Communications of the IIMA

Volume 10 | Issue 1 Article 3

2010

Using 3-D Virtual Worlds as a Platform for an Experiental Case Study in Information Systems Auditing

Donals R. Moscato
Iona College

Diana M.E. Boekman
Utrecht University of Applied Sciences

Recommended Citation

Moscato, Donals R. and Boekman, Diana M.E. (2010) "Using 3-D Virtual Worlds as a Platform for an Experiental Case Study in Information Systems Auditing," *Communications of the IIMA*: Vol. 10: Iss. 1, Article 3.
Available at: http://scholarworks.lib.csusb.edu/ciima/vol10/iss1/3

Using 3-D Virtual Worlds as a Platform for an Experiential Case Study in Information Systems Auditing

Donald R. Moscato
Iona College, New Rochelle, NY
dmoscato@iona.edu

Diana M. E. Boekman
Utrecht University of Applied Sciences
Utrecht, Netherlands
diana.boekman@hu.nl

ABSTRACT

The paper is a case study of an experiential exercise in information systems auditing of a virtual data center constructed in the 3-D virtual world of Second Life. A technology and data center was created and populated with numerous risk exposures for an organization. The objective is for information systems auditing students to perform a site visit and apply auditing principles as they canvass the physical site. After a number of audit findings are discovered, each student is expected to present their results in a professional manner using the reporting guidelines of the Institute of Internal Auditors.

INTRODUCTION

This paper describes a very creative way to teach the fundamental concepts and principles in performing a physical audit of a data center. To this end, students study the principles of audit and security as part of a graduate level course in an information systems program. In this paper we will present an overview of some of the basic principles of auditing and control in an information systems context. Information systems auditing can be taught as part of both accounting and information systems academic programs. It is important to understand that it is a teachable skill set. IS auditing has a body of knowledge and is recognized as an extension and application of basic auditing principles (Ciampa, 2007). A fundamental concern is how best to teach and practice these skills acquired in a formal academic context? In this case we will concentrate on the performance of a physical site visit to a data center. It is a tangible component of a total systems audit which might include software (system and applications) as well as networks and human resource dimensions.

The authors created a virtual technology and data center in the metaverse known as Second Life (Robbins & Ball, 2008; Rymaszewski, Au, Wallace, Winters, Ondrejka, Batstone-Cunningham, & Rosedale, 2008*)*. It is a virtual world and is used by hundreds of thousands of "players" for a myriad of activities. It is global in its orientation and uses language translators to facilitate communication among members who are represented as avatars. Since it is a virtual world, inhabitants are not limited by the typical real world physical limitations. Avatars are capable of flying, seeing into buildings and teleporting around the universe almost instantaneously. The platform was selected for the experiential exercise for several reasons. Second Life provides for a more visual platform for students to interact with the environment of the data center. The platform allows students to engage in joint audits from anywhere in the world. Students meet at the site to perform the audit regardless of their host country. This promotes intercultural group activities across multiple campuses (Moscato & Moscato, 2009a, 2009b). As part of the audit, students can "fly" around the site and get a very efficient "lay of the land" as they audit the target system. The design of the site in this medium allows for the instructor to continuously change the configuration and exposures which facilitates repeated use but with different learning objectives possible. Students can take numerous screenshots to document and support their audit findings at little out of pocket cost.

LEARNING OBJECTIVES

To guide the development of the case study, several learning objectives were established. Since the case exercise could be tailored to either academic or professional venues. The design principle throughout was to maintain project design flexibility and to permit scalability. It is the intention of the authors to vary the physical or target system to include virtually any application. For example, airport, shipping port, petroleum plant energy and so forth are all possible extensions of this exercise.

The following learning objectives informed the design process of the exercise:

(1) To be able to demonstrate an understanding and application of the basic principles of information systems physical security;
(2) To be able to implement basic principles of IS auditing;
(3) To demonstrate an understanding and application of the Institute of Internal Auditors guidelines on presenting audit findings;
(4) To develop the auditor's observation skills as they canvass a physical targeted site;
(5) To develop a skill and practice in assessing risk exposures and their potential impact on an organization by prioritizing the exposures identified in the audit according to their perceived importance;
(6) To develop a skill and practice in presenting audit findings to management in a professional and convincing fashion according to the IIA guidelines;
(7) To have fun in learning to perform an audit in a highly interactive, experiential modality.

THE CONTROL ENVIRONMENT

In this section, we discuss several concepts that form the basis of understanding of some of the primary ways for an auditor to think about control. It is convenient and effective to view controls from a very simple perspective. There is a fundamental statement of the control which is followed by a discipline over that control. An example would be the control to keep all doors locked. That would be the basic control statement. However, unless an auditor verifies that the doors are indeed locked, then there is no compliance with that basic control statement. It is the discipline surrounding that control that makes it effective. Merely stating the control is never enough.

A useful way of implementing controls in any situation is to view them as a multi-layered process of controls. In the first instance we try to *prevent* an incident from happening that would breach a system. Often, most controls are set at this layer. Unfortunately, an adversary is able to penetrate a system and, if successful, has free reign over the target areas. To counter this possibility, controls are placed to *detect* a breach to the system. In this manner, if a perpetrator gains access we are at least able to know that something improper has occurred. Finally, provision must be made to *correct* the problem resulting from the breach to that part of the system. These three layers-preventive, detective and corrective form the basis of layering controls on a particular asset to be protected. The following is an example of layering the controls on a system. Take the example of a "man trap" entry system to a building. The double door system tries to prevent improper entry by unauthorized personnel. If the person is able to enter the first door and announces herself to the intercom and that person should not be given entry then the second door prevents further access and locks the first door behind the individual. The system prevented the person from entering the building. It detected an unauthorized person trying to enter. Finally, a security guard can proceed to the entry way and take corrective action.

It is good practice to recognize that these layers of control support the recognition that threats to a system asset can occur from several different intentions. A threat could be active on the part of the perpetrator (Newman, 2010; Solomon & Chapple, 2005). An example would be the deliberate destruction of a server farm in a datacenter. The threat can be passive. An example would be the benign neglect of backing up an important information asset at regular intervals. The absence of properly timed backups could compromise the system in the event of system failure. Finally, a threat can be accidental (Easttom, 2006). This category includes acts of nature such as floods, tsunamis and earthquakes as well as acts of people including electrical fires and liquids spilling on electronic devices.

In implementing any control system for a targeted asset it is imperative to understand the nature of any exposure. On some occasions your concern could be *disclosure* of the state of a particular asset. Example would be the balance in a bank account or the fact that an alarm to an area was in an inactive mode at a point in time. Other times, the exposure could be that an asset could be *modified*. Examples would be when a perpetrator could change the direction of an inquiry to a dangerous web site or when a firewall is set to an off mode unbeknownst to an organization. A third type of exposure would be when the intent is to *destroy* an asset (Pipkin, 2000). The goal is destruction and it could be as large as an entire intranet of a corporation to something as minor as the contents of a person's hard drive on their computer.

In order to facilitate the creation of a control system and its efficacy we can follow a straightforward process. There are many names given to this exercise and many variations of it but we present the following as one of many options to inform our actions. It makes little sense to insert controls at random in a system. This action can result in inefficiencies, poor control and wasted expense and frustration on the part of system's users. The first step is to systematically attempt to identify the types of breaches to the system that might occur. Examples could be a fire, robbery, etc. The next step is to ascertain at what point in the system (a control point) there should be a control inserted. Again, this control could be any one of the three types discussed previously-preventive, detective or corrective. The auditor must be assured that these controls are in fact in place as part of a formal audit. Finally, depending upon the importance of the audit target, a step by step approach must be designed to perform the audit in an expeditious manner.

There are many design principles that must be considered in designing an effective control system. Some of these are as follows: requisite variety, redundancy, granularity, protocols and standards, encryption and trust (Raval & Fichadia, 2007).

INFORMATION SYSTEMS AUDITING CONSIDERATIONS

There is a very simple process that an auditor follows when on a site visit. It involves asking a series of questions and reflecting on the answers to them. The questions are as follows: who, what, when, where, why, how and which (Moscato, 1995). However, an audit is far more complex than simply asking a few basic questions and reporting the results. The auditor must be guided by a clear control objective and audit objective or countless resources will be wasted. Each audit has a control objective. Its purpose is to ensure that an asset is properly protected at the desired level. In order to ascertain this state, the auditor establishes a specific audit objective. The ultimate purpose of the audit objective is to be able to determine whether or not the control objective has been met. It should be noted that a control objective might be financial in nature (Are assets properly valued?), non-financial in nature (Are data archived?) or operational (Is a facility properly secured?). The audit objective eventually is translated into an audit program that is drilled down to the audit steps necessary to carry out the actual site audit. Typically, the auditor performs tests on the targeted system. These tests are either substantive or compliance in nature. A substantive test is a text of data values and usually involves accessing a company's data base and verifying balances contained therein. Emphasis is placed on material values and not always a direct enumeration of all the data. A compliance test is one that is concerned with a review of operations with the purpose of rendering an opinion on whether or not a proper policy or procedure is being followed at a data center. In this case study, we are concerned only with compliance testing of the controls in place at the physical site and not with any data contained within databases.

The Institute of Internal Auditors (IIA) has developed a series of guidelines that are to be followed in presenting the audit results to corporate management in a concise and standardized manner. As part of this case study, the students are expected to follow these guidelines in presenting their audit findings as a result of their site visits to the data center. Each audit finding is documented and then prioritized in terms of risk exposure to the organization. The following five points constitute the architecture of the audit findings framework.

(1) *The Statement of Condition*

This contains the factual (observed) evidence of the current state. It can be thought of as the "what was" part of the report.

(2) *The Criteria*

This is our reference point or standard/protocol that is used to measure against the current condition observed by the auditor.

(3) *The Effect*

Preferably stated with a monetary value, it represents the degree of risk or exposure incurred as a result of the deviation from the standard.

(4) *The Cause*

This is the auditor's opportunity to explain why there is a deviation from the stated standard. Often, this is a result of someone not performing their assigned duties but can also be the result of no one person being held responsible for an entity.

(5) *The Recommendation*

This is the opportunity for the auditor to state to management what could be done to rectify the identified exposure. In other words what to do now? (Institute of Internal Auditors, 2010).

By following this audit findings template all identified risk exposures are presented in a uniform format to corporate management. Each audit finding could be ranked in terms of corporate impact. Its design facilitates communication and keeping the focus on the facts of the audit and the generally accepted standards of the profession. It is important to note that it is not the responsibility of the auditor to set standards but, rather, to identify any deviations from those standards identified in his/her audit of the data center.

In order to assist the information systems auditor in carrying out his responsibilities it is incumbent upon each professional to have a basic competency level on a basic skill set. We can identify several of these skills and requirements. There are guidelines and standards provided in COBIT, ISO and from the IIA (Whitman & Mattord, 2008;

Dhillon, 2007). Audits of data centers are carried out by having formal site visits. The time of these visits is a judgmental call-during work hours or when the site is closed. Conducting a physical site visit is expensive in both time and money. Often, there is a need to have interaction with key people and the actual site itself. Care should be taken to make sure the site is available at the time the auditor is going to visit. In this case study, the visit is carried out after hours when only a security person is staffing the front desk of the building. The auditor is to observe the site looking for both exposures resulting from errors of commission as well as errors of omission. Using the virtual world modality allows for an auditor to view the physical site from many angles: top, sides, front and back. Another advantage is that multiple visits can be made (easier and less costly than in person visits).

Typically, the auditor would rely on selected interviews during the site visit. For purposes of the case study, all relevant parameters are laid out in the case documentation. Other auditing principles are competence, objectivity and independence. In the case study, the students have been studying information systems auditing principles (competency), they are not employees of the data center but of the auditing department (objectivity and independence) (Newman, 2010).

RISK MANAGEMENT

In this section we will discuss briefly some concepts that guide the company in designing a successful risk management initiative. There must be a delicate balance achieved between putting controls in place that results in a direct out-of-pocket cost to the organization versus achieving an acceptable level of risk exposure that a company is willing to bear. Risk exposure is often defined as a categorization of events that could cause adverse effects to an organization. It does not discuss the probability that those events will occur. Risk analysis takes into account the possibilities. However, for purposes of this paper, the auditor must be informed of the overall risk management perspective. In performing a site visit of a data center, the auditor focuses on observations. He is not always privy to the overriding concerns embodied in the risk management program undertaken by the whole organization. Therefore, the authors only cite the approaches that an organization could use to employ as part of its risk management program. These approaches are as follows:

Risk avoidance
Risk reduction
Risk retention
Risk Transfer (Raval & Fichadia, 2007).

Therefore, when an auditor performs a particular site visit, embedded in the controls in place, is the over-arching notion that these approaches have been factored into the control architecture followed by the organization.

THE CASE STUDY

Second Life is a metaverse consisting of simulated islands (64,000 square meters in size) called sims. These islands are located in a 3 dimensional universe with each having a unique set of coordinates. Each island or sim can be subdivided into smaller parcels. The case study described in this paper is based on a building located on a particular sim. It occupies a designated amount of space. It is depicted in **Figures 1** and **2**. The building houses the Technology and Data Center of an organization. The emphasis of the audit is on the security and control that is physically implemented in the target structure.

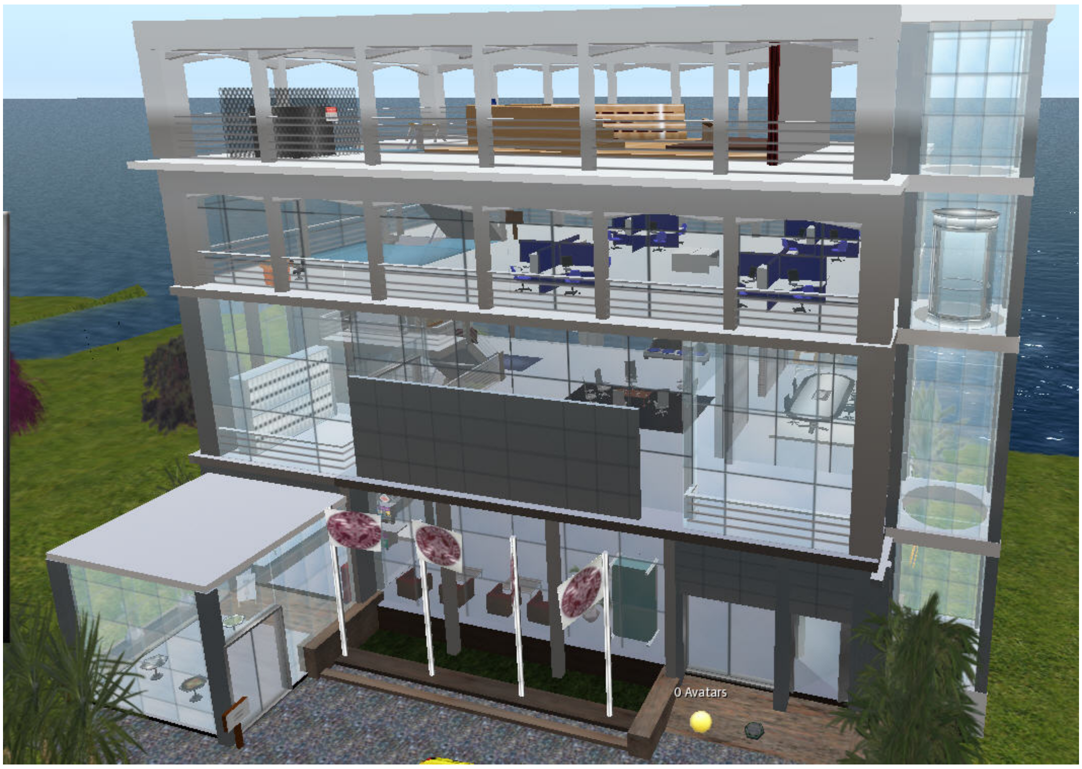

Figure 1: Technology Data Center, Front View

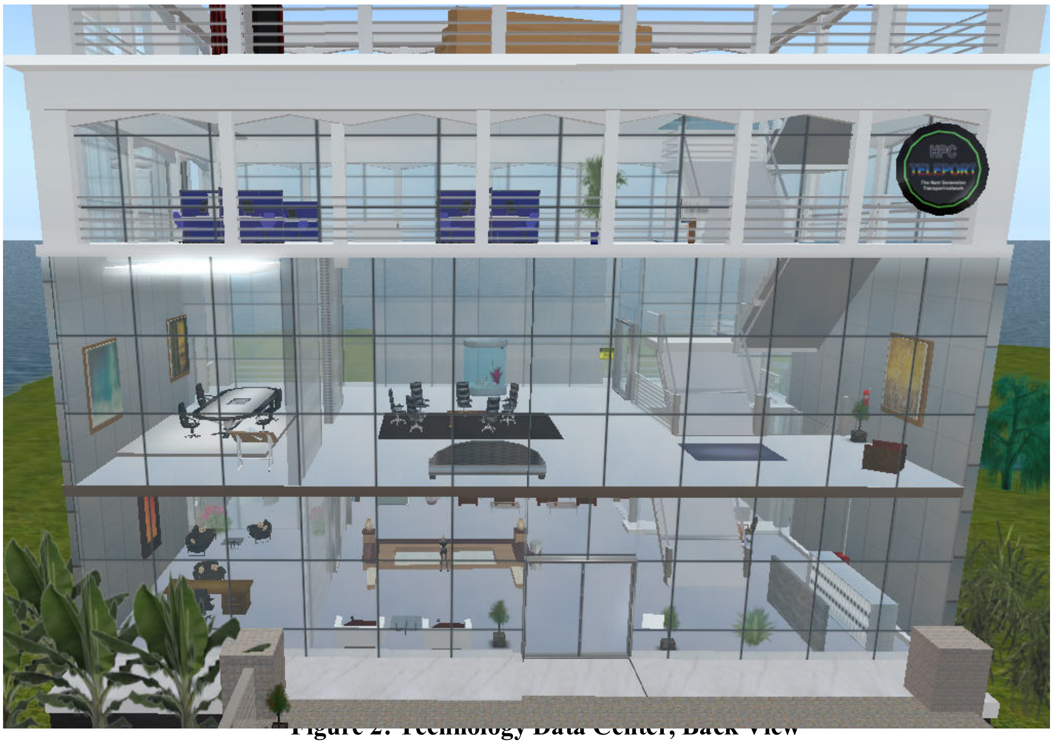

Figure 2: Technology Data Center, Back View

The building consists of 4 floors the first being on ground level. Access to all floors is via a conventional elevator located within the building. The authors populated each floor with a number of risk exposures. In addition to the building itself, there are exposures based on the location of the building and how it can interact with its immediate environment. The structure of the experiential exercise permits the trainer to readily add or remove the specific exposures incorporated in the exercise. In this manner, the degree of difficulty of the assignment can be scaled both in terms of the number of exposures included as well as their complexity in terms of IS auditing concepts. The present version contains more than two dozen plausible risk exposures.

SCENARIO BACKGROUND of the TECHNOLOGY and DATA CENTER

We include this section in the format that it will be presented to the students in its actual verbiage. It will serve as the "charge" that they receive as the auditors on the engagement. The students, after reading and understanding the scenario, will enter the virtual world and conduct the audit of the technology and data center.

The company operates both a LAN (local area network) as well as a WAN (wide area network) from this building. The former is for internal activity whereas the latter interacts with the global environment. The timing of the audit is after hours when the regular cast of staff is not working at their normal stations. The only person in the building is a security person stationed at the reception desk. She will not interact with the auditor during the performance of the audit.

The building is the site of both technical as well as administrative information technology functions. It also contains a training center that is used by both internal staff as well as outside guests who may be suppliers and/or customers.

In performing the audit, you should be proactive. You will be able to touch objects and interact with them to ascertain their functionality. This will help in determining the existence or not of any risk exposure to the corporation. Look for areas of activity (commission) as well as areas that should be present (omission) but are not. Be creative, yet realistic, in your identification and findings of any risk exposures.

Auditor Tasks

This section describes the instructions that are given to the student auditors and the deliverables that are required for the experiential exercise. It is assumed that all students are familiar with navigation skills in the Second Life environment. They have created their avatars, practiced in the SL environment and are able to perform basic functions. Therefore, these instructions only pertain to the auditing exercise.
The tasks will be presented in bullet format for readability.

(1) Teleport to the targeted sim in SL
(2) Explore the Technology and Data Center and its immediate environment using conventional means as you would do as an auditor.
(3) Using your knowledge and understanding of physical security standards and information systems auditing principles, apply them as you canvass the premises.
(4) During your site visit identify all risks inherent within the building and its surroundings.
(5) Using the IIA Statement of Audit Findings template complete a form for each observation that you deem an exposure. Make your arguments convincing to management who is the recipient of your findings.
(6) Rank order the audit findings in terms of importance of risk exposure from highest to lowest.
(7) In your audit investigation, be keenly aware of risk exposures due to both actions of omission as well as actions of commission.

SUGGESTIONS FOR FURTHER STUDY

This case is a continuing component of ongoing research into social networks by the authors. Further research should be done about the use of social networks in education. The case presented here will be used as a simulation in a university class in computer auditing and security. Future subjects to be addressed are as follows:

(1) Does a simulation like this represent real life well enough?
(2) Will students come to the same conclusions about the security issues in the building in this virtual setting as they would in a real world setting? Will they perhaps find more problems? Will they not be as aware due to the simulated venue? Are they able to “translate” this virtual setting into a real life one?
(3) It will also be interesting to know what students think about learning and working in a virtual- environment? Will they use it as a game? Are they interested in virtual worlds? What will students use virtual worlds for?
(4) What other possibilities arise when working and doing research in a virtual environment? How about working with people all over the world, on a daily basis as we did in preparing this simulation case? It was almost like working with your colleagues at work. What kind of possibilities will this create?

There are many more questions about virtual worlds versus real life. Questions arise about communication, marketing and conducting business? But also in what areas virtual environments can be used. Education was mentioned, but what about healthcare, culture, informing people about all kinds of subjects, conferences, etc? We seem to be just at the start of a whole new way of communicating and interacting with each other. Will this change our lives as profoundly as the Internet did?

SUMMARY AND CONCLUSIONS

This paper presented a case study of how skills in auditing information systems can be taught using the modality of 3-D virtual worlds like Second Life. The focus of the exercise was on the physical audit of a data center. After discussions of control environments and auditing considerations the actual case study was presented. Illustrations of the data center were included so the reader can visualize what the actual data center looked like. It replicates what an auditor can expect to find in the real world. The design of the exercise was both flexible and scalable so that future modifications can be made with minimal difficulty.

The use of a virtual world to teach auditing concepts has several clear advantages. First, the environment of Second Life and its ilk contains a richness that cannot be captured with traditional case study approaches that utilize words only. Second Life is visual, interactive and fun. A properly designed sim can replicate the characteristics of a real world auditing environment at a significantly lower cost than the real thing. Of course, this presupposes the ability to access a real data center and perform an audit for training purposes. The costs would be prohibitive.

Second, auditors in training have the opportunity to hone their observation skills which are necessary in any site visits they will make in the real world. As they navigate the data center, they can carefully match their training to what they see before them in the building. They will be seeing images of what they will encounter in any real world audit.

Third, by focusing on the IIA template for the presentation of audit findings, the student will reinforce the major elements of an audit finding that will prove invaluable in actual practice. They will develop a concise, effective writing style that emphasizes the importance of framing the relevant issues in an understandable and consistent manner.

Fourth, by having to rank order the audit findings according to priority, the auditor develops the skill in assessing what is really a major finding from a minor finding in an audit context. This fact makes him/her a valuable member of the management team.

Lastly, learning and applying auditing of information systems principles in an actual setting as captured in a virtual environment can actually be fun as well as educational.

REFERENCES

Ciampa, M. (2007). *Security awareness: Applying practical security in your world*, (2nd Ed.). Boston, MA: Thomson Course Technology.

Dhillon, G. (2007). *Principles of information systems security*. Hoboken, NY: John Wiley.

Easttom, C. (2006). *Computer security fundamentals*. Upper Saddle River, NJ: Pearson Prentice Hall.

Institute of Internal Auditors. (2010). Retrieved from http://www.theiia.org.

Moscato, D. (1995). *Computer assisted auditing techniques: An illustrative approach.* Rye Brook, NY: Metamation Systems.

Moscato, D. R., & Moscato, E. D. (2009a). A case study in implementing second life in a graduate distance learning e-commerce class. *Communications of IIMA, 9*(1), 91-98.

Moscato, D. R., & Moscato, E. D. (2009b). A critical analysis of the use of 3-D virtual world environments in e-commerce strategy. *Issues in Information Systems, 9*(2), 267-274.

Newman, R. C. (2010). *Computer security: Protecting digital resources*. Sudbury, MA: Jones and Bartlett.

Pipkin, D. L. (2000). *Information security: Protecting the global enterprise*. Upper Saddle River, NJ: Prentice Hall.

Raval, V., & Fichadia, A. (2007). *Risks, controls and security.* Hoboken, NJ: John Wiley.

Robbins, S., & Ball, M. (2008). *Second life for dummies.* Indianapolis, IN: John Wiley.

Rymaszewski, M., Au, W. J., Wallace, M., Winters, C., Ondrejka, C., Batstone-Cunningham, B., Rosedale, P. (2008). *Second Life-the official guide*. Indianapolis, IN: John Wiley.

Solomon, M. G., & Chapple, M. (2005). *Information security illuminated.* Sudbury, MA: Jones and Bartlett.

Whitman, M. E., & Mattord, H. J. (2008). *Management of information security* (2nd ed.). Boston, MA: Thomson Course Technology.