
Sorene Assefa1 and Prof. Von Solms2

1 Academy for Information Technology, University of Johannesburg, P.O. Box 524, Auckland Park, Johannesburg, 2006, South Africa, soreneas@yahoo.com, 200605244@student.uj.ac

2 Academy for Information Technology, University of Johannesburg, P.O. Box 524, Auckland Park, Johannesburg, 2006 South Africa, 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.


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
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 the 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 on 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 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 on 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 activity 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 that 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 counter measures 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 counter measures 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\textsuperscript{1}

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 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.

\textsuperscript{1} The six Information Security Services:
- **Identification and Authentication** ensures only authorized (legal) users are allowed access to an e-LMS environment \cite{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 \cite{7}.
- **Confidentiality** ensures that the content of the information during storage and transmission are protected from unauthorized access and disclosure \cite{1, 7 and 9}.
- **Integrity** ensures that the content of the information during storage and transmission are protected from unauthorized alteration or change \cite{7}.
- **Non-Repudiation** ensures that accountability for the execution of any action on the e-LMS is enforced \cite{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 \cite{6}. 

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

**3.1. Requirements for the ISRFe-LMS components**

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

An 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 as well verifies compliance to the e-LMS information security Policies and Procedures.

<table>
<thead>
<tr>
<th>An e-LMS should have a defined monitoring mechanism. Some of the common elements of Information Security Mechanisms for the e-LMS are:</th>
</tr>
</thead>
<tbody>
<tr>
<td>● An e-LMS must have an information security monitoring mechanism to determine where the defined information security policies and procedures are enforced;</td>
</tr>
<tr>
<td>● An e-LMS must have a mechanism that measures the level of user awareness; and</td>
</tr>
<tr>
<td>● An e-LMS must have a mechanism to determine if the ISG is enforced throughout the system.</td>
</tr>
</tbody>
</table>

3.1.5. Technical dimension

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.

\[\text{2 The Information Security Mechanisms for the six Information Security Services [6, 8 and 24]:}\]

- 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.
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.

References