Canadian Journal of Pure and Applied Sciences
Vol. 13, No. 2, pp. 4781-4791, June 2019
Online ISSN: 1920-3853; Print ISSN: 1715-9997
Available online at www.cjpas.net

Canadian Journal of pure & applied sciences

EFFECTIVENESS OF SOFTWARE AND HARDWARE ACQUISITION CONTROLS IN INFORMATION SYSTEMS ORGANIZATIONS

*Muhammad Asif Khan[1] and Ali Al Ghadeer[2]
[1]College of Computer Science and Engineering, Taibah University, Madinah al Munawwara, Saudi Arabia
[2]Saudi Credit and Savings Bank, Riyadh, Saudi Arabia

ABSTRACT

Information Systems (IS) organizations are experiencing a mounting pressure to contribute organizational success and to secure information asset, therefore, protection of information assets has become a paramount concern in IS organizations. IS organizations recognize the importance of evaluation of information systems and implemented controls so that any risk either could be removed or mitigated for their information asset and infrastructure by implementing appropriate measures. The aim of this paper is to analyze, explain and demonstrate the effectiveness of software and hardware acquisition controls in IS organizations to ensure optimum benefits in the organizations. Also, the study determines that whether organizations are careful in implementing the preventative controls and how effectively the organizations benefit from the controls for software and hardware acquisition. In order to complete the current study data has been collected from different financial organizations, which have an existing IS audit function in place. The data has been analyzed and approach used by these organizations has been evaluated in view of specific industry standards of IS audit and control set by organizations.

Keywords: Information systems organizations, Preventative acquisition controls, audit and controls, software acquisition controls.

INTRODUCTION

Enterprises execute their applications on various hardware that spread over multiple locations. In this situation organizations avail help of a management software that may face security problems and therefore, audit and controls problems may arise. Essentially firms would like to acquire effective software and hardware controls that could guard their information assets. Also, IS auditing is to ensure the effectiveness of the implemented controls in organizations. In a study (Almohammadi *et al.*, 2011) it is stated that an IS audit includes assessment of controls, gathering evidence, resources for computing, reviewing documents etc. According to (Majdalawieh and Zaghloul, 2009) an IS audit is a measurement of compliance of a system to the defined procedures, policies, rules and regulations that ensure integrity of data. Likewise, (Mahzan and Veerenkutty, 2011) underscored on auditing and stressed on effectiveness of policies and procedures that are complied with the defined rules in organizations. Organizations can achieve their objectives by effective risk management and governing process (Reding *et al.*, 2013).

*Corresponding author e-mail: asifkhan2k@yahoo.com

IS audit is a process to gather evidence and perform an assessment to ensure information assets security and data integrity (Li, 2016). In a study Mishra and Dhillon (2008) it argues that in organizations information systems function at three levels and controls should operate at all levels at the same time so that information systems show effectiveness. If controls are not properly in place in organizations or do not operate appropriately, the data integrity is on stack and valuable information likely to be compromised. Therefore, firms perform audit of the implemented controls at times to ensure sustainability of security of information systems. Ana-Maria *et al.* (2010) argue that minimum set of controls and security policy need to be audited in order to ensure risks at acceptable level. A continuous auditing is necessary for sustainability in security of information assets. A study Alifah *et al.* (2014) was carried out for sustainability of information systems auditing in which different techniques for continuous auditing have been discussed. Enterprises strive to maintain the controls operational in order to protect information assets. This study examines different software and hardware acquisition controls and their effectiveness in financial institutions.

MATERIALS AND METHODS

The aim of this study is to determine the level of effectiveness of software and hardware controls in order to mitigate risks, vulnerabilities and weaknesses in IS organizations. In order to complete the study, data from three financial institutions (i.e. Bank A, Bank B and Bank C)was collected by using data collection techniques such as interviews, observations, reviewing documents were used. A survey instrument was also developed and distributed at various personnel levels in both the banks. In the survey instrument, different indicators were used to allow respondents to rate the importance, effectiveness before audit, effectiveness after audit, risk rate before audit and risk rate after audit. The indicators used in the questionnaire are as follows:

Importance – importance of control (level)
Effectiveness before audit - effectiveness of the control before the IS audit in the bank
Effectiveness after audit – effectiveness of the control after the IS audit in the bank
Risk rating before audit – risk level an IT function experienced before the IS audit was carried out
Risk rating after audit – risk level an IT function experienced after the IS audit was conducted

A Likert's scale 1-5 was used to determine the indicators where 1 indicates minimum and 5 depicts maximum (i.e. 1 = minimum, 2 = low, 3 = medium, 4 = high, 5 = maximum). If an indicator, for example, Importance, has been rated as 5 (i.e. maximum) shows that the control is extremely important to govern the technology process. Similarly, an indicator with value 1 (i.e. minimum) shows poor effectiveness of the control.

In the following section we discuss software acquisition and hardware acquisition controls and their description which have been studied in the financial institutions under study.

Software Acquisition Controls

Policies and Procedure
Policies are high-level documents that document the senior management's way of thinking, sometimes referred as the "corporate philosophy". Procedures are detailed documents which document the business processes and the controls embedded therein, therefore combine together Policies and Procedures are considered as preventative controls, because if complies to accurately without failure, the impact of the risks can be reduced and/or mitigated.

Acquisition Methodology
An appropriate acquisition methodology ensures that the acquisition process is carried out as efficiently and effectively possible, thus preventing and/or mitigating acquisitions risks.

Annual Maintenance Contracts
Annual Maintenance Contracts ensure that regular updates, patches, releases, maintenance, troubleshooting and debugging is provided by the vendor.

Escrow Agreements
Escrow agreements ensure that the source code can be retained in case the vendor goes out of business by the customer, where the source code is held under an escrow with an agreed upon third party. This is considered to be a preventative and corrective control.

Updates and Patches
Regularly updating and patching the software ensures that possible vulnerabilities are eliminated, enhanced functionality is provided, etc. Practicing regular updating and patching prevents and/or reduces risks, detects risks if occurred and corrects it in a best possible way.

Third Party Monitoring
Monitoring third party performance helps the organization to determine its value-for-money of the AMCs and if the vendors or third party service providers are providing them with the required level of service. Monitoring is usually a detective control.

Third Party Qualifications
Ensuring high qualification of third party service providers ensures better quality of service. This serves as an adequate preventative control where an organization ensures that it is employing the best available third party on the investment its making.

Third Party Contracts
This consists of various contracts such as confidentiality contracts, service contracts, implementation contracts, etc.

Hardware Acquisition Controls

Policies and Procedures
Policies are high-level documents that document the senior management's way of thinking, sometimes referred as the "corporate philosophy". Procedures are detailed documents which document the business processes and the controls embedded therein, therefore combine together Policies and Procedures are considered as preventative controls, because if complies to accurately without failure, the impact of the risks can be reduced and/or mitigated.

Acquisition Methodology
An appropriate acquisition methodology ensures that the acquisition process is carried out as efficiently and

effectively possible, thus preventing and/or mitigating acquisitions risks.

Assessment of new hardware
An appropriate acquisition methodology ensures that the acquisition process is carried out as efficiently and effectively possible, thus preventing and/or mitigating acquisitions risks.

Technology standards
Defining acceptable technology standards prevents organizations from utilizing hardware or technological infrastructure below the standards predefined by them.

Preventative maintenance
Preventative maintenance ensures that hardware and technology equipment are prevented from failure and malfunctions.

Annual Maintenance Contracts
Annual Maintenance Contracts ensure that regular updates, patches, releases, maintenance, troubleshooting and debugging is provided by the vendor.

Third Party Monitoring
Monitoring third party performance helps the organization to determine its value-for-money of the AMCs and if the vendors or third party service providers are providing them with the required level of service. Monitoring is usually a detective control.

Third Party Qualifications
Ensuring high qualification of third party service providers ensures better quality of service. This serves as an adequate preventative control where an organization ensures that it is employing the best available third party on the investment its making.

Third Party Contracts
This consists of various contracts such as confidentiality contracts, service contracts, implementation contracts, etc.

RESULTS AND DISCUSSION

The data collected for the above stated software and hardware acquisition controls in the financial institutions has been analyzed and discussed separately as follows

Software Acquisition Controls (Bank A)
Both Policies and Procedures and Acquisition Methodology were rated “Maximum” for Importance. Their effectiveness before IS Audit were not at the required level. Therefore, the risk rating was not at an acceptable level to the management. The IS Audit function recommended for some enhancements to the existing policies and procedures and acquisition methodology to improve the effectiveness of these controls. As a result the risk of inappropriate acquisitions and investments was reduced and/or mitigated.

Annual Maintenance Contract were well in place even before the IS Audit function because number of systems are third party systems (i.e. vendor supplied software) and require a contract to maintain these systems. However, the IS Audit function identified one or two third party solutions that the Bank did not have an Annual Maintenance Contract signed with. This was accordingly rectified thereby increasing the control effectiveness and reducing and/or mitigating the risk of the supplier failing to provide timely support, updates, patches and debugging services on annual basis.

Because not all vendors provide escrow agreements, the Bank was unable to improve the control effectiveness and avoid the risk. However, there were no escrow agreements for some third party applications for which their vendors provided such agreements as well. These vendors were identified by the IS Audit function and rectified accordingly. The controls was improved and the risk of the Bank being unable to retain the source code in case the vendor goes out of business was reduced and/or mitigated.

Receiving updates and patches from the vendor on annual basis is an important control for any organisation using third party application. Because these updates and patches address potential weaknesses, program errors and bugs. This control was effective before the IS Audit function, however, it was slightly improved after the IS Audit function and dropping the risk to an acceptable level to the management.

Monitoring Third Party was performed before IS Audit but not as effectively as required to reduce the risk to an acceptable level to the management. The IS Audit function introduced techniques such as third party feedback forms to be filled in by the IT staff after every third party provided its service. Thus reducing the risk of unacceptable and unreliable third party service.

Third Party Qualifications were not assessed at all before availing their services. This created a risk of unreliable and qualified service being provided. The IS Audit function successfully identified this weakness and recommended that Third Party Qualifications are assess before hiring their services. The risk was reduced to an acceptable level to the management.

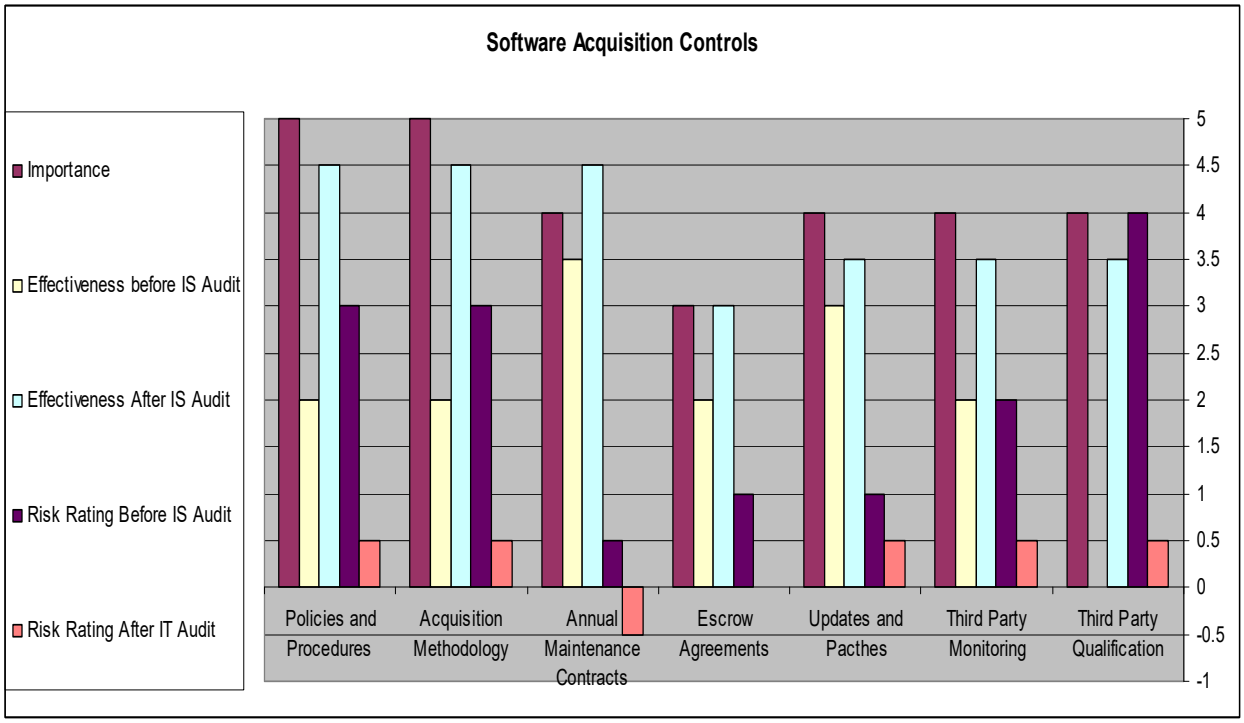

Fig. 1. Software Acquisition Controls – Bank A.

As illustrated in the Figure 1 of the Software Acquisition Controls it is noted that Policies and Procedures and Acquisition Methodology were rated "Maximum" (score 5) for Importance. Annual Maintenance Contracts, Updates and Patches, Third Party Monitoring and Third Party Qualification were rated as "High" (score 4). Escrow Agreements was rated as "Medium" (score 3).

Effectiveness before IS Audit for Policies and Procedures, Acquisition Methodology, Escrow Agreements and Third Party Monitoring were rated as "Low" (score 2). Annual Maintenance Contracts was rated as "Medium/High" (score 3.5). Updates and Patches were given a score of "Medium" (score 3) and Third Party Qualification was rated as "None" (score 0).

Effectiveness after IS audit for Policies and Procedures, Acquisition Methodology and Annual Maintenance Contracts increased to "High/Maximum" (score 4.5). Escrow Agreements increased to "Medium" (score 3). Updates and Patches, Third Party Monitoring and Third Party Qualification increased to "Medium/High" (score 3.5).

Risk rating before IS Audit for Policies and Procedures and Acquisition Methodology was "Medium" (score 3). Annual Maintenance Contracts was at "None/Minimum" (score 0.5).

Escrow Agreements and Updates and Patches was rated at "Minimum" (score 1). Third Party Monitoring was rated as "Low" (score 2) and Third Party Qualification was rated as "High" (score 4).

It was noted that rating for risk after IS Audit for all the controls dropped to "None/Minimum" (score 0.5) except for Annual Maintenance Contracts where it dropped to "None" (score -0.5) and Escrow Agreements where it dropped to "None" (score 0).

Hardware Acquisition Controls (Bank A)

Both Policies and Procedures and Acquisition Methodology were rated "Maximum" for Importance. Their effectiveness before IS Audit were not at the required level. Therefore, the risk rating was not at an acceptable level to the management. The IS Audit function recommended for some enhancements to the existing policies and procedures and acquisition methodology to improve the effectiveness of these controls. As a result the risk of inappropriate acquisitions and investments was reduced and/or mitigated.

The Bank had effective techniques to assess new hardware, which was introduced to the organisation. It also had high technology standards. The risk rating for both these controls was at an acceptable level to the management as it was "None". The IS Audit function just improved these controls and dropped the risk rating to a level which is even lower than the management's expectations.

Preventative Maintenance of hardware was as effective as it should be as per the IS Audit functions

recommendations as well. Therefore, the IS Audit function could not recommend anything to further strengthen the controls because it was effective enough to an acceptable level to the management. The risk rating also remained the same after IS Audit function as it was before the IS Audit function.

Annual Maintenance Contract were well in place even before the IS Audit function because all the hardware are provided by third parties and require a contract to perform preventative maintenance after the warranty period is over. However, the IS Audit function identified couple of suppliers that the Bank did not have an Annual Maintenance Contract signed with. This was accordingly rectified thereby increasing the control effectiveness and reducing and/or mitigating the risk of the supplier failing to provide timely support, replacement, repair and services on annual basis. The risk was reduced to an acceptable level to the management.

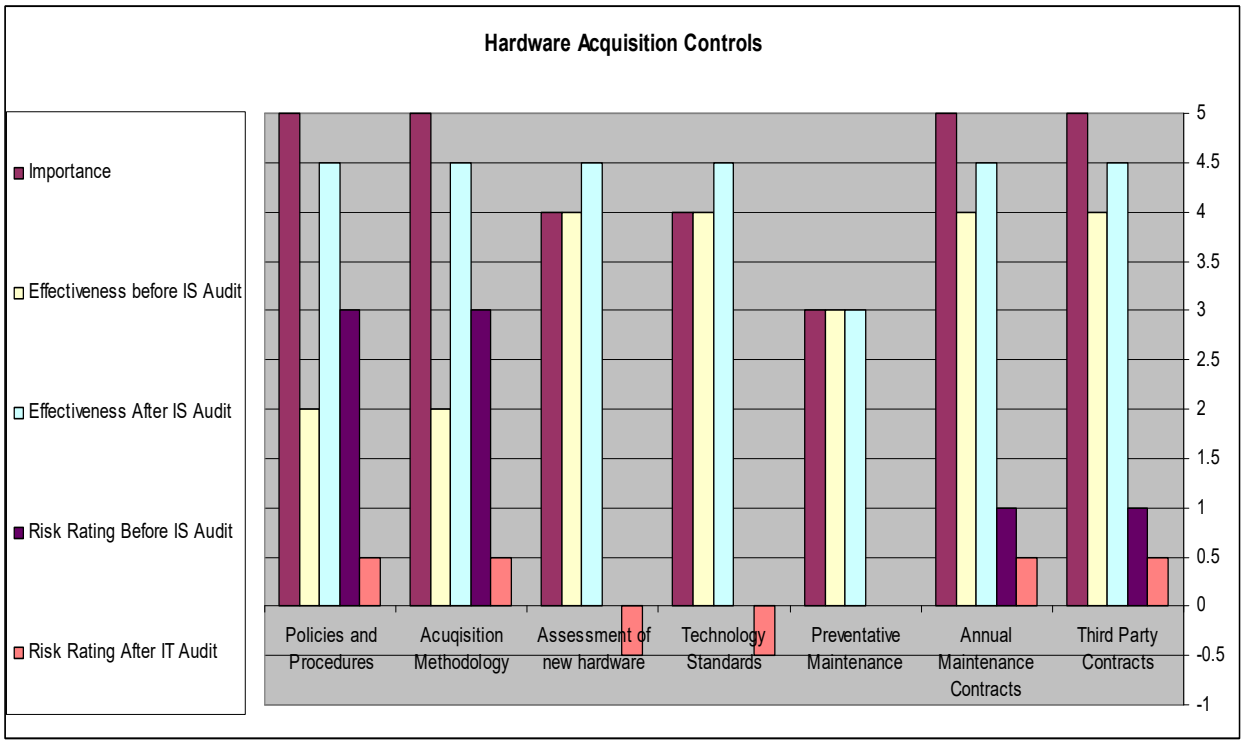

Fig. 2. Hardware Acquisition Controls – Bank A.

As it can be noted from the Figure 2 that the Importance of Policies and Procedures and the Acquisition Methodology was rated as "Maximum" (score 5). The effectiveness before IS Audit was given a rating of "Low" (score 2) as a result the risk rating before IS Audit was "Medium" (score 3) for both the controls. The effectiveness of Policies and Procedures and the Acquisition Methodology after IS Audit increased to be at "High/Maximum" (score 4.5), subsequently the risk rating after IS Audit dropped to "None/Minimum" (score 0.5) for both the controls.

The Importance of Assessment of new hardware and Technology was rated as "High" (score 4). The effectiveness before IS Audit was given a rating of "High" (score 4) as a result the risk rating before IS Audit was "None" (score 0) for both the controls. The effectiveness of these controls increased to be at "High/Maximum" (score 4.5) after IS Audit, subsequently the risk rating after IS Audit dropped to "None" (score -0.5) for both the controls.

Preventative Maintenance's Importance was rated as "Medium" (score 3). The effectiveness before and after IS Audit for this control remained the same. Therefore the risk rating before and after IS Audit also remained the same.

The Importance of Annual Maintenance Contracts and Third Party Contracts was rated as "Maximum" (score 5). The effectiveness before IS Audit for both the controls was given a rating of "High/Maximum" (score 4.5) as a result the risk rating before IS Audit was "Minimum" (score 1). The effectiveness of these controls increased to be at "High/Maximum" (score 4.5) after IS Audit, subsequently the risk rating after IS Audit dropped to "Minimum/Now" (score 0.5) for both the controls.

Software Acquisition Controls (Bank B)

Policies and Procedures and Acquisition Methodology were rated "Maximum" for Importance. Their effectiveness before IS Audit was not at the required level. Therefore, the risk rating was not at an acceptable level to the management. The IS Audit function recommended for some enhancements to the existing policies and procedures and acquisition methodology to improve the effectiveness of these controls. As a result the risk of inappropriate acquisitions and investments was reduced and/or mitigated.

Annual Maintenance Contract were well in place even before the IS Audit function because number of systems are third party systems (i.e. vendor supplied software) and require a contract to maintain these systems. However, the IS Audit function identified one or two third party solutions that the Bank did not have an Annual Maintenance Contract signed with. This was accordingly rectified thereby increasing the control effectiveness and reducing and/or mitigating the risk of the supplier failing to provide timely support, updates, patches and debugging services on annual basis.

The Bank was successful to improve the Escrow Agreements' effectiveness and avoid the risk. However, there were no escrow agreements for some third party applications for which their vendors provided such agreements. These vendors were identified by the IS Audit function and rectified accordingly. The control was improved and the risk of the Bank being unable to retain the source code in case the vendor goes out of business was reduced and/or mitigated.

Receiving updates and patches from the vendor on annual basis is an important control for any organisation using third party application. Because these updates and patches address potential weaknesses, program errors and bugs. This control was effective before the IS Audit function, however, it was slightly improved after the IS Audit function and dropping the risk to an acceptable level to the management.

Monitoring Third Party and Third Party Qualification assessment were effectively performed before IS Audit to reduce the risk to an acceptable level to the management. The IS Audit function introduced small changes to reduce the risk, of unacceptable and unreliable third party service, to lower than the acceptable level to the management.

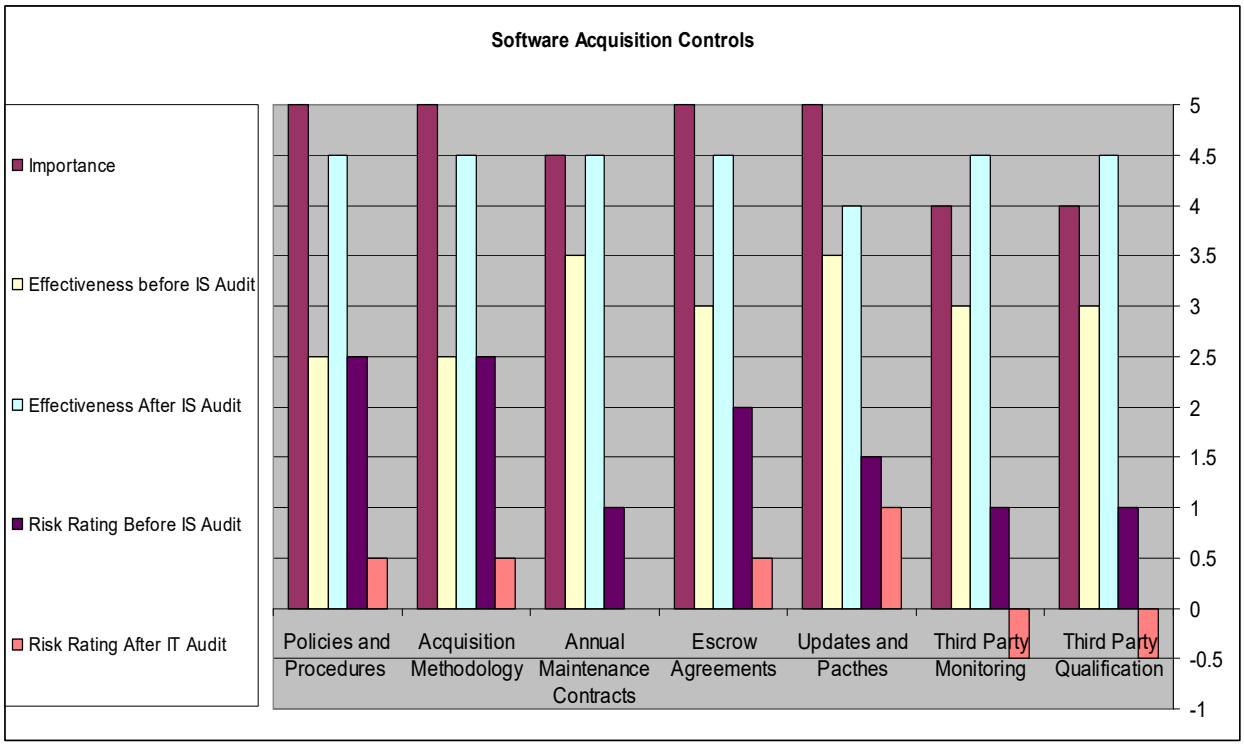

Fig. 3. Software Acquisition Controls – Bank B.

As given in the Figure 3 of the Software Acquisition Controls it is observed that Policies and Procedures, Acquisition Methodology, Escrow Agreements and Updates and Patches were of "Maximum" (score 5) Importance. Annual Maintenance Contracts was rated as "High/Maximum" (score 4.5). Third Party Monitoring

and Third Party Qualification were rated as "High" (score 4).

Effectiveness before IS Audit for Policies and Procedures and Acquisition Methodology was rated as "Low/Medium" (score 2.5). Annual Maintenance Contracts and Updates and Patches were rated as "Medium/High" (score 3.5). Escrow Agreements, Third Party Monitoring and Third Party Qualification were rated as "Medium" (score 3).

As a result the risk rating before IS Audit for Policies and Procedures and Acquisition Methodology was "Low/Medium" (score 2.5). Annual Maintenance Contracts, Third Party Monitoring and Third Party Qualification were rated as "Minimum" (score 1). Escrow Agreements was rated as "Low" (score 2) and Updates and Patches was rated as "Minimum/Low" (score 1.5).

Effectiveness after IS audit for nearly all the controls increased to "High/Maximum" (score 4.5) except Updates and Patches where it increased to "High" (score 4).

Therefore, the risk rating after IS Audit for Policies and Procedures, Acquisition Methodology and Escrow Agreements dropped to "None/Minimum" (score 0.5). Risk Rating after IS Audit for Annual Maintenance Contracts dropped to "None" (score 0), for Updates and Patches to "Minimum" (score 1) and for Third Party Monitoring and Third Party Qualification to "None" (score -0.5).

Hardware Acquisition Controls (Bank B)

Policies and Procedures, Acquisition Methodology, Technology Standards and Preventative Maintenance all these controls were rated "Maximum" for Importance. The effectiveness of these before IS Audit were not at the required level. Furthermore, the risk rating was not at an acceptable level to the management. The IS Audit function recommended for some changes to improve the effectiveness of these controls. As a result the risk of was reduced and/or mitigated.

The Bank had effective techniques to assess new hardware, which was introduced to the organisation. It also had high technology standards. However, the IS Audit function recommended improvements over these controls to drop the risk rating to "None" a level which is meets the management's expectations.

Technology Standards and Preventative Maintenance of hardware were not as effective as they should be. The IS Audit function recommended to further strengthen the controls in order to reduce the risk rating to an acceptable level to the management.

Annual Maintenance Contracts and Third Party Contract were well in place even before the IS Audit function because all the hardware are provided by third parties and require a contract to perform preventative maintenance after the warranty period is over. The IS Audit function could identify only minor changes that could merely drop the risk rating.

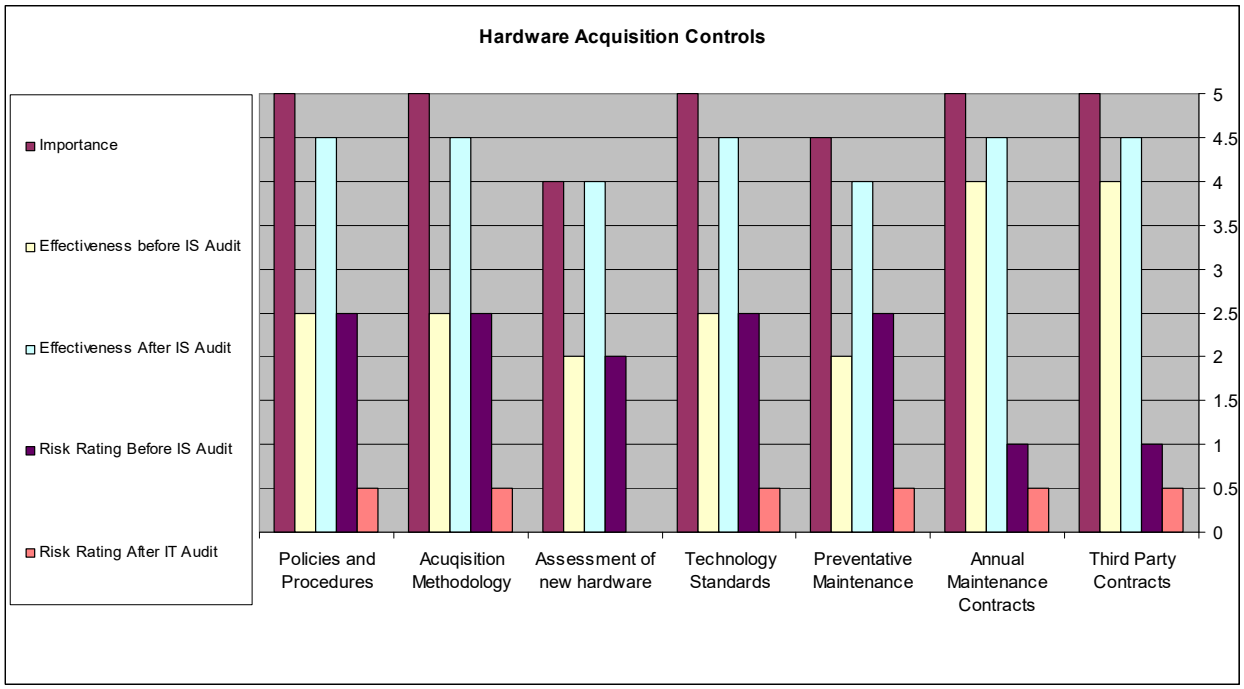

Fig. 4. Hardware Acquisition Controls – Bank B.

As given in the Figure 4 of the Hardware Acquisition Controls it is observed that majority of the controls were of "Maximum" (score 5) Importance except for Assessment of New Hardware and Preventative Maintenance where they were assigned a rating of "High" (score 4) and "High/Maximum" (score 4.5) respectively.

Effectiveness before IS Audit for Policies and Procedures, Acquisition Methodology and Technology Standards was rated as "Low/Medium" (score 2.5). Assessment of New Hardware and Preventative Maintenance were rated as "Low" (score 2).Annual Maintenance Contracts and Third Party Qualification were rated as "High" (score 4).

As a result the risk rating before IS Audit for Policies and Procedures, Acquisition Methodology, Technology Standards and Preventative Maintenance was "Low/Medium" (score 2.5). Assessment of New Hardware was rated as "Low" (score 2). Annual Maintenance Contract and Third Party Contracts were rated as "Minimum" (score 2) and Updates and Patches was rated as "Minimum/Low" (score 1).

Effectiveness after IS audit for almost all the controls increased to "High/Maximum" (score 4.5) except for Assessment of New hardware and Preventative Maintenance where they both increased to "High" (score 4).

Thus, the risk rating after IS Audit for all the controls dropped to "None/Minimum" (score 0.5) except for Assessment of New Hardware, where it went further down to "None" (score 0).

Software Acquisition Controls (Bank C)

Policies and Procedures and Acquisition Methodology both these controls were rated "Maximum" for Importance. Their effectiveness before IS Audit was slightly lower than the required level. Therefore, the risk rating was somewhat to an acceptable level to the management. However, the IS Audit function recommended for some enhancements to the existing policies and procedures and acquisition methodology to further improve the effectiveness of these controls. As a result the risk of inappropriate acquisitions and investments was reduced and/or mitigated.

Annual Maintenance Contracts were well in place even before the IS Audit function because number of systems are third party systems (i.e. vendor supplied software) and required a contract to maintain these systems. The IS Audit identified some weaknesses and recommended their rectification thereby increasing the control effectiveness and reducing and/or mitigating the risk of the supplier failing to provide timely support, updates, patches and debugging services on annual basis.

Receiving updates and patches from the vendor on annual basis is an important control for any organization using third party application. Because these updates and patches address potential weaknesses, program errors and bugs. This control was effective before the IS Audit function, however, it was slightly improved after the IS Audit function and dropping the risk to an acceptable level to the management.

The Bank was successful to improve the control effectiveness and avoid the risk. However, there were no escrow agreements for some third party solutions for which their vendors provided such agreements. These vendors were identified by the IS Audit function and rectified accordingly. The control was improved and the risk of the Company being unable to retain the source code in case the vendor goes out of business was reduced and/or mitigated.

Monitoring Third Party and Third Party Qualification assessment were not performed as effectively as they should be performed before IS Audit in order to reduce the risk to an acceptable level to the management. The IS Audit function introduced small changes to reduce the risk, of unacceptable and unreliable third party service, to lower than the acceptable level to the management.

As given in the Figure 5 of the Software Acquisition Controls it is observed that majority of the controls were of "Maximum" (score 5) Importance except for Third Part Monitoring and Third Party Qualification where they were assigned a rating of "High/Maximum" (score 4.5).

Effectiveness before IS Audit for Policies and Procedures and Acquisition Methodology was rated as "/Medium/High" (score 3.5). For Annual Maintenance Contracts and Updates and Patches it was rated as "High" (score 4). Escrow Agreements, Third Party Monitoring and Third Party Qualification were rated as "Low/Medium" (score 2.5) for effectiveness before IS Audit.

As a result the risk rating before IS Audit for Policies and Procedures and Acquisition Methodology was "Minimum/Low" (score 1.5). For Annual Maintenance Contract and Updates and Patches it was rated as "Minimum" (score 1). Escrow Agreement was rated as "Low/Medium" (score 2.5). Third Party Monitoring and Third Party Qualification was rated as "Low" (score 2) for risk rating before IS Audit.

Effectiveness after IS audit for almost all the controls increased to "High/Maximum" (score 4.5) except for Third Party Monitoring and Third Party Qualification where they both increased to "High" (score 4).

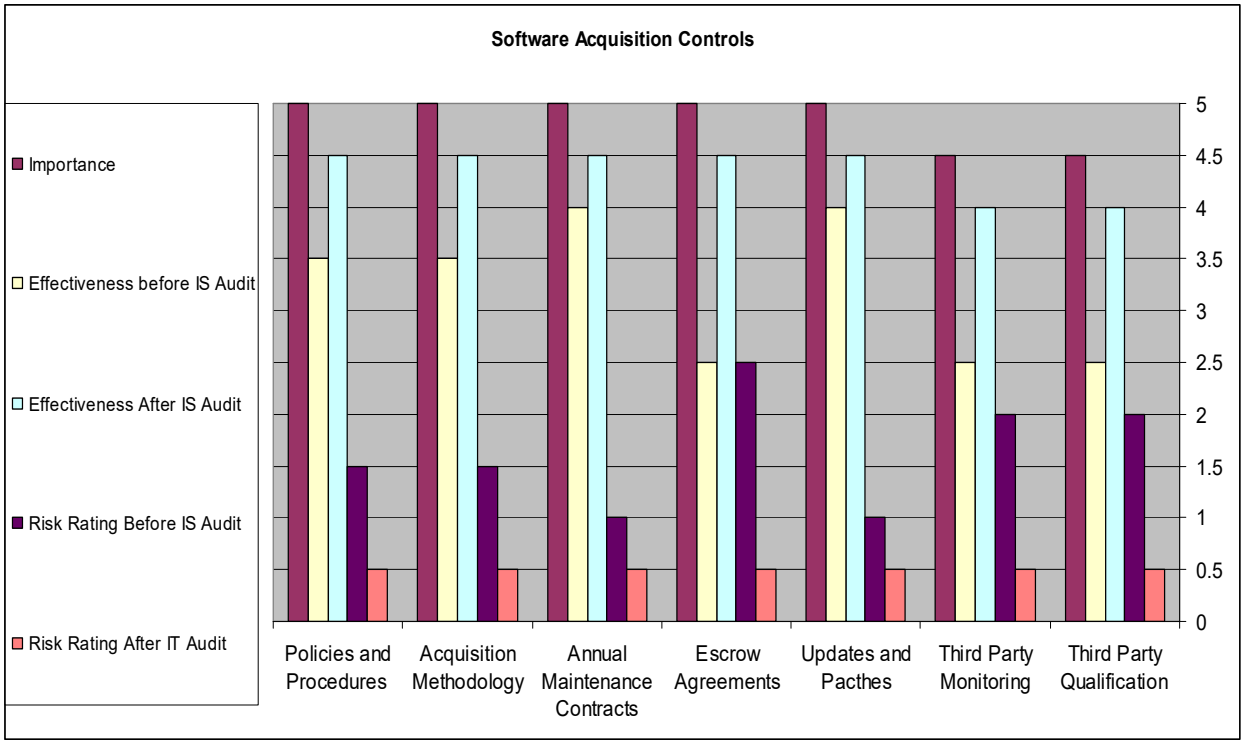

Fig. 5. Software Acquisition Controls – Bank C.

Thus, the risk rating after IS Audit for all the controls, without any exceptions, dropped to "None/Minimum" (score 0.5).

Hardware Acquisition Controls (Bank C)

Policies and Procedures and Acquisition Methodology were rated "Maximum" for Importance. The effectiveness of these before IS Audit were somewhat in close proximity to the required level. Furthermore, the risk rating was fairly acceptable to the management. The IS Audit function recommended for some changes to further improve the effectiveness of these controls. As a result the risk of was further reduced and/or mitigated.

The Company had effective techniques to assess new hardware, which were installed by the organisation. The IS Audit function recommended improvements over these controls to drop the risk rating to "None" a level which is meets the management's expectations.

Technology Standards were not as effective as they should be. The IS Audit function recommended to further strengthen the controls in order to reduce the risk rating to an acceptable level to the management.

Preventative Maintenance was not performed as effectively as it should be performed before IS Audit in order to reduce the risk to an acceptable level to the management. The IS Audit function suggested to perform preventative maintenance in order to reduce the risk of failure of hardware during critical business hours.

Annual Maintenance Contracts and Third Party Contract were well in place even before the IS Audit function because all the hardware are provided by third parties and require a contract to perform preventative maintenance after the warranty period is over. The IS Audit function could identify only minor changes that could drop the risk rating to "None".

As it can be observed in the Figure 6 above of Hardware Acquisition Controls it can be noted that the Importance of Policies and Procedures, Acquisition Methodology and Technology Standards was rated as "Maximum" (score 5). Annual Maintenance Contracts and Third Party Contracts were rated as "High/Maximum" (score 4.5). Assessment of New Hardware and Preventative Maintenance were rated as "High" (score 4) for Importance.

Effectiveness before IS Audit for Policies and Procedures, Acquisition Methodology, Assessment of New Hardware and Annual Maintenance Contracts was at "Medium/High" (score 3.5). For Technology Standards it was at "Medium" (score 3). Preventative Maintenance and Third Party Contracts were at "Minimum/Low" (score 1.5) and "High" (score 4), respectively.

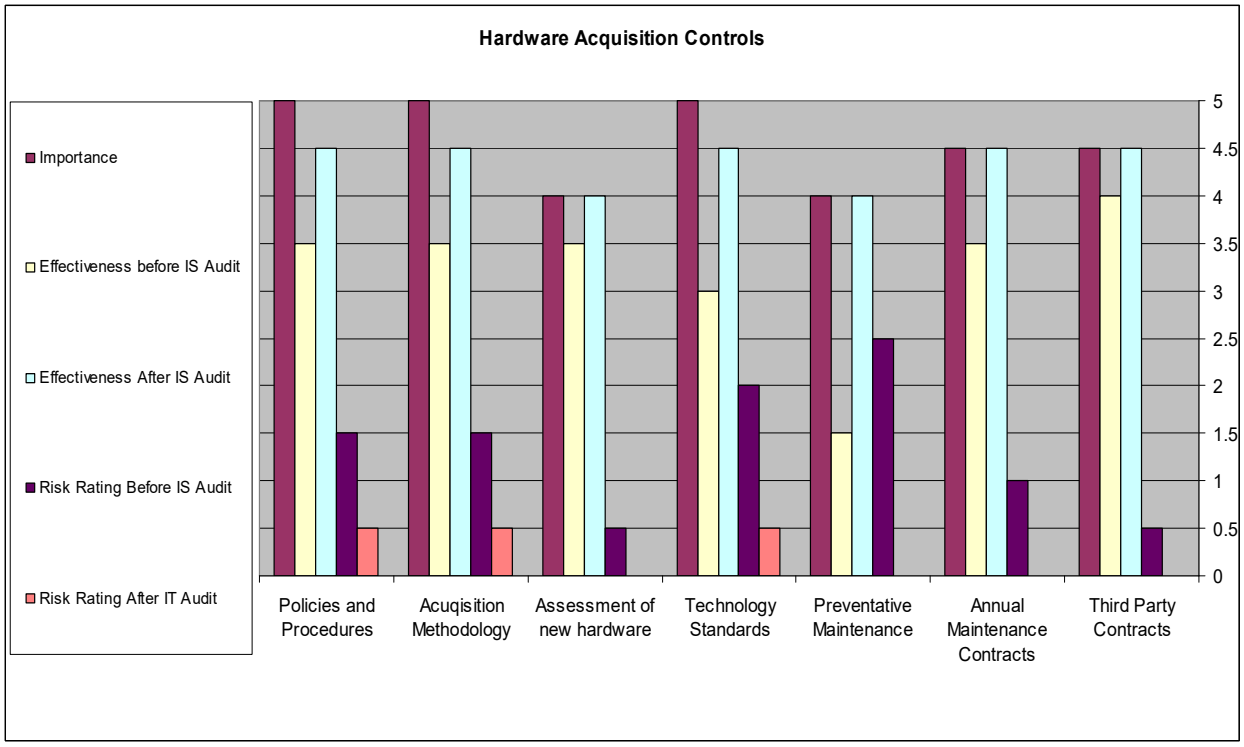

Fig. 6. Hardware Acquisition Controls – Bank C.

Effectiveness after IS audit for almost all the controls increased to "High/Maximum" (score 4.5) except for Assessment of New Hardware and Preventative Maintenance where it increased to "High" (score 4).

Risk rating before IS Audit for Policies and Procedures and Acquisition Methodology was at "Minimum/Low" (score 1.5). For Assessment of New Hardware and Third Party Contracts it was at "None/Minimum" (score 0.5). Technology Standards was at "Low" (score 2), Preventative Maintenance was at "Low/Medium" (score 2.5) and Annual Maintenance Contract was at "Minimum" (score 1) for risk rating before IS Audit.

The risk rating after IS Audit for Policies and Procedures, Acquisition Methodology and Technology Standards dropped to "None/Minimum" (score 0.5). Assessment of New Hardware, Preventative Maintenance, Annual Maintenance Contracts and Third Party Contracts dropped to "None" (score 0) for risk rating after IS Audit.

CONCLUSION

This study shows the financial institutions under investigations were apprehended in providing detailed information, however, enough data was provided to achieve the desired objectives. It was noted there were some controls were not implemented in either of the organizations and the data integrity could be compromised. The main reason was the lack of communication and enforcement of rules from the management. It was found that entailing rules, regulations and standards specified by the industry leaders such as ISACA, ITGI and ISC2 helped identifying the vulnerabilities and weaknesses of controls. Therefore, it is recommended to comply with the industry standards to adequately safeguard information systems in organizations.

REFERENCES

Abdolmohammadi, MJ. and Boss, SR. 2011. Factors associated with IT audits by the internal function. International Journal of Accounting Information Systems. 11:140-151.

Ana-Maria, S., Bîzoi, M. and Filip, G. 2010. Audit for Information Systems Security. Informatica Economica Journal. 14.

Alifah, R., Nemrat, A. and Preston, D. 2014. Sustainability in Information Systems Auditing. European Scientific Journal. 3:458-472.

Li, T. 2016. The IT audit research based on the information system success model and COBIT, In proceedings of 10th International Conference on Intelligent Systems and Controls (ISCO). 1-3.

Majdalawieh, M. and Zaghloul, I. 2009. Paradigm shift in information systems auditing. Managerial Auditing Journal. 24(4):352-367.

Mahzan, N. and Veerankutty, F. 2011.IT auditing activities of public auditors in Malaysia. African Journal of Business Management. 5(5):1551-1563.

Mishra, S. and Dhillon, G. 2008. Defining Internal Control Objectives for Information Systems Security: A Value Focused Assessment. In proceedings of 16th European Conference on Information Systems. ECIS. 1334-1345.

Reding, K., Sobel, P., Anderson, U., Head, M., Ramamoorti, S., Salamasick, M. and Riddle, C. 2013. Internal auditing. Altomonte Springs, Fla. Institute of Internal Auditors. Research Foundation.

Received: March 20, 2019; Accepted: May 7, 2019