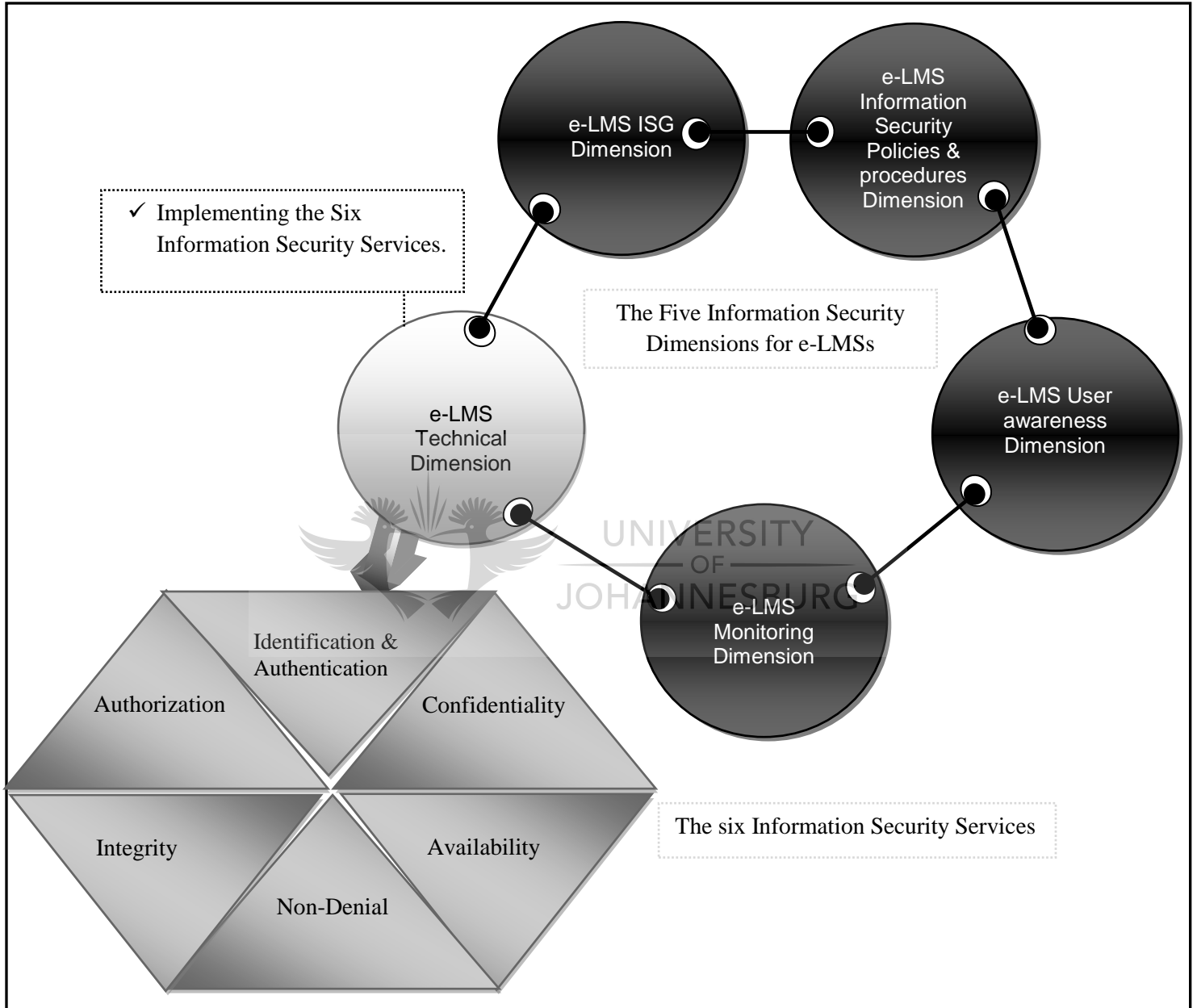
Information security can be defined as the establishment and maintenance of controls and measures aimed at minimizing the risk of loss, disclosure, corruption, and disruption of access of information resources [26]. From this definition, it is clear that the main purpose of information security is to protect and ensure that the confidentiality, integrity and availability of information resources are maintained at all times.

The Technical Dimension deals with the six Information Security Services - Identification and Authentication, Authorization, Confidentiality, Integrity, Non-Denial and Availability - that are necessary to enhance the information security of the e-LMS

environment [16]. The ISO 27002 code of practice for Information Security Management recommends the following controls to enforce the six information security services [28]:

1. Implement a unique secret code for each user and utilize a suitable authentication technique in order to verify the claimed identity of a user: *to enforce Identification and authentication.*
2. Implementation of an appropriate user access management system: *to maintain Authorization and confidentiality.*
3. Implement cryptography control: *to protect confidentiality and integrity.*
4. Implement an effective backup system and business continuity management process: *to maintain integrity and Availability.*
5. Implement a digital signature: *to enforce Non-Denial.*

Figure 5.3. depicts the six Information Security Services in relation to the five Information Security Dimensions identified in section 5.3.1..



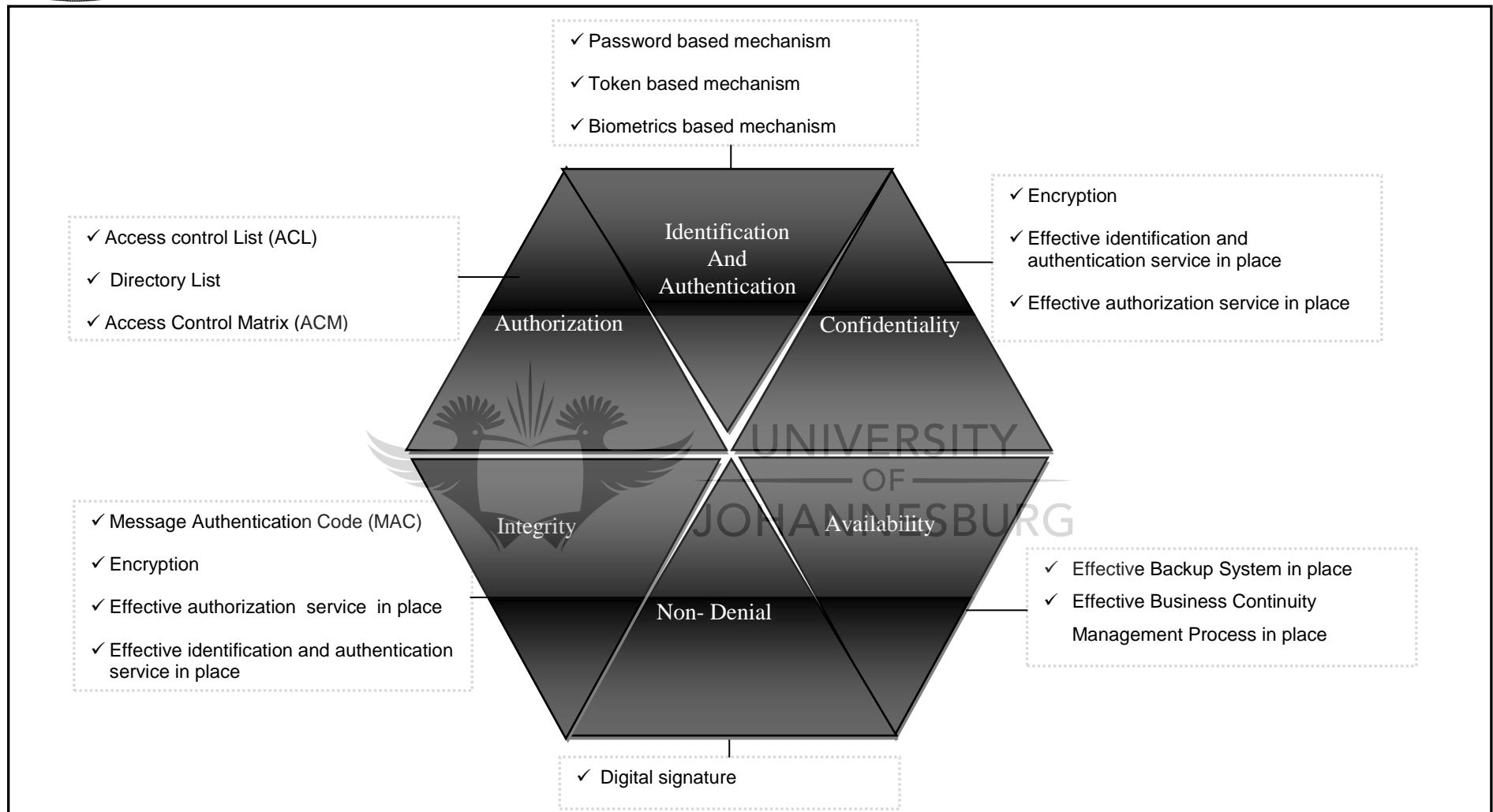
Source: Author's own composition

**Figure 5.3.: The Relationships Between the Six Information Security Services and the Five Information Security Dimensions.**

Each of these six information security services and the information security mechanisms used to enforce the relevant service are depicted in Figure 5.4.. This section deals with the technical dimension of information security and shows how the technical dimension can contribute in achieving the e-LMS security objectives.







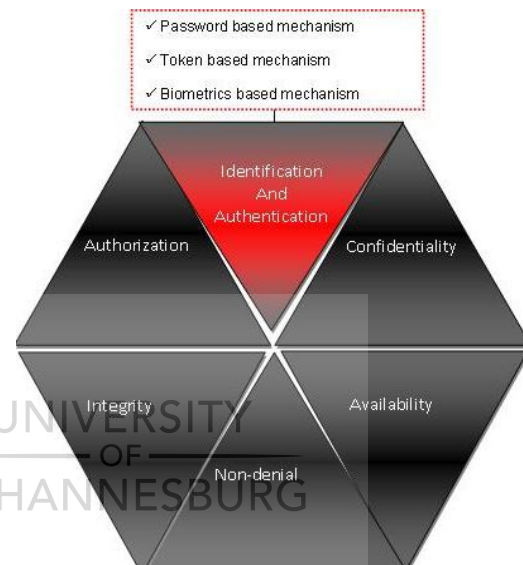
Source: Author's own composition

**Figure 5.4.: The Six Information Security Services and Mechanisms.**

Each of the six information security services, as well as the information security mechanisms that will be used to implement information security services (as shown in Figure 5.4.), will be discussed in detail in the next section of this chapter.

### 5.3.1.5.1. IDENTIFICATION AND AUTHENTICATION

The main purpose of the Identification and Authentication Information Security Service is to allow only authorized (legal) users and prevent unauthorized users from accessing an e-LMS environment. To achieve this main objective, the Identification and Authentication information service follows a two-step process:



- ✓ **Step 1** is the process of identifying the user as a legal user (i.e. Identification); and
- ✓ **Step 2** is the process of ensuring that the identified person (i.e. in Step 1) is really who he/she claims to be (i.e. Authentication).

The Identification and Authentication Service is restricted to registered users, where the user's identity is known by the e-LMS. According to [1 and 3], the Identification and Authentication Information Security Service is implemented by one or a combination of

the following Information Security Mechanisms, which are Password Based, Token Based and Biometrics Based mechanisms.

1. **Password based:** something the user knows such as a user id and password [16].

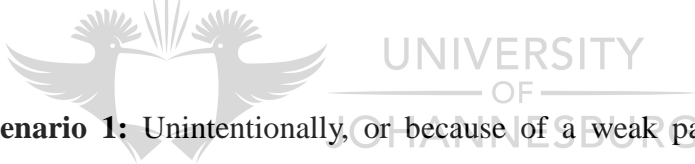
In order to make use of a Password Based Information Security Mechanism, users have to select unique usernames and passwords. The combination of username and password is stored in the e-LMS database, which is used to identify and authenticate users. Therefore, Password based authentication relies on the username and password that the user chooses when he/she signs up. To have an efficient identification and authorization Information Security Service through Password Based mechanisms, it is necessary to take the following into consideration [1 and 30]:

- No Group identity: the e-LMS must force every user to have a unique user identity.
- An e-LMS must log the authentication information, which helps to track users' activities as well as enforce Non-Repudiation/Non-Denial.
- The system must avoid any security hole for anyone to bypass the Identification and Authentication phases.
- The Confidentiality and Integrity of the authentication information should be protected during storage and transmission.

Password based authentication is the most inexpensive and easy to implement, which therefore makes it the obvious choice for most e-LMSs [8]. The question one should then ask is: *Does password based authentication provides adequate security for the most sensitive and integral parts of an e-LMS such as the e-assessment module?*

Password based authentication depends on the secrecy of the password. Since there is no guarantee that the password will be kept safe and secure; the author believes that password based authentication cannot provide adequate security.

Examine the following scenarios:

- 
- **Scenario 1:** Unintentionally, or because of a weak password choice, a learner could give out his/her password to an unauthorised user.
  - **Scenario 2:** Learner ( $L_1$ ) can give his/her password to his/her friend ( $L_2$ ) willingly so that  $L_2$  can write an exam on the behalf of  $L_1$ . In this case, for a system that depends on password based authentication, it is difficult to differentiate the original user (i.e. owner of the password) from the deceiving user (i.e. user who logs in with someone else's password) since both have the correct password. If this issue is not addressed, the overall integrity of the system is compromised.

Some of the possible solutions to mitigate the problem are:

- An e-LMS should implement the password policy and procedures, which the user should follow during the creation and usage of accounts (i.e. user identity and password).
- The e-LMSs should have a functionality that prevents the user from selecting bad passwords.
- Exams should be supervised to ensure that the integrity of the exam is not compromised [36]. However, this solution detracts from the main aim of having an e-LMS, which is to allow anyone to have access to information and do exams regardless of the geographical location.
- Effective implementation of a User Awareness program.



Although password based mechanism is the most widely used mechanism, it has been proven not to be the strongest as users might choose a bad password or pass on their password intentionally. The other two possible authentication mechanisms that could be used to solve this problem are the Token based and Biometrics based Information Security Mechanisms, which will be discussed in the next section.

2. **Token based:** Something the user possesses such as smart cards, memory card, and magnetic cards [16].

The strength of the Token Based Information Security Mechanism depends on keeping the token object, such as the smart card or memory card, away from unauthorized users. If any unauthorized person gets this object, the security of the e-LMS environment is compromised. One of the possible solutions presented by [1] is the use of the Password Based Information Security Mechanism together with Token Based adds one extra security layer. The authors of [3 and 36] also propose that the use of Biometrics Based Information Security Mechanism as the most reliable means of enforcing Identification and Authentication information security service. Biometrics Based Authentication Systems will be discussed in the next section.

3. **Biometrics based:** Something unique to each user such as finger prints, iris scans and voice prints [16].

Biometrics can be defined as unique, measurable physical and/or behavioural characteristics of the person which can be digitised and stored with the user id in the system database and then utilised to verify the identity of the user [1]. Finger prints, iris scans and palm prints are examples of physical characteristics. Some examples of behavioural characteristics are voice prints and signature verification. Unlike Password Based and Token Based Information Security Mechanisms, Biometrics Based Information Security Mechanisms depend on the user's unique

characteristics or attributes (i.e. what the user is) which makes it relatively difficult to tamper with. It is thus the most secure and convenient Identification and Authentication mechanism [1]. Some of the considerations that should be taken into account during the implementation of Biometrics Based Information Security Mechanism are:

- ✓ The Confidentiality and Integrity of user information should be protected during storage and transmission.

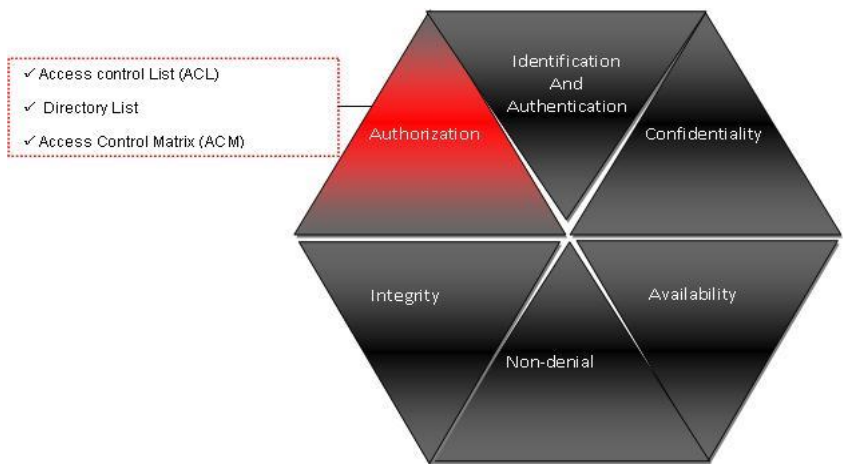
To implement an even stronger Identification and Authentication information security service, the combination any of the above three information security mechanisms could be implemented.



Enforcing Identification and Authentication Information Security Service is the first step towards creating a secure environment. The second step will be enforcing authorization that will be discussed in the next section.

#### 5.3.1.5.2. AUTHORIZATION

The Authorization Information Security Service is also known as Logical Access Control (LAC). Authorization is the



process of determining whether or not an identified individual has been granted access rights to an information resource and determining what type of access is allowed [30]. As noted from this definition the main purpose of the authorization Information Security Service is to ensure that each e-LMS user (i.e. Learners, Lecturers, and Administrator) only access information resources or perform certain action according to their roles and privileges.

Each e-LMS user has different roles, responsibilities and privileges assigned to them. In order to make sure that each user performs according to their roles, responsibilities, and privileges, the following information security mechanisms could be used [16]:

- **An Access Control List (ACL)**
- **A Directory List**
- **An Access control Matrix (ACM)**

UNIVERSITY  
OF  
JOHANNESBURG

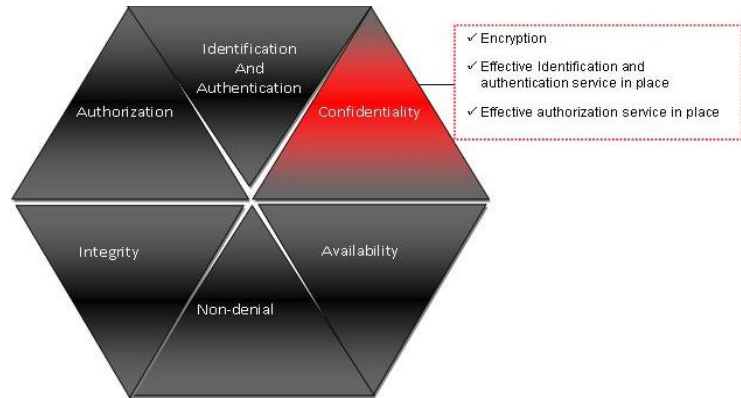
The content of ACLs, directory lists and ACMs should be protected from unauthorized access, modification and fabrication.

The next Information Security Service that will be discussed is the Confidentiality Information Security Service.



### 5.3.1.5.3. CONFIDENTIALITY

The main purpose of the Confidentiality Information Security Service is to protect the content of the information during storage and transmission from unauthorized access and disclosure [1 and 30].



The three mechanisms that could be used to enforce Confidentiality information security services are:

1. **Through effective use of the Identification and Authentication Information Security Service.**

2. **Through effective use of the Authorization Information Security Service.**

3. **Encryption** can be defined as a scrambling mechanism which protects the information from being viewed and altered by unauthorized person [16].

Encryption is the most common information security mechanism used to achieve Confidentiality. To protect the Confidentiality of the information during storage, the person who is sending the message will encrypt the message with a secret encryption key and then send the message to the recipient. The legitimate receiver, possessing the secret decryption key, will be able to decrypt and retrieve the message in the original format. The two types of encryption systems are symmetric (i.e. secret key) and asymmetric (i.e.

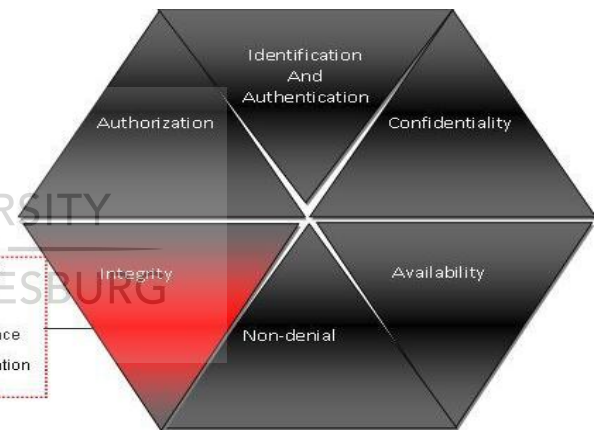
public key) encryption systems. DES and AES are example of symmetric encryption and RSA is an example of asymmetric encryption [41].

The fourth Information Security Service that will be discussed in the next section is Integrity information security service.

#### 5.3.1.5.4. INTEGRITY

The main aim of the Integrity Information Security Service is to protect the content of the information from unauthorized alteration/modification and deletion during storage and transmission [30]. The three

- ✓ Message Authentication Code (MAC)
- ✓ Encryption
- ✓ Effective authorization service in place
- ✓ Effective identification and authentication service in place



mechanisms that could be used to enforce Integrity information security services are:

1. **Through effective use of Identification and Authentication Information Security Service.**
2. **Through effective use of the Authorization Information Security Service.**
3. **A Message Authentication Code (MAC):** A MAC is a mechanism that provides an Integrity check based on a secret key (i.e. will be shared between the sender and intended receiver) and a cryptographic hash function such as MD5 and SHS-1 [5]. It is therefore, the purpose of a MAC to ensure Integrity

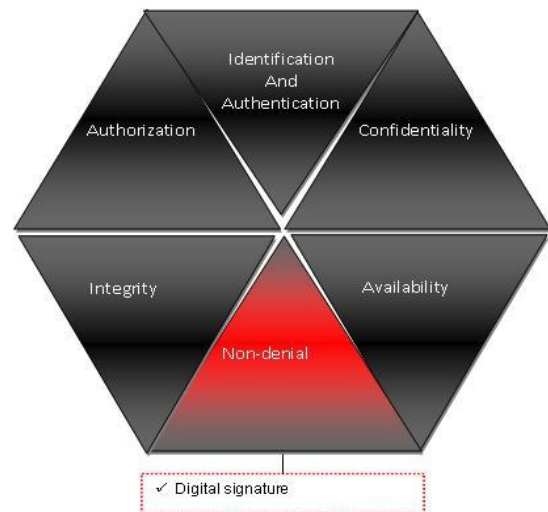
of the message. Cryptographic hash function based on MAC, is known as an HMAC function. How an HMAC function can be used as an Integrity checker is shown below [5]:

- The sender calculates the  $MAC_1$  using an HMAC function which take a message and a shared secret key as input. The output is known as  $MAC_1$ . The sender sends the  $MAC_1$  with the original message to the intended receiver.
- The receiver calculates the  $MAC_2$  using the HMAC function, which takes the received message and shared secret key as input. The HMAC function and the secret key are the same as was used by the sender. Finally, the receiver compares  $MAC_2$  with  $MAC_1$ ; if they match, the Integrity of the message is maintained.

The next Information Security Service that will be discussed is Non-Denial, which ensures the system doesn't open a door for denial of any action.

#### 5.3.1.5.5. NON-DENIAL

The Non-Denial Information Security Service is also known as Non-Repudiation. The main purpose of the Non-Denial Information Security



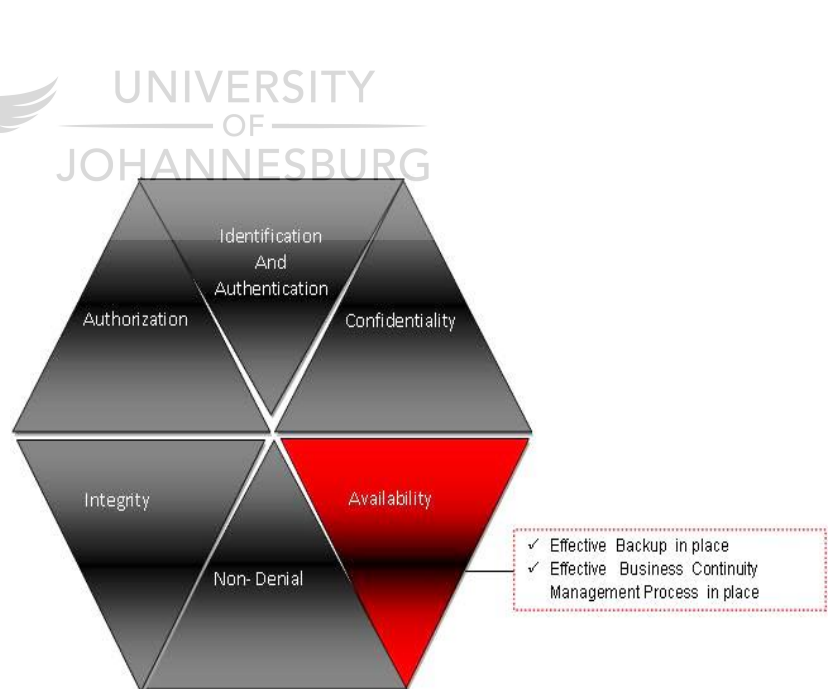
Service is to enforce accountability for the execution of any action on the e-LMS [1]. An information security mechanism that could be used to implement the Non-Denial Information Security Service is:

- **A Digital Signature:** it is an electronic simulation of a paper based signature. A digital signature scheme uses asymmetric (public key) cryptography. The private key is used to create and the public key is used to verify the digital signature [10].

The last Information Security Service that will be discussed in the next section is Availability.

#### 5.3.1.5.6. AVAILABILITY

The main purpose of the Availability Information Security Service is to ensure timely, reliable access to the information resources of the e-LMS [30]. The Availability Information Security Service is one of the most



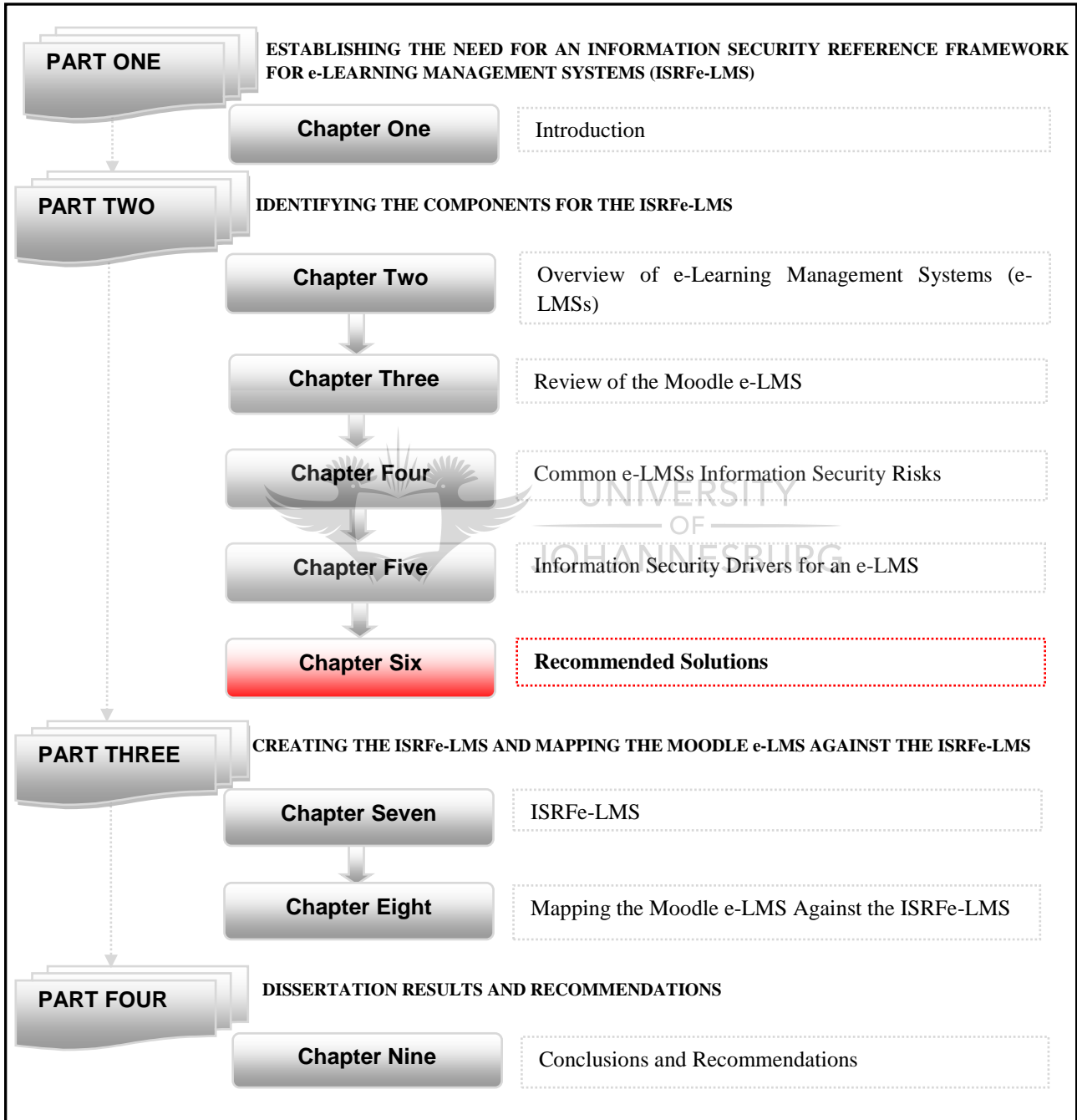
important elements of securing an e-LMS. The e-LMSs have to be available and reliable at all times, especially during online assessments. Thus, the Availability Information Security Service should ensure that the data Integrity is preserved after an interruption of

any means such as power cuts. Through the implementation of effective backup systems and business continuity management process, Availability Information Security Service could be enforced [28].

#### 5.4. CONCLUSION

A web based e-LMS achieves the learning/teaching objectives through different kinds of media such as the Internet, Intranet and Extranet, which are inherently exposed to security risks. This chapter has highlighted that information security should be treated as a multi-dimensional discipline and identified the five most important information security dimensions that should be considered in creating a secure e-LMS environment. Moreover, the chapter stresses the fact that each of the five dimensions is important and it is necessary to take all five dimensions into account to implement and maintain the security of an e-LMS environment.

In the next chapter, of the five information security dimensions, the technical dimension will be discussed with great emphasis on how it plays an important role in creating a secure e-LMS.



## CHAPTER SIX

### RECOMMENDED SOLUTIONS

#### 6.1. PREVIEW

As has been emphasised in the previous chapters, information security should be considered a multi-dimensional discipline. For the purpose of this dissertation, the author identified the five most important dimensions that need to be considered to implement and maintain a secure e-LMS; these dimensions are comprised of both non-technical and technical aspects of information security.

- The non-technical information security dimensions includes:
  - Ensuring Information Security Governance (ISG) for e-LMSs;
  - Developing Information Security Policies and Procedures for e-LMSs;
  - Creating User Awareness for e-LMSs; and
  - Developing Monitoring Mechanisms for e-LMSs.
- The technical information security dimension deals with the identification and implementation of the six Information Security Services. The six Information Services are:
  - Identification and Authentication;
  - Authorization;
  - Confidentiality;

- Integrity;
- Non-Denial; and
- Availability.

The objective of this chapter is to motivate the six Information Security Services as the core information security countermeasures in support of the non-technical information security dimensions. This chapter focuses on mapping the technical dimension against the information security risks identified in section 4.4., guided by the following research question:

*Sub-question 5:*

---

What role should the six Information Security Services, as identified [16], play in the dimensions identified in sub-question 4? (See section 1.5.)

The Confidentiality, Integrity and Availability Information Security Services are often referred as security goals [6]. However, as learned from Chapters Four and Five, the Identification and Authentication, Authorization, and Non-Denial information security services are as important as Confidentiality, Integrity and Availability in securing an e-LMS environment and should also be considered as security goals. The purpose of this chapter is to motivate the need of all six Information Security Services in order to create a secure e-LMS. This is done by mapping the information security risks identified in Chapter Four against the six Information Security Services. To do that, the author will be



using the approach in which an Information Security Service needs to be in place for each activity to ultimately ensure a securely running e-LMS. The author has developed a risk-to-the information security services mapping framework that will be used throughout the coming section. The Risk to the Information Security Services Mapping Framework is depicted in the figure below.

KEYS	
❖ <b>Risk:</b> provides the description of the risk related to a specific activity;	
❖ <b>Reason:</b> provides the cause of the risks by identifying the information security services that have not been enforced;	
❖ <b>Motivation:</b> provides the need for information security countermeasures in place;	
❖ <b>Action:</b> provides the information security countermeasures that need to be in place.	
❖ If the risk is caused from not enforcing a particular information security service(s), this is marked with a 'X'	

Risk	Reason
Identification and Authentication	
Authorization	
Confidentiality	
Integrity	
Non- denial	
Availability	
<b>Motivation</b>	
	<b>Action</b>

*Source: Author's own composition*

**Figure 6.1.: The Risk to the Information Security Services Mapping Framework**

For a more detailed explanation, see the figure below. This provides a detailed example on the Risk to the Information Security Services Mapping Framework.

**EXAMPLE**

**Activity:** Manage his/her profile: for instance, create his/her account, change his/her password or contact details.

If e-LMSs environment does not enforce the six Information Security Services, the following risk may occur:

2. **Risk 1:** An unauthorized person can view, change or/ and delete the profile of the lecturer. The mapping of Risk 1 against the six Information Security Services is depicted below.

<b>Risk 1</b>	An unauthorized person can view, change or/ and delete the profile of the lecturer.	<b>Reason</b>
Identification and Authentication		<b>X</b>
Authorization		<b>X</b>
Confidentiality		<b>X</b>
Integrity		<b>X</b>
Non-Denial		
Availability		<b>X</b>
<b>Motivation</b>	An unauthorized person can only have access to the system and then view, change or/ and delete content of the lecturer's profile if the e-LMS does not have effective Identification and Authentication, Authorization, Confidentiality, Integrity and Availability information security services in place	
Identification and Authentication, Authorization, Confidentiality, Integrity, and Availability information security services need to be enforced.		<b>Action</b>

**Table 6.1.: The Mapping of Risk 1 with the Six Information Security Services.**

*Source: Author's own composition*

**Figure 6.2.: Example of the Risk to the Information Security Services Mapping Framework**

In the next section, by using the Risk to the Information Security Services Mapping Framework, the author will be mapping the information security risks identified in Chapter Four, section 4.4. against the six Information Security Services and the result of the mapping will be used to suggest the possible information security service(s) as countermeasures.

## **6.2. MAPPING OF THE INFORMATION SECURITY RISKS AGAINST THE SIX INFORMATION SECURITY SERVICES**

In this section, the information security risks related to each user (i.e. Learners, Lecturers and Administrator) will be mapped against the six Information Security Services to determine the possible Information Security Service(s) countermeasures. The user is advised to review sections 4.4.1. to 4.4.3. at this stage

### **6.2.1. LECTURERS**

#### **6.2.1.1. Activity:** Manage his/her profile.

One of an e-LMS's functional features is creating accounts, which allows e-LMS users to create, edit/update and delete their account profiles. The profile information consists of personal information such as their name, email address, contact address and description of their roles, and it is the most important to be protected from any unauthorized access.

If e-LMSs environment does not enforce the six Information Security Services, the following risk may occur:

- **Risk 1:** An unauthorized person can view, change or/and delete the profile of the lecturer. The mapping of Risk 1 against the six Information Security Services is depicted below in Table 6.1..

<b>Risk 1</b>	An unauthorized person can view, change or/and delete the profile of the lecturer.	<b>Reason</b>
	Identification and Authentication	<b>X</b>
	Authorization	<b>X</b>
	Confidentiality	<b>X</b>
	Integrity	<b>X</b>
	Non-Denial	
	Availability	<b>X</b>
<b>Motivation</b>	An unauthorized person can only have access to the system and then view, change and/or delete the content of the lecturer's profile if the e-LMS does not have effective Identification and Authentication, Authorization, Confidentiality, Integrity and Availability information security services in place.	
Identification and Authentication, Authorization, Confidentiality, Integrity and Availability information security services need to be enforced.		<b>Action</b>

Table 6.1.: The Mapping of Risk 1 of Activity 6.2.1.1. With the Six Information Security Services

**6.2.1.2. Activity 2:** Create course materials and identify and attach all information to the course: for instance; register information (i.e. dates, pre-requisites), rules and regulation (i.e. drop policies).

**6.2.1.3. Activity 3:** Upload the course material created.

Some of the risks related to activities 2 and 3 are:

- **Risk 1:** Fake course material can be created and uploaded by unauthorized users.

- **Risk 2:** Course material may be viewed an unauthorized person.
- **Risk 3:** Course material may be altered an unauthorized person.
- **Risk 4:** Course material may be deleted by an unauthorized person.

Risk 1	Reason
Fake course material can be uploaded by unauthorized users.	
Identification and Authentication	<b>X</b>
Authorization	<b>X</b>
Confidentiality	
Integrity	
Non-Denial	<b>X</b>
Availability	
<b>Motivation</b>	An unauthorized person can only have access to the system and upload fake course material if the e-LMS does not have effective Identification and Authentication, Authorization and Non-Denial service in place.
Identification and Authentication, Authorization and Non-Denial Information Security Services must be enforced.	<b>Action</b>

Table 6.2.: The Mapping of Risk 1 of Activities 6.2.1.2.and 6.2.1.3. With the Six Information Security Services.

Risks 2, 3 and 4 of Activities 6.2.1.2. and 6.2.1.3 will be combined and mapped against the information security services in Table 6.3..

<b>Risk 2, 3 and 4</b>	Uploaded course material may be viewed, altered or deleted by unauthorized persons.	<b>Reason</b>
	Identification and Authentication	<b>X</b>
	Authorization	<b>X</b>
	Confidentiality	<b>X</b>
	Integrity	<b>X</b>
	Non-Denial	
	Availability	<b>X</b>
<b>Motivation</b>	An unauthorized person can only have access to the system and viewed, altered or deleted uploaded course material if the e-LMS does not have effective Identification and Authentication, Authorization, Confidentiality, Integrity, Availability service in place.	
	Identification and Authentication, Authorization, Confidentiality, Integrity and Availability Information Security Services must be enforced.	<b>Action</b>

Table 6.3.: The Mapping of Risks 2, 3 and 4 of Activities 6.2.1.2. and 6.2.1.3. With the Six Information Security Services.

**6.2.1.4. Activity 4:** Create and upload online assessment materials such as quizzes in the form of true or false, multiple choices, matching and so on.

**6.2.1.5. Activity 5:** Set up and post assignment(s). Some of the risks related to activities 4 and 5 are:

- **Risk 1:** Fake assignments can be uploaded.
- **Risk 2:** The assessment materials set up by the lecturer can be viewed before the due date.
- **Risk 3:** The assessment material can be altered by an authorized person.
- **Risk 4:** The assessment material can be deleted when a student knows that he/she is not ready.

- **Risk 5:** An assignment and/or assessment material could not be available due to technical problems.

<b>Risk 1</b>	Fake assignments can be uploaded	<b>Reason</b>
	Identification and Authentication	<b>X</b>
	Authorization	<b>X</b>
	Confidentiality	
	Integrity	
	Non-Denial	<b>X</b>
	Availability	
<b>Motivation</b>	An unauthorized person can only have access to the system and upload fake course material if the e-LMS does not have effective Identification and Authentication, Authorization and Non-Denial service in place.	
Identification and Authentication, Authorization and Non-Denial information security services must be enforced.		<b>Action</b>

Table 6.4.: The Mapping of Risk 1 of Activities 6.2.1.4. and 6.2.1.5. With the Six Information Security Services.

<b>Risk 2</b>	The assessment materials set up by the lecturer can be viewed before the due date.	<b>Reason</b>
	Identification and Authentication	<b>X</b>
	Authorization	
	Confidentiality	<b>X</b>
	Integrity	
	Non-Denial	
	Availability	
<b>Motivation</b>	An unauthorized person can only have access to the system and view the uploaded assessment materials before due date if the e-LMS does not have effective Identification and Authentication and Confidentiality service in place.	
Identification and Authentication and Confidentiality information security must be enforced.		<b>Action</b>

Table 6.5.: The Mapping of Risk 2 of Activities 6.2.1.4. and 6.2.1.5. With the Six Information Security Services.

Risks 3 and 4 of Activities 6.2.1.4. and 6.2.1.5. will be combined and mapped against the information security services in Table 6.6..

<b>Risks 3 and 4</b>	Uploaded assignments may be altered or deleted by unauthorized persons.	<b>Reason</b>
Identification and Authentication		<b>X</b>
Authorization		
Confidentiality		
Integrity		<b>X</b>
Non-Denial		
Availability		<b>X</b>
<b>Motivation</b>	An unauthorized person can only have access to the system and altered or deleted the uploaded assignment if the e-LMS does not have effective Identification and Authentication, Integrity and Availability service in place.	
Identification and authentication, Integrity and Availability information security must be enforced.		<b>Action</b>

Table 6.6.: The Mapping of Risks 3 and 4 of Activities 6.2.1.4. and 6.2.1.5. with the Six Information Security Services.

<b>Risk 5</b>	An assignment could not be available due to technical problems.	<b>Reason</b>
Identification and Authentication		
Authorization		
Confidentiality		
Integrity		
Non-Denial		
Availability		<b>X</b>
<b>Motivation</b>	The e-LMSs have to be available and reliable at all times, especially online assessments and assignments.	
Availability Information Security Service must be enforced.		<b>Action</b>

Table 6.7.: The Mapping of Risk 5 of Activities 6.2.1.4. and 6.2.1.5. With the Six Information Security Services.



**6.2.1.6. Activity 6:** Set up grading scales.

**6.2.1.7. Activity 7:** Evaluate the assignments submitted by learners and then upload the

results for learners. Some of the risks related to Activities 6.2.1.6. and 6.2.1.7. are:

- **Risk 1:** Fake grading scales can be uploaded by an authorized person;
- **Risk 2:** Fake assessment results can be uploaded;
- **Risk 3:** Assessment results may be viewed by an unauthorized person;
- **Risk 4:** Assessment results may be changed by an authorized person; and
- **Risk 5:** Assessment results may be deleted by an authorized person.

Risks 1 and 2 of Activities 6.2.1.6. and 6.2.1.7. will be combined and mapped against the information security services in Table 6.8..

Risks 1 and 2	Fake assessment grading scale and assessment results can be uploaded.	Reason
Identification and Authentication		<b>X</b>
Authorization		<b>X</b>
Confidentiality		
Integrity		
Non-Denial		<b>X</b>
Availability		
<b>Motivation</b>	An unauthorized person can only have access to the system and upload fake Grading scale if the e-LMS does not have effective Identification and Authentication, Authorization and Non-Denial service in place.	
Identification and Authentication, Authorization and Non-Denial information security services must be enforced.		<b>Action</b>

Table 6.8.: The Mapping of Risks 1 and 2 of Activities 6.2.1.6. and 6.2.1.7. With the Six Information Security Services.

Risks 3, 4 and 5 of Activities 6.2.1.6. and 6.2.1.7. will be combined and mapped against the information security services in Table 6.9..

<b>Risks 3,4 and 5</b>	Unauthorized persons may view, change and/or delete assessment results posted by a lecturer.	<b>Reason</b>
Identification and Authentication		<b>X</b>
Authorization		<b>X</b>
Confidentiality		<b>X</b>
Integrity		<b>X</b>
Non-Denial		
Availability		<b>X</b>
<b>Motivation</b>	An unauthorized person can only have access to the system and view, alter and/or delete posted assessment results if the e-LMS does not have effective Identification and Authentication, Authorization, Confidentiality, Integrity and Availability service in place.	
Identification and Authentication, Authorization, Confidentiality, Integrity and Availability Information Security Services must be enforced.		<b>Action</b>

Table 6.9.: The Mapping of Risks 3, 4 and 5 of Activities 6.2.1.6. and 6.2.1.7. With the Six Information Security Services.

**6.2.1.8. Activity 8:** Use communication means such as synchronous (i.e. chat) and asynchronous (i.e. forums) communication media to keep in touch with their learners and subordinates. Some of the risks related to this activity are:

- **Risk 1:** An unauthorized person may act as a legitimate lecturer during discussion.
- **Risk 2:** The email/chat messages could be viewed/ altered by unauthorized person.

<b>Risk 1</b>	Unauthorized persons may act as a legitimate lecturer during discussion	<b>Reason</b>
	Identification and Authentication	X
	Authorization	X
	Confidentiality	
	Integrity	
	Non-Denial	X
	Availability	
<b>Motivation</b>	An unauthorized person can only have access to the system and act as legitimate lecturer if the e-LMS does not have effective Identification and Authentication, Authorization and Non-Denial service in place.	
	Identification and Authentication, Authorization and Non-Denial Information Security Services must be enforced.	<b>Action</b>

Table 6.10.: The Mapping of Risk 1 of Activity 6.2.1.8. With the Six Information Security Services.

<b>Risk 2</b>	The email/chat messages could be viewed/alterd by unauthorized persons.	<b>Reason</b>
	Identification and Authentication	X
	Authorization	X
	Confidentiality	X
	Integrity	X
	Non-Denial	
	Availability	X
<b>Motivation</b>	An unauthorized person can only have access to the system and view, alter and/or delete email/chat messages if the e-LMS does not have effective Identification and Authentication, Authorization, Confidentiality, Integrity and Availability service in place.	
	Identification and Authentication, Authorization, Confidentiality, Integrity and Availability Information Security Services must be enforced.	<b>Action</b>

Table 6.11.: The Mapping of Risk 2 of Activity 6.2.1.8. With the Six Information Security Services.

**6.2.1.9. Activity 9:** Register and/or deregister learners for a course based on a learner's request.

In e-LMS, the lecturer is responsible for the confirmation of the registration and deregistration based on the learner's request. If e-LMSs environment doesn't enforce the six Information Security Services, the following risks may occur:

- **Risk 1:** Learners could deny requesting their intent to register and/or deregister to a course when they change their mind.
- **Risk 2:** An unauthorized person can act as a legitimate learner and request for registration and deregistration.

<b>Risk 1</b>	Learners could deny requesting their intent to register for a course when they change their mind.	<b>Reason</b>
	Identification and Authentication	
	Authorization	
	Confidentiality	
	Integrity	
	Non-Denial	<b>X</b>
	Availability	<b>X</b>
<b>Motivation</b>	A learner can only deny the action carried out by him/her if the e-LMS does not have effective Non-Denial and Availability Information Security Services in place.	
	Non-Denial and Availability Information Security Services need to be enforced.	<b>Action</b>

Table 6.12.: The Mapping of Risk 1 of Activity 6.2.1.9. With the Six Information Security Services.

<b>Risk 2</b>	An unauthorized person can act as legitimate learner and request for registration and deregistration.	<b>Reason</b>
	Identification and Authentication	X
	Authorization	X
	Confidentiality	
	Integrity	
	Non-Denial	
	Availability	X
<b>Motivation</b>	An unauthorized person can only have access to the system and act as legitimate learner if the e-LMS does not have effective Identification and Authentication, Authorization and Availability Information Security Service in place.	
	Identification and Authentication, Authorization and Availability Information Security Services must be enforced.	<b>Action</b>

Table 6.13.: The Mapping of Risk 2 of Activity 6.2.1.9 With the Six Information Security Services.

## 6.2.2. LEARNERS

### 6.2.2.1. Activity: Manage his/her profile.

If the e-LMSs environment does not enforce the six Information Security Services, the following risk may occur:

- **Risk 1:** An unauthorized person can view, change and/or delete the profile of the lecturer. The mapping of Risk 1 against the six Information Security Services is depicted below in Table 6.14..

<b>Risk 1</b>	An unauthorized person can view, change and/or delete the profile of a learner.	<b>Reason</b>
	Identification and Authentication	X
	Authorization	X
	Confidentiality	X
	Integrity	X
	Non-Denial	
	Availability	X
<b>Motivation</b>	An unauthorized person can only have access to the system and then view, change and/or delete the content of a learner's profile if the e-LMS does not have effective Identification and Authentication, Authorization, Confidentiality, Integrity and Availability information security services in place	
	Identification and Authentication, Authorization, Confidentiality, Integrity and Availability Information Security Services need to be enforced.	<b>Action</b>

Table 6.14.: The Mapping of the Risk 1 of Activity 6.2.2.1. With the Six Information Security Services

**6.2.2.2. Activity:** Access course materials. Some of the risks related to this activity is:

- **Risk 1:** Someone can access course material by pretending to be the learner.
- **Risk 2:** The course material may not be available due to technical problems. e-LMS users should have access to the course material at all times during the period for which that student is eligible.

<b>Risk 1</b>	Someone can access course material by pretending to be a learner.	<b>Reason</b>
	Identification and Authentication	X
	Authorization	X
	Confidentiality	X
	Integrity	
	Non-Denial	
	Availability	
<b>Motivation</b>	An unauthorized person can only have access to the system and access the course materials as legitimate learner if the e-LMS does not have effective Identification and Authentication, Authorization and Confidentiality service in place.	
Identification and Authentication, Authorization, Confidentiality Information Security Services need to be enforced.		<b>Action</b>

Table 6.15.: The Mapping of Risk 1 of Activity 6.2.2.2. With the Six Information Security Services

<b>Risk 2</b>	The course material may not be available due to technical problems.	<b>Reason</b>
	Identification and Authentication	
	Authorization	
	Confidentiality	
	Integrity	
	Non-Denial	
	Availability	X
<b>Motivation</b>	The e-LMSs have to be available and reliable at all times, regardless of interruption that may occur.	
Availability Information Security Services must be enforced.		<b>Action</b>

Table 6.16.: The Mapping of Risk 2 of Activity 6.2.2.2. With the Six Information Security Services

**6.2.2.3. Activity:** Take online assessment exams or quizzes that are set by the lecturer.

Some of the risks related to this activity are:

- **Risk 1:** The learner can pass his/her personal Identification and Authentication information to his/her friend so that the friend can write the exam on his/her behalf.
- **Risk 2:** One learner's answers may be copied or changed by fellow learners.
- **Risk 3:** Learners may deny writing the exam when they figure out they are failing.
- **Risk 4:** When a learner finds out he/she cannot pass the test, he/she can create a Denial of Service attack (DOS) to sabotage the exam.
- **Risk 5:** The online assessment may break down due to the technical problems.
- **Risk 6:** Cheating during exams, which includes getting unauthorized help from someone, through the use of a synchronous and asynchronous collaboration tool during exam [36].



<b>Risk 1</b>	The learner can pass his/her personal Identification and Authentication information to a friend so that the friend can write the exam on his/her behalf.	<b>Reason</b>
	Identification and Authentication	<b>X</b>
	Authorization	
	Confidentiality	
	Integrity	
	Non-Denial	
	Availability	
<b>Motivation</b>	The e-LMSs have to implement a strong Identification and Authentication mechanism(s) (i.e. Biometrics based, Token based or the combination of the two) to avoid dishonesty.	
	Identification and Authentication Information Security Service must be enforced.	<b>Action</b>

Table 6.17.: The Mapping of Risk 1 of Activity 6.2.2.3. With the Six Information Security Services

<b>Risk 2</b>	One learner's answers may be copied or altered by fellow learners.	<b>Reason</b>
	Identification and Authentication	
	Authorization	<b>X</b>
	Confidentiality	<b>X</b>
	Integrity	<b>X</b>
	Non-Denial	
	Availability	<b>X</b>
<b>Motivation</b>	For a learner to be able to copy or change his/her fellow learners' assessment answer(s) if the e-LMS does not have effective Authorization, Confidentiality, Integrity and Availability Information Security Services in place.	
	Authorization, Confidentiality, Integrity and Availability Information Security Services must be enforced.	<b>Action</b>

Table 6.18.: The Mapping of Risk 2 of Activity 6.2.2.3. With the Six Information Security Services

<b>Risk 3</b>	Learners may deny writing the exam when they figure out they are failing.	<b>Reason</b>
	Identification and Authentication	
	Authorization	
	Confidentiality	
	Integrity	
	Non-Denial	<b>X</b>
	Availability	
<b>Motivation</b>	A learner can only deny the action carried out by him/ her if the e-LMS does not have effective Non-Denial service in place.	
Non-Denial Information Security Service must be enforced.		<b>Action</b>

Table 6.19.: The Mapping of Risk 3 of Activity 6.2.2.3. With the Six Information Security Services

<b>Risks 4 and 5</b>	The online assessment may break down due to the technical problems caused naturally or deliberately.	<b>Reason</b>
	Identification and Authentication	
	Authorization	
	Confidentiality	
	Integrity	
	Non-Denial	
	Availability	<b>X</b>
<b>Motivation</b>	The e-LMSs have to be available and reliable at all times, regardless of interruption that may occur.	
Availability information security services must be enforced.		<b>Action</b>

Table 6.20.: The Mapping of Risks 4 and 5 of Activity 6.2.2.3. With the Six Information Security Services

<b>Risk 6</b>	Cheating during exams, which include getting unauthorized help from someone, through the use of a synchronous and asynchronous collaboration tool during exam [36].	<b>Reason</b>
	Identification and Authentication	X
	Authorization	X
	Confidentiality	
	Integrity	
	Non-Denial	X
	Availability	
<b>Motivation</b>	During online assessments, the e-LMS should be able to block all the other e-LMS's functional features to could open door for dishonesty.	
	Identification and Authentication, Authorization and Non-Denial Information Security Services must be enforced.	<b>Action</b>

Table 6.21.: The Mapping of Risk 6 of Activity 6.2.2.3, With the Six Information Security Services

**6.2.2.4. Activity:** Complete posted assignments offline and submit it online for feedback.

If the e-LMS's environment does not enforce the six Information Security Services, the following risks may occur:

- **Risk 1:** Someone can submit a fake assignment pretending to be the learner.
- **Risk 2:** The student can deny submitting the assignment when he/she figures out that he/she won't pass.
- **Risk 3:** Submitted assignments can be viewed, copied, changed or deleted.

<b>Risk 1</b>	Someone can submit a fake assignment pretending to be the learner.	<b>Reason</b>
	Identification and Authentication	<b>X</b>
	Authorization	<b>X</b>
	Confidentiality	
	Integrity	
	Non-Denial	<b>X</b>
	Availability	
<b>Motivation</b>	An unauthorized person can only have access to the system and post a fake assessment if the e-LMS does not have effective Identification and Authentication, Authorization and Non-Denial service in place.	
Identification and Authentication, Authorization and Non-Denial Information Security Services must be enforced.		<b>Action</b>

Table 6.22.: The Mapping of Risk 1 of Activity 6.2.2.4. With Risk to the Information Security Services

<b>Risk 2</b>	The student can deny submitting the assignment when he/she figures out that he/she will not pass.	<b>Reason</b>
	Identification and Authentication	
	Authorization	
	Confidentiality	
	Integrity	
	Non-Denial	<b>X</b>
	Availability	
<b>Motivation</b>	A learner can only deny the action carried out by him/ her if the e-LMS does not have effective Non-Denial service in place.	
Non-Denial Information Security Service must be enforced.		<b>Action</b>

Table 6.23.: The Mapping of the Risk 2 of Activity 6.2.2.4. With Risk to the Information Security Services

Risk3	Submitted assignments can be viewed, copied, changed or deleted.	Reason
Identification and Authentication		<b>X</b>
Authorization		<b>X</b>
Confidentiality		<b>X</b>
Integrity		<b>X</b>
Non-Denial		
Availability		<b>X</b>
<b>Motivation</b>	An unauthorized person can only have access to the system and view, alter or delete submitted assignments if the e-LMS does not have effective Identification and Authentication, Authorization, Confidentiality, Integrity and Availability Information Security Service in place.	
Identification and Authentication, Authorization, Confidentiality, Integrity and Availability Information Security Services must be enforced.	<b>Action</b>	

Table 6.24.: The Mapping of Risk 3 of Activity 6.2.2.4. With the Six Information Security Services

#### 6.2.2.5. Activity: Access their assessment result.

If the e-LMS's environment does not enforce the six Information Security Services, the following risks may occur:

Authorization and Confidentiality information security services must be enforced. Action

- **Risk 1:** Grade results may also be viewed, altered and/or deleted by unauthorized persons.

Risk 1	Grade results may also be viewed, altered and/or deleted by unauthorized persons.	Reason
Identification and Authentication		X
Authorization		X
Confidentiality		X
Integrity		X
Non-Denial		
Availability		X
<b>Motivation</b>	An unauthorized person can only have access to the system and view, alter or delete grade result if the e-LMS does not have effective Identification and Authentication, Authorization, Confidentiality, Integrity and Availability Information Security Services in place.	
Identification and Authentication, Authorization, Confidentiality, Integrity and Availability Information Security Services must be enforced.		<b>Action</b>

Table 6.25.: The Mapping of Risk 1 of Activity 6.2.2.5. With Risk to the Information Security Services



**6.2.2.6. Activity:** Use communication means such as synchronous (i.e. chat) and asynchronous (i.e. forums) communication media to keep in touch with their lecturers and fellow classmates.

- **Risk 1:** An unauthorized person may act as a legitimate lecturer during discussions.
- **Risk 2:** The email/chat messages could be viewed/alterd by unauthorized persons.

<b>Risk 1</b>	Unauthorized persons may act as a legitimate learner during discussions.	<b>Reason</b>
	Identification and Authentication	X
	Authorization	X
	Confidentiality	
	Integrity	
	Non-Denial	X
	Availability	
<b>Motivation</b>	An unauthorized person can only have access to the system and act as legitimate learner if the e-LMS does not have effective Identification and Authentication, Authorization and Non-Denial service in place.	
	Identification and Authentication, Authorization and Non-Denial Information Security Services must be enforced.	<b>Action</b>

Table 6.26.: The Mapping of Risk 1 of Activity 6.2.2.6. With the Six Information Security Services

<b>Risk 2</b>	The email/chat messages could be viewed/alterd by unauthorized persons.	<b>Reason</b>
	Identification and Authentication	X
	Authorization	X
	Confidentiality	X
	Integrity	X
	Non-Denial	
	Availability	X
<b>Motivation</b>	An unauthorized person can only have access to the system and view, alter and/or delete email/chat messages if the e-LMS does not have effective Identification and Authentication, Authorization, Confidentiality, Integrity and Availability Information Security Services in place.	
	Identification and Authentication, Authorization, Confidentiality, Integrity and Availability Information Security Services must be enforced.	<b>Action</b>

Table 6.27.: The Mapping of Risk 2 of Activity 6.2.2.6. With Risk to the Information Security Services

**6.2.3 ADMINISTRATOR**

**6.2.3.1. Activity:** Manage their profiles: for instance create an account, change a password or contact details. One risk related to this activity is:

- **Risk 1:** An unauthorized person may alter/delete the profile of the administrator.

Risk 1	An unauthorized person can view, change and/or delete the profile of the lecturer.	Reason
	Identification and Authentication	X
	Authorization	X
	Confidentiality	X
	Integrity	X
	Non-Denial	
	Availability	X
Motivation	An unauthorized person can only have access to the system and change content of the administrator's profile only If the e-LMS does not have effective Identification and Authentication, Authorization, Confidentiality, Integrity and Availability Information Security Services in place.	
Identification and Authentication, Authorization, Confidentiality, Integrity and Availability Information Security Services need to be enforced.		Action

Table 6.28.: The Mapping of Risk 1 of Activity 6.2.3.1. With the Six Information Security Services

**6.2.3.2. Activity:** Set up roles and privileges.

**6.2.3.3. Activity:** Assign roles and privileges to learners and lecturers.

One of the administrator's roles is to define the user's roles and assign privileges accordingly. This access control information should not be edited by anyone other than the administrator.

If the e-LMS's environment does not enforce the six Information Security Services, some of the risks related to activities 6.2.3.2. and 6.2.3.3. are:



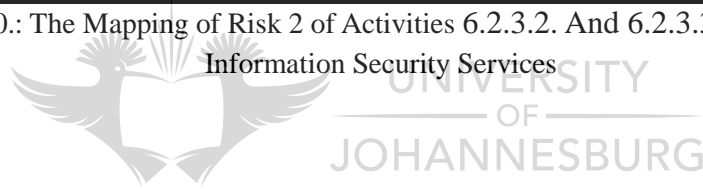
- **Risk 1:** Fake roles and privileges could be set by an unauthorized user.
- **Risk 2:** The roles and privileges could be altered by an unauthorized user.

Risk 1	Reason
Fake roles and privileges could be set up by unauthorized person.	
Identification and Authentication	<b>X</b>
Authorization	<b>X</b>
Confidentiality	
Integrity	
Non-Denial	<b>X</b>
Availability	
<b>Motivation</b>	An unauthorized person can only have access to the system and upload Fake role and privileges if the e-LMS does not have effective Identification and Authentication, Authorization, and Non-Denial service in place.
Identification and Authentication, Authorization and Non-Denial Information Security Services must be enforced.	<b>Action</b>

Table 6.29.: The Mapping of Risk 1 of Activity 6.2.3.2. and 6.2.3.3. With the Six Information Security Services

<b>Risk 2</b>	The roles and privileges information of users may also be altered by unauthorized persons.	<b>Reason</b>
Identification and Authentication		<b>X</b>
Authorization		<b>X</b>
Confidentiality		<b>X</b>
Integrity		<b>X</b>
Non-Denial		
Availability		<b>X</b>
<b>Motivation</b>	An unauthorized person can only have access to the system and change content of the roles and privileges information if the e-LMS does not have effective Identification and Authentication, Authorization, Confidentiality, Integrity and Availability Information Security service in place.	
Identification and Authentication, Authorization, Confidentiality, Integrity and Availability Information Security Services must be enforced.		<b>Action</b>

Table 6.30.: The Mapping of Risk 2 of Activities 6.2.3.2. And 6.2.3.3. With the Six Information Security Services



**6.2.3.4. Activity:** Assign lecturers to a course(s). One of the risks related to this activity is:

- **Risk 1:** An unauthorized person may act as a legitimate administrator and assign lecturers to a course.

<b>Risk 1</b>	An authorized person can act as a legitimate administrator and assign lecturers to a course.	<b>Reason</b>
Identification and Authentication		<b>X</b>
Authorization		<b>X</b>
Confidentiality		
Integrity		
Non-Denial		<b>X</b>
Availability		
<b>Motivation</b>	An unauthorized person can only have access to the system and act as legitimate Administrator if the e-LMS does not have effective Identification and Authentication, Authorization and Non-Denial service in place.	
Identification and Authentication, Authorization and Non-Denial Information Security Services must be enforced.		<b>Action</b>

Table 6.31.: The Mapping of Risk 1 of Activity 6.2.3.4. With the Six Information Security Services

### 6.3. CONCLUSION



UNIVERSITY  
OF  
JOHANNESBURG

This chapter focused on how the technical dimension could be used as information security countermeasures for the information security risks identified in Chapter Four with the support of the four non-technical dimensions of information security. A Risk to the Information Security Services Mapping Framework has been used throughout the chapter to motivate how important all of the information security services are in creating a secure e-LMS environment. This chapter concluded that, despite the growth in popularity of the e-LMS, it has been witnessed that e-LMSs are exposed to various information security vulnerabilities and all the six Information Security Services need to be taken in to account in creating a secure e-LMS. In the next chapter the ISRF-e-LMS will be created

as a possible information security countermeasure for e-LMSs information security vulnerabilities.



Part Two consists of Chapters Two to Six; all of the chapters are interrelated with unique deliverables. Chapter Two provides insight into the concepts and terminology of e-LMSs in general and background information; Chapter Three focuses on the Moodle e-LMS, which will be mapped against ISRFe-LMS in Chapter Eight. Based on the previous two chapters, Chapter Four summarizes the most generic information security vulnerabilities facing e-LMSs from each user's perspective. In order to provide information security countermeasures, it is first necessary to determine which of the information security dimensions are necessary for the security of an e-LMSs environment. Chapter Five identifies the five most important information security dimensions that should be considered in creating a secure e-LMS environment. Chapter Six highlights how the six Information Security Services could be used as information security countermeasures in order to mitigate the information security risks (i.e. as identified in Chapter Four).

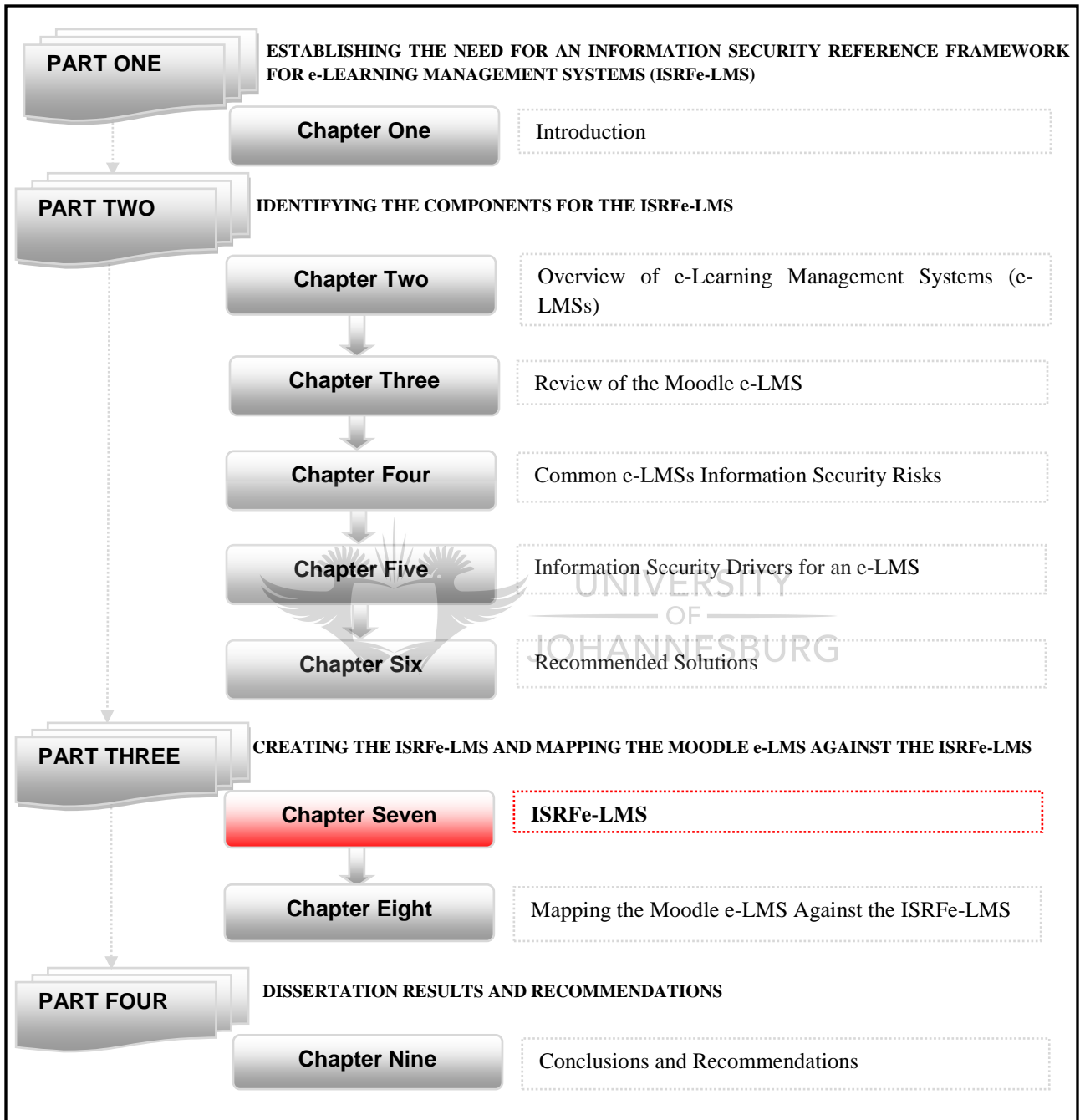
All of the results from Part Two will be considered in determining components of the information security reference framework for e-Learning Management Systems (ISRFe-LMS) that will be created and discussed in the next part of the dissertation.

Part Three consists of Chapters Seven and Eight, which will be briefly reviewed as follows:

Chapter Seven provides a description of the ISRFe-LMS. This chapter is actually the culmination of all of the work in this dissertation.

Chapter Eight provides the actual mapping of Moodle e-LMS against the ISRFe-LMS.





## CHAPTER SEVEN

# AN INFORMATION SECURITY REFERENCE FRAMEWORK FOR e-LEARNING MANAGEMENT SYSTEMS (ISRFe-LMS)

### 7.1. PREVIEW

The deliverables of Part Two were:

- The basic functional features expected from e-LMSs have been identified (*Chapter Two*).
- The Moodle e-LMS was investigated (*Chapter Three*).
- The main Information Security Risks related to the e-LMS users' activities were identified (*Chapter Four*).
- The five Information Security Dimensions that should be considered in securing an e-LMS were identified and discussed (*Chapter Five*).
- A summary of the six Information Security Services for e-LMSs were provided (*Chapter Six*).

Part Two formed the necessary information security requirements that should be included in an information security reference framework for e-LMSs.



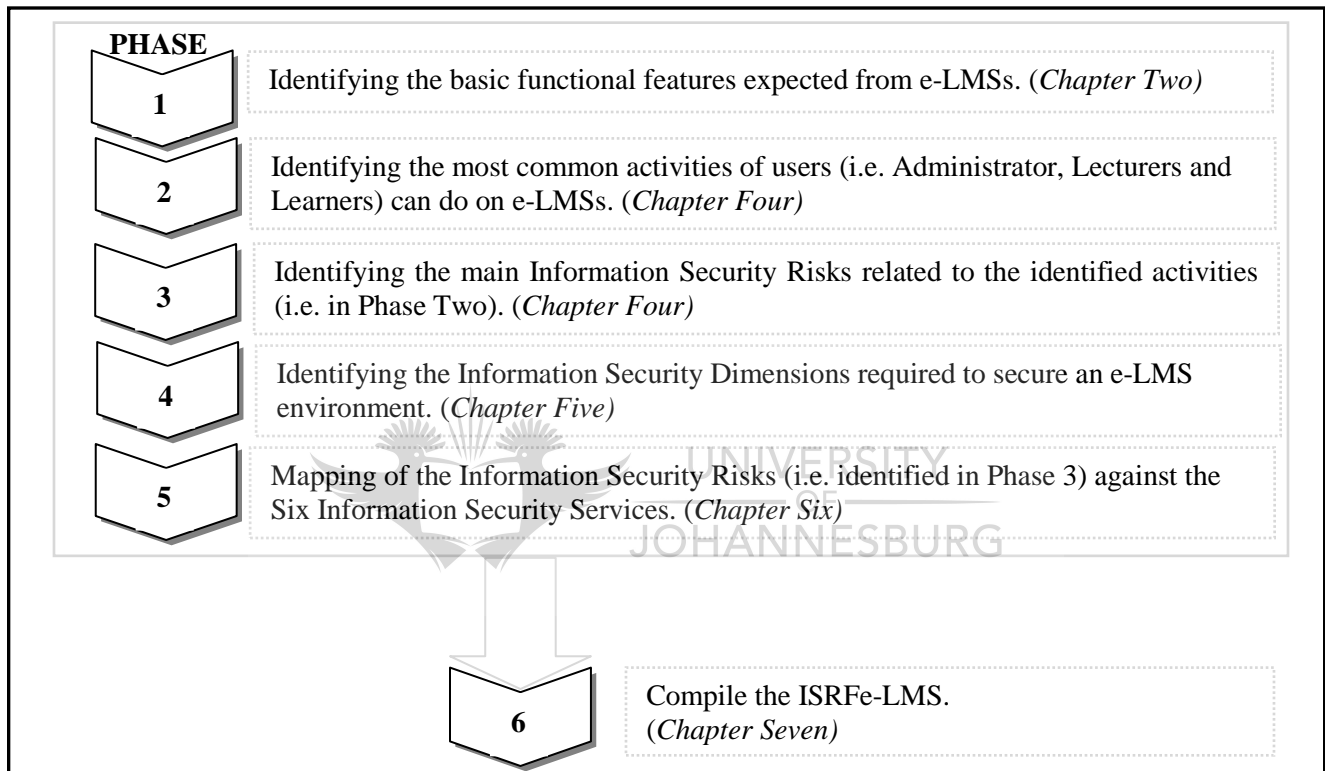
The objective of this dissertation is to secure an e-LMS through the creation of an Information Security Reference Framework, namely the Information Security Reference Framework for e-Learning Management Systems (ISRFe-LMS). All the deliverables from Part Two will be consolidated to determine the components of the ISRFe-LMS. The purpose of this chapter is to provide a brief description of the ISRFe-LMS that was created as part of this dissertation.

## 7.2. BACKGROUND

As highlighted by [3], having Web and Operating System (OS) Security alone in place does not automatically make the e-LMS environment secure. However, they are important requirements of the ISRFe-LMS. As explained by [3], web security deals with securing the server running the web applications. Hardware and software firewalls are some of the examples of the web security mechanisms. Microsoft Windows, Solaris and Linux are some of the most commonly used OSs. The OS security deals with securing the system software. Web and OS security are beyond this dissertation and will not be covered.

### 7.2.1. THE DEVELOPMENT PHASES OF THE ISRFe-LMS

The author followed six phases to develop the ISRFeLMS. These development phases are depicted as follows.



*Source: Author's own composition*

**Figure 7.1.: The Development Phases of the ISRFe-LMS**

The high level description of the ISRFe-LMS's components as well as how each of the components play an important role in creating a secure e-LMS will be examined in the next section.

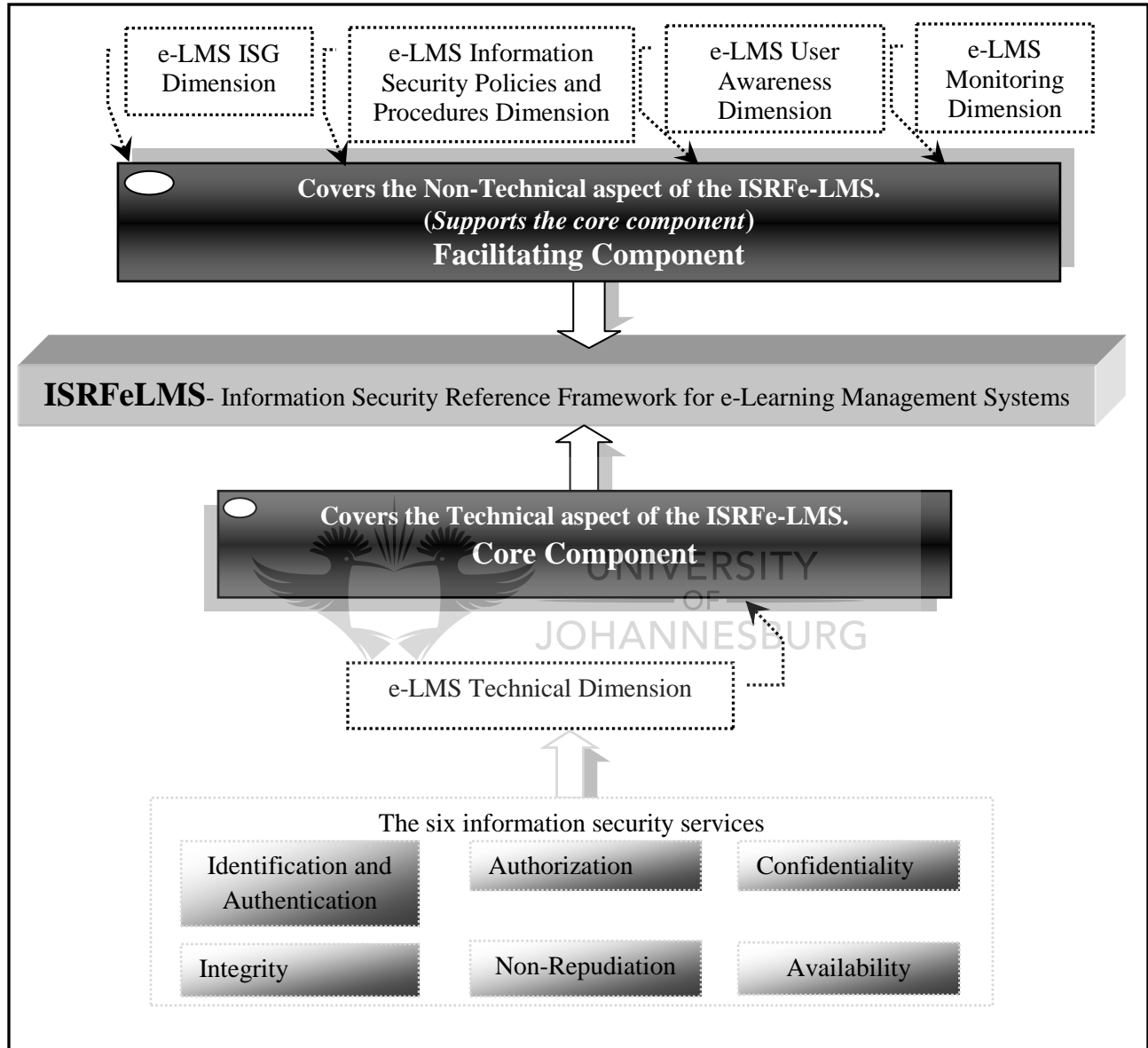
### 7.3. ISRFe-LMS

The ISRFe-LMS is made up of two components, the core and facilitating components, each covering a different aspect of Information Security.

The core component covers the technical Information Security aspects of the ISRFe-LMS. The Core component actually deals with the implementation of the six Information Security Services: Identification and Authentication, Authorization, Confidentiality, Integrity, Non-Denial and Availability.

The facilitating component supports the core component. The facilitating component comprises of four non-technical Information Security dimensions, namely: the e-LMS Information Security Governance (ISG) dimension, the e-LMS Information Security Policies and Procedures Dimension, the e-LMS User Awareness Dimension and the e-LMS Monitoring Dimension.

The facilitating and core components go hand-in-hand; without one another, they cannot achieve the objective of the ISRFe-LMS. The graphical representation of the ISRFe-LMS information security reference framework is depicted in the Figure 7.2..



Source: Author's own composition

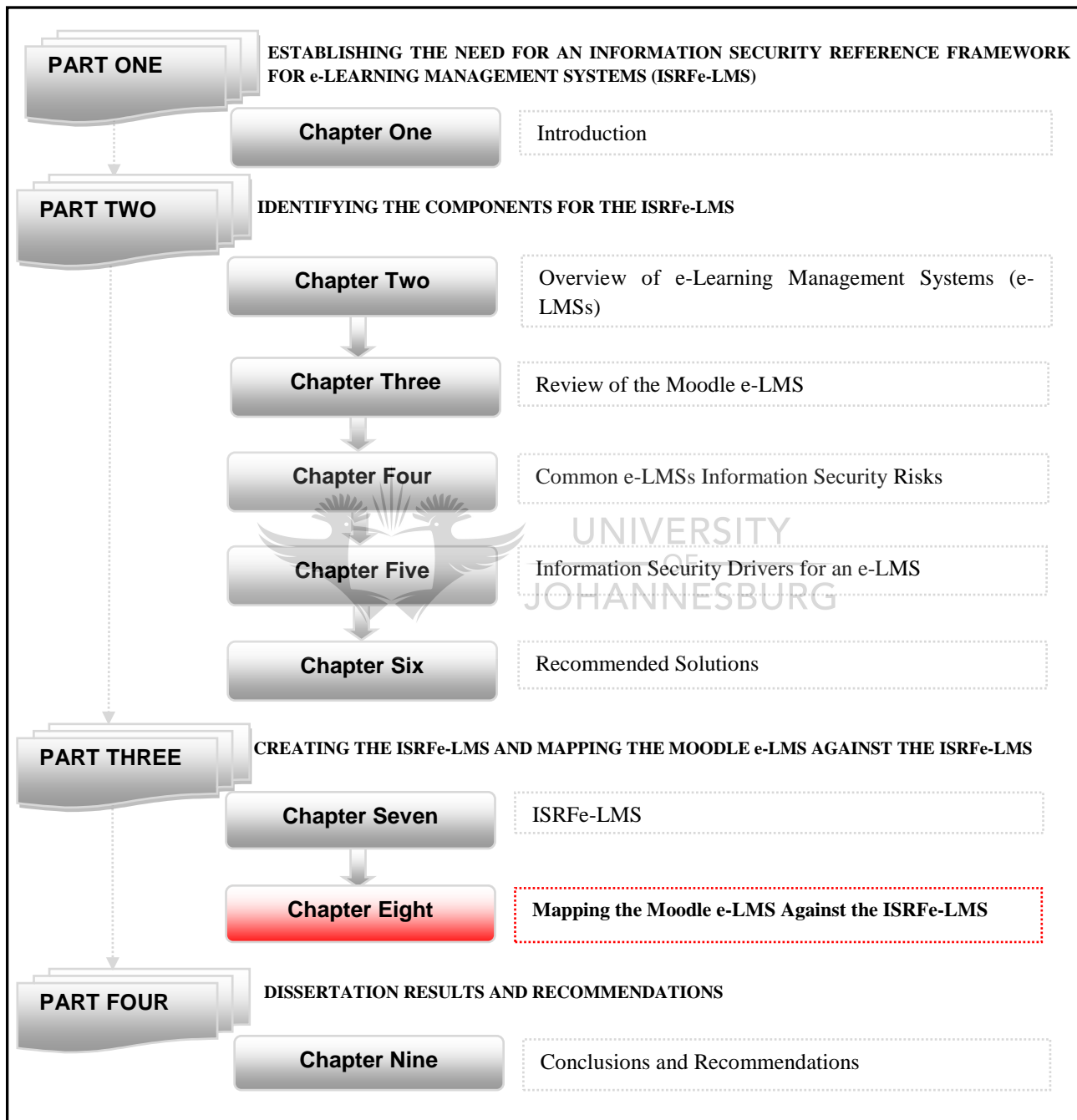
Figure 7.2.: The Graphic Representation of the ISRFe-LMS

Figure 7.2. depicts the high level representation of the ISRFe-LMS. The author has developed an Implementation Guideline for the ISRFe-LMS to provide guidance to users in the implementation of the ISRFe-LMS. For further information on the implementation guideline, see Appendix A.

## **7.4. CONCLUSION**

The author has created an Information Security Reference Framework for e-LMSs (ISRFe-LMS) based on the ISO 27002 standards for Information Security Management. The ISRFe-LMS is composed of the five information security dimensions that cover both the technical and non-technical aspect of the e-LMS information security, e-LMS ISG, e-LMS Information Security Policies and Procedures, e-LMS User Awareness, e-LMS Technical, and e-LMS Monitoring Dimensions. The chapter highlighted that both core and facilitating components of the ISRFe-LMS are equally important and it is necessary to take all into account to create the security of an e-LMS.

This chapter provided a high level explanation of the development phases used to create the ISRFe-LMS. In the next chapter, the actual mapping of Moodle e-LMS against the ISRFe-LMS will be performed.



## CHAPTER 8

# MAPPING THE MOODLE e-LMS AGAINST THE ISRFe-LMS

### 8.1. PREVIEW

In the previous chapters, a detailed description of the ISRFe-LMS and its components was discussed. The purpose of this chapter is to map the non-operational Moodle1.9 e-LMS against the ISRFe-LMS in order to determine its information security conformance.



### 8.2. BACKGROUND

In this chapter, Moodle1.9 e-LMS has been selected to be mapped against the ISRFe-LMS to determine its information security conformance. At this point, the user is advised to review Chapter Three for further information on Moodle e-LMS.

### 8.3. SCOPE

For the purpose of this dissertation, only the non-operational Moodle 1.9 e-LMS will be considered. Since it is a non-operational system, it can only be mapped against the core component of the ISRFe-LMS. As discussed in Chapter Seven, the core component of the ISRFe-LMS covers the technical information security aspect of the ISRFe-LMS, by enforcing the six information security services.

### 8.4. METHODOLOGY

Available Moodle e-LMS documentations are limited. Therefore, the mapping of Moodle1.9 e-LMS against the ISRFe-LMS is based solely on the practical test on the information security functionalities of the system.

### 8.5. EVALUATION REPORTS

Based on the investigation carried out, Moodle 1.9 e-LMS has adopted technical and non-technical information security controls to enforce the six information security services. Some of the information security controls are discussed as follows:

- Identification and Authentication
  - Moodle1.9 uses a password based mechanism to enforce Identification and Authentication.



- Authorization
  - Moodle1.9 e-LMS supports Role Based Access Control (RBAC) mechanisms for controlling access to the information resources.
- Confidentiality
  - Moodle1.9 e-LMS enforce Confidentiality through the implementation of effective Identification and Authentication as well as Authorization information security service.
  - Moodle1.9 has also used a unique key called an enrolment key that is assigned to each resource such as course material. Only a user who knows the correct enrolment key will be able to access the resource.
- Integrity
  - Moodle1.9 enforces the integrity Information Security Service through the use of strong Identification and Authentication as well as the Authorization Information Security Service.
- Non-Denial
  - Moodle1.9 enforces the Non-Denial Information Security Service through the implementation of an effective Identification and Authentication service.
  - Moodle1.9 supports the activity log feature which provides users' activity histories.

- Availability
  - Moodle 1.9 ensures the reliability of the system through the use of a backup system which allows the system to stay stable and maintain its data integrity.

In addition to the above the six information security services, Moodle 1.9 also provides the following extra features.

- Allows one to formulate information security policies and procedures according to their information security requirements and objectives.
- Enforce the password policies based on the setting provided above.
- Automatically log out if a user has been idle for a set period of time.
- Information security guidelines:
  1. Avoid posting of any security vulnerability on public forms;
  2. Report all the security exploit directly to the Moodle tracker;
  3. Have a good backup measure;
  4. Perform regular updates;
  5. Disable unused services; and
  6. User Dual firewall.

## 8.6. CONCLUSION

This chapter places emphasis on the Moodle 1.9 e-LMS information security features with a view to determining how they conform to the ISRFe-LMS. The technical dimension of the ISRFe-LMS was used in determining the Moodle 1.9 information security conformance.

Moodle 1.9 implements the Information Security Services of Identifications and Authentication, Authorization and Availability by using password based mechanisms, Role Based Access Control (RBAC) and backup facility. Therefore, in these aspects, Moodle 1.9 conforms well with the ISRFe-LMS. The Information Security Services of Confidentiality, Integrity and Non-Denial are not at all well implemented by Moodle 1.9, and in some cases not at all. In these aspects, Moodle 1.9 conforms badly to the ISRFe-LMS.

Part Three consists of Chapters Seven and Eight. Chapter Seven provided a brief discussion of the ISRFe-LMS; Chapter Eight provided an Evaluation report on the mapping of the Moodle 1.9 e-LMS against the ISRFe-LMS. The findings, results and recommendations for further studies will be discussed in the next part of the dissertation.

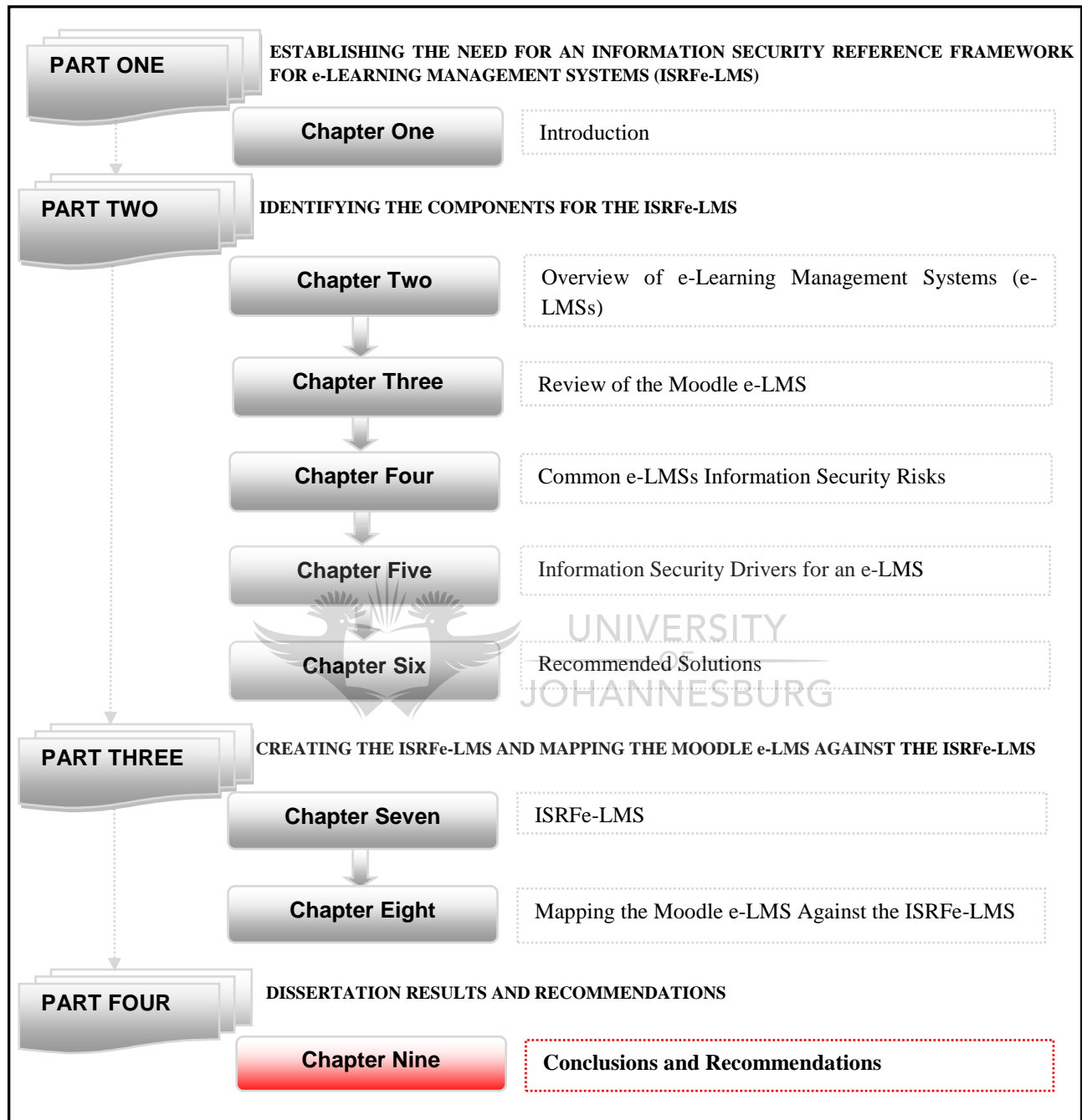


In Part Three, the ISRFe-LMS was created and an investigation in the mapping of the Moodle 1.9 e-LMS against the ISRFe-LMS was undertaken.

Part Four consists of Chapter Nine which will be briefly reviewed as follows:

Chapter Nine provides the summary of findings and recommendations for further studies.





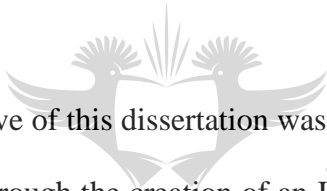
## CHAPTER 9

# CONCLUSIONS AND RECOMMENDATIONS

### 9.1. PREVIEW

The purpose of this chapter is to provide an overview of the research findings, discuss if the objectives of this dissertation have been met and also to identify and recommend areas for further possible research.

### 9.2. DISSERTATION SUMMARY



The main objective of this dissertation was to create and enhance the information security of the e-LMSs through the creation of an Information Security Reference Framework for e-LMS (ISRFe-LMS).

To attain a reasonable level of information security in an e-LMS environment, it will be necessary to have a good understanding of the information security risks involved in using the e-LMS. The author, has thus investigated the possible Information Security Risks related to the e-LMS's environment from each user group's (i.e. Learners, Lecturers and Administrators) perspective. The investigation conducted clearly illustrated the potential Information Security Risks and determined that unless Information Security countermeasures are identified and implemented, the e-LMS's integrity will be

compromised. The author understand that information security should not be seen solely as the implementation of the technical Information Security countermeasures but as a multi-dimensional discipline, where each dimension needs to be considered in order to create a comprehensively secure e-LMS environment. Both practical and literature studies were used in this investigation.

The objective of this dissertation, which is to develop an Information Security Reference Framework for e-Learning Management Systems (ISRFe-LMS), has been accomplished. The ISRFe-LMS was established utilizing an internationally accepted standard, the ISO 27002, which is standard for Information Security Management.

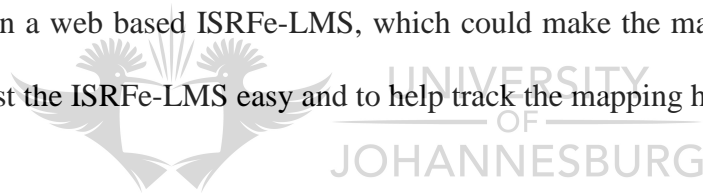
The ISRFe-LMS comprises of the facilitating and core components, each with elements of varied information security dimensions. In order to achieve the acceptable level of Information Security through the ISRFe-LMS for e-LMSs, one has to consider both components and follow the recommended implementation guidelines for the ISRFe-LMS presented in Appendix A.



### 9.3. FURTHER RESEARCH

The study has created an Information Security Reference Framework for e-Learning Management Systems (ISRFe-LMS) and identified the following research opportunities:

- Include more Information Security dimensions, such as Ethics and Law, in the ISRFe-LMS to make it more comprehensive.
- Refine the implementation guideline for the ISRFe-LMS.
- Establish whether the ISRFe-LMS is successful in determining the information security status of an e-LMS.
- Design a web based ISRFe-LMS, which could make the mapping of e-LMSs against the ISRFe-LMS easy and to help track the mapping history.



# APPENDIX A

## IMPLEMENTATION GUIDELINE FOR THE ISRFe-LMS

The implementation Guideline for the ISRFe-LMS that should be considered in creating a secure e-LMS has been divided into five sections where each section covers diverse information security issues of an e-LMS. To discuss each section, the author has adopted a structure that has the following categories:

- **Information Security Objective(s):** provides the Information Security Objective(s) of the section;
- **Controls:** provides the list of recommended measures that should be used to achieve these objectives;
- **Further Explanations:** provides additional information and samples.

### A.1. SECTION 1: e-LMS Information Security Governance (ISG)

**Information Security Objective(s):** To promote good information security practices within an e-LMS.

#### Controls

1. Develop an appropriate Information Security Governance strategy for an e-LMS.
2. Review the Information Security Governance strategy developed.

- ✓ The Information Security Governance strategy should be reviewed periodically to evaluate its effectiveness.

3. Enforce the Security Governance strategy.

**Further Explanations:** See Section 5.3.1.1.

## **A.2. SECTION 2: e-LMS Information Security Policies and Procedures**

**Information Security Objective(s):** To provide a standard framework that governs all users' actions related to achieving the information security objectives of the e-LMS environments.

### **Controls**

1. Develop Information Security Policies and Procedures for an e-LMS.
2. Review the Information Security Policies and Procedures developed.
  - ✓ The Information Security Policy and Procedures should be reviewed periodically to evaluate effectiveness.
3. Enforce the Information Security Policies and Procedures.

**Further Explanations:** Sample Information Security Policy is provided in Appendix B.1.

### A.3. SECTION 3: e-LMS User Awareness

**Information Security Objective(s):** To create Information Security awareness within e-LMS users so that they perform and do not compromise the information security objective of the e-LMS environment.

#### Controls

1. An e-LMS must have an appropriate Information Security User Awareness program in place.
  - ✓ The User Awareness program should include information that explains the e-LMS Information Security Policy and Procedures that are already in place.
2. Review the Information Security User Awareness program.
  - ✓ The User Awareness program should be reviewed periodically to evaluate its effectiveness.
3. Enforce the User Awareness program.
  - ✓ The User has to do the mandatory information security user awareness training program before being granted with any access to the e-LMS.

**Further Explanations:** Sample User Awareness Program is provided in Appendix B.2..

#### A.4. SECTION 4: e-LMS Technical

**Information Security Objective(s):** To enforce the six information security services in an e-LMS.

#### Controls

1. Enforce Information Security Mechanisms.
  - Identification and Authentication
    - ✓ Identify and authenticate users. The three possible mechanisms that could be used to enforce Identification and Authentication Information Security Service are: password based, token based and biometrics based mechanisms (*Section 5.3.1.5.1.*).
  - Authorization
    - ✓ Control users' rights and privileges. Some of the information security mechanisms that could be used are Access Control List (ACL), Directory List, and Access control Matrix (ACM) (*Section 5.3.1.5.2.*).
  - Confidentiality
    - ✓ Protect the e-LMS's assets from unauthorized view. The three mechanisms that could be used to enforce Confidentiality information security services are Encryption, through effective use of the Identification and Authentication and effective

authorization information security services (*Section 5.3.1.5.3*).

- Integrity
  - ✓ Protect the e-LMS's assets from unauthorized alteration and/or deletion. The three mechanisms that could be used to enforce Confidentiality information security services are a Message Authentication Code (MAC), through effective use of the Identification and Authentication information security service and effective authorization information security service (*Section 5.3.1.5.4*).
- Non-Denial
  - ✓ Each user must be accountable for all actions performed on the system with his/her identification information (user id and password). One of the information security mechanisms that could be used is Digital Signature (*Section 5.3.1.5.5*).
- Availability
  - ✓ The e-LMS must be available and reliable at all times. Establishing back up measures is one of the information security mechanisms to consider in ensuring reliable access to the e-LMS (*Section 5.3.1.5.6*).

## 2. Review the Information Security Mechanisms.

- ✓ The Information Security Mechanisms should be reviewed periodically to evaluate its effectiveness.

**Further Explanations:** Refer to Chapter Five section 5.3.1.5. and Chapter Six section 6.3..

#### **A.5. SECTION 5: e-LMS Monitoring**

**Information Security Objective(s):** To develop an Information Security Monitoring Mechanism in order to determine whether the control implemented has been effective.

#### **Controls**

1. Review the enforcement of the ISG in an e-LMS environment.
2. Review the enforcement of the information security policies and procedures.
3. Review compliance with the information security policies and procedures.
4. Evaluate users' level awareness of the information security policy.
5. Review technical security compliance.

**Further Explanations:** See Section 5.3.1.4..

# APPENDIX B

## B.1. PASSWORD POLICY FOR XYZ E-LMS

2009

XYZ e-Learning Management System  
(LMS)

Author : Sorene Assefa

The sample password policy herein is by no means comprehensive but covers the basic elements that an e-LMS password policy should include. The XYZ e-LMS utilizes a password based Identification and Authentication mechanism. Listed below are the minimum password policies that must be implemented in order to ensure the effectiveness of password based security mechanism.

**SECTION 1:** All e-LMS users are responsible for complying with the following Password rules:

1. Identification information (user id and password) must never be shared with another person.
2. Password must have a minimum length of 6 characters.
3. Passwords should be changed at least every six weeks.
4. The password must not be easily guessed; for instance, something related to the user or a dictionary word.
5. Passwords should be a combination of alpha and numeric characters.



**SECTION 2:** The e-LMS is responsible for complying with the following password Rules:

1. No Group identity: the e-LMS must force every user to have a unique user identity.
2. The system must enforce the minimum length of password allowed.
3. The system must enforce the change of password after at least six weeks from creation.
4. The system must discourage a user from selecting a password that relates to his/her identity or common words.
5. The system must disable the user account after three failed attempts.
6. The system must lock itself if idle for more than 15 minutes.
7. The system must allow users to enter the password as a non-displayed field.
8. The system must maintain Confidentiality and Integrity of the authentication information during storage and transmission.
9. An e-LMS must log the authentication information in order to be able to track users' activities, and also enforce Non-Repudiation/Non-Denial.

**SECTION 3:** The password policy applies to all e-LMS users with a possible disciplinary action that can be instituted for any of the following actions:

1. Unauthorized disclosure of identification information (user id and password).
2. Using other user(s) identification information (user id and password).
3. Intentional disruption of the e-LMS operation.



**B.2. INFORMATION SECURITY USER AWARENESS  
PROGRAM**

For  
**XYZ e-Learning Management System**

Implementing technical information security control by itself does not ensure information security; it is necessary that end users are aware of it and act in a way that does not compromise the technical system. e-LMS should have an information security awareness training program in order to create an acceptable level awareness about the information security policies and procedures, and thereby enable users adhere to best information security practices.

Sorene Assefa  
2009

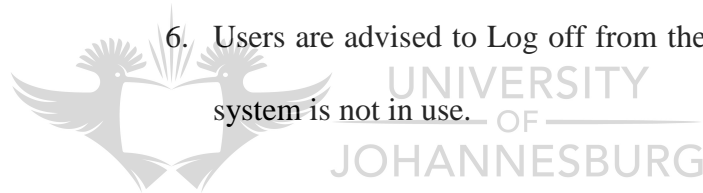
There are numerous techniques for the delivery of information security related user awareness programs, such as: posters, newsletters, fliers and web pages, etc. For the purpose of this dissertation, the author has designed a prototype for a web based Information Security User Awareness program for the XYZ e-LMS, which will be a mandatory prerequisite for all users before they can be granted access.

The system is designed with “ease of use” in mind. A user-friendly graphical user interface (GUI) makes it possible for the user to easily interact with the system. The system consists of the following components:

- **Access control** is implemented and therefore only authorized users have access to the system. This is accomplished by using a password based mechanism.
- **Guidelines:** A brief explanation of the information security laws related to the use of each functional feature of the XYZ e-LMS. Some of the aspects that have to be addressed in this section are Login, Password, PC Security, Email usage, Intellectual Property laws (Resource Utilization), Computer virus, and Backups. For the purpose of this dissertation, the login aspect will be discussed as follows:

**Login:** This generally means entering a username (user’s identity information) and password (the secret key related to the username) into the XYZ e-LMS. Some of the guidelines that XYZ e-LMS’s users should be aware of in order to log in into the system are discussed as follows:

1. Never share your login (username/password) information with anyone.
2. Check your surroundings before entering your password.
3. Follow the password policy as provided by the XYZ e-LMS.
4. Users only have three attempts to login into the XYZ e-LMS.
5. The user is responsible for any action carried out with their account information.
6. Users are advised to Log off from the system when the system is not in use.



- **Assessment:** provides quizzes to evaluate the user's knowledge on the subject that was covered and thus determine the level of awareness about the information security. Upon successful completion of the assessment, system access will be granted.
- **Incident Reporting:** provides contact information for reporting incidents.
- **Additional Resources:** provide useful links for further study on information security laws, concepts as well as definitions.

# APPENDIX C

## AN INFORMATION SECURITY REFERENCE FRAMEWORK FOR e-LEARNING MANAGEMENT SYSTEMS (ISRFe-LMS)

The following article was presented at the IFIP World Conference on Computers in Education (WCCE), 27-31 July, 2009, Brazil, and will be published in the proceedings of the conference

**Sorene Assefa<sup>1</sup> and Prof. Von Solms<sup>2</sup>**

<sup>1</sup> Academy for Information Technology, University of Johannesburg, P.O. Box 524, Auckland Park, Johannesburg, 2006, South Africa, [soreneas@yahoo.com](mailto:soreneas@yahoo.com) [200605244@student.uj.ac](mailto:200605244@student.uj.ac)

<sup>2</sup> Academy for Information Technology, University of Johannesburg, P.O. Box 524, Auckland Park, Johannesburg, 2006 South Africa, [basievs@uj.ac.za](mailto:basievs@uj.ac.za)



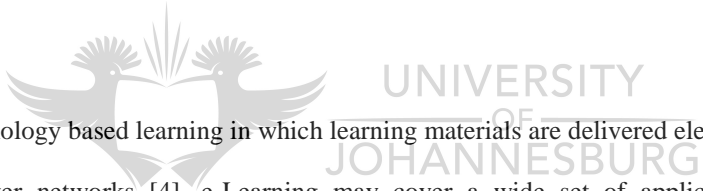
**Abstract:** Despite the widespread acceptance of e-Learning Management Systems (e-LMS), information security, trust and dependability issues still remain the biggest challenge. This paper argues that e-LMS is mainly dependant on Information and Communication Technologies (ICTs) that have inherent Information Security Risks, as they have only technical Information Security Mechanisms, such as password based identification and authentication and access control, which do not necessarily ensure that the security of the e-LMS environment is maintained at all times. This paper investigates how to secure e-LMSs through the creation of an Information Security Reference Framework (ISRFe-LMS) based on the International Organization for Standardization's (ISO) 27002. ISO 27002 is internationally accepted standard for good practice for Information Security Management. The ISRFe-LMS is created for use as a comprehensive standard for the evaluation of existing e-LMS packages within the context of security conformance.

**Keywords:** e-Learning Management Systems, Information and Communication Technologies (ICTs), Information Security, Information Security Governance, Information Security Policies and Procedures,

Information Security Risks, Information Security Services, User Awareness, Monitoring, Technical Information Security Dimension.

## 1. Introduction

It is traditionally accepted that there are two major knowledge sharing systems: the traditional system and the Information and Communication Technologies (ICTs) based system. The need for unlimited access to information, intellectual skills and knowledge is the driving force for the creation and enhancement of ICT based education. One of the knowledge sharing systems that emerged from the use of ICTs is electronic Learning (e-Learning).



e-Learning is a technology based learning in which learning materials are delivered electronically to remote learners via computer networks [4]. e-Learning may cover a wide set of applications, systems and processes, such as e-Learning Systems, Web Based learning, and Computer Based Learning (CBL) [8]. e-Learning Systems is a technology that makes use of network technology such as the Internet, Intranet, Extranet (LAN/WAN), audio and video tape, satellite broadcast, interactive TV, CD-ROM and more to deliver or administer contents [8]. e-Learning Systems cover a wide range of systems: e-Learning Management Systems (e-LMS), and e-Learning Content Management Systems (e-LCMS) are some examples of e-Learning Systems. An e-LMS is a comprehensive software application with various functional features that enables the design, management and delivery of e-Learning content to remote learners via ICTs [8]. Some examples of e-LMSs are WebCT, Claroline, Moodle and ILIAS.

The article originated from the realization that the integrated and dynamic nature of e-LMS should make it clear that information security is one of the most important aspects to be considered during the implementation and usage of the e-LMS. In spite of the abundance of literature in e-Learning Systems, the security aspect of e-LMS has been given very little consideration. Moreover, based on the investigation conducted by the authors, there is no Information Security Reference Framework comprehensive enough to be used as a standard for the mapping and evaluation of existing e-LMS packages within the context of information security conformance.

The purpose of this article is to focus strictly on creating and enhancing the security of e-LMSs through the creation of an information security reference, called an Information Security Reference Framework for e-Learning Management Systems (ISRFe-LMS), which is based on the ISO 27002 standard for Information Security Management. The article is thus guided by the following question: *Which components should a comprehensive information security reference framework entail?*

The paper starts by investigating the possible Information Security Risks related to the e-LMSs. It further argues that the fact that e-LMSs rely on ICT makes them vulnerable to further Information Security Risks and if these risks are not properly addressed and mitigated, the integrity of the entire e-Learning process will be compromised. For this reason, the authors attempt to identify the most common Information Security Risks related to the e-LMS's environment from each user group's (i.e. learners, lecturers and administrators) perspective.

## **2. e-LMS Information Security Risks**

This article attempts to identify the Information Security Risks related to the e-LMS's environment from the perspective of each user's activities. To accomplish this, the authors first identify the most common

activities performed by each user and then develop scenarios to illustrate some of the potential Information Security Risks related to each activity.

Please note that the scenarios presented in the next section are not the only examples and do not refer to a specific e-LMS but e-LMSs in general.

## ***2.1. Users and Their Roles in e-LMS***

Each user group has roles and responsibilities on the e-LMS.

### **2.1.1. Lecturer**

A lecturer is one of the user groups of an e-LMS who is responsible for coaching as well as tracking the performances of the respective learner(s). The lecturer can:

1. **Activity 1:** Create and upload online assessment materials such as quizzes in the form of true or false, multiple choices, matching and so on.
2. **Activity 2:** Establish and post assignment(s). Some of the risks related to activities 1 and 2 will be discussed in section 2.2.1..

### **2.1.2. Learner**

The learner is another user of the e-LMS who uses the e-LMS in order to achieve learning objectives.

Learners can:

1. **Activity 1:** Take online assessment exams or quizzes, which are set by the lecturer. Some of the risks related to this activity will be discussed in section 2.2.2..



### 2.1.3. Administrator

An administrator is the person who oversees and moderates the activities carried out on the e-LMS. One of the administrator's roles is to define the users' roles and assign privileges accordingly. This access control information should not be edited by anyone other than the administrator. The administrator can:

1. **Activity 1:** Establish roles and privileges and assign it to respective users. Some of the risks related to activity 1 will be discussed in section 2.2.3..

Without proper Information Security Mechanisms, an e-LMS could be exposed to various Information Security Risks, which will be discussed in the next section.

## 2.2. Investigating the Information Security Risks of Using an e-LMS

In this section, scenarios will be formulated and discussed to illustrate the Information Security Risks related to each user's activities (i.e. as discussed in section 2.1.).

### 2.2.1. Lecturer

Some of the risks related to activities 1 and 2 of section 2.1.1. are:

1. Risk 1: Fake assignments can be uploaded.

**Motivation:** *An unauthorized person can only have access to the system and upload fake assignment if the e-LMS does not have an effective Identification and Authentication, and Authorization Information Security Services in place.*

2. Risk 2: The exam set up by the lecturer can be viewed before the due date.

**Motivation:** *An unauthorized person can only have access to the system and view the uploaded exams before the due date if the e-LMS does not have an effective Identification and Authentication, Authorization, and Confidentiality Information Security Service in place.*

3. Risk 3: The exam can be deleted when a student knows that (s)he is not ready.

**Motivation:** *An unauthorized person can only have access to the system and delete uploaded assignment if the e-LMS does not have an effective Identification and Authentication, Authorization, Integrity, Non- Repudiation and Availability Information Security Service in place.*

### 2.2.2. Learner

Some of the risks related to activity 1 of section 2.1.2. are:

1. Risk: The learner can pass his/her personal identification and authentication information to a friend so that the friend can write the exam on the learner's behalf.

**Motivation:** *It is difficult for a system to determine whether it is the authentic learner (i.e. the owner of the secret key) or someone else on his/her behalf who has entered the authentication information, so long as the secret key supplied is valid. In that, if this issue is not addressed, the overall integrity of the system can be compromised. Some of the possible solutions to mitigate the problem are:*

- *Setup effective Identification and Authentication Information Security Services such as the Biometrics Based Information Security Mechanisms, which are relatively harder to tamper with;*
- *Implement effective e-LMS Information Security Policies and procedures;*
- *Implement an effective user awareness program;*
- *Enforce a supervised environment which would create an extra security layer.*

### 2.2.3. Administrator

Some of the risks related to activity 1 of section 2.1.3, are:

1. Risk: The roles and privileges could be altered by an unauthorized user.

***Motivation:** An unauthorized person can only have access to the system and alter the access control information if the e-LMS does not have an effective Identification and Authentication, Authorization Integrity and Availability Information Security Services in place.*

The scenario above clearly illustrates the potential Information Security Risks; unless Information Security countermeasures are identified and implemented, the e-LMSs integrity will be compromised, which could compromise the reputation of the institution.

Information Security is all about the implementation of Information Security countermeasures to protect a system's information assets from a wide range of threats [3]. Although most of the current e-LMSs have some sort of Information Security Mechanism, such as password based identification and authentication and access control in place, security still remains a crucial issue for most institutions. The solution developed by the author is an Information Security Reference Framework for e-LMS (ISRFe-LMS). The ISRFe-LMS is designed to be used as a guideline and standard for the evaluation of existing e-LMS packages within the context of security conformance. As highlighted by [3], having Web and Operating System (OS) Security in place alone does not automatically make the e-LMS environment secure. However, they remain the main requirements of the ISRFe-LMS. In the next section, the components of the ISRFe-LMS will be discussed.

### 3. ISRFe-LMS<sup>1</sup>

The ISRFe-LMS is made up of two components: the facilitating and core components.

The core component deals with the technical Information Security Dimension; which is implementing the Six Information Security Services, namely: Identification and Authentication, Authorization, Confidentiality, Integrity, Non-Repudiation and Availability.

Facilitating components are those that support the core components. The facilitating components comprise of the four non-technical Information Security Dimensions, namely: e-LMS Information Security Governance (ISG), e-LMS Information Security Policies and Procedures, User Awareness and Monitoring dimension.

Facilitating and core components go hand-in-hand; without one another, they cannot achieve the objective of the ISRFe-LMS. The graphical representation of the ISRFe-LMS is depicted in the figure below.

---

<sup>1</sup> The six Information Security Services :

**Identification and Authentication** ensures only authorized (legal) users are allowed access to an e-LMS environment [7].

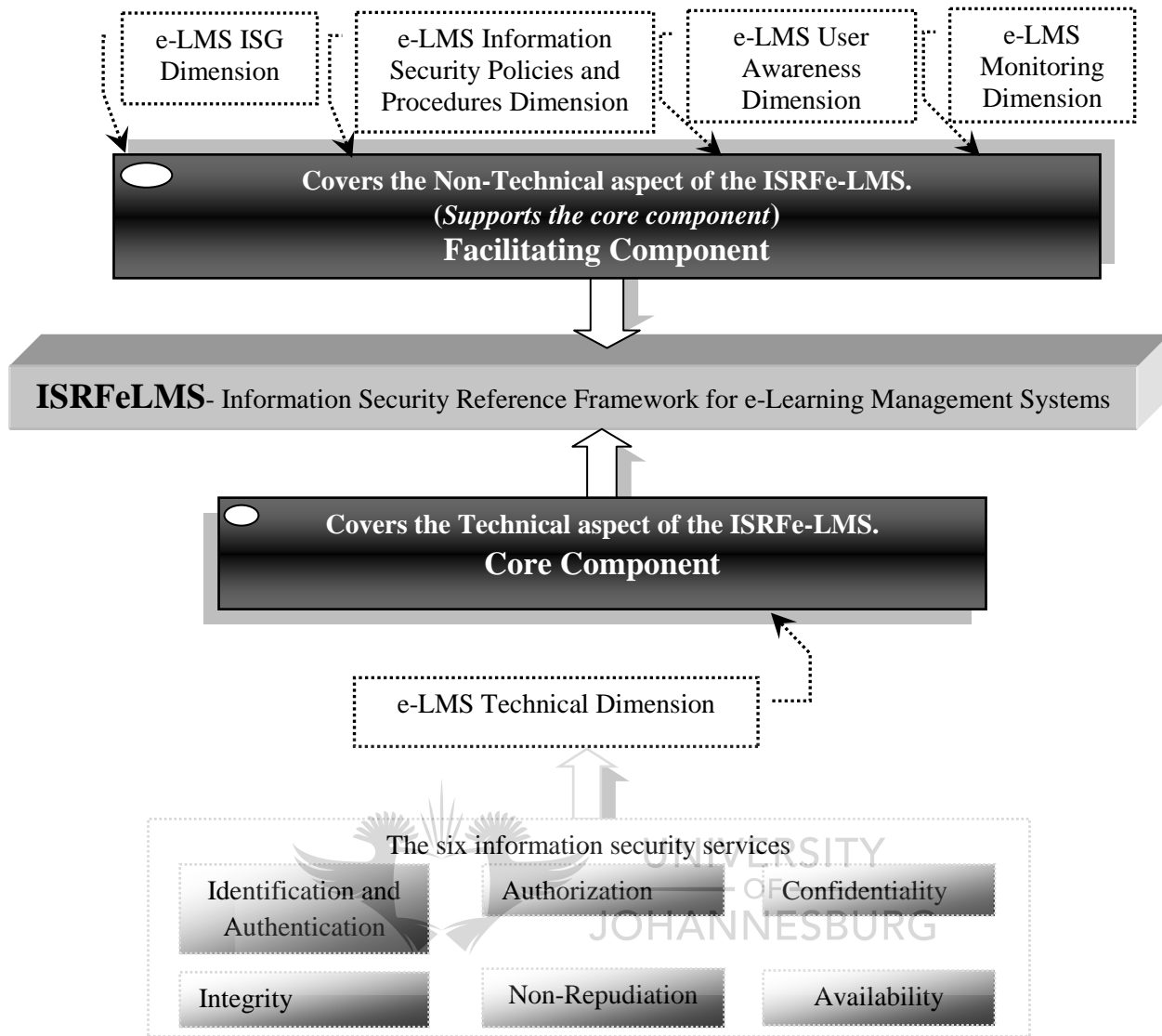
**Authorization** ensures that each e-LMS user group (i.e. learners, lecturers, and administrator) access only information resources or perform certain action according to their roles and privileges [7].

**Confidentiality** ensures that the content of the information during storage and transmission are protected from unauthorized access and disclosure [1, 7 and 9].

**Integrity** ensures that the content of the information during storage and transmission are protected from unauthorized alteration or change [7].

**Non-Repudiation** ensures that accountability for the execution of any action on the e-LMS is enforced [1].

**Availability** An e-LMS should be available timely and has to be reliable at all times specifically during online Assessment. The available information security service ensures that the e-LMS's information content data Integrity is preserved after an interruption of any means such as power cuts [6].



Source: Author's own composition

Figure 1: The Graphic representation of the ISRF e-LMS

Figure 1 depicts the high level representation of the ISRF e-LMS. In the next section, a detailed discussion of requirements for each dimension will be provided.

### 3.1. Requirements for the ISRF e-LMS components

To create a secure e-LMS through the use of the ISRF e-LMS, the requirements of the ISRF e-LMS components must be satisfied. In the following section, the main requirements for the ISRF e-LMS components will be discussed.

### 3.1.1. e-LMS Information Security Governance (ISG) Dimension

The main goal of Information Security Governance (ISG) is to develop information security goals and objectives for an e-LMS environment [4]. It is therefore necessary to introduce and ensure information security measures are implemented to make sure the security objectives of the e-LMS are achieved.

e-LMS ISG for the top management of the institute that utilize the e-LMS to create a complete online learning system or support the traditional (face-to-face) learning system should include:

- An e-LMS must have a document that shows the top management's commitment for information security objectives of the e-LMSs, which should include ensuring that the six information security services (i.e. Identification and Authentication, Authorization, Confidentiality, Integrity, Non-Repudiation and Availability) are in place.

### 3.1.2. e-LMS Information Security Policies and Procedures Dimension

An Information Security Policies and Procedures Dimension is all about creating a standard framework that governs all the relevant action related to achieving the information security objectives of the e-LMS environments.

An e-LMS must have a distinct information security policies and procedures in place. For example, Password Based Identification and Authentication should have a Password Policy for the e-LMS user groups that can be used as guideline during the creation and usage of user account. Some of the most common elements for a password policy are:

- The minimum length of password allowed by the e-LMS;
- Kind of characters allowed by the system;
- How frequently the passwords should change; and
- Discouraging a learner from selecting a password that relates to his/her identity or common words.

### 3.1.3. User Awareness Dimension

The objective of a User Awareness Dimension is to create a user awareness program that enables users to perform in such way that they do not compromise the information security objective of the e-LMS.

An e-LMS must have a user awareness program which can be online or in documents.

- An e-LMS should force each user group to take the created user awareness course at their first access to the system.

### 3.1.4. Monitoring Dimension

A Monitoring Dimension determines if the Information Security Mechanisms implemented have achieved their purpose and also verifies compliance to the e-LMS information security Policies and Procedures.

An e-LMS should have a defined monitoring mechanism. Some of the common elements of Information Security Mechanisms for the e-LMS are:

- An e-LMS must have an information security monitoring mechanism to determine where the defined information security policies and procedures are enforced;
- An e-LMS must have a mechanism that measures the level of user awareness; and
- An e-LMS must have a mechanism to determine if the ISG is enforced throughout the system.

### 3.1.5. Technical dimension<sup>2</sup>

The purpose of the Technical Dimension is to ensure the Six Information Security Services (i.e. Identification and Authentication, Authorization, Confidentiality, Integrity, Non-Repudiation and Availability Information Security Service) are enforced.

An e-LMS should have a mechanism to evaluate the system for the Six Information Security Services.

- An administrator can check if the Six Information Security Services are enforced by performing frequent testing on the system as well as gathering survey from each User Groups.

## 4. Conclusion

This paper has highlighted how important it is to ensure information security within an e-LMS environment. The authors have created an Information Security Reference Framework for e-LMSs (ISRFe-LMS) based on the ISO 27002 Standard for Information Security Management. The ISRFe-LMS take account of the five most relevant information security dimensions necessary in creating a secure e-LMS environment. It has two components: the Core (i.e. Technical Dimension) and the Facilitating (i.e. e-LMS ISG, e-LMS Information Security Policies and Procedures, User Awareness, and Monitoring Dimension). Both the core and facilitating component's requirements need to be met in order to create a secure e-LMS environment with the ISRFe-LMS.

---

<sup>2</sup> The Information Security Mechanisms for the six Information Security Services [6, 8 and 24] :

- ✓ Password Based, Token Based and Biometrics Based Information Security Mechanisms could be used to enforce the Identification and Authentication Information Security Service;
- ✓ Access Control List (ACL), Directory List, and Access Control Matrix Information Security Mechanisms could be used to enforce the Authorization Information Security Service;
- ✓ The Confidentiality Information Security Service could be enforced through the use of encryption, effective identification and authentication, and authorization information security;
- ✓ The Integrity Information Security Service could be enforced through the use of Message Authentication Code (MAC), effective identification and authentication, and authorization information security;
- ✓ Digital Signature Information Security Mechanisms could be used to enforce the Non-Repudiation Information Security Service; and
- ✓ Good backup system is one of the means of ensuring the Availability Information Security Services.



## References

- [1] Addison, T. M., Munron, K. I. and Rollason, J. D. (2002) "IS Security: User identification and Authentication with reference to South African Financial Services Case Study". University of the Witwatersrand.
- [2] Argles, D., Marais, E. and Von Solms, B. (2006). Security Issues Specific to e-Assessment. In 8<sup>th</sup> Annual Conference on WWW Applications, 6 - 8 September, 2006. Bloemfontein.
- [3] Eible, C. J., Schubert, S. and Von Solms, B. (2006). A Framework for Evaluating the Information Security of E-learning Systems.
- [4] Kritzinger, E. and Von Solms, S. H. (2006). "e-Learning: Incorporating Information Security Governance". *Issues In Information Science and Information Technology*. Volume 3, 2006.
- [5] Pflieger, S. L. (2003). 3<sup>rd</sup> edition. *Security in Computing*. Prentice-Hall PTR.
- [6] Psaros, V. C. (2003). "Information Security in Web-Based Teleradology".
- [7] Scheneier, B. (2000). *Security and Lies: Digital Security in a Networked World*. Addison Wesley.
- [8] Von Solms, S. H. (2005). "Information security Governance in ICT based educational systems".
- [9] Unknown. (2007). IS-3 Electronic Information: Reference to questions to information resources and communications. Security IS Services Information Systems- Business and finance Bulletin, University of California.

## APPENDIX C

### INFORMATION SECURITY DRIVERS FOR e-LEARNING MANAGEMENT SYSTEMS (e-LMS)

The following article was presented at the eLearning Africa 2009 - 4<sup>TH</sup> *International Conferences on ICT for Development, Education and Training*, 27-29 May, 2009, Dakar, Senegal, and has been published in the proceeding of the conference.

**Sorene Assefa<sup>1</sup> and Prof. Von Solms<sup>2</sup>**

<sup>1</sup> Academy for Information Technology, University of Johannesburg, P.O. Box 524, Auckland Park, Johannesburg, 2006, South Africa, [soreneas@yahoo.com](mailto:soreneas@yahoo.com) [200605244@student.uj.ac](mailto:200605244@student.uj.ac)

<sup>2</sup> Academy for Information Technology, University of Johannesburg, P.O. Box 524, Auckland Park, Johannesburg, 2006 South Africa, [basievs@uj.ac.za](mailto:basievs@uj.ac.za)

#### ABSTRACT

In order to make e-Learning systems more relevant, it is first necessary to understand the elements required to have an effective e-Learning system. One of the most important elements is Information Security.

In spite of the abundance of varied literature on e-Learning Management Systems (e-LMS), information security aspects related to the systems have been given little consideration. The primary reason for attaching key importance to information security in the e-LMS environment is due to the fact that the e-LMS is mainly dependent on Information Communication Technologies (ICTs). ICTs have inherent Information Security risks; if these risks are not properly addressed and mitigated, the integrity of the whole e-Learning process may be compromised. This article highlights how the Information Security serves as the most important element to ensure that all information within e-LMSs is protected and the overall integrity of the system is maintained. e-LMSs do provide some form of Technical Information Security counter measures, such as Password Based Identification and Authentication to protect the valuable information assets of the system. However, having only Technical Information Security countermeasures in place does not necessarily ensure that the security of the e-LMS environment is maintained at all times. Therefore, Information Security should be taken as a multi-dimensional discipline. The authors identify and discuss the most important information security dimensions that need to be considered in creating a secure e-LMS environment.

**Keywords:** E-Learning Management Systems, Information Security, Information Security Governance, Information Security Policies and Procedures, Information Security Risks, User Awareness, Monitoring, Technical Dimension.

One of the knowledge sharing systems that emerge from the use of Information and Communication Technologies (ICTs) is an e-Learning Management System (e-LMS). An e-LMS is a comprehensive software package with various functional features that enables the management and delivery of online content to remote users via ICT [7]. Some examples of e-LMS are WebCT, Claroline, and Moodle. One of the main advantages of using an e-LMS is being able to access and share information regardless of the geographic location and time.

In spite of the abundance of literature on e-LMS, the information security aspect of e-LMS has been given very little consideration. This article originated from the realisation that the integrated and dynamic nature of e-LMS should make it clear that information security is one of the most important aspects to be considered during the implementation and usage of an e-LMS, and the information security is a multi-dimensional discipline [6].

The purpose of this article is to identify and recommend the most important information security dimensions that need to be considered in creating a secure e-LMS environment. The article is thus guided by the following question. *Which information security dimensions are most relevant in creating a secure e-LMS environment?*

To attain a reasonable level of information security in an e-LMS environment, it will be necessary to have a good understanding of the information security risks involved in using the e-LMS. The paper starts by investigating the possible Information Security Risks related to the e-LMS's environment from each user group's (i.e. Learners, Lecturers and Administrators) perspective. The scenario below illustrates some of the growing Information Security challenges of e-LMSs.

- **Scenario:** Using an e-LMS, a lecturer can upload both online and offline assessment material(s) for learners to access.

If there are no proper Information Security countermeasures in place, the following risks could arise:

2. Fake assessment material(s) could be created and uploaded by unauthorized users.
2. The assessment material(s) could be viewed by unauthorized users pretending to be a legitimate learner.
3. The assessment material(s) could be altered and/or deleted by unauthorized users.
6. The learner can pass on his/her personal Identification and Authentication information to a third person who may write the online assessment test on the learner's behalf.
7. When a learner discovers he/she cannot pass the online test, he/she (the learner) can create a Denial of Service attack (DOS) to sabotage the assessment.
8. Someone can submit a fake assignment under the guise of being a legitimate learner.
9. The student can deny submitting an assignment if he/she thinks that he/she will not pass.
10. Submitted assignments can be viewed, copied, changed or deleted.

The scenario above clearly illustrates the potential Information Security Risks; unless Information Security counter measures are identified and implemented, the e-LMSs integrity will be compromised. The authors observed that information security should not be seen as solely the implementation of technical Information Security countermeasures but as a multi-dimensional discipline, where each dimension needs to be considered in order to create a comprehensively secure e-LMS environment [6].

To create a reasonable information security in an e-LMS environment, the authors identified and recommend the five most essential information security dimensions that should be in place for a proper information security within e-LMS environments. The e-LMS Information Security Governance (ISG), e-LMS Information Security Policies and Procedures, User Awareness, Monitoring and Technical Dimensions are identified as the most fundamental elements in securing an e-LMS environment.

The scenario below illustrates how necessary all the five information security dimensions are to enforce an effective Identification and Authentication Information Security Service in an e-LMS environment.

- **Scenario:** ‘Bob’, the system administrator, has decided to use a password based mechanism (i.e. the Technical Dimension). To create a strong identification and authentication, Bob creates password policy and procedures that need to be followed by users during the creation of identity (username/ password) as well as utilizing the mechanism (i.e. the Policy and Procedure Dimension). Bob decides to create an information security awareness program so that end users are aware of the information security policies and procedures and act in a way that does not compromise the technical measures (i.e. the User Awareness Dimension). Bob wants to make sure that the information security mechanism implemented has served its objectives (i.e. the Monitoring Dimension). Bob agrees to ensure the Information Security Governance (ISG) is implemented throughout the e-LMS environment.

The paper stresses the fact that each of the five Information Security Dimensions are equally important, and it is necessary to consider all of these dimensions in a coordinated way for implementing and maintaining information security in an e-LMS environment.

## **ACKNOWLEDGMENTS**

We would like to thank the National Research Foundation (NRF) and University of Johannesburg (UJ) for the financial support.

## REFERENCES

- [1] Conner, F.W. and Coviello, W.A. (2004). "Information Security Governance – A call to Action". National Cyber Security Summit Task Force.
- [2] Du Plessis, L. and Von Solms, R. (2002) Information Security Awareness: Baseline Educator and Certification. Port Elizabeth Technikon .
- [3] Grobler, T. and Louwrens, B. (2005). "New Information Security Architecture". University of Johannesburg.
- [4] Hone, K. (2004). "The Information Security policy: An Important Information Security Management Control".
- [5] Kritzinger, E. and Von Solms, S.H. (2006). "E-Learning: Incorporating Information Security Governances". Issues in Informing Science and Information Technology, Vol. 3.
- [6] Von Solms, S.H. (2001). "Information Security – A Multi-dimensional Discipline". Elsevier Science Ltd.
- [7] Von Solms, S.H. (2005). *Information Security Governance in ICT Based Educational Systems.*



## APPENDIX E

### SYMBOLS AND ABBREVIATIONS

		<b>A</b>
<b>ACL</b>	Access Control List	
<b>ACM</b>	Access Control Matrix	
<b>AICA</b>	Availability, Integrity, Confidentiality and Authentication	
		<b>C</b>
<b>CBL</b>	Computer Based Learning	
<b>CMS</b>	Course Management System	
		<b>D</b>
<b>DoS</b>	Denial of Service attack	
		<b>E</b>
<b>e-Learning</b>	electronic Learning	
<b>e-Learning System</b>	electronic Learning System	
<b>e-LCMS</b>	electronic Learning Content Management System	
<b>e-LMS</b>	electronic Learning Management System	
		<b>G</b>
<b>GUI</b>	Graphical User Interface	
		<b>I</b>
<b>ICT</b>	Information and Communication Technology	
<b>ILIAS</b>	Integrated Learning Information and CooperAction System	
<b>ISO</b>	International Organization for Standardization	
<b>ISRFeLMS</b>	Information Security Reference Framework for e-Learning Management Systems	
<b>ISG</b>	Information Security Governance	
		<b>L</b>
<b>LAC</b>	Logical Access Control	
<b>LAMP</b>	Linux, Apache, MySQL and PHP	
		<b>M</b>
<b>MAC</b>	Message Authentication Code	
<b>Moodle</b>	Modular Object Oriented Dynamic Learning Environment	
		<b>P</b>
<b>PHP</b>	Hypertext Preprocessor	
		<b>R</b>
<b>RBAC</b>	Role Based Access Control	

---

## BIBLIOGRAPHY

---

- [1] Addison, T.M., Munro, K.I. and Rollason, J.D. (2002). "User Identification and Authentication with reference to South Africa Financial Services Case Study". In: *Proceedings of the ISSA2002 (Information Security for South Africa) Conference*, 10-12 July, 2002, Muldersdrift, Gauteng.
- [2] Argles, D., Marais, E. and Minnar, U. (2006). "Plagiarism in e-Learning System: identifying and solving the problem for practical assignments". In: *The 6th IEEE International Conference on Advanced Learning Technologies*, July 5-7, 2006, Kerkrade, Netherlands.
- [3] Argles, D., Marais, E. and Von Solms, B. (2006). "Security Issues Specific to e-Assessment". In: *8<sup>th</sup> Annual Conference on WWW Applications*, 6<sup>th</sup>-8 September, 2006, Bloemfontein
- [4] Barman, S. (2002). *Writing Information Security Policies*. 2<sup>nd</sup> Edition. United State of America: New Riders.
- [5] Bement, A.L., Bond, P.J. and Evans, D.L. (2002). "The keyed-hashed Message Authentication code (HMAC)." Federal Information processing standards publication.198. <http://csrc.nist.gov/publications/fips/fips198/fips-198a.pdf> (Accessed October 28, 2008).
- [6] Bornman, W.G. (2004). *Information Security Risk Management: A Holistic Framework*. M.Com work, Faculty of Economic and Management Science at the Rand Afrikaans University, South Africa.
- [7] Brown, K.G., Simmering, M.J., Weish, E.T. and Wenberg C.R. (2003). "e-Learning: Emerging uses, empirical results and future directions". International Journal of Training Development. 7, 4(2003):245-258.



- [8] Chang, J. and Wang, S. (1999). "Smart card based Secure Password authentication Scheme". Elsevier Science Ltd 15, 3(1999):231-237.
- [9] Chauan, A. and Pavri, S. (2004). "Open Source Learning Management with Moodle"  
LINUX Journal. [http:// www.linuxjournal.com/article/7478](http://www.linuxjournal.com/article/7478). (Accessed January 10, 2008).
- [10] Daley,W.M, and Kammer,R.G. (2000). Digital Signature Standard (DSS) Federal Information Processing Standards Publication.186-2. <http://csrc.nist.gov/Publications/fips/fips186-2/fips186-2-change1.pdf> (Accessed November 10, 2008).
- [11] Dietinger, T. (2003). *Aspects of e-Learning Environments*. PhD work, Institute for Information Systems and Computer Media (IICM), Faculty of Computer Science at Graz University of Technology, Austria.
- [12] Dougiamas, M., and Taylor, P.C. (2003). "Moodle: Using Learning Communities to create an open source Course Management System". In: D. Lassner and C. McNaught (eds.). (2003) *Proceedings of World Conference on Educational Multimedia, Hypermedia and Telecommunications 2003*. (pp. 171-178).
- [13] Du Plessie, L. and Von Solms, R. (2002). "Information Security Awareness: Baseline Educator and Certification". In: *Proceedings of the ISSA2002 Information Security for South Africa Conference*, 10-12 July, 2002, Muldersdrift, Gauteng.
- [14] EduTools. (2008). "ArchiveCMS: Product Comparison System". EduTools.com. <http://www.edutools.info/compare.jsp?pj=8&i=358,386>. (Accessed May 10, 2008)
- [15] Eible,C.J. Schubert, S. and Von Solms, B (2006). "A Framework for Evaluating the Information Security of E-learning Systems", In: *2<sup>nd</sup> International Conference on Information in secondary Schools: Evolution and Perspectives (ISSEP2006)*,

- Vilnius, Lithuania, 2-11November 2006, published in the Conference Proceedings.
- [16] Eloff., H.P and Von Solms, S.H. (2004). *Information Security*. 2<sup>nd</sup> Edition. South Africa, 2004.
- [17] El-Khatib, K., Korba, L., Xu, Y., and Yee, G. (2003). “Privacy and Security in E-Learning”. International Journal of Distance Education.1, No. 4 (2003).
- [18] Frank, C. (2003). *Conceptual Design of the Web-Based Case Method-A Pedagogical Perspective*. Faculty of Business Administration and Economics at the University of Paderborn, Germany.
- [19] Friesher, T. and Hart, M. (2004). “Plagiarism and poor academic practice–A Threat to the extension of e-Learning in Higher education?” Electronic Journal on e-Learning (EJEL) 2 (2004).
- [20] Gallaher, J., Kanfer, A., La Fleur, J., Wang, C., Waight, C. and Wentling, T.L. (2000). *E-Learning – A Review of Literature*. Knowledge and Learning Systems Group, University of Illinois. at the Urban Champaign September, 2000.
- [21] Gehrke, M., Mayer, M. and Schafer, W. “An Architectural Framework for distributed E-Learning Systems”. Software Engineering Group, Institute of Computer Science at the University of Paderborn, Germany. <http://www.campussource.de/org/projects/>. (Accessed August 27, 2008).
- [22] Govindaraju, P. and Kumar, C.J. (2008). “Applications of ICTs in Virtual Universities”. UNESCO: ICT-in-Education Online Community <http://www.unescobkk.org/forum/education/ict/download.php?id=25&sid=874275d101862a18ab1.89a662a3aa748>. (Accessed February 18, 2008).
- [23] Grobler, C.P. (2003). *A Model to access the information Security status of an organisation with special reference to the policy dimension*. Magister Philophae work, Faculty of Natural Science at the Rand Afrikaans University, South Africa.

- [24] Grobler , T. and Louwrens, B. (2005). “New Information Security Architecture”. In: *Proceedings of ISSA2005 New Knowledge Today conference, 29 June-1 July, 2005, Sandton, South Africa.*
- [25] Harwood, I. and Warburton, B.I. (2004). “Thinking the Unthinkable: using project risk management when introducing computer Assisted Assessments”. In: *8th International Computer Assisted Assessment (CAA) Conference, 6-7 July 2004, Loughborough, UK .*
- [26] Hone, K. (2004). *The Information Security policy: An Important Information Security Management Control.* M.Com work, Faculty of Economic and Management Science at the Rand Afrikaans University, South Africa.
- [27] Horne, T. and Naude, E. (2006). “Cheating or Collaborative work: does it pay?”. *Issues in Informing Science and Information Technology.* 3 (2006):459-466 an University, South Africa.
- [28] ISO/IEC1779:2005(E) Information Technology – Security Technique - Code of Practice for Information Security Management.
- [29] ISO27K Information Security Management (2007). “Top Information Security risks for 2008. ISO 27001 Security Home”. [http://www.iso27001security.com/Top\\_information\\_security\\_risks\\_for\\_2008.pdf](http://www.iso27001security.com/Top_information_security_risks_for_2008.pdf). (Accessed September 30, 2008).
- [30] IS Series Information Systems (2008). “Security IS Services Information Systems”. University of California. <http://www.ucop.edu/ucophome/policies/bfb/is3.pdf> (Accessed February 27, 2009).
- [31] IT Governance Institute. (2006). “Information Security Governance: Guidance for Boards of Directors and Executive Management”. 2<sup>nd</sup> Edition, United State of America. <http://isaca.org/ContentManagement/ContentDisplay.cfm?ContentID=34997> (Accessed Feb 14, 2009).

- [32] Johnson, E.C. (2006). "Awareness training, Security awareness: switch to a better programme". Network Security.2006, 2(2006):15-18.
- [33] Jordaan, A. (2004). *An information security policy Architecture with special reference to a tertiary institution*. M.Phil. work, Faculty of Science at the Rand Afrikaans University, South Africa.
- [34] Karyda, M., Kiountouzis, E. and Kokolakis, S. (2005). "Information Security policies: a contextual Perspective". Computer and Security. 24, 3(2005):246-260.
- [35] Kritzinger, E. and Von Solms, S.H. (2006). "E-Learning: Incorporating Information Security Governances". Issues in informing Science and Information Technology. 3, (2006):319-326.
- [36] Levy, Y. and Remim, M.M. (2007). "A Theoretical Approach for Biometrics Authentication of e-Exam". Nova South Eastern University. [http://telem-pub.openu.ac.il/users/chais/2007/morning\\_1/M1\\_6.pdf](http://telem-pub.openu.ac.il/users/chais/2007/morning_1/M1_6.pdf). (Accessed March 30, 2008).
- [37] Moodle.(2008). "Moodle: Open Source Community based tools for learning". <http://moodle.org/>.(Accessed February 10, 2008).
- [38] Nickolov, E. and Nickolova, M. (2007). "Threat Model for User Security in E-Learning Systems". Information Technologies and Knowledge.1 (2007):341-347.
- [39] Raymond, L. and Roy, A. (2008). "Meeting the Training Needs of SMEs:is e-Learning a Solution?". Electronic Journal of e-Learning (EJEL).6, 2(2008):89-98.
- [40] Rice,W.H. (2006). *Moodle E-Learning Course Development: A complete guide to successful learning using Moodle*. Birmingham, UK: Packt Publishing Ltd.
- [41] Rivest, R.L. (2000). "Chaffing and Winnowing: Confidentiality without encryption". CryptoBytes(RSA Laboratories) 1, No.1(2000):12-17.

- [42] Schlaff, R. (1998). ‘Confidentiality using Authentication’. *Cross Roads: The ACM Student Magazine*, Winter, 1998, Issue 5.2
- [43] Smith, J. (2008).”Literature Review on the use of E-learning for Healthcare Practitioners”. South West E-Learning. [www.swel.nhs.uk/documents/litreview.doc](http://www.swel.nhs.uk/documents/litreview.doc), (Accessed May 20, 2008).
- [44] Suilleabhain, G.O. (2003). *Principles, structure and framework of e-learning*. MScEcon Wok, DEIS Department for Education Development at the Cork Institute of Technology, Ireland.
- [45] SunTrust Equitable Securities (1999). “E-Learning and Knowledge Technology”. <http://www.intered.com/extra/papers/techknow4.pdf>. (Accessed January 10, 2008).
- [46] Von Solms, B. (2001). “Corporate Governance & information Security”. *Computer & Security*, 20, No.3 (2001):215-218
- [47] Von Solms, B. (2001). “Information Security – A Multidimensional Discipline”. *Computers and Security*, 20, No.6 (2001):504- 508.
- [48] Von Solms, S.H. (2005). “Information Security Governance in ICT based Educational systems”. In: *Proceeding of the 4<sup>TH</sup> International Conference on ICT and Higher Education*, 28-30 September, 2005, Bangkok, Thailand, (pp.109-119).
- [49] Wikipedia.(2008). Wikipedia: the free encyclopedia. [http://en.wikipedia.org/wiki/Learning\\_management\\_system](http://en.wikipedia.org/wiki/Learning_management_system) (Accessed April 11, 2008)
- [50] Wolmarans, A. (2003). *Implementation an Effective Information Security Awareness Program*. M.Sc work, Faculty of Science at the Rand Afrikaans University, South Africa.