CHAPTER V

DISCUSSION AND CONCLUSION

5.1 INTRODUCTION

With the advancement of information and communications technologies and increasing accessibility to the Internet, Institutions become vulnerable to both insiders and outsiders threats. A danger is a portrayal of a potential undesirable occurrence. Data systems are continually presented to different sorts of threats, and these threats can bring about distinctive sorts of harms, which might lead to significant financial losses. Sizes of these harms can extend from little lapses, which just damage the trustworthiness of databases, integrity, confidentiality, availability, to those that devastate entire computer centers. Thus protecting assets from these threats becomes a major concern for toward both people and Organizations. Dangers originate from distinctive sources, for example, employees' activities, mistakes in data entry or hacker's attacks.

5.2 DISCUSSION

There were three Research Objectives (RO) followed by three Research Questions (RQ) that have been tested during this study. All these research objectives have been achieved as discussed below.

RO1: To identify the information security threats faced by GOALS in USIM.

This objective has been achieved when RQ1 has been answered that is; Technological threats is the type of information security threats faced by GOALS in USIM. Technological threats here involves interruption to access the system by lecturers and students due to poor bandwidth, server problem and other reason. Then, it also involves interception to the system that disable or disconnect lecturers or students when they upload or download files in the system, and also when student conduct quiz or test.

RO2: To conduct information security risk assessment for GOALS in USIM.

This objective has been achieved when RQ2 has been answered that is; Risk assessment method proposed by Rausand (2013) has been chosen as information security risk assessment for GOALS in USIM.

RO3: To propose remedies for information security threats faced by GOALS in USIM.

This objective has been achieved when RQ3 has been answered that is; Access control using firewall (as proposed by Barik and Karfoma, 2012) has been chosen as remedies for information security threats faced by GOALS in USIM. A firewall is a blend of equipment and programming security system secured to avert unapproved access to a corporate system from outside the organization.

5.3 CONCLUSION

This research studied Information Security Risk Assessment of E-learning System on Global Open Access Learning System (GOALS) in Universiti Sains Islam Malaysia (USIM). The objectives of this research were to conduct risk assessment in order to

determine information security threats faced by GOALS in order propose remedies to overcome those threats. Results showed that Technological threats is the type of information security threats faced by GOALS in USIM. It involves interruption to access the system by lecturers and students due to poor bandwidth, server problem and other reason. Then, it also involves interception to the system that disable or disconnect lecturers or students when they upload or download files in the system, and also when student conduct quiz or test. Access control using firewall, as proposed by Barik and Karforma (2012) has been chosen as remedies for information security threats faced by GOALS in USIM. It is hope that through this research will help to identify information security threats faced by GOALS so that appropriate measures can be taken overcome those threats.

5.4 FUTURE WORK

It is suggested for future work that the population of risk assessment for GOALS in USIM being expanded to lecturers and students to obtain more accurate results on risk assessment of GOALS e-learning system.