Journal of Economic Cooperation and Development, **41**, 2 (2020), 67-90

Availability of General Control Procedures of the Security of Accounting Information System (AIS): Evidence from Yemen

Yahya Maresh H. Hazaa[1] and Jogdand D. A.[2]

Accounting information system AIS is the most important tool on which the institutions rely so as to conduct their business. Therefore, it is important to pay attention to the availability of general control procedures GCP in order to protect the security of AIS. The main objective of this study is to determine the extent of the availability of GCP of AIS security in commercial banks in Yemen. A descriptive analytical approach is used. Data is collected through a questionnaire distributed to the principals and specialists in departments of finance, information technology IT, and internal auditor in the head offices of commercial banks. Out of the distributed questionnaire, only 78 are valid and suitable for the analysis. The study finds that there is an availability of GCP depending on organizational control, security, and protection procedures in maintaining AIS. It also encourages the management of commercial banks to pay attention to a high-level of GCP in their AIS.

Keywords: Accounting Information Systems (AIS), General Control Procedures (GCP), Availability, AIS Security, Organizational Control, Commercial Banks.

1. Introduction:

The business environment had witnessed many developmental trends and changes due to the revolution of information technology IT and the increase in global competition. As a result, the accounting profession and its methods of operation were greatly affected by such changes. The organizations adopted the accounting information system AIS to provide accurate, timely, and efficient information for decision-making. The

[1] Research scholar, at Dr. Babasaheb Ambedkar Marthwada University (BAMU), Aurangabad, (M.S) India. E-mail: ymhh2013@gmail.com; comm.ymh@bamu.ac.in
[2] Associate professor, head & research guide of department of commerce, Adv. Ankushrao. Tope Arts Science & Commerce College, Jalna, (M.S) India.
E-mail: jogdand.dadasaheb@gmail.com

banking sectors rely heavily on AIS which may increase risks and threats for information systems. According to Steinbart and Romney (2009) the AIS is known as a system for collecting, recording, storing, and processing data to obtain information for decision-makers. The internal control is defined by Committee of Sponsoring Organizations (COSO, 2004) as: "a process, effected by an entity's board of directors, management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in the effectiveness and efficiency of operations, the reliability of financial reporting, and the compliance of applicable laws and regulations". So it is noted that the internal control provides confidence and reliability of AIS particularly, and for financial reports in general. In this context, the importance of general control procedures GCP, as the main internal control procedures, comes from the direct interest in securing the quality of management operations (Vaassen, et al., 2009), as well as the importance comes from the main role of commercial banks in the national economy. Likewise, Khoury (1996) stated that the importance comes from the large and varied bank operations, in addition, the accounts of customers deposit and borrowers which exceed many times the value of shareholders' equity.

However, some previous studies concluded that the organizational control and system security procedures of AIS are weak and inadequate to meet the requirements of control procedures of AIS (Al-Hadithy, 1993; Al-Qatnani, 2005; Musleh, 2007). Also, Dhillon and Torkzadeh (2006) argued that it is necessary to go beyond technical considerations and adopt organizationally in maintaining information system security in organizations. Bani-Khalid (2009) recommended that it is necessary to enhance the procedures and policies related to methods of organizational control in commercial banks. Moreover, Bawaneh (2014) found that banks do not apply solid security policy and do not conduct a risk assessment procedure, He encouraged to study the security of organizational environments of AIS. (Abu-Musa, 2006; Hayale and Abu-Khadra, 2008; Abidin, et al., 2019; Ahmad, et al., 2019) indicated that the most security threats in banks and institutions are internally generated and unintentional, because of employees tend to ignore policies, operating procedures, sharing of passwords, computer viruses, and directing outputs to people who are not entitled to receive. Furthermore, Beasley et al. (2005) encouraged to examine the effectiveness of system and risks management to protect shareholders and other parties as one of the factors that management responsible for. Whereas the changing in the nature of

the integration of the stock markets including financial institutions and commercial banks affected by financial shocks and crises (Kassim, 2012), the competition in the commercial banks' sector is high should be reformed in the creation of competition among banks (Najarzadeh, et al., 2013; Sabir and Qayyum, 2018). So, that implies that the commercial banks should attend and adopt a strong GCP and security of AIS.

It is essential to highlight the importance of GCP and security of AIS in commercial banks in Yemen, as a vital in the financial system in Yemen and working in a competition environment, changing technology, and high risks due to the Arab Spring revolution and political issue since 2011. Hence, there is a need to study the extent of the availability of GCP of the security of AIS in commercial banks in Yemen, through the organizational control and system security procedures, so as to protect AIS and reduce threats and risks, as well as to produce efficient, timely, and qualitative information for decision making. Besides that, the contribution of this study deals with one of the most important issues which link the GCP to the security of AIS. It may further address the importance of the GCP in the management of commercial banks as an early warning to adopt the appropriate GCP to maintain and develop their GCP. Therefore, the study hopefully seeks to achieve the main objective which is 'the extent of the availability of GCP of security of AIS in commercial banks in Yemen', through two sub-objectives; 1) determining the extent of availability of organizational control procedures which is necessary for the security of AIS. And 2) determining the extent of availability of procedures of security and protection which is necessary for the security of AIS.

2. Literature Review

Many organizations and banking sectors are suffering due to internal of AIS security breaches, whether the accidental and intentional entry of bad data or accidental destruction of data by employees (Abu-Musa, 2006, 2010; Hayale and Abu-Khadra, 2008). Similarly, Ji, et al. (2016) concluded that the existence of internal control weaknesses has a negative effect on accounting conservatism in China, furthermore, the assurance of internal control reports can mitigate the negative impact of internal control weaknesses on accounting conservatism. So, Susanto, (2017) found that despite the internal control system affects the quality of AIS, but as a result of flexibility of AIS, it became easy to access the system,

which affects the security and integrity of the AIS. Also, Lari et al., (2019) found that weakness in internal controls has a significant negative relationship with financial reporting quality. On the other hand, Abidin, et al. (2019) and Ahmad, et al. (2019) concluded that the employees tend to ignore policies and standard operating procedures, even though they realize this issue will result in a severe impact on the reputation of the organization. Then, the next part will discuss the literature review about GCP and the security of AIS and then theoretical foundation and hypotheses development, as follows:

2.1. General Control Procedures GCP and the Security of AIS

General controls is known as the tools that make sure that the organization's control environment is stable and well managed (Romney and Steinbart, 2018, p. 198). There are many risks related to the usage of AIS, Al-Otaibi (2013) classified the risks as follows: First, the source of risks, internal and external ones, which deducted that the employees are the main internal source of risks and hackers, natural disasters are the main external source of risks. But the internal risks are more dangerous than the external risks because the employees are more aware about the weakness of control procedures, and they are authorized to access the system and they can distort, edit, and add its data. Second, in terms of intentional; and classified into risks resulting from deliberate or intentional behaviors such as the intentional introduction of incorrect data or intentional destruction of data, or risks resulting from unintentional or unintentional acts, such as intentional or inadvertent destruction as a result of oversight or error. Inadequate mistakes can often be avoided through staff training and good supervision. Third, risks related to the phases of the system, such as the risk of inputs, processes, and outputs. Furthermore, Steinbart and Romney (2009, p. 208) stated that recent studies noticed 67% of companies have been hacked by their systems, and 60% of them have been declared financial losses as a result of this penetration. On the other hand, accompanied banking services a lot of operational risks resulting from internal processes and employees, inadequate or failed systems, reputational risks, and legal risks as well as traditional banking risks of credit risk, liquidity risk, market risk and foreign exchange risk (Glauay, 2014, p. 59-60).

As for the measures of prevention and reduction risks in commercial banks there are many appropriate methods to reduce the risks of banking operations according to SAMA (2008). They are as follows:

- Commitment to integrity, ethical values, application of appropriate organizational structure, an independent audit committee, and effective monitoring of staff performance.
- Design, implement and maintain an internal control system that involved active control procedures, segregation of duties, authorities and direct remote access limited to the system… etc.
- Perform internal and external audit procedures, install software of fraud detection and detection systems, and appoint a computer security officer at the bank.
- Insurance for customer deposits, develop emergency or contingency plans and store backups of data and software in secure locations.

2.2. GCP which maintains the security of AIS:

Using computers in the operation of accounting data led to a reconsideration of the internal controls. A complete set of procedures and controls were developed to suit the electronic data operation and the treatment of its implications (Suliman, 1999, p. 14; Barakat and Shuraim, 2009, p. 282-291). And according to He and Chen (2010), the general control includes organizational control and system development control, operating security control. The procedures of GCP can be explained as follows:

Organizational control procedures OCP in commercial banks:

The procedures of OCP aim to establish general and necessary control over the activities of information systems. They provide a reasonable degree of confidence that internal controls have achieved its objectives, as follows:

A) Regulatory control procedures in commercial banks: includes:

- Select a qualified, trained staff and clear HR policy for incentives, promotions, and career rotation. (Hamada, 2010, p. 318)
- Independent of the IT department and separate conflicting functions between its part and other departments, as well as making a manual of job descriptions for each job. (Al-Qatnani, 2005).

- Insurance against breach of trust (Yahya and Abdulwahab, 2001).
- Training controls: these controls focus on knowledge that should be provided to employees and the importance of security procedures, also, to support and finance training from senior management.

B) Control procedures for documenting and developing the system in commercial banks: It includes all regulatory procedures related to the documentation and description of information systems with their physical, logical and database components, a document of last-user procedures, as well as document of all ongoing development, and updating of the system (Hamada, 2010)

Procedures of security and protection system in commercial banks:

Information security is a complex technical issue. So Steinbart and Romney (2009, p. 334) and Abu-Musa (2010, p. 227) discussed that the security is a management issue, not a technical issue. In other words, the management is recognized for this issue not only IT department because it is responsible for the design, implementation, and maintenance of the internal control system. Besides that, Hamada (2010, p. 319-320) mentioned that the security procedures are designed to prevent and detect errors and irregularities, which occur as a result of unauthorized access and use of the system and its data. There are some of the security procedures as follows:

1- Physical access controls: these controls include placing computer and servers in secure locations, not allowed entering to the servers room except people who are authorized, must be walls of the serves room not flammable, using ID card to enter through a particular access point, a receptionist or guard should be placed at the main entrance to check users IDs, using guestbook and sign on entry and exit, and accompany visitors inside the building by a staff member. Also use physical features such as card readers, digital keyboards, like a pupil, retina scanners, fingerprint readers or sound features, all these to adjust access to the server room. Rooms must be closed protectively, all doorways and exits should be monitored by television systems and alarms.

2- Logical access controls: these controls consist of the user password, classify data according to its importance & sensitivity, encrypt data, firewalls, intrusion testing, message receipt techniques, policies dealing with system errors & procedures, and the access control matrix.

3- Control of availability and protect system: Hamada (2010, p. 320) and Steinbart and Romney (2009, p. 421-424) stated that it is necessary to do the following:

- Back up files of system software and information and data automatically during close periods.
- Keep backups out of the bank and in a secure and remote geographical area.
- Insurance for central computer against theft, fire, and natural disasters.
- Develop a special emergency plan for disaster information systems.
- Fabricating emergencies to test the effectiveness of physical protection measures and procedures of the system.
- Use of licensed, sophisticated and adequate software to protect your hardware and software from the risk of viruses and external and internal intrusion and update them continuously.

In addition, Romney and Steinbart (2018, p. 337) mentioned many security procedures as follows: "

- Storage of data in a secure file library and restriction of physical access to data files.
- Logical access controls and an access control matrix
- Proper use of file labels and write-protection mechanisms
- Concurrent update controls
- Data encryption for confidential data
- Virus protection software
- Off-site backup of all data files
- Checkpoint and rollback procedures to facilitate system recovery."

Theoretical foundation

The study relies on the theory of agency and theory of stakeholders, which focus on achieving mutual interests between owners, shareholders, and other parties, so GCP and security of AIS work to stabilize and continue

to achieve interest between those parties, through the contribution and enhancing the aspects of security, confidence, and efficiency of AIS outputs that contribute to rationalizing the decisions of the institution and related parties. Moreover, the high institution's interest in the availability of GCP and the security of AIS is also among the requirements of the institutional theory (Kuchinke, 2000), that takes into account legislation, organizational structures, policies and organizational procedures of the institution, as these procedures are reliable guides of the institution's behavior and contribute to the survival and continuity of the institution and its competitiveness.

Hypotheses Development

There are many studies related to this study, such as Al-Hadithy (1993) aimed to evaluate the internal control systems of financial and banking institutions that use computers in Jordan. The study concluded that there is a weak in implementation of the regulatory, access, and security controls, as well as there is an intermediate on documentation controls, system development, and application controls. Institute of Information Systems Control ISACA (2005) evaluated the control procedures of Charles Scoop Credit Company in the US by using the COBIT standards. ISACA concluded that Scoop uses a complex and diverse information environment. Therefore, the company should develop the control procedures used in line with the technological developments, and makes the work more flexible. Also, Chow et al. (1996) attempted to evaluate the control procedures of institutions and their effect on manipulated databases and short-term management, by comparison between the Japanese company Toshiba and a similar large American company (did not disclose its name). The study found that the Toshiba company used strong control procedures. On the other hand, the American counterpart has a clear imbalance in the control procedures, as well as the study discovered the existence of functional corruption in the American company.

Furthermore, Al-Qatnani (2005) explored and evaluated the control procedures in AIS in a case study of Housing bank for trading in Jordon. He found that an inconsistent the characteristics of the AIS with the regulatory control procedures, and great weakness in the system security procedures. Also, found a moderate application of regulatory procedures related to the documentation and system development. On the same side,

Musleh (2007) sought that there is a weakness in some general control procedures. And found that a high applied application control procedures. And Bani-Khalid (2009) discussed the internal control methods to ensure the security of computerized AIS in Jordanian commercial banks. And concluded that internal control procedures are available to ensure computerized information security, and showed that the degree of internal control procedure was generally moderate, with the arithmetic average of internal control methods 4.29.

Moreover, Al-Ajmi (2009) aimed to know the role of IT in the development of the internal control system in Kuwaiti commercial banks. It found that the control regulatory, documentation, equipment, access to the system, inputs and outputs procedures, all these lead to develop the internal control system in commercial banks. As well as the use of IT provides high credibility on the outputs of the accounting system. And a nice study was by Hamada (2010) which aimed to study the effect of general control procedures of computerized AIS in increasing the reliability of the accounting information. The study found that there is a significant effect of the controls of general of AIS in increasing the reliability of accounting information in companies, the most important control procedures were regulatory and system security.

On the other hand, Qeshta (2013) aimed to identify the relationship of IT used effectively to the internal control system in the national banks - Gaza Strip, the study concluded that there is a positive relationship between the IT and the effectiveness of the internal control system in the national banks operating. Besides that, the study of Al-Hanini (2015) discussed the reliability of the internal control methods on the computerized information systems in banks operating in Jordan. The study concluded that the methods of internal control provide the availability, security, maintenance and adjustment, and integration requirements of the systems on the computerized AIS.

The study of Hayale and Abu-Khadra, (2008) investigated perceived security threats of computerized AIS that face Jordanian banking sector, they found that the entry of bad data by employees intentionally or unintentionally, and sharing their passwords are the top security threats that facing banks.

Moreover, Abu-Musa, (2010) examined the existence and implementation of information security governance in Saudi organizations, the study found that although the majority of Saudi organizations recognize the importance of information security governance ISG, but most of them have no clear or written ISG, have no disaster recovery plans to deal with security of information or incidents and emergencies. The study shows that there is a poor overall business strategy and not adequately implemented, then the study recommended to improve implementing and measuring the ISG performance in Saudi organizations.

Also, Alzamil, (2018) studied the information security practice in Saudi organizations, and found that organizations have established information security policy, but have not enforced and publicized effectively and efficiently, and the study suggested that should develop a national framework for information security to guide the governmental and non-governmental organizations in order to avoid any vulnerability that may lead to violations of the security of their information.

The study of Abbaszadeh, et al. (2019) aimed to investigate the relationship between IT and internal controls in agencies in Iran, they found that there is a significant relationship between IT and internal controls which included administrative, financial, and accounting controls, risk assessment, information and communication, control activities and monitoring.

Furthermore, the study of Abidin, et al. (2019) identified weaknesses in current internal control systems in protecting customer data and its impact of customer data theft on the organization, from Malaysian organization's experience. The study found that customer data theft still occurred despite the company having an internal control system. In addition, the employees tend to ignore policies and standard operating procedures, providing opportunities for data theft and fraud to occur, although they realize this will result in a severe impact on the reputation of a company. Similarly, Ahmad, et al. (2019) discussed the influence of information security monitoring and other social learning factors on employee's security assurance behavior and information and computer security in Malaysia, they found that employees tend to abandon security behavior when the behavior is perceived as inconvenient.

Despite the scholarly growing attention given to the relationship between GCP and security of AIS, the study of the availability of GCP in the security of AIS is considered the first study in Yemen according to the researchers' knowledge. In addition, the importance of the time dimension of the study in the verification of the differences or stability and strength is compared with the results of previous studies on the subject of study. Based on the above discussion, the following hypotheses are proposed for empirical examination.

H_{01}: There is no statistically significant availability of organizational control procedures in maintaining of security of AIS.

H_{02}: There is no statistically significant availability of procedures of security and protection in maintaining the security of AIS.

3. Methods

The study population consists of eleven commercial banks in Yemen until 2015. The questionnaire is developed according to the guidelines mentioned in the book of Steinbart and Romney (2009) and other related materials available in the literature, such as Yahya and Abdulwahab (2001), Al-Qatnani (2005), Bani-Khalid (2009), and Hamada (2010), which are included in table 4 and table 6. The questionnaire is also formed and developed according to the study variables, objectives, hypotheses. For testing the reliability, the questionnaire was arbitrated by ten referees including academicians in Yemeni universities, Malaysian Open University-Yemen, and experts from Yemeni SAI.

The questionnaire consists of two main sections: Section I: contains the demographic characteristics, which include; qualification, specialization, current job, and experience. And section II: is divided into two parts into 30 items. The response to the questionnaire is according to the Likert scale quintet, with the measurement: Strongly agree = 5, agree = 4, not sure = 3, disagree = 2, and strongly disagree = 1.

The primary data were collected through the questionnaire distributed to the sample of study in the head office of ten commercial banks, in Sana'a (capital of Yemen). 120 questionnaires were distributed to the principals and specialists in departments of finance, IT, internal auditor, only 78 questionnaires were valid and suitable for the analysis.

The study used the analytical descriptive approach. SPSS and analysis tools (mean, standard deviation, frequency distributions, percentage, correlation analysis, and one-sample t-test, etc.) were used to analyze the data and test the hypotheses.

To measure the extent of the availability of general control procedures of the security of AIS, the mechanism for interpreting the averages and judging the items were determined based on the answers to these questions, namely the range between (Very High) and (Very Weak) = (5 - 1 = 4) and (4 ÷ 5 = 0.8), as follows:

Table 1: Categories of answers and the corresponding grades

Categories	Grades of availability
From 4.21 – 5	Very High
From 3.41 – 4.20	High
From 2.61 – 3.40	Moderate
From 1.81 – 2.60	Weak
From 1 – 1.80	Very Weak

Moreover, the analysis of the data and testing hypothesis were calculated by the arithmetic mean and t-test at the default, t-test value = 3, with significance level at 0.05, which corresponds to the confidence level, 95%.

4. Results and Discussion

Before we discuss the data of the study, we will test the credibility and stability of the study by using test of Cronbach Alpha and Spearman-Brown correlation coefficients to measure the internal consistency and stability of the study instrument for all dimensions (Sekaran and Bougie, 2010). In table 2 the result of testing shows that the value of the stability coefficient is 0.810, which is greater than 60%. This indicates a high degree of internal consistency, a high degree of reliability and consistency which makes the statistical analysis acceptable.

Table 2: Testing the Stability of the study tool

Variable	No. of Questions	Alpha Coefficient Value
Var. 1: The general regulatory procedures	13	.815
Var. 2: Procedures of security and protection system	17	.877

**. Level of correlation is significant at the 0.05

According to the analysis of demographic characteristics, it is clear from the below table 3 that the majority of respondents are qualified, bachelor degree holders and above, with a percentage of 92.3%. And most of them are specialized in accounting and IT with a percentage of 65.4 and 20.5. As well as their experience exceeds five years. The conclusion of that, the answers of respondents will be positive, accurate and objective.

Table 3: Frequencies and Percentages of Demographic Characteristics

Dimension	Descriptions	Frequency	Percent %
Qualification	Diploma	6	%7.7
	Bachelor	61	%78.2
	Master	10	%12.8
	Ph.D	1	%1.3
Specialization	Accounting	51	%65.4
	Business Administration and Finance	4	%5.1
	Information Technology IT	16	%20.5
	Other	7	%9.0
Function	Finance Manager	4	%5.1
	IT Manager	3	%3.8
	Internal Auditor	12	%15.4
	Database & IT department	12	%15.4
	Accounts department	41	%52.6
	Other	6	%7.7
Experience	Less of 5 years	13	%16.7
	5-10 years	33	%42.3
	11-15 years	18	%23.1
	Above 15 years	14	%17.9

For discussing the items of the study and testing hypotheses, the researchers started with the first variable which is organizational control procedures, and then the second variable which is security and protection of the system, as follows:

4.1. Organizational control procedures and test of the first hypothesis:

In table 4 item no. 2 'selection and appointment of specialized and qualified employees' comes in first place with an average of 4.667 and a level of significance less than 0.05 with a positive value of T-test. This means that the respondents are aware of the importance of item 2, and it is very high to ensure the security of AIS in commercial banks in Yemen. Furthermore, the respondents are aware of that as a reflection of their high qualifications and specialization. Also item 4 'training for employees ...etc.', and item 9 'Inquire and punish on the aggressor for information security', range in the second and third ranks respectively with an average of 4.5897 and 4.5769 respectively, and levels of significance less than 0.05 with a positive value of T-test. That means the respondents are aware of the importance of these items, and they are very high to ensure the security of AIS in commercial banks in Yemen. Obviously, the respondents' answers show that most items of the first variable are very high on the security of AIS with averages between 4.66 and 4.28 with positive T value, except items 1, 6, and 8, they show only high but not very high. On the other hand, item 8 'Insurance against breach of trust' gets a low average 3.9103 with positive T value. That means the respondents may not prefer insurance against breach of trust because there are other preventive procedures that may be in consideration, as well as they provide commercial guarantees when they start their employment.

Table 4: Analysis of the first dimension of organizational control procedures

No.	Statement	Grade	Mean	St. Deviation	T-test	Sig.
1	The IT department should be separate and follows the board of directors.	12	4.1282	1.03646	9.613	.000
2	Selection and appointment of specialized and qualified employees.	1	4.6667	.47446	31.024	.000
3	Write & develop a manual that includes a clear division for all IT functions.	5	4.5256	.55184	24.417	.000

No.	Statement	Grade	Mean	St. Deviation	T-test	Sig.
4	Execute training courses for employees in IT in accordance with variables of the banking environment.	2	4.5897	.69199	20.290	.000
5	The rotation of employees among jobs to examine their works by each other.	10	4.2821	.75416	15.014	.000
6	System operators should be taken for their annual leave.	11	4.1282	.79542	12.527	.000
7	Take an undertaking from IT employees to keep data and information confidential.	6	4.4744	.80137	16.249	.000
8	Take insurance against breach of trust.	13	3.9103	1.05911	7.591	.000
9	Inquire and punish the aggressor for information security.	3	4.5769	.57024	24.423	.000
10	Taking prior approval from the authorized to modify and develop the programs.	8	4.4231	.65504	19.187	.000
11	Making a clear plan to control the development and maintenance of systems and software.	4	4.5641	.52446	26.339	.000
12	Participation of beneficiary departments, accountants and auditors in the system development process.	9	4.3205	.72959	15.985	.000
13	Testing the development process with actual data and another server, and document that.	7	4.4359	.71332	17.778	.000
	General average		**4.3866**	**.39038**	**23.382**	**.000**

Testing the first hypothesis:

Table 5 has shown that the general control procedure is very high on the security of AIS, with total arithmetic mean 4.3866, which is higher than the hypothesis mean 3, and that there is no big standard deviation as the average reached 0.3904. Besides, the t-test is positive with value 23.382, as well as the level of significance = 0.000 is less than specified moral level 0.05. Moreover, the degree of agreement is generally very high, which means the null hypothesis is rejected and the alternative hypothesis

is accepted. This means that *'There is statistically significant availability of organizational control procedures in maintaining the security of AIS'*.

Table 5: Result of Testing H_{01}

Hypothesis	Mean	St. deviation	T value	Sig.	Result
There is NO statistically significant availability of organizational control procedures in maintaining the security of AIS.	4.3866	.39038	23.382	.000	Reject

4.2. System security and protection, and test of the second hypothesis:

It is clear from the below table 6 that item no. 10 'Automatically backup data and information during closed periods' comes in the first place with an average of 4.7436. And item 9 'Backup software and files of the system' comes in second place with an average of 4.6923. Also, item 5 'Use a password for each employee' come in third place, with an average of 4.6923. All of the above are very high with levels of significantly and less than 0.05 with a positive value of T-test. On the other side, item 3 'Close the AIS at specified end-of-service period...' shows only high with an average of 4.1282 and positive T value, that means the respondents imply that the close of AIS is not necessary, because it is important for using ATM machines by customers.

Table 6: Analysis of second dimension of system security procedures

No.	Statement	Grade	Mean	St. Deviation	T- test	Sig.
1	Adhere to the selection criteria of the IT location in the bank, in terms of wall, doors, decks, alarms and TV cameras to control access to the system room.	10	4.5641	.57184	24.157	.000
2	Use the employee ID card and fingerprint to control access to the system room.	11	4.5513	.55003	24.909	.000
3	Close the AIS at a specified end-of-service period until the next business day.	17	4.1282	.93084	10.704	.000
4	Determine which programs each user can access.	12	4.5000	.59761	22.168	.000

No.	Statement	Grade	Mean	St. Deviation	T- test	Sig.
5	Use a password for each employee to access the system.	3	4.6923	.56540	26.434	.000
6	Change frequently for the password, review of authorities from time to time due to change of tasks and functions.	4	4.6795	.52207	28.411	.000
7	Delete password for users who left their function.	8	4.6026	.58863	24.045	.000
8	Check the control access report and events of the system by chief security officer through Log analyses (Historical record).	15	4.3077	.74394	15.524	.000
9	Backup software and files of the system.	2	4.6923	.54195	27.578	.000
10	Automatically backup data and information during close periods.	1	4.7436	.43948	35.039	.000
11	Keep backup data out of the bank located in secure and remote location areas.	5	4.6667	.50108	29.376	.000
12	Insurance on the AIS's servers against theft, fire, and natural disasters.	13	4.4359	.81527	15.555	.000
13	Provide adequate alternatives for continued operation at electricity power failure.	6	4.6282	.56082	25.641	.000
14	Making a special emergency plan for IT management against disaster recovery.	7	4.6154	.54010	26.415	.000
15	Forming an emergency committee to restore operation in case of disasters.	14	4.3974	.72685	16.980	.000
16	Fabricating emergencies to test the effectiveness of physical protection procedures of the system.	16	4.2564	.76338	14.536	.000
17	Use of licensed, sophisticated and adequate software to protect hardware and software from the risk of viruses and external and internal intrusion and update them continuously.	9	4.5897	.56834	24.704	.000
	General average		**4.5324**	**.38074**	**35.547**	**.000**

Testing the second hypothesis:

It is clear from table 7 that the respondents believe that the procedures of security and protection in maintaining the security of AIS have a very high significance, with total arithmetic mean 4.5324, which is higher than the hypothesis mean 3. However, there is no big standard deviation as the average reached 0.3807. Furthermore, the t-test is positive with value 35.547, as well as the level of significance is = 0.000 which is less than specified moral level 0.05. Besides, the degree of agreement is high effect, which means to reject the null hypothesis and accept the alternative hypothesis. This means that *'There is statistically significant availability of procedures of security and protection in maintaining the security of AIS'*.

Table 7: Result of Testing H_{02}

Hypothesis	Mean	St. deviation	T value	Sig.	Result
There is NO statistically significant availability of procedures of security and protection in maintaining the security of AIS.	4.5324	.38074	35.547	.000	Reject

5. Conclusion

In conclusion, it is clear that the AIS is the most important tool which commercial banks rely on to get an accurate, efficient, and timely information for decision-making. For this purpose the availability of GCP in maintaining the security of AIS in commercial banks shows very high statistically significance within the procedures of organizational control and procedures of security and protection of AIS, with an average of 4.387 and 4.532 respectively, with positive t-test and level of significance. In general, there is a very high statistically significant availability of GCP in maintaining the security of AIS in commercial banks, with an average of 4.460, with positive t-test and level of significance 0.000 less than 0.05. Furthermore, this result is in the contrast with the results of studies of (Al-Hadithy, 1993; Al-Qatnani, 2005; Musleh, 2007). In other words, the GCPs of AIS are very important to help commercial banks to produce accurate, timely and efficient information for rationalization of decision-making. Moreover, the study recommends the commercial banks management to enhance the performance of the employees, through participation in specialized training courses and workshops related to AIS and its risks and threats. However, the study has some limitations that

should be considered when evaluating and generalizing its conclusions such as it does not cover the application control procedures of AIS. So, the generalization of the study results must be taken with cautions.

References

Abbaszadeh, M. R., Salehi, M. and Faiz, S. M. (2019). Association of information technology and internal controls of Iranian state agencies. *International Journal of Law and Management, 00-00.* doi:10.1108/ijlma -12-2017-0304

Abidin, M. A. Z., Nawawi, A. and Salin, A. S. A. P. (2019). Customer data security and theft: a Malaysian organization's experience. *Information and Computer Security*. doi:10.1108/ics-04-2018-0043

Abu-Musa, A. A. (2006). Exploring perceived threats of CAIS in developing countries: the case of Saudi Arabia. *Managerial Auditing Journal*, 21(4), 387–407. doi:10.1108/02686900610661405

Abu-Musa, A. (2010). Information security governance in Saudi organizations: an empirical study. *Information Management & Computer Security*, Vol. 18 No. 4, pp. 226-276. https://doi.org/10.1108/09685221011079180

Ahmad, Z., Ong, T. S., Liew, T. H. and Norhashim, M. (2019). Security monitoring and information security assurance behaviour among employees. Information and Computer Security. doi:10.1108/ics-10-2017-0073

Al-Ajmi, M. A. H. (2009). *Role of Information Technology in Developing the Internal Control System of Kuwaiti Commercial Banks*, Master Thesis, Aal alBayt University, Jordan.

Al-Hadithy, E. S. N. (1993). *Evaluation of Internal Control Systems for Computer-Using Institutions*, A Field Study on Financial and Banking Institutions in Jordan, Master Thesis, University of Jordan.

Al-Hanini, E. (2015). Evaluating the reliability of the internal control on the computerized accounting information systems: An empirical study on banks operating in Jordan. Research Journal of Finance and Accounting, 6(8), 176-186. https://doi.org/10.25255/jss.2017.6.1.156.177

Al-Otaibi, A. S. M. (2013). Analytical study of the impact of information and communication technologies (ICT) on accounting practices. *Journal of King Abdulaziz University: Economics and Administration*, 105 (3171) pp1-18. https://doi:10.4197/Eco.27-2.3

Al-Qatnani, K. M. H. (2005). *Controls in computerized accounting information systems*- analytical study in commercial banks in Jordan, Doctoral dissertation, Damascus University, Syria .

Alzamil, Z. A. (2018). Information Security Practice in Saudi Arabia: Case Study on Saudi Organizations. *Information and Computer Security, 00–00*. doi:10.1108/ics-01-2018-0006

Bani-Khalid, T. O. E. (2009). *Extent of providing internal control methods to ensure the security of computerized accounting information in Jordanian commercial banks*. Master Thesis, Aal al-Bayt University, Jordan. Retrieved from https://oumwalide.com/product/5c5d3e27255cb600047608b5

Barakat, L. H. and Shuraim, O. S. (2009). *Auditing Principles*, Al-Ameen Center for Publishing, Sana'a, Yemen.

Bawaneh, S. S. (2014). Information security for organizations and accounting information systems a Jordan banking sector case. *International Review of Management and Business Research*, *3*(2), 1174. Retrieved from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.678.3552&rep =rep1&type=pdf

Beasley, M. S., Clune, R. and Hermanson, D. R. (2005). Enterprise risk management: An empirical analysis of factors associated with the extent of implementation. *Journal of Accounting and Public Policy, 24(6), 521–531.* https://doi.org/10.1016/j.jaccpubpol.2005.10.001

Chow, C. W., Kato, Y. and Merchant, K. A. (1996). The use of organizational controls and their effects on data manipulation and management myopia: A Japan vs US comparison. *Accounting, Organizations and Society*, *21*(2-3), 175-192. https://doi.org/10.1016/0361-3682(95)00030-5

COSO (2004). *Enterprise risk management- integrated framework*, Committee of Sponsoring Organizations, available at: Retrieved from www.coso.org/ publications/ERM/COSO_ERM_ ExecutiveSummary.pdf, (accessed 18 January 2007).

Dhillon, G. and Torkzadeh, G. (2006). Value-focused assessment of information system security in organizations. *Information Systems Journal*, 16(3), 293–314. https://doi:10.1111/j.13652575.2006.00219.x

Glauay, R. (2014). *Banking Supervision and its role in activating the performance of banks*, Master Thesis, University of Akli Mohand Oulhaj, Algeria. Retrieved from http://193.194.80.38:8080/jspui/handle/123456789/1814

Hamada, R. (2010). The Effect of General Auditing Controls on Electronic Accounting Information Systems in Increasing the Reliability of Accounting Information (Field Study), *Damascus University Journal of Economic and Legal Sciences*, Volume 26, First Issue, pp. 305-334. Retrieved from http://new.damascusuniversity.edu.sy/mag/law/images/stories/305-334.pdf

Hayale, T. H. and Abu Khadra, H. A. (2008). Investigating Perceived Security Threats of Computerized Accounting Information Systems An Empirical Research applied on Jordanian banking sector. Journal of Economic and Administrative Sciences, 24(1), 41-67. doi:10.1108/10264116200800003

He, Q. and Chen, G. (2010, November). Research of the Security of Enterprise Group Accounting Information System under Internet Environment. In *2010 International Conference on E-Product E-Service and E-Entertainment* (pp. 1-3). IEEE. https://doi: 10.1109/ICEEE.2010.5660143

ISACA (2005). COBIT Case study: Charles Schwab, Retrieved from *http://www.isaca.org/Template.cfm?Section=Case_Studies3&CONTENTID=8036&TEMPLAT=/ContentManagement/ContentDisplay.cfm,USA*.

Ji, X., Lu, W. and Qu, W. (2016). Internal control weakness and accounting conservatism in China. *Managerial Auditing Journal*, 31(6/7), 688–726. doi:10.1108/maj-08-2015-1234

Kassim, S. H. (2012). Evidence of Global Financial Shocks Transmission: Changing Nature of Stock Markets Integration during the 2007/2008 Financial Crisis. *Journal of Economic Cooperation & Development*, *33*(4) 117-138

Khoury, N. (1996). Internal Control in Banks and Financial Institutions, *Journal of the Auditor*, No. 29, October.

Kuchinke, K. P. (2000). Debates over the nature of HRD: an institutional theory perspective. *Human Resource Development International*, 3(3), 279–283. doi:10.1080/13678860050128474

Lari Dashtbayaz, M., Salehi, M. and Safdel, T. (2019). The effect of internal controls on financial reporting quality in Iranian family firms. Journal of Family Business Management. doi:10.1108/jfbm-09-2018-0047

Musleh, N. A. (2007). *The Impact of using of computer on the internal control systems in banks* of *Gaza*, (Master thesis) Islamic University, Palestine. Retrieved from http://alqashi.com/th/th76.pdf

Najarzadeh, R., Reed, M. and Mirzanejad, H. (2013). A Study of the Competitiveness of Iran's Banking System. *Journal of Economic Cooperation & Development*, *34*(1), 93-110.

Qeshta, E. S. (2013). *Relationship of Information Technology Used Effectively to Internal Control System in National Banks* - Gaza Strip, Master Thesis, Al-Azhar University, Gaza. Retrieved from http://www.alazhar.edu.ps/ Library/aattachedFile.asp?id_no=0046753

Romney, M. B. and Steinbart, P. J. (2018). *Accounting information systems*, 14th edition, Pearson Higher Education AU.

Sabir, S. and Qayyum, A. (2018). Competition in the Banking Sector of Pakistan: Evidence from Unscaled and Scaled Revenue Equations1. *Journal of Economic Cooperation & Development*, *39*(1), 19-37.

Saudi Arabian Monetary Agency (SAMA) (2008). *Manual on Combating Fraud and Financial Fraud and Supervision Guidelines*, Department of Banking Inspection, KSA. Retrieved from http://www.sama.gov.sa/ar-sa/AntiMoney/Anti Documents/8A.pdf

Sekaran, U. and Bougie. R. (2010*). Researchs for business: A skill building approach*, (5th ed). Chichester: John Wiley & Sons Ltd.

Steinbart, P. J. and Romney, M. (2009). *Accounting Information Systems*, Translated by Qassim Ibrahim Al-Husseini, Dar Al Marikh for Publishing, KSA.

Suliman, M. H. M. (1999). *Study and Evaluation of Internal Control Systems under Electronic Data Operating Systems*, Master Thesis, Alexandria University, Egypt.

Susanto, A. (2017). The effect of internal control on accounting information system. *International Bussiness Management*, *10*(23), 5523-5529. Retrieved from http://www.feb.unpad.ac.id/dokumen/files/jurnal-internasional-IBM11_3-5523-5529XXXXXX.pdf

Vaassen, E., Meuwissen, R. and Schelleman, C. (2009). *Accounting information systems and internal control*. Wiley Publishing.

Yahya, O. and Abdulwahab, I. (2001). *Principles of Auditing*, the new library of Al-Jalaa, Mansoura, Egypt.