Design and Emergence of a Pedagogical Online InfoSec Laboratory as an Ensemble Artefact

Sarfraz Iqbal
Department of Computer Science, Electrical and Space Engineering
Luleå University of Technology
Luleå, Sweden
sarfraz.iqbal@ltu.se

ABSTRACT

Information security (InfoSec) education becomes increasingly important. Building hands-on capabilities to tackle challenges is a precondition to mitigate and eliminate cyber threats. Existing studies, however, show that the field lacks pedagogically founded information security laboratories that can be used flexibly to educate both on-campus and online learners. To address this issue, this paper reports on an online InfoSec laboratory. Development of the laboratory follows an action design research approach. For this purpose, initial design principles were used that are derived from the existing pedagogical theories such as Conversational Framework, Constructive Alignment, and Personalized System of Instruction, literature reviews and empirical data. Through iterative cycles of building, intervention, and evaluation of an InfoSec laboratory, and side-by-side critical reflections, this study refines the conceptual model of an online InfoSec laboratory and initial design principles and provides general guidelines on the process of establishing a pedagogically underpinned online InfoSec laboratory for hands-on exercises. This study contributes by serving two major purposes. First, this study proposes a conceptual model of an online InfoSec laboratory that comprises important entities: Laboratory Infrastructure, Exercise (document), Exercise Processing and Management Interface (EPI), and Concrete Exercise Interface. Secondly, the research proposes design principles for implementing a conceptual model of an online InfoSec laboratory in different educational contexts.

Keywords: Security, Online education, Online laboratory, Action design research, Personalized system of instruction (PSI)

1. INTRODUCTION

Information security has been recognized as a core subject in the Information Systems (IS) curriculums (Ayyagari and Tyks, 2012; Reid and Van Niekerk, 2013). Online learning has gained popularity (Allen and Seaman, 2010; Liu and Burn, 2007; Rodriguez, 2012) in the education sector. Accordingly, to fulfill the growing need for information security specialists, many institutes, including XYZ University, offer a Master's program in information security for both on-campus and online education. Online education brings unique challenges, (Allen and Seaman, 2010; Hentea, Dhillon, and Dhillon, 2006; Rodriguez, 2012) such as how to design a course that can impart theoretical and practical knowledge, while the students are located in different places and time zones. The availability of an efficient learning management system can resolve the issues of providing equal access to course material and submitting course assignments. However, the issues of arranging hands-on information security exercises remain a dilemma for online learners due to time, space, and bandwidth constraints. Hands-on education requires that online learners be given access to an online information security laboratory. However, there are many challenges in the design, development and implementation of an online InfoSec laboratory such as issues of accessibility to the laboratory resources, secure communication, minimizing student-introduced security risks, isolating the InfoSec laboratory, scalability of the laboratory, pedagogical alignment of laboratory activities, providing an easy to use interface, tackling issues regarding back-up and recoverability, providing remote access, and issues regarding configuration (Chen, Chen, and Chen, 2011; Choi, Lim, and Oh, 2010; Tikekar and Bacon, 2003; Yang et al., 2004). The XYZ University could not adopt a ready-made model of a pedagogical online InfoSec laboratory due to the lack of such pedagogically founded laboratory concepts. Hence, this study focused on the question of how to design a pedagogical online InfoSec laboratory for hands-on education.

The absence of explicit pedagogical approaches and design principles for online InfoSec laboratories hinder the accumulation of rigorous technical and pedagogical knowledge. Likewise, the existing tool view of the online InfoSec laboratory often does not consider the important building blocks or entities of the laboratory, the relevant stakeholders, and the interrelationships of these entities. A laboratory cannot be taken for granted as a black box tool. Hence, this study proposes an ensemble perspective (Orlikowski and Iacono, 2001) to design and develop an online InfoSec laboratory. The ensemble view provides understanding of the complex and fragmented emergence of the laboratory as a socio-technical system. Ensemble means collection of things considered as whole. Ensemble artefact means that all the parts of an IT artefact are considered together in a bundled form (Goldkuhl, 2012; Sein et al., 2011). Ensemble view emphasizes the dynamic interactions between people and technology and thus leads towards development of an ensemble artefact (Orlikowski and Iacono, 2001; Sein et al., 2011).

This study concurs on the issue of understanding the nature of online InfoSec laboratories as ensemble artefacts to understand many of their critical implications both intended and unintended, for individuals, groups, organizations, and society (Orlikowski and Iacono, 2001; Sein et al., 2011). Hence, conceptualizing and developing the online InfoSec laboratory as an ensemble artefact will help to develop a pedagogical design model that is usable, scalable, and adapts to different educational contexts for various exercise scenarios in the field of information security. IS research has two missions: to provide assistance to solve the current problems and to anticipate problems of practitioners and also to make theoretical contributions (Benbasat and Zmud, 1999; Iivari, 2003; Rosemann and Vessey, 2008; Sein et al., 2011). Thus, the researcher argues that theorizing IT artefacts, such as the online InfoSec laboratory, is significant as regards understanding their meanings, capabilities and uses, their multiple, emergent, and dynamic properties, as well as the recursive transformations occurring in the various social worlds in which they are embedded (Orlikowski and Iacono, 2001).

The current work builds on a prior research phase (Iqbal, 2013; Iqbal, Awad, and Thapa, 2014; Iqbal et al., 2015; Iqbal and Päivärinta, 2012; Iqbal and Thapa, 2013) in order to (a) design and carry out an intervention in courses at XYZ University, and (b) to reflect on the conducted work and systemize knowledge for the contribution to design knowledge in the area of hands-on information security education. The research approach adopted in this study is action design research (ADR). ADR leads to conceptualizing the IT artefacts as ensembles, a result of an emergent perspective on design, use and refinement in context through continuous interaction between technology and organization during the design process (Sein et al., 2011). Pilot design and testing of laboratory and related exercises has led the researcher to derive four important entities of the laboratory and a set of design principles (Iqbal and Thapa, 2013; Iqbal et al., 2015). Pedagogical kernel theories such as Constructive Alignment (Biggs, 1996), Conversational Framework (Laurillard, 2002), and the Personalized System of Instruction (PSI) (Keller, 1968) guided the research process to derive initial design principles used to build the laboratory.

The rest of the paper is organized as follows: Section 2 discusses related research. Section 3 describes the methodology. Section 4 describes the research context, which includes a brief background, problem formulation and summary of the Building, Intervention, and Evaluation (BIE) phase - 1 & 2. Section 5 discusses the process of laboratory design and development through the ADR phase of BIE-3 in detail. Section 6 discusses the contribution and concludes the paper with a future research agenda.

2. RELATED RESEARCH

An initial literature review (Iqbal and Päivärinta, 2012) revealed that cost-effective features of virtual technologies play an important role in making the virtual laboratories popular. The fact that the security equipment, both hardware and software, is expensive makes it very challenging for educational institutes to build and maintain their information security laboratories (Iqbal and Päivärinta, 2012). This situation has led to development of server virtualization platforms. Existing literature reveals a broad variety of servers, operating systems and virtualization techniques (Burd et al., 2011; Gaspar et al., 2008; Krishna et al., 2005; Lahoud and Tang, 2006; Li, Toderick, and Lunsford, 2009; Summers and Martin, 2005; Wang, Hembroff, and Yedica, 2010). However, descriptions of explicit design methods or pedagogical approaches adopted to design and develop laboratories and related exercises are ignored largely.

In the later stage of the project, pilot design and testing of the laboratory and exercises led to the development of a conceptual model of an online InfoSec laboratory. The conceptual model comprises a few important entities of an online InfoSec laboratory, i.e. Laboratory Infrastructure, Exercise, Exercise Processing and Management Interface (EPI) and Concrete Exercise Interface (Iqbal et al., 2015). The problem and solution are continuously evaluated in the ADR process. A second literature review was therefore conducted whilst keeping the conceptual model of an online InfoSec laboratory as a guiding framework. Existing literature on the online information security laboratory was examined in light of the four identified entities of an online InfoSec laboratory. The articles selected for this study were also analyzed for the use of pedagogical approaches.

The literature search was conducted by using key words: "information security laboratory," "online information security lab," "information security curriculum," "virtual information security lab," "information security education," and "information security pedagogy." This search produced more than 600 articles. After initial scrutiny, 270 relevant articles were selected for further analysis. After careful examination of the articles, 29 relevant articles were found that specifically discussed information about the security laboratory concept in an online context. The articles that discussed the campus-located or isolated laboratory concepts without remote access, as well as purely curriculum-related discussions, were omitted.

The literature review revealed that only five articles incorporated general discussions on all four information security laboratory entities (Anderson, Joines, and Daniels, 2009; Krishna et al., 2005; Lahoud and Tang, 2006; Willems and Meinel, 2011). Many exercises are mentioned in the reviewed articles but the articles rarely provided any details on the elements of curriculum and rationale behind the chosen laboratory exercises. The issues of pedagogical alignment of course goals, program goals and the use of pedagogical approaches to support the design and development of InfoSec laboratory exercises were mostly ignored. The lack of a systematic approach in design, development and implementation of online InfoSec laboratories was noticeable due to the absence of an explicitly defined scientific method or design theory. Such a situation also raises concerns about the validity of the claims regarding the utility and effectiveness of the proposed solutions. Concepts such as constructionist learning theory (Uludag et al., 2012), zone of proximal development (Nestler and Bose, 2011), offensive teaching approaches (Willems and Meinel, 2012) and cooperative learning strategies (Chen et al., 2011) are mentioned, yet in most cases there was no demonstration of how these concepts were actually implemented in the exercises' design.

Orlikowski and Iacono (2001) propose that the researcher community should theorize about the IT artefacts explicitly and incorporate those theories into their studies to enhance the contribution of their research work. They propose five meta-categories to conceptualize the technology: the tool view, the proxy view, the ensemble view, the computational view and the nominal view. This research focuses on the ensemble view of the online InfoSec laboratory. The ensemble is defined as a "web of equipment, techniques, applications, and people that define a social context including the history of commitments in making up that web, the infrastructure that supports its development and use, and the social relations and processes that make up the terrain in which people use it" (Orlikowski and Iacono, 2001 p. 122). Moreover, four variants to conceptualize the ensemble view are described that focus on the dynamic interactions between people and technology whether during construction, implementation or use in organizations or during the deployment of technology in society at large (Iqbal et al., 2015; Orlikowski and Iacono, 2001). The four variants are technology as development project, technology as production network, technology as embedded system, and technology as structure. Two conceptualizations among the four variants of the ensemble view focus primarily on the ways in which technologies come to be developed with a secondary emphasis on use and two conceptualizations focus primarily on how technologies come to be used in certain ways with a secondary emphasis on development.

The primary focus in this research is on the conceptualization of online InfoSec laboratories and the ways in which laboratories come to be developed with a secondary emphasis on use of laboratories to enhance hands-on education. The research focuses on the ensemble view of online InfoSec laboratories from the perspective of technology as development project. This research explores the conceptual foundations of an online InfoSec laboratory in terms of a generalized model describing its building blocks, examines the roles of key stakeholders in the development process and how such roles influence the design in different ways and the influence of inclusive methodology on the development process.

3. METHOD

This project adapts the ADR approach. ADR is appropriate for research projects where the goal is to conceptualize an ensemble IT artefact as a result of an emergent perspective on design, use, and refinement in context through continuous interaction between technology and organization during the design process. This section briefly describes the stages of ADR.

Problem formulation: The ADR approach (Sein et al., 2011) mainly deals with two challenges:

1. Addressing a problem situation encountered in a specific organizational setting by intervening and evaluating. For instance, this research project was triggered when teachers encountered poor hands-on education, while there was also a need to develop an online InfoSec laboratory for online education in information security and a need to enhance e-learning platforms.
2. Constructing and evaluating an IT artefact that addresses the problems typified by the encountered situation.

Building interventions and evaluation: The early design of an IT artefact, based on the premise of a problem formulation stage, is further shaped by organizational intervention and subsequent design cycles. The problem and the artefact are continuously evaluated and the design principles are developed during the building, intervention and evaluation (BIE) phases.

Reflection and learning: The reflection and learning phase helps to adjust the research process, and is based on the early evaluation results in order to reflect the increased understanding of the ensemble artefact being developed.

Formalization of learning: Researchers should outline the achievements from the artefact, and describe the organizational results in order to formalize the learning. The knowledge gained through the design, development and use of the artefact in this context is utilized to develop generalized solution concepts for a class of field problems.

Evaluation Strategy: Evaluation of the design artefacts and design theories is considered a central activity in Design Science Research (DSR) (Gregor and Jones, 2007; March and Smith, 1995; Sein et al., 2011; Vaishnavi and Kuechler, 2004; Venable, Pries-Heje, and Baskerville, 2014; von Ala et al., 2004). Venable, Pries-Heje, and Baskerville (2014) proposed a framework for evaluation in DSR (FEDS), which comprises four steps: explicate the goals, choose the evaluation strategy or strategies, determine the properties to evaluate and design the individual evaluation episode. This research adopted the FEDS framework to evaluate the online InfoSec laboratory.

The goals for the online InfoSec laboratory were that it should be flexible, usable, scalable and adaptable in different contexts for different exercise scenarios. The Human Risk & Effectiveness evaluation strategy was selected for this research work (Venable, Pries-Heje, and Baskerville, 2014). The Human Risk & Effectiveness evaluation strategy emphasizes formative evaluations earlier in the process with artificial, formative evaluations, which progress quickly into more naturalistic formative evaluations. The summative evaluations that come at the end of this strategy focus on evaluating the effectiveness of the artefact, which means that the utility benefits of the artefact will continue to accumulate over the long term, even when the artefact is put into operation in real organizational situations (Venable, Pries-Heje, and Baskerville, 2014). In this research, the properties of the IT artefact, i.e. the online InfoSec laboratory, were subjected to evaluation in order to assess its applicability, usability and efficacy. The consequent laboratory exercises that were developed for online learners were also intended to be usable, reliable and to stimulate flexible learning.

The evaluation of the intervention when using an ADR method is an on-going process and takes various forms. This process included interviews with the stakeholders in the online InfoSec laboratory, observation, presentations at departmental workshops/meetings where future planning regarding the laboratory design and development was also discussed, and obtaining feedback from all participants. Feedback was also obtained from the students via a survey questionnaire and learning diaries. The work related to the design and development of the online InfoSec laboratory was presented on different occasions at department meetings and workshops, which was very useful in terms of receiving feedback from all the relevant stakeholders during the research process. The researcher noted comments from discussions, which further refined the design of the laboratory. In addition to feedback, these open presentations in the department helped to secure funding from the upper management for this project. For example, acquiring a separate room facility was a great challenge. The small quantity of equipment bought at the start of this project was placed in the developer's room. Later on, the program's management team agreed to provide a bigger laboratory facility to develop the laboratory's infrastructure. Furthermore, the presentations helped to form an ADR team at the program level. The researcher was able to analyse helpful comments from different meetings and this resulted in a sense of engagement for different stakeholders.

Henceforth, this article will describe the online InfoSec laboratory project focusing on details of the BIE phase using the laboratory entities and design principles to further enhance the academic understanding related to the design and development of online InfoSec laboratories.

4. RESEARCH CONTEXT: ONLINE INFOSEC LAB PROJECT

4.1 Problem Formulation

XYZ University has offered an MSC program in information security since 2007 both on-campus and through online education. The problem formulation stage began with a needs assessment activity through interviews and pedagogical analysis of courses in the information security Master's program. The results revealed that the percentage of online students enrolling in different courses on information security had recently increased (75-80% online learners on every course), but most of these online learners left without completing the courses for various reasons. A majority of the students complained about the lack of hands-on exercises. The absence of an InfoSec laboratory was considered to be the major reason. The majority of the online learners were professionals who preferred to work and study individually when and where it suited them (Iqbal and Thapa, 2013). Perusal of the strategic planning documents and interviews with the management personnel provided a clear organizational perspective regarding research and education in the IS department. The program's management team was also interested in finding ways to facilitate individual and flexible learning to support students' learning preferences. The IS department wanted to improve the information security graduate program by specifically focusing on the hands-on education of students. Together, the researcher and the program management team suggested that they develop an effective and meaningful e-learning program for both online and on-campus students, while at the same time focusing on the design and development of an online InfoSec laboratory. The laboratory should enable students to practice their security skills flexibly from anywhere, in accordance with the practical demands of the courses (Iqbal and Thapa, 2013). The review (Iqbal and Päivärinta, 2012) showed that mostly technical implementations were targeted in the literature while the pedagogical elements of the curriculum and the rationale behind them were ignored. None of the reviewed articles demonstrated design theory or design method trailed for the design, development and implementation of online InfoSec laboratories. The search results further suggested that there is a general absence of systematically founded design principles for pedagogical online InfoSec laboratories.

To contribute to filling this knowledge gap, an initiative was taken to design and develop a pedagogical online InfoSec lab. Following an ADR method, the principles of practice-inspired research and theory-ingrained artefact were implemented. Practice-inspired research principles focus on viewing the field problems as knowledge creation opportunities (Sein et al., 2011). The problems faced by the IS department at XYZ University included lack of hands-on exercises, the absence of an online InfoSec laboratory, the need for a flexible e-learning system, an absence of pedagogical approaches when teaching information security, and mastery of course topics. ADR pursues these opportunities at the intersection of technological and organizational domains.

The theory-ingrained artefact principle emphasizes that the ensemble artefacts created and evaluated via ADR are informed by theories. To follow this principle, a theoretical framework consisting of constructive alignment theory (Biggs, 1996) and conversational framework (Laurillard, 2002) was proposed to analyze existing e-learning resources and the courses in the information security program (Iqbal, 2013). The theories, i.e. constructive alignment and conversational framework, have their advantages and limitations. For instance, constructive alignment presents a holistic view of course development that guides the instructional designer or teacher, from stating the course objectives to properly aligning the course objectives with intended teaching/learning activities and suitable assessment methods. However, it does not provide any specific guidelines as regards the media to be used for communication and interaction between teachers and students in the classroom. The conversational framework on the other hand discusses in detail the media types to be used during teaching. Hence, after analyzing the existing e-learning platform, the theoretical framework suggested categorizing Learning Management System (Fronter) for interactive purposes and Virtual classroom (Adobe Connect Pro) for communicative purposes. Existing e-learning media is used for interactive and communicative purposes such as accessing course materials, submitting assignments, and conducting live lectures and seminars. However, productive media was not available. It was therefore suggested that the online InfoSec laboratory could be developed for productive purposes, to provide InfoSec students with the media to implement security solutions to test and improve their security skills. Keeping in mind the strategic objectives and practical demands of the future related to provision of hands-on exercises in the different courses of an information security program, a road map in the form of a framework to develop and implement an online InfoSec laboratory was proposed (Iqbal and Thapa, 2013). The framework proposed to proceed with this research work suggested that the technological, pedagogical, and organizational goals interact during the design of an online InfoSec laboratory.

Overall research was conducted in three BIE iterations. This article explains the third iteration in detail, whereas a summary of the previous two iterations is provided below.

4.2 Summary of BIE Phase 1

In this phase of BIE, an ADR team was created that included researcher, developer, IT personnel at the university, assistant teacher, and practitioners such as teachers on the courses in server security architecture and information security (Appendix A) who agreed to take part in the project to pilot test the building and implementation of an online InfoSec laboratory in their courses. The literature review, interviews, observations and reflections on the pedagogical approach, i.e. Personalized System of Instruction (PSI) (Keller, 1968) to develop an online InfoSec laboratory, together led the researcher to formalize five initial design principles (contextualization, collaboration, flexibility, cost-effectiveness and scalability) (Iqbal and Thapa, 2013). These principles were followed later in building the online InfoSec laboratory to intervene in the course on server security architecture. The organizational and course goals demanded that the online InfoSec laboratory should provide remote access to online students from anywhere in the world. For instance, utilizing the contextualization principle, the contextual requirements were gathered from different sources such as organizational goals, course goals, and pedagogical requirements. The collaboration principle was used as a means to motivate all the stakeholders (including researcher, developer, IT staff, and teacher) by arranging regular meetings to prepare an appropriate design for the online InfoSec laboratory and related exercises. The BIE form selected was an IT-dominant BIE that allows the continuous instantiation of an IT artefact in different contexts. A few laboratory assignments for hands-on practice were prepared, including network topology configuration and firewall configuration and testing. These assignments were implemented in the server security architecture course with the students. The design of the online InfoSec laboratory dealt with different issues such as flexibility in terms of availability and accessibility, scalability and robustness.

The ADR method suggests formative evaluation during preparation of the alpha version. The initial version of the online InfoSec laboratory was therefore tested by the development team to reveal its weaknesses at an early stage and correct them before launching the system for testing by the students. During the laboratory development and alpha testing process, it was found necessary to make the laboratory robust to ensure that students could not damage laboratory configurations. The principle of robustness (that emerged during BIE) was therefore applied. By considering the robustness principle, the laboratory should be able to handle any inappropriate student activity that may damage laboratory software or hardware facilities. The robustness issue could also be managed by providing the students with clearly stated, step-by-step assignments, monitoring student behavior, and building back-ups of the working configurations. During the implementation phase of the ADR process, end-users (teachers, assistant teachers and students) were involved in the process for experience and the beta version of the online InfoSec laboratory was deployed in the course. The formative evaluation conducted at this stage was more naturalistic as the laboratory was deployed in the course with the real students (Venable, Pries-Heje, and Baskerville, 2014). The functionality of the online InfoSec laboratory was observed and tested with students, teacher and assistant teacher. A survey questionnaire (Appendix B) was developed to obtain feedback from students for evaluation purposes. The feedback received from 30 students highlighted the fact that there were some disconnections faced by the students during their work on exercises. Students mentioned some discrepancies such as: “the exercise document was not easy to understand, needs more clarification.” The students considered the laboratory a usable learning medium for online hands-on education. One of the students wrote, “The exercises provided added value to the course.” The flexible approach based on the pedagogical criteria of PSI to access the higher-level course modules, including laboratory exercises, was also appreciated. The critical reflections of the other stakeholders, including the teacher, showed that it was slightly early to implement the laboratory in the course. Hence, the design, development and implementation process was quick and could not provide real understanding about important building blocks of an online InfoSec laboratory. The stakeholders were also not content with their roles, which were not properly identified during this process. The stakeholders therefore jointly suggested conducting a pilot test of an exercise with test users instead of directly implementing the exercise in the course.

The first iteration involved building of the online InfoSec laboratory, and intervention in a pilot course on server security architecture through implementation and evaluation of its effect. The iteration generated six design principles (Table 1).

Design Principle	Description
Contextualization	Contextual factors need to be obtained from organizational goals, course goals, teacher goals, constraints, and requirements. Pedagogical approach.
Collaboration	Regular meetings should be held between different laboratory stakeholders for design, development, and implementation purposes. Researcher (acts as instructional designer), practitioners (developer, IT staff) end users (teachers, assistant teacher, students).
Flexibility	Remote access to laboratory resources. Laboratory activities should be modularized. Laboratory should be accessible without interruption to students preferably 24/7 or at least when a student books a particular time for laboratory activities.
Cost-effectiveness	Optimal resource allocation to develop the laboratory. Virtual technologies can be utilized to keep expenses low.
Scalability	Laboratory can be upgraded and easily modified based on the practical requirements of different courses.
Robustness (emerged principle)	Handle inadvertent damage by users. Quickly recover configurations. Prepare back-ups of assignment configurations.

Table 1: Design principles for Online InfoSec Laboratory (Iqbal et al., 2014)

4.3 Problem Redefinition

The pilot implementation of the online InfoSec laboratory and exercises in the server security architecture course opened up another important question. Is this all that laboratory stakeholders need to know about the online InfoSec lab? Several things needed more explanation, for example, the issue of important building blocks of the laboratory was not paid much attention. This was an initial experiment that informed the stakeholders about how to unfold the ensemble view of the online InfoSec lab. For instance, during the design, development, and implementation process of the online InfoSec laboratory many different stakeholders are involved in the entire process. These stakeholders also collaborate with each other on different occasions based on the contextual needs arising during the design and development process. In the same way, since design and development began, different actors have influenced and participated at different stages of the BIE process. This situation demanded that different entities of the online InfoSec laboratory should be described in more detail to understand the role of the different stakeholders in the design, development and implementation process of the laboratory and its related exercises. This situation led to further pilot testing and the implementation of the online InfoSec laboratory.

4.4 Summary of BIE Phase 2

Subsequently, in the next BIE phase 2, pilot design and implementation of an exercise using test users was conducted in the online InfoSec lab. This pilot testing provided more understanding of the whole procedure, from planning a laboratory exercise to designing and implementing a laboratory exercise in an online InfoSec lab. The teacher, assistant teacher, developer, researcher, two guest users (to test the system), and the IT support personnel participated and collaborated in this pilot testing. The information obtained during this pilot project enhanced knowledge of the laboratory stakeholders and a conceptual model of an online InfoSec laboratory was proposed (Iqbal et al., 2015). The conceptual model considers the laboratory to be an ensemble artefact comprising the following four intertwined entities:

- Exercise
- Exercise Processing and Management Interface (EPI)
- Laboratory Infrastructure
- Concrete Exercise Interface

In the second BIE iteration, a pilot exercise in the online InfoSec laboratory was constructed and evaluated using test users. The evaluation was formative but more naturalistic (Venable, Pries-Heje, and Baskerville, 2014) as the exercise was implemented in the laboratory in real time for test purposes. For instance, the pilot exercise “Firewall configuration and testing” was designed involving the relevant stakeholders, including, for example, teacher, assistant teacher, developers and test users. The evaluations of the online InfoSec laboratory and exercise at this point led to identifying the main entities of the laboratory and the stakeholders. Also in this iteration, the online InfoSec laboratory prototype was redesigned and a conceptual model of an online InfoSec laboratory (Figure 1) that identified the main entities, was designed, developed and described. The emergent knowledge based on the stakeholders’ reflections also helped to refine the initial design principles. Based on stakeholders’ learning and emergent knowledge, the design principles were mapped to particular entities. Each individual lab entity encompasses its own stakeholders and functionality and thus implies different design principles (see Table 2).

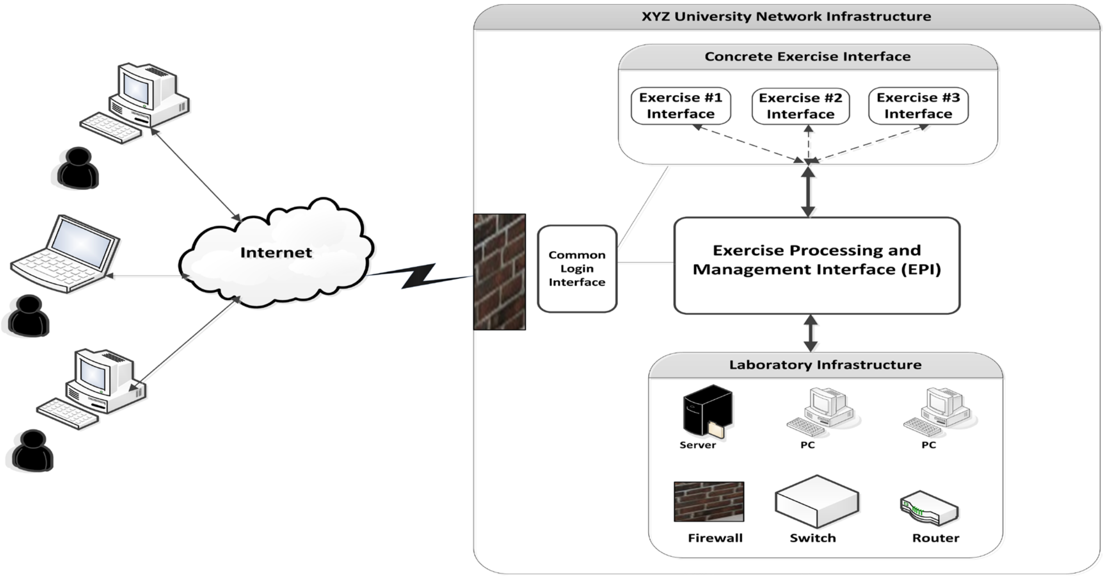
XYZ University Network Infrastructure
Concrete Exercise Interface
Exercise #1 Interface
Exercise #2 Interface
Exercise #3 Interface
Internet
Common Login Interface
Exercise Processing and Management Interface (EPI)
Laboratory Infrastructure
Server
PC
PC
Firewall
Switch
Router

Figure 1. Conceptual Model of an Online InfoSec Laboratory

Laboratory Entities	Design Principles
Exercise	• Contextualization based on course goals • Pedagogical alignment of laboratory activities • Flexible learning
Exercise Processing and Management Interface (EPI)	• Isolate the laboratory network • Flexible configuration management • Ease of remote access • Availability of laboratory resources • Collaboration
Lab Infrastructure	• Contextualization based on programme goals • Scalability • Easy configuration and reconfiguration • Back-up and Recoverability • Hardware integration • Cost-effectiveness
Concrete Exercise Interface	• User-friendly interface with properly arranged resources and targets • Easy to use • Tracking and debugging errors

Table 2. Outcome of the initial phase of implementation and evaluation using ADR (Iqbal et al., 2015)

5. BIE PHASE 3

5.1 Building and Intervention in an Information Security Course

5.1.1 Course info and requirement: The information security course is the first course of the Master's program. As the main stakeholders, the researcher and the teacher collaborated on designing the course so as to align practical and theoretical parts. The course was composed of the following teaching and learning activities and forms of assessments: lectures: individual study of the literature and reflection using learning diaries; interactive seminars after each lecture; individual theoretical assignments; practical laboratory assignments; supervision that included monitoring and feedback by the teacher and assistant teacher on laboratory assignments; case study discussion; and a final written exam.

5.1.2. Pedagogy applied: The pedagogical approach PSI (Keller, 1968) was utilized for the design of the information security course to further realize the course goals and begin the teaching/learning activities based on the course requirements. The course objectives were aimed at providing the students with an individual and flexible learning environment. The distinctive features of the PSI are as follows:

- Provide clear study objectives
- Division of course content into smaller modules/units
- Flexibility (study at your own pace)
- Mastery of the course unit/module
- Provide immediate feedback on each course unit/module
- Use of teacher, assistant/proctor

PSI helped to divide the course content into smaller modules. The initial ideas for designing and developing the online InfoSec laboratory were based on the PSI criteria of individual and flexible access to the laboratory resources from anywhere. The practical laboratory exercises were designed as related modules, which helped the students to master the course contents practically and strengthen their individual security skills.

5.1.3. Application of InfoSec laboratory assignments: By considering the initial design principles carefully, the laboratory stakeholders (researcher, developer, and teacher) worked in close collaboration to streamline the contextual requirements of the InfoSec laboratory to offer these hands-on exercises: 1) InfoSec laboratory access, 2) Data encryption at rest and 3) Network traffic monitoring. Moreover, in order to enhance the knowledge level of the students, the mastery of the course content feature of the PSI was put into action by designing the assignment tasks carefully and in such a way that the students were given low level assignments before they were ready to deal with the higher level assignments. Four individual written assignments were also prepared and delivered to students after they finished every laboratory assignment. It also helped the students to develop a deeper understanding of the theoretical and practical aspects of the course. The students were informed in the study guide that in order to proceed to the next assignment, they needed to finish the previous assignment and upload a report to the Fronter (learning management system) to get individualized feedback. The students were given the flexibility to proceed at their own pace, but in an effort to avoid procrastination, they were encouraged to follow the deadlines or leave the course voluntarily and join next time. Eventually, the laboratory design was prepared by applying a conceptual model of an online InfoSec laboratory and design principles (developed in BIE 2) following the ADR research method. In the next section, the researcher will explain the exercise on network traffic monitoring in detail to explain the laboratory's development using the conceptual model and design principles.

5.2 Network Traffic Monitoring

Figure 2 highlights the lab entities. The network traffic monitoring exercise is explained in detail below in light of the four lab entities.

The objective of this exercise is to enable students to collect and examine the network traffic using Wireshark. The students investigated the encrypted network traffic over encrypted connections. The design scenario used to conduct the exercise is as follows:

The foremost stakeholder for the exercise entity is the teacher. The teacher selected the network traffic monitoring exercise keeping the course goals in mind. The detailed exercise document was prepared with the help of an assistant teacher. The main stakeholder for the EPI entity is the laboratory developer, who is responsible for exercise processing and management. The teacher handed this document over to the developer to start the process of EPI entity. The developer selected the required resources such as a suitable server with enough physical storage and RAM capacity from the available resources in the laboratory infrastructure. The teacher and developer held various meetings to mutually agree on an exercise design based on the exercise requirements. Furthermore, the exercise document informed the developer that the teacher had chosen PSI for the underlying pedagogical approach. This required individualized, flexible access for end-users (students). During the process of concrete exercise interface development, the developer involved the other stakeholders in EPI, for example the IT department personnel so they could provide the necessary help regarding networking issues. The interrelationships of the different entities revealed that collaboration among the stakeholders was extremely important for quick processing and effective decision-making. The developer's careful examination of the available laboratory resources resulted in a suggestion to use virtual technologies, and all the stakeholders agreed to create virtual machines for individual students. Finally, the individual virtual machines were prepared for the students and the concrete exercise interface was developed. The students were granted individual access rights to their virtual machines. Students are the major stakeholders in the concrete exercise interface. They were provided with a written PDF or Word document of the exercise, which provided the necessary information on the steps involved to conduct the exercise successfully.

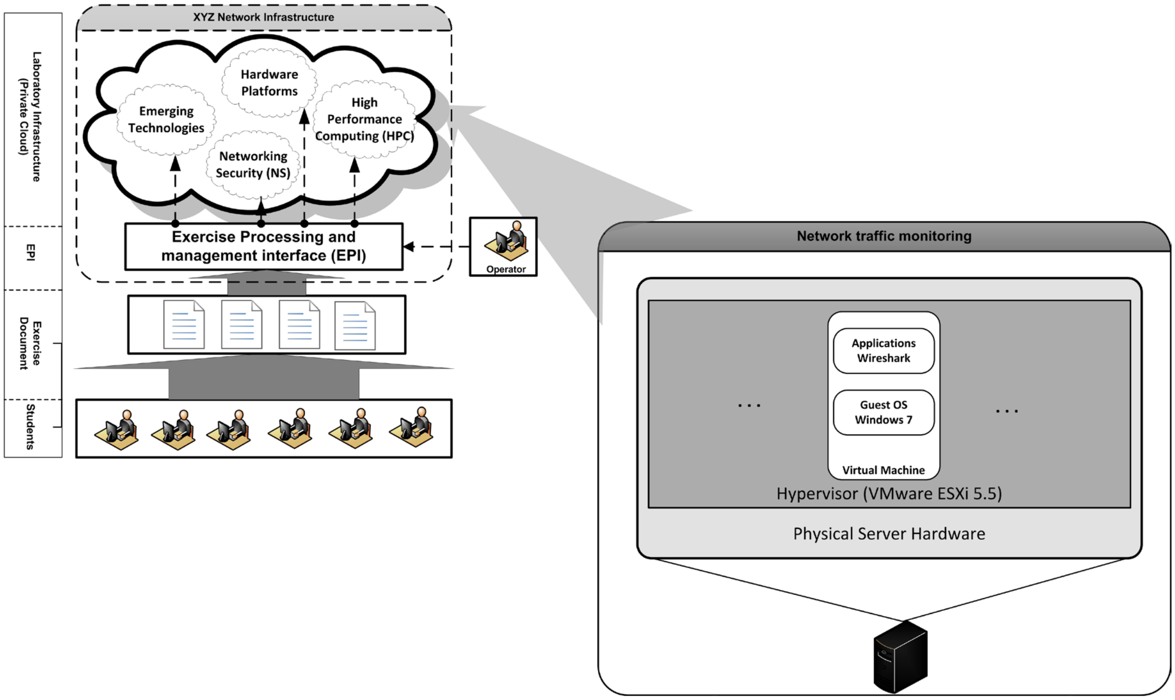
XYZ Network Infrastructure
Laboratory Infrastructure (Private Cloud)
Hardware Platforms
Emerging Technologies
High Performance Computing (HPC)
Networking Security (NS)
EPI
Exercise Processing and management interface (EPI)
Operator
Exercise Document
Students
Network traffic monitoring
Applications Wireshark
Guest OS Windows 7
Virtual Machine
Hypervisor (VMware ESXi 5.5)
Physical Server Hardware

Figure 2. Online InfoSec Laboratory Network Traffic Monitoring

The students used an ESXi 5.5 VMware vSphere Hypervisor client to connect to the university's server as part of their ESXi server operating system. The students were provided with log-in details (username and password) as a regular user and the IP address of the server in order to access their virtual machines (Windows 7 Enterprise 64-bit) desktop. This virtual machine is configured in such a way that it has access to the Internet. The first thing that the students did on their virtual machines was to install Wireshark. Wireshark is supported on all Windows, Mac, and Linux/Unix machines. Wireshark is available free of charge at www.wireshark.org. The students then downloaded the 32- or 64-bit version depending on which operating system was installed on their virtual machine. The installation of Wireshark includes installing WinPcap, which is the library that Wireshark uses to capture traffic. Once the student had successfully installed Wireshark, the default start-up screen for Wireshark appeared.

The next step was to start capturing the network traffic from the list of available devices. When the students tried to select a device using the "list the available capturing devices" function, the students were able to see their virtual Ethernet card in their virtual machine. The students were thus able to monitor their own traffic. Once the Ethernet card has been selected for monitoring network traffic, the packets (units of data) can be captured. Wireshark starts to detect the traffic; the packet capture window in Wireshark will display lines where each line represents a packet or unit of data that was sent over the network. Different columns in display windows provide the details about the source and destination, protocol type and number and time of packets captured during this process. Furthermore, in this exercise, the students learn how to monitor the different types of encrypted and unencrypted traffic.

5.3 Description of Design Principles

ADR generates abstract knowledge in the form of design principles. Its implications are twofold: first, to guide the process of building an IT artefact (InfoSec laboratory in this context) and second, to generalize the knowledge to a class of problems (such as developing a platform for hands-on exercises). In this section, the design principles for each laboratory entity are described in order to explain how the principles of each entity were used to formulate the laboratory according to the requirements of the particular context.

5.4 Design Principles' Implementation for Exercise

5.4.1 Contextualization based on course goals: The laboratory environment of the information security course was contextualized in the light of course goals. The network traffic monitoring exercise was planned to *enable the student's practical skills* in examining network traffic. This course served as the starting point for the Master's program; therefore, it was extremely important to train their cognitive skills for investigation of encrypted and unencrypted traffic over the network. As the main stakeholder, the teacher for this exercise entity decided to *allow the students to work individually on this exercise.* The time allocated for the exercise was 1 hour. The teacher and assistant teacher together decided that the assistant teacher would be available (via email & phone) during the entire duration of the exercise to provide any necessary help to the students.

5.4.2 Pedagogical alignment of lab activities: The theoretical and practical parts of the information security course were balanced in order to provide an effective course. The different practical lab activities, including the network traffic monitoring exercise, were selected to *strengthen the theoretical concepts*. The teacher aimed to train each student to have individual information security skills and therefore decided to use the PSI approach as the underlying pedagogical approach for the design of this particular exercise.

5.4.3 Flexible learning: The PSI approach (Keller, 1968) guided the teacher to divide the practical laboratory exercises into smaller modules. The modular approach is a good way to provide a *flexible mode of learning to students*. The students were provided with an exercise document to help them understand the exercise and proceed accordingly. The students were provided with remote access to laboratory resources in order to conduct the network traffic monitoring exercise through the use of the Hypervisor client so that the students could access the laboratory from anywhere using the Internet.

5.5 Design Principles' Implementation for EPI

5.5.1 Isolate the network: The technical support personnel put the two servers into a special section of network that could be accessed without interrupting the university network. The VMware vSphere client was used to give the students access to the virtual machines located in the online InfoSec laboratory. The students were given the main IP address of the server, a username and a password to connect to the InfoSec laboratory virtual machines.

5.5.2 Flexible configuration management: A virtual machine was prepared (Windows operating system was installed, security patches were applied and Windows was updated). This virtual machine was considered to be a reference virtual machine. The EPI developer created copies of the reference virtual machine manually, using ESXi commands over SSH to create several virtual machines in accordance with the course requirements.

5.5.3 Ease of remote access: The students used ESXi 5.5 VMware vSphere Hypervisor client to connect to the virtual machine. This client makes it very *easy for the students to access* the remote virtual machines located in the InfoSec laboratory. This client gives the students full access to work with the virtual machines.

5.5.4 Availability of lab resources: Ideally, the lab resources should be *available 24/7 during the course*. The initial arrangement was made in such a way that the lab resources were available for the students during the time slots that they had selected and booked with the help of the assistant teacher. The assistant teacher was also available via telephone and email to provide necessary support during the times when the students were remotely conducting the exercise. Similarly, the teacher was also available, in case of interruptions or any other problems that might arise during the exercise.

5.5.5 Collaboration: Initially, the teacher and assistant teacher *collaborated* to rationalize the exercise and to select a pedagogical approach. Once the exercise document was written as a step-by-step plan, the meeting with the developer who was responsible for exercise processing and management interface (EPI) took place. This was to further discuss the availability of resources and to develop the concrete exercise interface for individual students. The EPI developer and the other IT department personnel also held separate discussions and meetings to provide remote access to the lab resources and to isolate the lab from the rest of the network to avoid any damage.

5.6 Design Principles' Implementation for Lab Infrastructure

5.6.1 Contextualization based on programme goals: The issue of contextualizing the different lab activities based on program goals is very important. The online InfoSec lab is supposed to be used during the entire degree program, and this implies that any suggestion to align the lab exercises into different courses should come from all the stakeholders of an InfoSec lab. In order to align lab activities with the program goals, the recommendations from all the stakeholders (including all of the course teachers and the program management team) were considered in order to plan, design and develop the lab exercises. This included the network traffic monitoring exercise for the information security course. This principle helped to not only avoid any kind of overlap with other exercises being offered during the program but also encouraged the developer to use the lab resources efficiently when developing different exercises.

5.6.2 Scalability: There were servers with specific hardware capabilities. In order to efficiently use these resources, requirements for each course included in the information security degree program were collected. Then EPI could create virtual machines according to the requirements of each course. After EPI had created virtual machines for each course, EPI grouped them and shut off the machines that were not needed at that time. Then EPI could switch on the virtual machines when needed for another course. One limitation was that this system was dependent on the number of students in each course and how many courses were running at the same time because it required a lot of resources from the InfoSec lab. However, it is possible to swap virtual machines between two servers. For instance, EPI can divide the required virtual machines to be used on both available servers.

5.6.3 Easy configuration and reconfiguration: EPI used the standard ESXi 5.5 VMware vSphere Hypervisor to access the entire operating system of servers, create virtual machines, copy virtual machines, and create a resource pool for each course, as well as giving access to students, the assistant teacher, the teacher, and many other users at different levels of access. This configuration had been done once in the course and it could be expanded by just using a copy/paste method. For instance, the memory size of the virtual machine and number of assigned CPUs can be increased as required. It was easy to configure and reconfigure resources of the virtual machines according to the exercise or course requirements.

5.6.4 Back-up and recoverability: Two options were used to back-up the virtual machine or the configured virtual machine: 1) Save the virtual machine on the data store (the hard disk of the server) and omit or remove any unauthorized access to this data store (the EPI administrator has access to the machine's back-up); 2) Download the virtual machine itself to the local computer of the EPI administrator (personal computer).

5.6.5 Hardware integration: There were no issues related to the hardware integration in different exercises during this course. This principle ensures that all the equipment that is needed from different manufacturers to extend the laboratory for other courses' exercises could be integrated without any problem.

5.6.6 Cost-effectiveness: There were 69 students in the class. Virtualization technologies were used to provide every individual student with his/her own specific virtual machine. Virtualization technologies offer capabilities to integrate advanced topics into courses by providing students more control for hands-on activities (Lunsford, 2009).

5.7 Design Principles' Implementation for a Concrete Exercise Interface

5.7.1 User-friendly interface with properly arranged resources and targets: The interface for the exercise was the ESXi 5.5 VMware vSphere Hypervisor, which is itself a *user-friendly graphical user interface*. It has many icons. The students were able to recognize the resources needed to perform certain tasks in order to complete the assignment.

5.7.2 Easy to use: The feedback from students reveals that students did not find anything difficult about using the ESXi 5.5 VMware vSphere Hypervisor. The students appreciated the environment, which meant that the interface was *easy to use* and easy to follow. The graphical user interface contained many icons that easily guided the students when completing the assignment.

5.7.3 Tracking and debugging errors: This principle ensures that the tracking and handling of errors is done efficiently. If the student faced any problems, the assistant teacher could log-in to the same virtual machine and try to track the problem and help resolve it. The ESXi interface could provide multiple access instances to the same virtual machines, so the student and assistant teacher could be at the same place at the same time. The assistant teacher could track errors and help the student to avoid more trouble.

5.8 Evaluation of BIE 3

The evaluation in the third iteration was summative, as the refined set of design principles and the conceptual model of the online InfoSec laboratory were used to develop and instantiate a fully functional online InfoSec laboratory to be used for hands-on education in the information security program. A refined and complete beta version of the online InfoSec laboratory was implemented in the actual information security course with students. A survey questionnaire was sent to the 69 students to inquire about their experience of using the online InfoSec laboratory. Students' learning diaries also provided their reflections on the online InfoSec laboratory's utility and efficacy. The results showed that the majority of the students liked the idea of having personalized instructions regarding assignment tasks provided to them. The students also stated that the learning process was flexible and they liked the approach to access higher-level course topics after the successful completion of lower level course topics. Lab performance was rated satisfactory where a majority of the students agreed that it was *easy to establish a connection remotely*. However, some students mentioned minor issues with disconnections during lab work. Overall results showed that the students found the online InfoSec lab system *easy to use and stable.*

5.9 Reflection and Learning from BIE Phase 3

This study was conducted to develop an online InfoSec laboratory for the hands-on education of information security students. The online InfoSec laboratory underwent testing and evaluation phases. The alpha and beta interventions helped to unfold the ensemble perspective of the laboratory and to identify the different stakeholders of laboratory entities. Through this experimentation, it was learned that collaboration is extremely important in order to involve the stakeholders in the design, development and implementation process effectively. All of the stakeholders have different influential roles, which can sometimes be a challenge when designing an operational artefact.

The online InfoSec lab's development and implementation process showed that the issues surrounding technical and theoretical competence for the selection design and implementation of exercises are important. There is still a need to overcome the issues of responsibility and time management. For instance, without disclosing the ensemble view of the laboratory, it was just assumed that the laboratory and related exercises would be developed quickly. Therefore, not enough attention was paid to the full amount of responsibility needed for the design, development, implementation and maintenance of the laboratory and related activities. The ensemble view of the laboratory revealed that there need to be defined roles for all the laboratory stakeholders. The specification of roles also correlates with time management (scheduled time for every lab stakeholder's duties during course commencement) and specifically with the budget allocated for each course.

The conceptual model of an online InfoSec laboratory and the design principles were refined based on the feedback obtained from the stakeholders. The emergent knowledge informed the stakeholders that the issues related to protection of the laboratory and its physical and virtual resources are more complex than initially thought. This helped the researcher to refine the design principle of "Isolate the laboratory network" to "Isolate the InfoSec laboratory" with a broader perspective. Laboratory isolation prevents attacks on the laboratory and from the laboratory on the external world. The exercise processing and management (EPI) entity should protect the laboratory infrastructure from any attacks. The EPI should provide the access to the laboratory network in such a way that the network could still be isolated. For instance, the laboratory contains a networking environment and a virtualization environment that are consecutively related to physical networking components to create network topologies for different exercises and the virtual machines installed on physical servers. The isolation of the laboratory can therefore be broadly categorized into two main categories: 1. "Intrinsic isolation of laboratory components" requires the EPI developer to develop a labeling scheme for physical isolation of physical laboratory resources; 2. "External isolation of laboratory" requires that the external university network be protected from any attacks coming from internal lab components. The role of IT personnel is very important in this scenario. Flexibility of internal isolation will not hinder the merger of lab components or different network topologies to prepare large-scale exercises for various student groups. Resilience emerged as a new design principle during this BIE. This refers to the capability of reloading the lab exercise in progress in case of a crash. For instance, a student can issue wrong commands in the middle of the exercise and get stuck due to that wrong command and require an emergency exit from this situation. In this case, the student will need help from the system to reset the exercise settings. Figure 3 shows the refined conceptual model of an online InfoSec laboratory. Laboratory stakeholders' feedback led to adding a laboratory infrastructure management interface (LIMI) as an alternative with access restricted to developer and laboratory administrator. The LIMI provides back door access to developer and laboratory administrator for management and to perform immediate actions such as backup and recoverability of laboratory infrastructure.

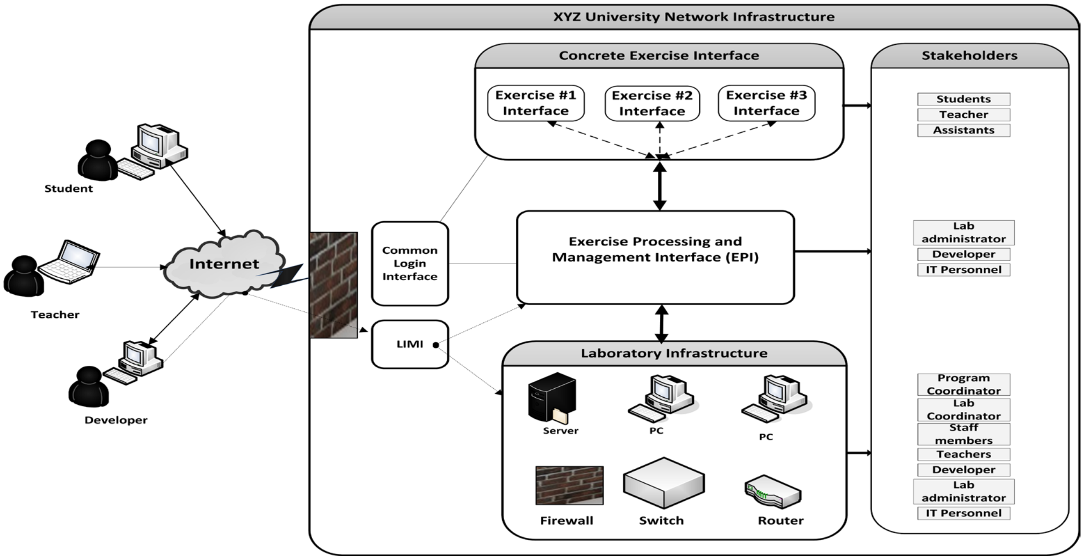

Figure 3. Conceptual Model of an Online InfoSec Laboratory

5.10 Summary of Results

The design and implementation process of the online InfoSec laboratory has been successful. Figure 4 provides a summary of the BIE cycles carried out during this research process. The right-hand side of the figure summarizes the contributions of the project.

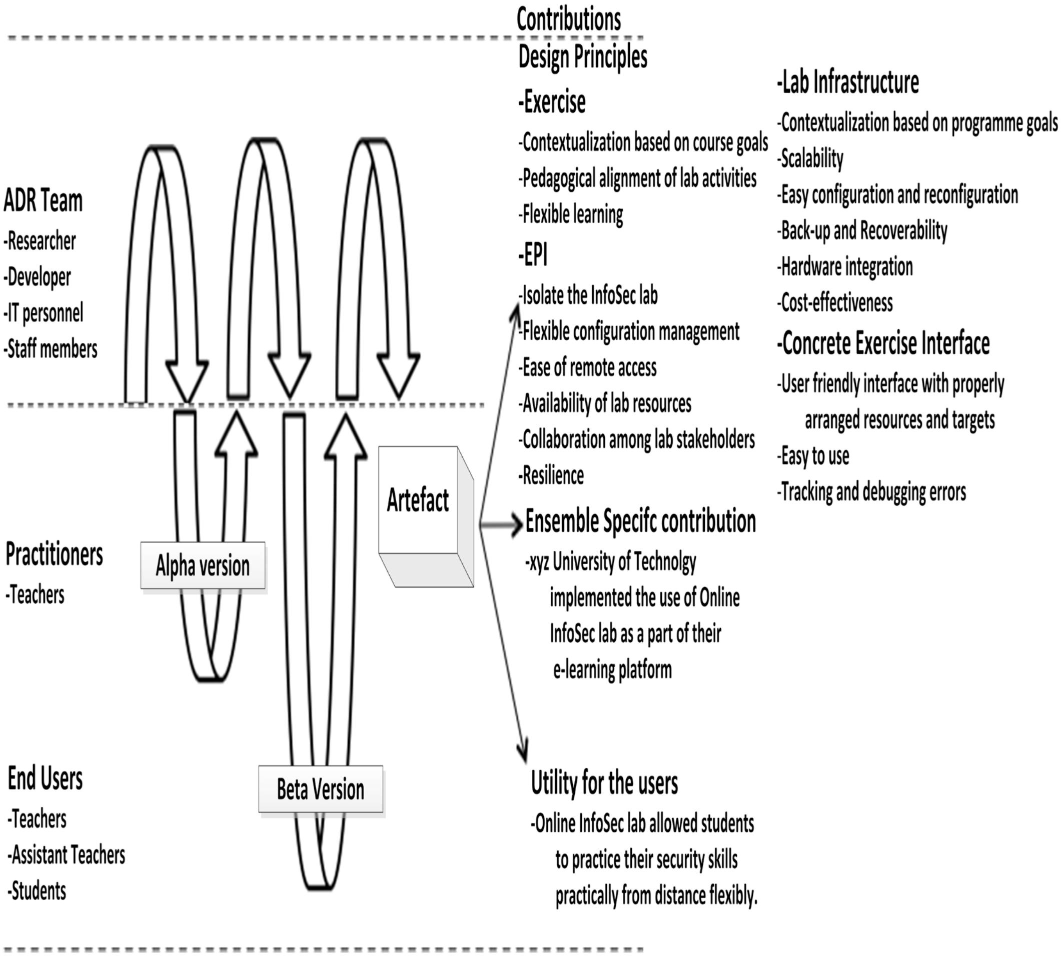
Contributions
Design Principles
-Exercise
-Contextualization based on course goals
-Pedagogical alignment of lab activities
-Flexible learning
-EPI
-Isolate the InfoSec lab
-Flexible configuration management
-Ease of remote access
-Availability of lab resources
-Collaboration among lab stakeholders
-Resilience
-Lab Infrastructure
-Contextualization based on programme goals
-Scalability
-Easy configuration and reconfiguration
-Back-up and Recoverability
-Hardware integration
-Cost-effectiveness
-Concrete Exercise Interface
-User friendly interface with properly arranged resources and targets
-Easy to use
-Tracking and debugging errors
ADR Team
-Researcher
-Developer
-IT personnel
-Staff members
Practitioners
-Teachers
Alpha version
Artefact
Ensemble Specifc contribution
-xyz University of Technolgy implemented the use of Online InfoSec lab as a part of their e-learning platform
End Users
-Teachers
-Assistant Teachers
-Students
Beta Version
Utility for the users
-Online InfoSec lab allowed students to practice their security skills practically from distance flexibly.

Figure 4. Schema for IT-dominant BIE and Contributions

6. DISCUSSION

Theorizing the IT artefacts is important to promote the understanding of issues related to design, development, and implementation in specific contexts (Benbasat and Zmud, 1999; Iivari, 2003; Orlikowski and Iacono, 2001; Rosemann and Vessey, 2008; Sein et al., 2011). Following this idea, this article provides the ensemble view of the online InfoSec laboratory. The study introduced a productive learning medium (InfoSec laboratory) that is designed to meet the active learning preferences of online learners of information security, such as support for flexible and individualized hands-on learning. In this IT-dominant BIE process, the researcher initially proposed a conceptual model and a set of initial design principles to design and develop an online InfoSec laboratory. In the next phase, the conceptual model was implemented using design principles. This research contributes through exhibiting the design, development and implementation of an online InfoSec laboratory to improve hands-on learning and the evaluation of its use for educational purposes.

Following technology as a development project perspective of ensemble view, this research contributes by serving two major purposes. First, the research proposed a conceptual model of an online InfoSec laboratory that comprises important entities: Laboratory infrastructure, Exercise, Exercise Processing and Management Interface (EPI), and Concrete Exercise Interface. Second, the research proposed design principles for implementing a conceptual model of an online InfoSec laboratory in different educational contexts for various exercise scenarios. The design principles are: contextualization based on course goals, pedagogical alignment of lab activities, flexible learning, isolate the InfoSec lab, flexible configuration management, ease of remote access, availability of lab resources, collaboration between stakeholders, contextualization based on program goals, scalability, resilience, easy configuration and reconfiguration, back-up and recoverability, hardware integration, cost-effectiveness, user-friendly interface with properly arranged resources and targets, easy to use, and tracking and debugging errors. The laboratory entities and design principles were shaped during this research work together with the other stakeholders. This article endeavours to encourage viewing a laboratory as an ensemble artefact by identifying and describing the core entities of an online InfoSec laboratory, the stakeholders for each entity, the interrelationships of the entities and the subsequent design principles when designing and implementing the laboratory for different contexts. The description of the online InfoSec laboratory as an ensemble artefact that explains its entities, stakeholders, and design principles explicitly was not provided in previous, similar works (Burd et al., 2011; Chen, Chen, and Chen, 2011; Crawford and Hu, 2011; Krishna et al., 2005; Lahoud and Tang, 2006; Li, Toderick, and Lunsford, 2009; Summers and Martin, 2005; Wang, Hembroff, and Yedica, 2010; Yang et al., 2004).

The conceptual model of an online InfoSec laboratory contributes to the existing literature in following ways. First, the ensemble view of an online InfoSec laboratory focuses on elaborating and solving the issues related to the socio-technical nature of an online InfoSec laboratory as an IT artefact. The description of laboratory entities presented in this study informs the academic community about the role of technical and social components that interact with each other in different ways during the whole process. The emergent socio-technical perspective of an online InfoSec laboratory emphasizes that equal attention should be given to the technical and social aspects. Specific entities are involved in the implementation of technology, integration of different hardware and software components, management and control of technical lab infrastructure, and at the same time stakeholders of each entity participate using their technical and social capabilities mutually to create and manage lab infrastructure, exercises and other resources. The interaction of social and technical infrastructure in a systematic manner results in the creation of an online InfoSec laboratory that is usable, scalable and stimulates flexible learning for hands-on education of information security students.

Second, this study elucidates how laboratory entities involve different stakeholders such as teacher, assistant teacher, developer, IT personnel, and students. This study explains how these stakeholders participate from laboratory planning to deployment, use and maintenance. Descriptions of the roles and responsibilities of the stakeholders in each entity clarify the need, importance and role of a laboratory team. Management of the laboratory and development of exercises are also complex issues and require a laboratory team. It is also correlated with the issues of availability of human resources and allocated and budgeted time management for a course. Teamwork can help to increase the teacher's efficacy in participating in the development and maintenance of the laboratory infrastructure and keep the teacher's focus on only one laboratory entity to design and manage the exercises.

Third, the conceptual model of the laboratory entities assists in clarifying the status of the laboratory and related exercises as an ensemble artefact. For instance, laboratory and exercise are mostly confused with each other, where some people may consider them to be the same thing. When people talk about an exercise, they might have a tendency to talk about it as a complete IT artefact in itself which is uniform, unified, single, seamless, stable and the same every time and everywhere. This makes it difficult to understand that while an exercise is definitely a central part of the technical IT artefact "InfoSec laboratory," it is nonetheless just one element in a package or ensemble artefact. This study aids in elucidating that the laboratory consists of different building blocks or entities. These entities together formulate the ensemble laboratory whereas an exercise is just a single entity of this InfoSec laboratory ensemble. The laboratory can be used for many different purposes concurrently, such as tutorials, simulations and exercises, depending on the available computing capacity. The laboratory can host several different exercises for different courses at the same time. The laboratory entities, such as exercises and laboratory infrastructure including stakeholders, are interdependent and connected to make a whole ensemble artefact.

Design principles are one of the main contributions of this study. The design principles presented in this study contribute to existing knowledge in the following ways. First, the design principles that emerged during the BIE processes can provide support to practically construct, implement and test the online InfoSec laboratory. Description of design principles clarifies how different challenges related to laboratory design, development and implementation are tackled, such as arranging laboratory infrastructure, issues pertaining to accessibility to the laboratory resources, minimizing student-induced security incidents, issues of laboratory scalability, pedagogical alignment of laboratory activities, provision of easy-to-use interface, arrangement of resources and targets for exercises, issues related to back-up and recoverability, error handling and configuration-related issues. The design principles presented in this article incorporate the socio-technical perspective.

The design principles such as the contextualization based on course goals, pedagogical alignment of lab activities, isolation of the InfoSec laboratory, flexible configuration management, and tracking and debugging errors provide insight to the practitioners (information security teachers). The practical implications of this research include contextualizing the practical and theoretical aspects of the course to design effective laboratory activities using contextualization based on course goals. The teaching and learning process in an academic institution is cognitive and the contextualization principle addresses the need to rationalize the laboratory activities within the boundaries of a specific course. This suggests that at the course level, the classroom environment should be contextualized for specified tasks, which will mainly be guided by course goals. The isolation principle provides important guidelines to practitioners such as developers as regards isolating the laboratory from the main university network for internal and external risk management and to secure laboratory resources, including hardware and software components. Similarly, the principle of flexible configuration management guides the developer to configure the laboratory resources in such a way that the laboratory resources can be extended easily when they need to create more exercise instances or to create large scale exercises for student groups. The tracking and debugging errors principle will allow the teacher and assistant teacher to provide quick help to the students during the exercise by accessing the same exercise environment where the students encounter problematic situations.

Furthermore, the study highlights the use of pedagogical approaches such as constructive alignment, conversational framework, and PSI. Pedagogical approaches provide help in categorizing the e-learning media for communicative, interactive, narrative and productive purposes. Pedagogical approaches also guide the teachers and other practitioners in aligning teaching/learning activities to stimulate active learning for individual as well as collaborative student activities. For instance, the PSI approach guided developer and teacher to provide an individual, flexible learning experience to students for laboratory exercises and to improve their mastery of course topics by utilizing the modularization feature. Pedagogical approaches have an impact on the design of a concrete exercise interface and the settings of the resources to be used when conducting the exercise. The exercise's design layout is also influenced by the choice of pedagogical underpinnings. For instance, in the case of providing individual exercises to the students, a PSI approach guides the developer in the EPI entity to arrange the settings in such a way that every student is given an individual concrete exercise interface. The privilege to access the laboratory resources is granted to individual students. On the other hand, if the teacher plans to provide an attack/defense exercise, a suitable pedagogical approach like cooperative learning strategy can be employed to allow students to work in different groups using the same environment and sharing with other group members.

From a research point of view, this study provides a starting point for researchers, specifically involved in the field of hands-on education in information security. The design principle of contextualization based on program goals contributes by providing guidelines to streamline and systemize the whole process of laboratory development at program level. This principle is developed using constructive alignment and conversational framework. This principle initiates the process of gathering requirements from all the stakeholders such as program coordinator, teachers of all courses and developer in order to align the program goals with the laboratory activities in different courses. This principle provides important guidelines to the information security teachers and program managers to make sure that the lab infrastructure should support all the exercises required in different courses of a degree program in information security. The design principle of contextualization based on program goals provides the research community with a starting point to ponder on the design and development of any hands-on laboratory to fit adequately for the whole program and not only for a single experiment. The InfoSec laboratory will be used during the complete study program at graduate level, which includes several courses for a specific purpose. Involving the stakeholders from each course earlier in the process while defining the scope of the laboratory will be useful in making the laboratory scalable and effective. This approach will help to enhance the academic understanding of the role of an InfoSec laboratory in different areas of research and teaching.

This research described the design and development of an online InfoSec laboratory as an ensemble artefact. Laboratory stakeholders will continue to deploy the conceptual model of the laboratory in new courses and a variety of information security exercises will be developed based on the requirements of the individual courses to enhance students' security skills. Further research should focus on refining the design principles for each entity. Further research on online InfoSec laboratories will enable the development of a design theory of online InfoSec laboratories in the future in order to systemize the knowledge more explicitly. Moreover, issues of students' security skills enhancement and competence development through participation in laboratory activities will also be potential areas for future work.

7. REFERENCES

Allen, I. E. & Seaman, J. (2010). *Learning on Demand: Online Education in the United States, 2009.* Sloan Consortium: Newburyport, MA.

Anderson, B. R., Joines, A. K., & Daniels, T. E. (2009). Xen Worlds: Leveraging Virtualization in Distance Education. *Proceedings of ACM SIGCSE Bulletin,* Vol. 41, 293–297.

Ayyagari, R. & Tyks, J. (2012). Disaster at a University: A Case Study in Information Security. *Journal of Information Technology Education*, 11, 85–96.

Benbasat, I. & Zmud, R. W. (1999). Empirical Research in Information Systems: The Practice of Relevance. *MIS Quarterly*, 23(1), 3–16.

Biggs, J. (1996). Enhancing Teaching Through Constructive Alignment. *Higher Education*, 32(3), 347–364.

Burd, S. D., Gaillard, G., Rooney, E., & Seazzu, A. F. (2011). Virtual Computing Laboratories Using VMWare Lab Manager. *Proceedings of 44th Hawaii International Conference on System Sciences (HICSS)*, 1–9.

Chen, F.-G., Chen, R.-M., & Chen, J.-S. (2011). A Portable Virtual Laboratory for Information Security Courses. *Advances in Computer Science, Environment, Ecoinformatics, and Education,* 245–250. Springer.

Choi, Y. B., Lim, S., & Oh, T. H. (2010). Feasibility of Virtual Security Laboratory for Three-Tiered Distance Education. *Proceedings of the ACM conference on Information Technology Education*, 53–58.

Crawford, E. & Hu, Y. (2011). A Multi-User Adaptive Security Application for Educational Hacking. *Proceedings of the World Congress on Engineering and Computer Science*, 19–21.

Gaspar, A., Langevin, S., Armitage, W., Sekar, R., & Daniels, T. (2008). The Role of Virtualization in Computing Education. *Proceedings of ACM SIGCSE Bulletin*, 40, 131–132.

Goldkuhl, G. (2012). What is an Ensemble Artefact? Presented at the Workshop on IT Artefact Design and Workpractice Intervention, 10 July 2012, Barcelona, Spain.

Gregor, S. & Jones, D. (2007). The Anatomy of a Design Theory. *Journal of the Association for Information Systems*, 8(5).

Hentea, M., Dhillon, H., & Dhillon, M. (2006). Towards Changes in Information Security Education. *Journal of Information Technology Education: Research*, 5(1), 221–233.

Iivari, J. (2003). The IS Core-VII: Towards Information Systems as a Science of Meta-Artifacts. *Communications of the Association for Information Systems*, 12(1).

Iqbal, S. (2013). Applying the Analytical Lens of Constructive Alignment and Conversational Framework for Course and E-Learning Platform Development. *Proceedings of Norwegian Konferanse for Organisasjoners Bruk Av Informasjonsteknologi, NOKOBIT*, 159-172.

Iqbal, S., Awad, A. I., & Thapa, D. (2014). Design Principles for Online Information Security Laboratory. *Proceedings of Selected Papers of the IRIS. The Scandinavian Chapter of the Association for Information Systems*, 65–79.

Iqbal, S. & Päivärinta, T. (2012). Towards a Design Theory for Educational On-Line Information Security Laboratories. *Advances in Web-Based Learning-ICWL*, 295–306, Springer-Verlag Berlin Heidelberg.

Iqbal, S. & Thapa, D. (2013). Initial Design Principles for an Educational, On-Line Information Security Laboratory. *Advances in Web-Based Learning–ICWL*, 89–100, Springer-Verlag Berlin Heidelberg.

Iqbal, S., Thapa, D., Awad, A. I., & Päivärinta, T. (2015). Conceptual Model of Online Pedagogical Information Security Laboratory: Toward an Ensemble Artifact. *Proceedings of 48th Hawaii International Conference on System Sciences (HICSS)*, 43-52.

Keller, F. S. (1968). Good-bye, teacher…. *Journal of Applied Behavior Analysis*, 1(1), 79–89.

Krishna, K., Sun, W., Rana, P., Li, T., & Sekar, R. (2005). V-NetLab: A Cost-Effective Platform to Support Course Projects in Computer Security. *Proceedings of 9th Colloquium for Information Systems Security Education (CISSE)*, Atlanta, GA.

Lahoud, H. A. & Tang, X. (2006). Information Security Labs in IDS/IPS for Distance Education. *Proceedings of the 7th conference on Information Technology Education*, 47-52.

Laurillard, D. (2002). Rethinking Teaching for the Knowledge Society. *EDUCAUSE Review*, 37(1), 16–24.

Li, P., Toderick, L. W., & Lunsford, P. J. (2009). Experiencing Virtual Computing Lab in Information Technology Education. *Proceedings of the 10th ACM conference on SIG-Information Technology Education*, 55–59.

Liu, Y. C. & Burn, J. M. (2007). Improving the Performance of Online Learning Teams - A Discourse Analysis. *Journal of Information Systems Education*, 18(3), 369-379.

Lunsford, D. L. (2009). Virtualization Technologies in Information Systems Education. *Journal of Information Systems Education*, 20(3), 339-348.

March, S. T. & Smith, G. F. (1995). Design and Natural Science Research on Information Technology. *Decision Support Systems*, 15(4), 251–266.

Nestler, V. & Bose, D. (2011). Leveraging Advances in Remote Virtualization to Improve Online Instruction of Information Assurance. *Proceedings of 44th Hawaii International Conference on System Sciences (HICSS)*, 1–8.

Orlikowski, W. J. & Iacono, C. S. (2001). Research Commentary: Desperately Seeking the "IT" in IT Research - A Call to Theorizing the IT Artifact. *Information Systems Research*, 12(2), 121–134.

Reid, R. & Van Niekerk, J. (2013). Towards a Brain-Compatible Approach for Web-Based, Information Security Education. *Proceedings of European Information Security Multi-conference (EISMC)*, Lisbon, Portugal, 59–68.

Rodriguez, C. O. (2012). MOOCs and the AI-Stanford Like Courses: Two Successful and Distinct Course Formats for Massive Open Online Courses. *European Journal of Open, Distance and E-Learning*, 15(2).

Rosemann, M. & Vessey, I. (2008). Toward Improving the Relevance of Information Systems Research to Practice: The Role of Applicability Checks. *MIS Quarterly*, 32(1), 1–22.

Sein, M. K., Henfridsson, O., Purao, S., Rossi, M., & Lindgren, R. (2011). Action Design Research. *MIS Quarterly*, 35(1), 37-56.

Summers, W. C. & Martin, C. (2005). Using a Virtual Lab to Teach an Online Information Assurance Program. *Proceedings of the 2nd Annual Conference on Information Security Curriculum Development*, 84–87.

Tikekar, R. & Bacon, T. (2003). The Challenges of Designing Lab Exercises for a Curriculum in Computer Security. *Journal of Computing Sciences in Colleges*, 18(5), 175–183.

Uludag, S., Guler, E., Karakus, M., & Turner, S. W. (2012). An Affordable Virtual Laboratory Infrastructure to Complement a Variety of Computing Classes. *Journal of Computing Sciences in Colleges*, 27(5), 158–166.

Vaishnavi, V. & Kuechler, W. (2004). Design Research in Information Systems. *Association for Information Systems. Last accessed October 23, 2013, http://desrist.org/desrist/content/design-Science-Research-in-Information-Systems.pdf.*

Venable, J., Pries-Heje, J., & Baskerville, R. (2014). FEDS: A Framework for Evaluation in Design Science Research. *European Journal of Information Systems*, 25(1), 77–89.

von Alan, R. H., March, S. T., Park, J., & Ram, S. (2004). Design Science in Information Systems Research. *MIS Quarterly*, 28(1), 75–105.

Wang, X., Hembroff, G. C., & Yedica, R. (2010). Using VMware VCenter Lab Manager in Undergraduate Education for System Administration and Network Security. *Proceedings of the ACM Conference on Information Technology Education*, 43–52.

Willems, C. & Meinel, C. (2011). Practical Network Security Teaching in an Online Virtual Laboratory. *Proceedings of International Conference on Security & Management (SAM)*, Las Vegas, NV.

Willems, C. & Meinel, C. (2012). Online Assessment for Hands-On Cyber Security Training in a Virtual Lab. *Global Engineering Education Conference (EDUCON),* 1–10.

Yang, T. A., Yue, K.-B., Liaw, M., Collins, G., Venkatraman, J. T., Achar, S., & Chen, P. (2004). Design of a Distributed Computer Security Lab. *Journal of Computing Sciences in Colleges*, 20(1), 332–346.

AUTHOR BIOGRAPHY

Sarfraz Iqbal is an Assistant Professor at Linnaeus University, Växjo, Sweden. He recently completed his Phd in Computer and Systems Science from Luleå University of Technology. His research interests include, information security, information systems, pedagogy and Information management.

APPENDICES

Appendix A

Server Security Architecture Course

Total students admitted	**Male**	**Female**
40	33	7
Geographical location	Sweden, European Union, Africa, Middle-East, India, Bangladesh, China.	
Total students who completed the course	30 Students participated in the course. G = 25, VG= 5	

Information Security Course

Total students admitted	**Male**	**Female**
101	85	16
Geographical location	Sweden, European Union, Africa, India, Pakistan, China.	
Total students who completed the course	69 Students participated in the course. G = 29, VG = 33 U = 7	

Some students dropped out of the courses even before the start of the course for various reasons.

Grading criteria

Code	**Type**	**Credits**	**Grade**
0001	Written exam	5.0	U G VG
0002	Individual assignments	2.5	U G#

(U = fail, G & G# = Pass, VG = Pass with distinction)

Appendix B

Questionnaire for the Evaluation of Information Security Course based on online information security lab

Your response will be seen only after the course results have been finalized and recorded, it will not have any effect on your course grades. The information will solely be used for the purpose of course and pedagogical improvement of lab activities.

Section1: Personal information & background
Name:
Age:
Gender:
Prior experience working with online InfoSec Lab:

Section2: Motivation and Comfort with E-Learning

Items	TA	A	NN	D	TD
General course overview was helpful to introduce the learning management system and strategy.					
It was a flexible learning course.					
The personalized instructions provided to me were very useful.					
Individual learning enhanced my capabilities and thinking.					
The time allocated for the lab exercises was sufficient for successful completion.					
I was motivated to work with the lab tasks by myself.					
Feedback on tasks was efficient and helpful.					
I feel that online learning is of at-least equal quality to traditional classroom learning.					

Put an X, TA= totally agree, A = agree, NN = neither nor, D = disagree, TD = totally disagree

Section3: System quality & Service Quality, User satisfaction (Fronter, Adobe connect, Lab):

Items	TA	A	NN	D	TD
You are satisfied with the course.					
You enjoyed the learning experience.					
You believe the system is successful.					
Easy to use					

Put an X, TA= totally agree, A = agree, NN = neither nor, D = disagree, TD = totally disagree

Section4: Lab performance

Item	TA	A	NN	D	TD
It was easy to establish a connection remotely.					
I didn't face any difficulties while working with online lab from distance.					
Depth of the exercise content was suitable.					
The effort required by students for lab work was sufficient.					
Access to the lab resources was easy.					
Approach to access higher-level course topics after the successful completion of lower level course topics was very effective.					
Lab and exercise interface was user friendly					
Lab resources were stable during work.					

Put an X, TA= totally agree, A = agree, NN = neither nor, D = disagree, TD = totally disagree

Section 5: Write short answers.

1. **How did you feel about your ability to work alone on the lab assignment?**

2. **Describe your experience of working with exercises in the online lab in this course?**
3. **Any improvement suggestions for lab performance**
4. **If you experienced any technical problems when working with online InfoSec lab resources please provide details here: -**
5. **The guidance provided by clear learning objectives and course outline was sufficient to complete the course?**
6. **Help provided during lab exercises by teacher / teacher assistant was sufficient?**
7. **Any other comments?**

aitp Association of Information Technology Professionals

No matter how sophisticated the technology, it still takes people! ™

EDSIG

Serving Information Systems Educators

STATEMENT OF PEER REVIEW INTEGRITY

All papers published in the Journal of Information Systems Education have undergone rigorous peer review. This includes an initial editor screening and double-blind refereeing by three or more expert referees.

ISSN 1055-3096