SENRA Academic Publishers, Burnaby, British Columbia
Vol. 2, No. 2, pp. 463-468, 2008
ISSN: 1715-9997

Canadian Journal of pure&applied sciences

EVALUATION OF SOFTWARE DEVELOPMENT CONTROLS IN INFORMATION SYSTEMS ORGANIZATIONS

*Muhammad Asif Khan and Saleh Al Turki
Department of Information Systems, College of Computer Sciences and Information Technology
King Faisal University, Kingdom of Saudi Arabia

ABSTRACT

Information Systems organizations have become more vigilant in identifying risks to their infrastructures. In fact, organizations have recognized the significance of IS audit and controls to remove or mitigate the risks for their infrastructures by implementing appropriate measures. The aim of this study is to analyze, explain and demonstrate that how Information Systems organizations implement and ensure that business applications are developed under a controlled environment, thus preventing and/or mitigating the risks involved in development. Also, the study focuses on whether organizations are careful in carrying out the acquisition process as efficiently and effectively possible. To complete our work we have collected and analyzed data from different large organizations in Saudi Arabia, which have an existing IS audit function in order to compare between the approach used by these organizations and the industry standards of IS audit and control set by organizations.

Keywords*:* Information systems, software development and acquisition, audit controls.

INTRODUCTION

The study of information systems deals with deployment of information technology in organizations, institutions and society at large. Information systems are becoming essentials for businesses to be more productive and efficient, and since the internet has taken a leading edge in business growth, control weaknesses and system vulnerabilities have become the top issues in organizations (Ciborra, 2002). In early 1970s IS organizations had not realized the extent of risks and losses of various business and technology sectors but thereafter, professionals from various sectors such as technology, security, business, manufacturing, government and general public joined efforts in order to confront these issues. Consequently, organizations, associations and institutions were established to lay down standards, guidelines and procedures, which were designed and developed by these professionals to address the increasing control weakness and security concerns.

Initially, security threats, system vulnerability and control weaknesses were given much consideration in applications and network infrastructure, but soon it was determined that the way the technology was developed and managed had a significant impact on organizations. Consequently, appropriate action was taken to further develop and evolve the control procedures to comprehend most of the major processes, which included the development, design, management and implementation of the information systems facility.

Since the focus started to comprise the business processes and the governing procedures, the concept of auditing evolved. Altar (2003) said that with the advent of computer systems, the scope of auditing expanded to encompass both general controls over computer installations and application controls for assuring that recording, processing and reporting of data are performed properly. CISA (2007) described that information systems auditing is a process that collects and evaluates evidence to determine whether the information systems and related resources adequately safeguard assets, maintain data and system integrity, provide relevant and reliable information, achieve organizational goals effectively, consume resources efficiently and have in effect internal that provide reasonable assurance that business, operational and control objectives will be met and that undesired events will be prevented or detected and corrected in timely manner.

Globally every organization should undergo a periodic security audit. A security audit is a systematic assessment of security level of a system and the effectiveness of controls. It is important to obtain an understanding of the audit area before a risk assessment can be accomplished, prioritized and categorized. Data regarding the existing controls of the audit area is collected, compiled and analyzed to evaluate the controls' appropriateness, adequacy, effectiveness and efficiency (Solomon, 2005).

METERIALS AND METHODS

The study was carried out with the aim to demonstrate the effectiveness of IS Audit and Control and analyze the effectiveness and efficiency of IS Audit in reducing and/or mitigating risks, vulnerabilities, security issues and weaknesses within IS organizations. We started our study

*Corresponding author email: asifkhan@kfu.edu.sa

by collecting data regarding the IS Audit approach through surveys and interviews with the companies identified [to maintain the privacy of the organizations we will denote the two financial organizations as F1, F2 and other public services organization as G]. Data about different technical infrastructure and operational practices in use, security techniques available, most commonly used approach for software development and acquisition, business continuity and disaster recovery planning were collected through interviews and surveys.

Our study started with a questionnaire prepared for the F1, F2 and G companies where IS audit function in place. The main aim of the questionnaire was to allow the companies under research to rate the importance, effectiveness before IS audit, the effectiveness after IS audit, risk rating before IS audit and the risk rating after IS audit. We have used following indicators in the questionnaire:

Importance – level of importance of the control.

Effectiveness before IS audit – effectiveness of the control before IS audit function in the company.

Effectiveness after IS audit - effectiveness of the control after it has been reviewed by the IS audit function in the company.

Risk rating before IS audit - risk level the IT function is exposed to with regard to the corresponding rated control area and the governed IS processes before an IS Audit review was conducted on that process.

Risk rating after IS audit - risk level after the corresponding control area and the governed processes was reviewed by the IS audit function.

We used the ratings from scale One to Five, one being the minimum and five is the maximum for all above stated indicators (i.e. 1 = Minimum, 2 = Low, 3 = Medium, 4 = High and 5= Maximum).

For example if the "Importance" was rated as 5 (i.e. Maximum) it implies that the control is of maximum and/or extreme importance to the management in order to govern the subsequent IT process. Likewise, if the "Effectiveness before/after IS Audit" was rated as 1 (i.e. Minimum) it means that the control is of poor effectiveness.

RESULTS AND DISCUSSION

In any software development environment operating systems have their significance and data was gathered to know operating systems in the companies. Following table 1 describes the available operating systems in the companies under research:

Table 1. Operating Systems used in the companies under research

Operating System	**F1**	**F2**	**G**
Windows	●	●	●
OS/400	●	●	
Unix	●	●	●
Linux			
Novell	●		●
Sun Solaris		●	

It is observed from the table 1 that the company F1 uses OS/400 for their core banking system due to its high security, reliability, scalability and efficiency. Unix is used for their other critical applications due to its reliability and Novell is used for their front-end banking solution. Windows is used as the network operating system.

The company F2 uses OS/400, Unix, Windows and Sun Solaris for their infrastructure. However, they use OS/400 and Unix for their critical applications. Only one application is hosted on Windows. According to them Windows is an excellent network operating system but not a secure application server.

The company G uses Windows, Unix and Novell operating systems. Unix is used for the core banking system due to its higher reliability, stability and security compared to Windows and Novell. Windows is used as their network operating system. According to them Windows provides the best networking service out of all operating systems. Novell is used for their legacy systems.

From the above, it is observed that operating systems such as OS/400 and Unix are more reliable and secure application operating systems than Windows. On the other hand Windows is a more reliable network operating system. Since databases are the backbone of software development, therefore, we carried out a research on available databases in the respective companies and following table 2 shows the databases in use in the companies:

Table 2. Databases used in the companies under research

Databases in use	**F1**	**F2**	**G**
Oracle	●	●	
SQL	●		
DB2	●	●	
MS Access	●		
Sybase			
Other(s)			●

Both companies F1 and F2 use Oracle and DB2 for their core applications systems due to their integrity, reliability

and security. The company F1 uses SQL and MS Access due to their business requirements, which demand some applications that utilize these databases.

Audit analysis

We carried out a comprehensive study with regard to the audit controls implemented in the organizations.

Company F1

Despite that Policies and Procedures was rated as "Maximum" Importance, it was completely ineffective before the IS Audit function and therefore the risk was at its maximum as well. The IS Audit function recommended to have policies and procedures in place to govern the Software Development function of the IT Division. Once this was done the risk rating reduced drastically.

Although Development Methodology and Project Management were also rated as "High" Importance, they were of "None" effectiveness before the IS Audit function. This means that no Development Methodology and Project Management controls were in place before IS Audit function. When the IS Audit function made its recommendations a Development Methodology and a Project Management approach were implemented subsequently increasing the effectiveness. As a result the risk, of unstructured software development approaches which might result in poor design software, expensive developments, inefficient software development and bad project management approaches was reduced.

User training was effective from the beginning at the F1 Company. The IT Audit function could only make small recommendations in order to improve the effectiveness of the user training thereby further reducing the risk of unqualified staff handling critical processes.

Software change management was not at the desired level of effectiveness until appropriate recommendations were made by the IS Audit function to bring it at the desired level of effectiveness to reduce and/or mitigate the risk of implementing unauthorized changes onto the application systems developed.

Protection over source code was not as sufficient as required before the IS Audit function, though its "Maximum" importance. The IS Audit function was able to identify weaknesses with a potential of losing the source code or it destruction. However, with appropriate recommendations this risk was reduced and/or mitigated and the effectiveness of the control was increase.

As shown in the figure 1, it is observed that Policies and Procedures, Software Change Management and Protection of Source Code were rated "Maximum" (score 5) for Importance. Development Methodology, Project Management and User Training were rated "High" (score 4). Effectiveness before IS Audit for Policies and Procedures, Development Methodology and Project Management were at "None" (score 0). User Training and Software Change Management were rated at "Medium" (score 3). As far as Protection of source code is concerned, it was rated as "Low" (score 2).

As a direct impact to the above the risk rating before IS

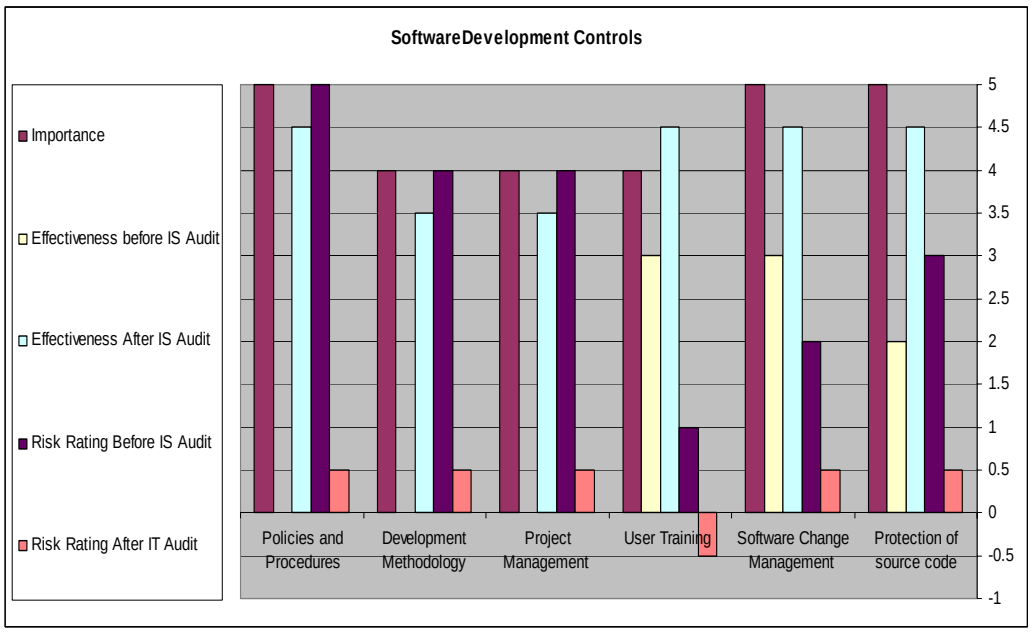

Fig. 1. Software Development Controls – Company F1.

Audit for Policies and Procedures was at "Maximum" (score 5). The risk rating before IS Audit for Development Methodology and Project Management was "High" (score 4). User Training it was at "Minimum" (score 1). For Software Change Management it was at "Low" (score 2) and for Protection of Source Code it was as at "Medium" (score 3).

Effectiveness after IS audit for most of the controls increased to "High/Maximum" (score 4.5) except for Development Methodology and Project Management where it increased to "Medium/High" (score 3.5) with a difference of 1 compared to the other controls. As a consequence the risk rating after IS Audit for all the controls dropped to "None/Minimum" (score 0.5) except for User Training where it dropped to "None" (score -0.5).

Company F2

There were only some policies and procedures governing software development. The IS Audit function recommended to have these policies and procedures complete to adequately govern the Software Development function of the IT Division. Once this was done the risk rating reduced significantly. A development methodology existed before the IS Audit function. However, its effectiveness improved after the IS Audit Methodology and the risk of inadequate developments reduced. A Project Management structure did exist before the IS Audit function as well. Its effectiveness improved after the IS Audit Methodology and the risk of inadequate developments reduced.

User training was effective from the beginning at F2 Company. The IT Audit function could only make small recommendations in order to improve the effectiveness of the user training thereby further reducing the risk of unqualified staff handling critical processes. Software Change Management and Protection of Source Code was not at the desired level of effectiveness until appropriate recommendations were made by the IS Audit function to bring it at the desired level of effectiveness to reduce and/or mitigate the risk of implementing unauthorized changes onto the application systems developed and losing the source code.

As illustrated in the figure 2, it is observed that most of the controls were of "Maximum" (score 5) Importance except for User Training where it was rated as "High" (score 4).

Effectiveness before IS Audit for Policies and Procedures was rated as "Minimum/Low" (score 1.5). Development Methodology and Project Management were rated as "Low/Medium" (score 2.5). User Training was rated as "Medium" (score 3). Effectiveness of Software Change Management and Protection of Source Code before IS Audit were rated as "Medium/High" (score 3.5). As a result the risk rating before IS Audit for Policies and Procedures was "Medium/High" (score 3.5). Development Methodology and Project Management were rated as "Low/Medium" (score 2.5). User Training was rated as "Minimum" (score 1). Software Change Management and Protection of Source Code were rated as "Minimum/Low" (score 1.5). Effectiveness after IS audit for nearly all the controls increased to "High/Maximum"

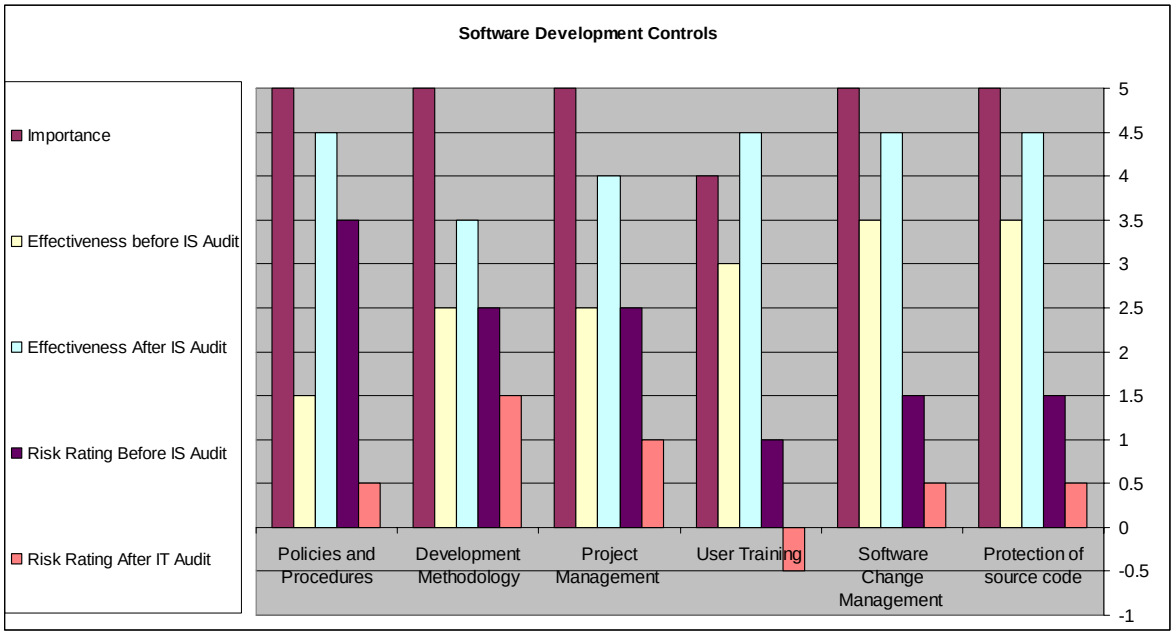

Fig. 2. Software Development Controls – Company F2.

(score 4.5) except for Development Methodology and Project Management where it increased to "Medium/High" (score 3.5) and "High" (score 4) respectively.

Therefore, the risk rating after IS Audit for Policies and Procedures, Software Change Management and Protection of Source Code dropped to "None/Minimum" (score 0.5). Risk Rating after IS Audit for Development Methodology dropped to "Minimum/Low" (score 1.5), for Project Management to "Minimum" (score 1) and for User Training to "None" (score -0.5).

Company G

There were sufficient policies and procedures governing software development. The IS Audit function recommended to have these policies and procedures refined to further reduce the risk rating. User training was also effective from the beginning. The IT Audit function could only make small recommendations in order to improve the effectiveness of the user training thereby further reducing the risk of unqualified staff handling critical processes. Source Code was also protected well enough.

The effectiveness of the above controls was increased by (0.5 points) and the risk rating was reduced by (0.5 points), thereby placing the risk rating after IS Audit to "None", which was much acceptable by the Company's management. Development Methodology and Project Management existed before the IS Audit function. However, their effectiveness improved after the IS Audit function and the risk of inadequate developments reduced. Software Change Management was not at the desired level of effectiveness until appropriate recommendations were made by the IS Audit function to bring it at the desired level of effectiveness to reduce and/or mitigate the risk of implementing unauthorized changes onto the application systems developed and losing the source code.

As pointed out in the figure 3 below, the Importance of Policies and Procedures, User Training and Protection of Source Code were rated as "High" (score 4). The effectiveness of these controls before IS Audit was given a rating of "Medium/High" (score 3.5) as a result their risk rating before IS Audit was "None/Minimum" (score 0.5). The effectiveness of these controls after IS Audit increased to be as "High" (score 4), subsequently the risk rating after IS Audit dropped to "None/Minimum" (score 0.5). The Importance of Development Methodology was rated as "High" (score 4). The effectiveness before IS Audit was given a rating of "Medium" (score 3) as a result the risk rating before IS Audit was "Minimum" (score 1). The effectiveness of this control after IS Audit increased to be at "Medium/High" (score 3.5), subsequently dropping the risk rating after IS Audit to "None/Minimum" (score 0.5). Project Management's Importance was rated as "Maximum" (score 5). The effectiveness before IS Audit was given a rating of "Medium/High" (score 3.5) as a result the risk rating before IS Audit was "Minimum/Low" (score 1.5). The effectiveness of this control increased to be at "High/Maximum" (score 4.5) after IS Audit, subsequently the risk rating after IS Audit dropped to "None/Minimum" (score 0.5). The Importance of Software Change Management was rated as "Maximum"

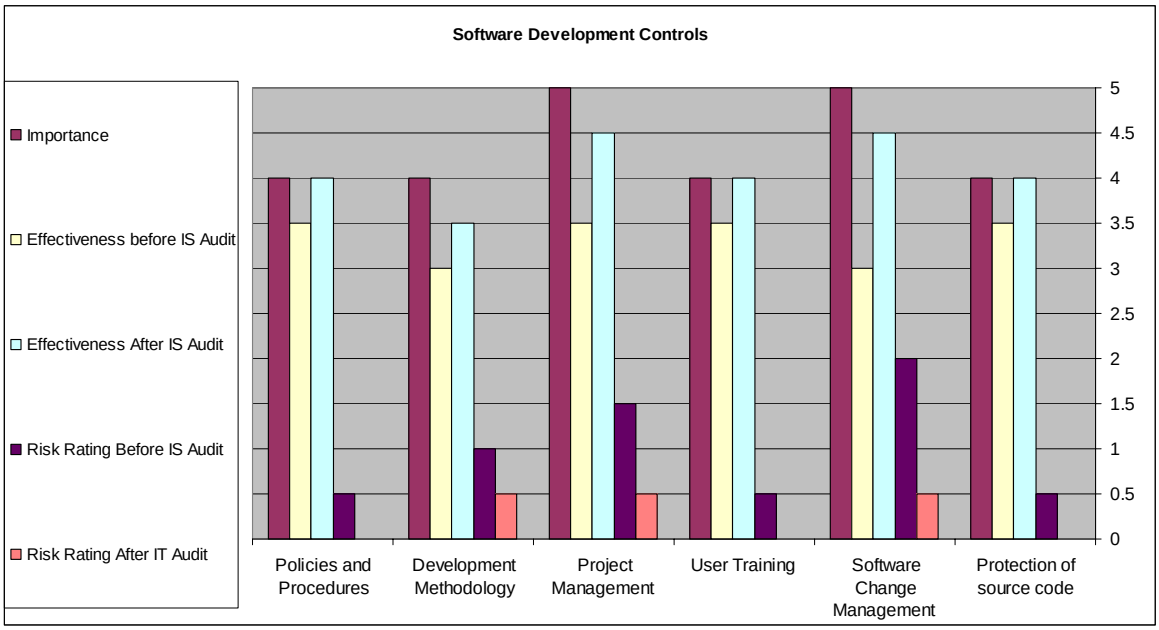

Fig. 3. Software Development Controls – Company G.

(score 5). The effectiveness before IS Audit was given a rating of "Medium" (score 3) as a result the risk rating before IS Audit was "Low" (score 2). The effectiveness of this control after IS Audit increased to be at "High/Maximum" (score 4.5), subsequently dropping the risk rating after IS Audit to "None/Minimum" (score 0.5).

We noticed from the technological infrastructure of the companies (i.e. F1, F2 and G) have almost similar infrastructure and methodologies due to the same standards that these organizations adopt. It is clearly evident that the effectiveness of the controls improved significantly after the IS Audit function, which one of its responsibilities is to ensure that the organizations adhere to best practices and international standards. The recommendations made by the IS Audit function to rectify the controls weaknesses also enhanced the control effectiveness. The standards put in place by international bodies such as ISACA, ISACF, ITGI and ISC2, proved to be effective and efficient in improving the control structure over the IT processes and management by stipulating the required controls. By adhering to the standards put in place by ISACA, ISACF, ITGI and ISC2, the organizations had a similar level of control effectiveness and compliance level after the IS Audit was conducted. At the company F1 it was observed that, the effectiveness of the controls increased and, the risk rating dropped, by an average of 2.1 points after IS Audit. For company F2 it was observed that, the effectiveness of the controls increased and, the risk rating dropped, by an average of 1.5 points after IS Audit. With regard to company G it was observed that, the effectiveness of the controls increased and, the risk rating dropped, by an average of 1.1 points after IS Audit.

CONCLUSION

It was observed that the organizations under the research did not reveal further information about their weaknesses, which somewhat affected the analysis of the control and risk evaluation. However, enough information was provided to conduct the research effectively. Furthermore, it was observed that some controls were not implemented despite the repeat recommendations of the IS Audit function. When further inquired, it was found that the higher management and/or the board of directors of that particular company were not applying enough force on the line management including IT to implement these controls. Based on the findings and analysis of the data gathered it is proved that, by implying the control objectives and standards stipulated by industry leaders such as ISACA, ISACF, ITGI and ISC2 using effective, efficient and adequate IS Audit methodologies, the IS Audit function was successfully able to identify and address control weaknesses, security, systems vulnerability and threat concerns of the information systems and supported business processed.

REFERENCES

Ciborra, C. 2002. Labyrinths of Information. Oxford University Press. 15-25.

Altar, S. 2003. Information Systems: a management perspective. Pearson Inc. USA. 480-486.

Solomon, GM. and Chapple, M. 2005. Information Security Illuminated. Jones and Bartlett Publishers, MA, USA. 340-343.

CISA Review Manual. 2007, ISACA, USA. 20-24.