An Empirical Examination of Maturity Model as Measurement of Information Technology Governance Implementation

Husam Abu Khadra[1], Majdy Zuriekat[2], and Nidal Alramhi[3]
[1]Department of Accounting Information System, Zarka Private University, Jordan
[2]Department of Accounting Information System, Baghdad University, Iraq
[3]Department of Accounting Information System, Yarmoke University, Jordan

Abstract: *The aim of this study is to evaluate information technology governance implementation in the Jordanian domestic banks using the maturity model. An empirical survey using self-administered questionnaire has been carried out to achieve the study objectives. The study results reveal that Jordanian domestic banks applied effective awareness and communications, responsibility and accountability, and skills and expertise dimensions mainly, while they do not do enough with regard to the other dimensions (tools and automation, "goal setting and measurement", and "policies, plans and procedures"). The study main recommendation for domestic banks is to give more attention to information technology governance. Professionals in Jordanian domestic banks should work more to increase the information technology governance strength for all of its dimensions.*

Keywords: *Accounting information system, control, security, information technology governance, maturity model.*

Received March 31, 2007; accepted June 24, 2008

1. Introduction

The say of "knowledge is a treasure but practices are the key to information technology" retells the fact of the knowledge advancement importance and the related technology in the current age and verify that the right practical employment is the key factor of technology and knowledge success [16]. Enterprises realize that growing importance of Information Technology (IT) and consider it as a treasure enhancing their competitive position, adding value to their businesses. But what remains as a challenge is, which key practices that organizations should apply to get IT under control in order to deliver that desirable value? In other words what should be done govern IT activities? [15].

[19] Described the IT governance debate and speculation with the "the blind men and elephant" that states the continuous efforts of IT governance[i] professionals and practitioners in order to find the best practical standards that could be applied for each environment according to it complexity and nature; but unfortunately no one has the full picture which looks similar to what the blind men had.

What meant of IT governance in this study is based on the definition proposed by the IT governance institute "the set of practices and responsibilities exercised by senior management as well as, "the control processes to ensure that the enterprise's IT sustains and extends the enterprise's objectives, and deliver the promised outcomes against the strategy" (COBIT 4.1). In other words, governance refers to the way the organization goes about ensuring that strategies are set, monitored and achieved. As applied to IT then, effective IT governance is about the way senior management interacts and communicates with IT leaders to ensure that technology investment enable the achievement of business strategy in an effective and efficient manner [20].

The current study aims to find the characteristics of IT governance in the Jordanian environment by using a self developed model that illustrates IT governance aspects that suites the Jordanian banking sector since no one size fits all [20], then applying this model on a sample from the Jordanian domestic banks. In addition, this study aims to answer the question of "how well IT is being managed and what is needed to be done in future to reach an adequate level of management and control over IT function?".

To date, little experience-based research have been conducted in Jordan and internationally to investigate what IT governance arrangement work best [27], where devising IT governance arrangements is challenging because the success of IT strategies and procedures is contingent upon a variety of internal and external factors [2].

2. Research Background

For many organizations, IT and it's infrastructure that constitute major investments, if not managed properly, may impair and incur losses rather than enhance the organization's competitive position, on other words, organizations with effective IT governance have profits that are higher than other companies pursuing similar strategies. Moreover, the lack of effective IT governance has been shown to have adverse impacts on organizations, such as business losses, bad reputation, "runaway projects," and inefficient operational activities [29].

The research into IT management practices at hundreds of organizations around the world has shown that most organizations are not generating optimal value from their IT investments. The most important factor distinguishing top-performing from substandard-performing is the level of leadership by business and senior managers in a handful of key IT decision. Selection from leading management literature shares the same basic idea "to be successful, the business side of an organization has to be involved and committed to what IT does". To deliver the services needs, IT has to be managed by business as a business. This is the core of IT governance [13]. Moreover, IT governance may be the great wall separating enterprise success from failure [25]. Jurgen *et al*. [11] Study indicates that several consultants such as Laartz, Jurgen; Eric Monnoyer; Alexandra Scherdin reported successes at leading companies where business and IT managers have been working closely together to change the way information technology supports the business.

The concept of IT governance has emerged as a response to the growing pressure on all organizations to ensure that they are achieving value for money from their investment in IT and information systems, which includes ensuring that investment is aligned with organizational strategic priorities. It is based on the premise that the way in which IT is used and managed within an organization really matters, and that an institutional approach to IT needs to become embedded into central strategic planning [6].

Consequently, both management and IT professionals concerned with design, implementation, and assessment of IT governance strategies to ensure that technology truly serve the needs of the business. Managers are increasingly aware that IT-related decisions and behaviors must be aligned with the organizational performance goals in order to generate value from IT, but many individuals throughout organizations make daily decisions influencing that value received. Consequently, IT governance is the process of which organizations align IT actions with their performance goals and assign accountability for those actions and their outcomes for all related parties that may affect this process [28].

The involvements of senior management in IT are positively influences on the overall effectiveness of IT governance as well as the existence of a culture of compliance in IT. Moreover, senior mangers awareness of IT governance is the best indicator of governance effectiveness; also managers that participate in management of IT are more progressive and advanced in their IT usage and impact [10, 22].

IT executives also play an important role in governing the IT activities through starting risk management by resolving factors associated with availability and access. Reducing these risks pays immediate benefits to the enterprise, and also provides a foundation for more difficult challenges of reducing accuracy and agility risks in other words the ability to implement new strategic initiatives [30].

Effective IT risk management requires three core disciplines. First, a well- managed, well-architected IT foundation. Second, a mature risk governance process including policies and procedures to identify, prevent and assess risky behavior. Third, risk awareness that helps everyone in the enterprise understand threats and mitigating opportunities [21].

One of the most enduring problems faced by the IT function is how it should organize and structure itself [3], where indeed implementing a sound IT governance strategy is believed to be key for having a successful IT function in organizations [4]. The accounting professions started to take IT governance concept as a part of the internal control system seriously since the declaration of Sarbanes-Oxley act in 2002 [18] and since the release of the Public Company Accounting Oversight Board's (PCAOB) auditing standard no. 2 (AS2) in 2004, even the release of Committee of Sponsoring Organization of the Treadway Commission's (COSO's) internal control- integrated framework in early of the previous decade; COSO was originally formed in 1985 to sponsor the national commission on Fraudulent Financial Reporting, an independent private sector initiative which studied the causal factors that can lead to fraudulent financial reporting and developed recommendations for public companies and their independent auditors, for the SEC and other regulators, and for educational institutions. The national commission was jointly sponsored by five major professional associations in the United States, the American accounting association, the American institute of certified public accountants, financial executives international, the institute of internal auditors, and the national association of accountants (now the institute of management accountants). The commission was wholly independent of each of the sponsoring organizations, and contained representatives from industry, public accounting, investment firms, and the New York stock exchange. COSO framework is a highly abstract conceptual framework that does not identify control objectives at a level of specificity sufficient to design detailed audit

test. Furthermore, the general nature of COSO does not address the complexity and special risk inherent in IT field [7]. Therefore, organizations and auditors in computerized environment start looking for a suitable framework, such as Control OBjectives for Information and related Technology (COBIT) to supplement COSO framework. COBIT was initially developed as an IT benchmark consisting of best practices, then it is developed to become a framework that could be applicable as a dual use framework by which organizations can achieve efficiencies in either operation and/or IT audits through its use.

The Information System Audit and Control Foundation (ISACF) developed the COBIT, which is a framework of generally applicable IS security and control practices of information technology control. This framework allows management to benchmark the security and control practices of IT environment. Additionally, it ensures that adequate security and controls exist [14].

However, control objectives under COBIT are defined in a process-oriented manner following the principle of business reengineering. This type of control is exercised at the domain and process level. The "IT control" concept is adapted by the ISACF report and defined as "A statement of the desired results or purpose to be achieved by implementing control procedures in a particular IT activity". This control is exercised at the IT activity level [8]. The COBIT IT domain consists of the following parts:

- Planning and organization.
- Acquisition and implementation.
- Delivery, support and monitoring.

Thirty four IT processes are identified within each of the four domains. Consequently, activities within processes are also identified activities to deal with day-to-day IT routines. The central control objective is to link IT domains, processes and activities to the entity's operational processes and activities. The basic objective of IT is to facilitate the accomplishment of business objectives. Business objectives are referred to as "Business Requirements for Information" which include the following [9]:

- Quality requirements (quality, cost and delivery).
- Fiduciary requirements, as defined by COSO (effectiveness and efficiency of operations, reliability of information and compliance with laws and regulations).
- Security requirements (confidentiality, integrity and availability).

COBIT contains other testable constructs including a comprehensive well-articulated maturity model for IT control. The maturity model enables management of a company to evaluate and determine where on the internal control spectrum their controls are currently located, especially with the increasing pressure on the senior managers to consider how well IT is being managed and what is needed to be done in future to reach an adequate level of management and control over IT function [24]. Maturity model enables enterprises not only to benchmark their present IT performance but also to identify future targets for improvements. COBIT's maturity model is influenced by the organization's business goals, the operating environment and the industry practices.

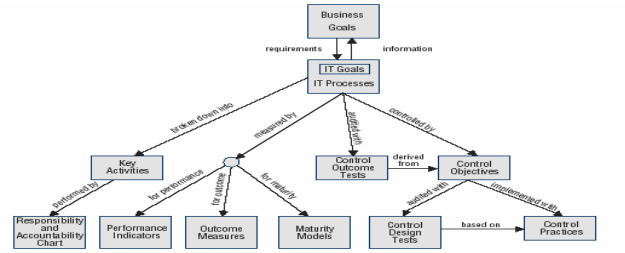

Figure 1. Interrelationship of COBIT components (COBIT 4.1 pp. 8).

Maturity modeling for management and control over IT processes is based on a method of evaluating the organization, so that it can be rated from a maturity level of non-existent (0) to optimized (5). The maturity levels are designed as profiles of IT processes that an enterprise would recognize as description of possible current and future status. They are not designed as a threshold model, where one cannot move to the next level without having fulfilled all conditions of the lower level. The right level is determined by the enterprise type, environment and strategy.

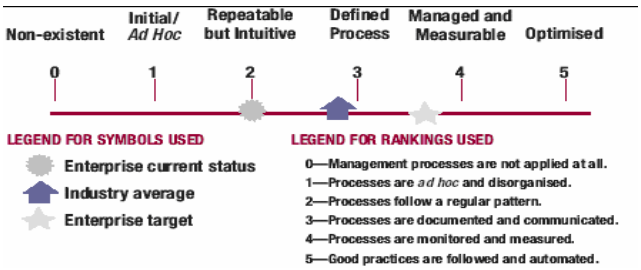

Figure 2. Graphic representation of maturity model (COBIT 4.1 pp. 18).

COBIT's maturity model consists of six major attributes:

- Awareness and communication.
- Policies, plans and procedures.
- Tools and automation.
- Skills and expertise.
- Responsibility and accountability.
- Goals and measurement.

Accordingly, the researchers will use the maturity model to evaluate the IT governance since this study to the best of the researchers' knowledge is the first that attempts to create an overall measurement for management involvement in implementing IT

governance using the six attributes of the maturity model.

3. Research Hypotheses

The current study examines the following hypothesis in null form:

$H_{0\,1}$: The Jordanian domestic banks do not have effective IT governance implementation. This hypothesis can be divided to the following null hypotheses:

1.1 The Jordanian banks do not have effective implementation of "IT awareness and communications".
1.2 The Jordanian banks do not have effective implementation of "IT Tools and automation".
1.3 The Jordanian banks do not have effective implementation of "IT staff skills and expertise".
1.4 The Jordanian banks do not have effective implementation of "responsibility and accountability".
1.5 The Jordanian banks do not have effective implementation of "goal setting and measurement".
1.6 The Jordanian banks do not have effective implementation of "policies, plan and procedures".

4. Methodology

The population of the study consists of all Jordanian domestic banks (Local and Foreign). The number of domestic banks in Jordan is twenty three banks. The researchers covered only the banks headquarters where the targeted respondents were expected to exist. The data is collected by using a self-administered questionnaire that measures the existence of maturity model dimensions attributes using nominal scale. The questionnaire was designed after a preliminary observation on the practice and reviewing the available literature. The researchers circulated the research questionnaire among the parties that had the ability and knowledge to answer it. Therefore, the researchers distributed the questionnaire to the domestic banks external auditors (CISA holders) and Head Of Computer Departments (HOCD), while the researchers were not able to circulate the questionnaire to CEOs.

The above mentioned Maturity Model attributes are categorized in the questionnaire under the following dimensions according to their functions and goals:

- Awareness and communications (question 1-3).
- Tools and automation (question 4-6).
- Responsibility and accountability (question 7-9).
- Skills and expertise (question 10-12).
- Goal setting and measurement (question 13-15).
- Policies, plans and procedures (question 16-33).

Forty questionnaires were distributed to the selected respondents; twenty two were received in a usable format, indicating a response rate of 55%. One way to assess the potential for non-response bias is to compare data from late respondents to data from on time respondents based on [26, 17]. In the current study three responses were received following a reminder. Those late responses were not significantly different from responses in any of the analysis reported the following results section.

To investigate study instrument validity, the researchers consulted fifteen experts (Professionals and Academics). The experts were asked to make sure that the research questionnaire does not miss any element that might affect the study results or create bias in the questions. The researchers used Cronbach's Alpha to check the questionnaire stability for all of its components. Furthermore, reliability analysis allowed the researchers to study the measurement scales and the items that make them up (SPSS tutorial). In the current study, the researchers did not use some of the central tendency measurements such as the mean, because it is only valid for the nominal scale. Consequently, the researchers did not calculate the mean for respondents' answers that were measured by using nominal scale (exist/ not exist). Furthermore, variance measure was not used because it is calculated by using squared distances from the mean since the researchers utilized the nominal scale. Finally, frequency distribution is a summary table in which the data is arranged into conveniently-established, numerically-ordered class grouping or categories. Due to that, frequency is a valid measurement for the nominal scale and used by the researchers in the current study.

For the hypothesis that measures the existence of maturity model attributes in the Jordanian Banks, the researchers used Z test for proportion that pertain to population proportion P maturity model attributes implementation percentage by calculating the sample proportion Ps, then the values of this statistic compared to the hypothesized value of the parameter P (Implantation Standards) so that the decision can be made about the hypothesis.

Herein and to apply the above mentioned statistics, the researchers convert the nominal scale qualitative responses to numerical (percentage) values through the following steps [9]:

- Coding the nominal scales (not exist, exist), where 0 given to not exist and 1 for exist.
- Summing up of all question values for each variable.
- Calculating the proportion by dividing the previous step result on the number of questions.

The materiality weights for the maturity model attributes were considered to be equal (Klapper and Love, 2002), because the materiality of each dimension is contingent upon a variety of internal and external factors related to each environment [2]. Additionally, the researchers used the P value in order to test the sampling distribution normality using the following rule: "If the number of success (X) and the number of failures are each at least five, the sampling distribution of proportion approximately follows a standardized normal distribution" [1].

5. Results

The majority of the respondents (83%), as shown in Table 1, reported that they had three or more years of experience in their current position, while only (17%) of the respondents had less than three years of experience in their current position.

Table 1. Frequency distribution of the respondents in their current position.

Experience in the Current Position	Frequency	Percent
1-3 Years	4	17%
3-7 Years	5	22%
7-11 Years	9	43%
11-15 Years	4	18%
Total	22	100%

Almost (81%) of the respondents declared that they had three or more years of experience in the same bank, while only (19%) reported that they had less than four years of experience in the observed bank.

Table 2. Frequency distribution of the respondents experience in the observed bank.

Experience	Frequency	Percent
1-3 Years	4	18%
3-7 Years	10	45%
7-11 Years	8	36%
Total	22	100%

It can be concluded from the above tables that the individuals who answered the questionnaire had the minimum required level of knowledge, which may increase the credibility and reliability of their answers.

The following sections however focuses on the statistical findings related to maturity model dimensions. It consists of descriptive statistics such as frequencies and percentages.

5.1. Awareness and Communications

To explore the existence and the implementation awareness and communication procedures, the respondents were asked to indicate the existence of such procedures at their banks. The statistical findings as shown in Table 3 revealed that all respondents (100%) indicated that their management created permanent communication channels with IT seniors (CIO) in order to guarantee identifying corporate strategy and goals. Furthermore, all respondents indicate that domestic banks management receives mapping report prepared by IT seniors that illustrate the predefined current and future business needs on hand, and the probable suitable information technology solutions on the other hand. The results also showed that 91% of the respondents believed that domestic banks management receives continuous reporting regarding IT alignment status with organization strategy, regulatory obligations and laws, prospective risks and point up the high value added from IT investments. These results indicate that domestic banks management are aware of the importance of aligning banks strategy with the IT goals and making sure to have suitable and permanent communication channels.

Table 3. Awareness and communications procedures (frequencies).

		Not Exist		Exists	
	Awareness and Communications	Freq.	Percent	Freq.	Percent
1	Management creates permanent communication channels with IT seniors (CIO) in order to guarantee identifying corporate strategy and goals.	0	-	22	100%
2	Management receives mapping report prepared by IT seniors illustrates the predefined current and future business needs on hand and the probable suitable information technology solutions on the other hand.	0	-	22	100%
3	Management receives continuous reporting regarding IT alignment status with organization strategy, regulatory obligations and laws, prospective risks and point up the high value added from IT investments.	2	9.1%	20	90.9 %

5.2. Tools and Automation

To investigate the existence and the implementation of adequate automation tools in the domestic banks, the respondents were asked to indicate whether the related procedure existed or not. The statistical findings as shown in Table 4 revealed that (45.5%) of the respondents claimed that their banks have automation solution which is a software that can detect, validate and report unauthorized changes out of policy action on the entire IT infrastructure in real time, offering immediate and effective corrections. On the other hand (82%) of the respondents reported that their banks have database activity auditing tool that can automatically monitor activities and detect control exceptions. Moreover, (27.3%) of the respondents claimed that their banks integrated software system that runs off a unified database such as Enterprise Resource Planning system (ERP), allowing departments to share information and communicate easily with each other. Such results reveal moderate level of using automation tools.

Table 4. Tools and automation procedures (frequencies).

		NoTexist		Exists	
	Tools and automation	Freq.	Percent	Freq.	Percent
4	The bank has automation solution which is software that can detect, validate and report unauthorized changes out of policy action on the entire IT infrastructure in real time, offering immediate and effective corrections.	12	54.5%	10	45.5%
5	The bank has database activity auditing tool that can automatically monitor activities and detect control exceptions.	4	18.18 %	18	81.82 %
6	The bank integrated software system that runs off a unified database such as enterprise resource planning system, allowing departments to share information and communicate easily with each other.	16	72.73 %	6	27.27 %

5.3. Responsibility and Accountability

According to all respondents, domestic banks implement all related procedures related to define responsibilities, document related procedures and follow up the implementation of these procedures as shown in Table 5.

5.4. Skills and Expertise

The statistical results in Table 6 revealed that all respondents reported that their banks state high hiring standards for sensitive positioned IT employees include back ground check, educational check, confidentiality agreements. Moreover, the management requests from the IT department a continuous employee performance review where employees must confirm their understanding of and compliance with the entity security policies.

Some of the respondents indicate that management did not request from the IT department a continuous employee performance review, while (91%) of the respondents claimed that their management requested it.

5.5. Goal Setting and Measurement

Based on the results showed in Table 7, domestic banks strategy clearly states the objectives of the IT department for each fiscal year while the IT department strategic plan cites the corporate business plan as the prioritization of its initiatives and projects. Management also conduct a strategic planning sessions during which all executives meet to determine the company's goals and strategies for the coming year, and where departments are urged to develop their operational plans for the year accordingly.

Significant percent of the respondents indicate that management did not measure IT department performance effectiveness and efficiency, while (64%) of the respondents claimed that their management measure it.

Table 5. Responsibility and accountability procedures (frequencies).

		Exists	
	Responsibility and Accountability	**Freq.**	**Percent**
7	Management has clear identification of the responsible employees for the different IT activities such as IT principles, IT architecture, IT infrastructure, business application needs and IT investment and prioritization.	22	100.00%
8	Management develops clearly stated policies that explicitly describe honest and dishonest behaviors. Such policies are of a written form and communicated to employees.	22	100.00%
9	Management requires material dishonest behaviors log report and the correction action for each incident.	22	100.00%

Table 6. Skills and expertise procedures (frequencies).

		Not Exist		Exists	
	Skills and Expertise	**Freq.**	**Percent**	**Freq.**	**Percent**
10	Management's state high hiring standards for sensitive positioned IT employees include back ground check, educational check, confidentiality agreements.	0	-	22	100.00%
11	Management requests from the IT department a continuous employee performance review, where employees must confirm their understanding of and compliance with the entity security policies.	2	9.09%	20	90.91%
12	Management requests implementing continuous employees training program to enhance employee's knowledge and skills and provide opportunities for individual career growth.	0	-	22	100.00%

5.6. Policies, Plans, and Procedures

The descriptive statistics presented in Table 8 revealed major discrepancies in this section where almost (73%) of the respondents indicate that domestic banks management did not approve employing DBMS that defines each type of data, the level of protection required for each type and to whom data is required (procedure no. 30). The same percent was also given to simulate a disturbance for thorough (full) testing of the Disaster Recovery Plan (DRP), (procedure no. 20).

Moreover, (64%) of the respondents believed that the domestic bank management did not request reports prepared by IT department periodically illustrating the required modification to internet security procedures such as, antivirus and firewalls (procedure no. 28). In addition, (55%) of the respondents claimed that domestic bank management did not approved the employment of automated data infrastructure management system, such system standardize IT operating procedures for maintaining, backups and upgrades for data libraries and directories (procedure no. 31). The same result was also given to "effectiveness of control procedures assessment" reports (procedure no. 32). On the other hand, all of the respondents believed that management requests that all critical personnel identified in a DRP are holding current version of the plan both onsite and offsite, requested periodic DRP checklist testing report and followed up to correct all discrepancies that were reported (procedure no. 16 & 22).

Table 7. Goal setting and measurement procedures (frequencies).

		Not Exist		Exists	
	Goal Setting and Measurement	**Freq.**	**Percent**	**Freq.**	**Percent**
13	The corporate strategy clearly states the objectives of the IT department for each fiscal year while the IT department strategic plan cites the corporate business plan as the prioritization of its initiatives and projects.	0	-	22	100.00%
14	Management conducts strategic planning sessions during which all executives meet to determine the company's goals and strategies for the coming year, and where departments are urged to develop their operational plans for the year accordingly.	0	-	22	100.00%
15	Management measures IT department performance effectiveness and efficiency, this is done by having integrated performance measurement system linking IT performance to business goals by global application of the IT balance scorecard.	8	36.36%	14	63.64%

Table 8. Policies, plans and procedures (frequencies).

		Does Not Exist		Exists	
	Policies, Plans and Procedures	**Freq.**	**Percent**	**Freq.**	**Percent**
16	Management requests that all critical personnel identified in a DRP are holding current version of the plan both onsite and offsite.	0	-	22	100.00%
17	Management periodically requests a DRP checklist testing report from DRP team; this report goes through the DRP procedures to identify gaps bottlenecks and other weaknesses in the plan.	0	-	22	100.00%
18	Management assigns personnel to monitor and document variation on procedures while implementing a DRP test.	6	27.27%	16	72.73%
19	Management simulates a disturbance for partial testing of the DRP.	6	27.27%	16	72.73%
20	Management annually simulates a disturbance for thorough (Full) testing of the DRP.	16	72.73%	6	27.27%
21	Management requests a DRP simulation test results report from DRP team, and activates required modifications and improvement to the tested plan.	6	27.27%	16	72.73%
22	Management follows up and orders to correct all discrepancies that were reported by the risk-management team concerning examined security threats.	0	-	22	100.00%
23	Management receives a report from the IT department on updated system description to authorized users regarding sensitive data access.	6	27.27%	16	72.73%
24	Management receives a report prepared by the IT department showing incident logs and potential significant security breaches in order to improve related security procedures.	6	27.27%	16	72.73%
25	Management sets and emphases policies prohibiting visitors from carrying cell phones, laptops, PDAs and other portable devices that could capture confidential information while touring the entities facilities.	8	36.36%	14	63.64%
26	Due to a new implementation or acquisition, management receives a report from the IT department on modification of existing physical and logical access security procedures or the development of new access procedures.	8	36.36%	14	63.64%
27	Management requests a periodic review report from the IT department regarding the appropriate use of internet resources (Trusted and un-trusted resources) within the organization.	4	18.18%	18	81.82%
28	Management requests report prepared by IT department periodically illustrating the required modification to internet security procedures such as, antivirus and Firewalls.	14	63.64%	8	36.36%
29	IT reports to the management frequently the audit trail record that detects material unauthorized network operations activity.	10	45.45%	12	54.55%
30	Management approves employing DBMS that defines each type of data, the level of protection required for each type and to whom data is required.	16	72.73%	6	27.27%
31	Automated data infrastructure management system is approved by the management to be employed, such system standardize IT operating procedures for maintaining, backups and upgrades for data libraries and directories.	12	54.55%	10	45.45%
32	Management requests periodic assessment reports from IT department on the effectiveness of control procedures concerning source data, data entry, data processing, data transmission and output controls.	12	54.55%	10	45.45%
33	Management emphases using strong security procedures for manual external data transmission that concerned to sensitive and confidential information.	0	-	22	100.00%

Table 9 below shows the statistical findings related to the hypothesis testing. To test the first major hypothesis and related minor hypotheses, *Z* test for proportion was conducted for the study population.

The developed norms are used as a cut point for the minimum accepted percentages of applying maturity model, where the bank is considered to apply the maturity model dimension if its own evaluation percentage exceeds this norm. The researchers then tested for significant differences between the applied

percentages in the Jordanian domestic banks and these norms using *Z* test for proportion.

Table 9. Z test for percent differences.

Dimension	Norms	%	Population Size (N)	Z-test	Value P	S*
Awareness and Communications	70%	91 %	22	2.14	0.0162	R**
Tools and Automation.	70%	27 %	22	(4.37)	0.9999	A***
Responsibility and Accountability	70%	100 %	22	3.07	0.0011	R
Skills and Expertise.	70%	91 %	22	2.14	0.0162	R
Goal Setting and Measurement.	70%	64 %	22	(0.65)	0.7452	A
Policies, Plans and Procedures.	80%	23 %	22	(6.71)	1.0000	A
Overall	70%	100 %	22	3.07	0.0011	R

* S: Success of Hypothesis
** R: Rejected
*** A: Accepted

Based on the results presented in Table 9, p-value appears to be less than 0.05 for awareness and communications, responsibility and accountability, and skills and expertise dimensions. The *Z* value is also higher than 1.96, which means it falls in a rejection area. All of that lead us to reject the null hypothesis. This implies that the Jordanian domestic banks apply the required procedures in these dimensions. While, *p* value is more than (0.05) for tools and automation, goal setting and measurement, and policies, plans and procedures, the *Z* values for them also were less than 1.96. Consequently, the researchers concluded that the Jordanian domestic banks are not using enough procedures to satisfy these dimensions.

According to the aforementioned results, we reject the main null hypothesis that stated, (Jordanian domestic banks do not have effective IT governance implementation). In addition we did not reject the second, fifth and sixth minor hypotheses, while reject the rest of the minor hypotheses.

6. Conclusion

The study showed that Jordanian domestic banks applied effective awareness and communications, responsibility and accountability, and skills and expertise dimensions mainly, while they do not do enough with regard to the other dimensions (tools and automation, "goal setting and measurement," and "policies, plans and procedures"). Due to the statistical findings of the current study, which indicate that half of the maturity model was not applied in a proper way, we believe that Jordanian domestic banks may increase efforts to IT governance. Jordanian domestic banks are required to invest more in the IT governance and guarantee having comprehensive implementation to cope with the technology advancements.

7. Limitations and Further Research Agenda

As with all research, this study is subject to number of limitations and these might be explored in future research. The study adopted the quantitative approach to test the study theoretical model, thus limiting the choice of methodology to a cross-sectional survey, which is only concerned with employing quantitative methods of data collection. Thus, a questionnaire survey was adopted in this study and the researchers were not able to question the respondents to ascertain in more details the exact nature of the responses. Therefore, extra care and caution is essential when interpreting questionnaire findings. However, the problems relating to questionnaire surveys can be minimized by undertaking a number of post-questionnaire interviews. However, a time constraint, interview accessibility, and the availability of interviewees for a significant amount of time constrain the researchers from undertaking interviews. Nevertheless, interviews to pursue issues raised by the survey results are a fruitful area for future research. In addition, the results of this study apply only to the target sample operating in Jordan. Thus, these results may not be generalizable to other sectors. Future research however needs to be extended to other industry sectors in order to generalize the results. Furthermore the current study is considered as exploratory one; consequently future research work might be explored in the future using different and more developed instruments which take into the consideration the frequency of IT governance procedures and result more valuable results.

Despite the limitations that have been identified previously, this study has provided several important insights into issues relating to IT governance. This study is one of the first to evaluate IT governance implementation in a Jordanian settings. Hopefully, this study will encourage researchers to conduct further empirical studies about the implementation of the IT governance to clarify some of the complexity and confusion that is accompanied with this approach.

References

[1] Berenson R., Garfield J., Del R., and Chance B., *Concepts and Application,* Prentice Hall, 2002.

[2] Bowen P., Cheung M., and Rohde F., "Enhancing IT Governance Practices: A Model and Case Study of an Organization's Efforts," *International Journal of Accounting Information Systems*, vol. 3, no. 1, pp. 191-221, 2007.

[3] Brown C. and Sambamurthy V.*, Repositioning the IT Organization to Enable Business Transformation*, Oxford University Press, US 1999.

[4] Brown C., "Examining the Hybrid IS Governance Solution: Evidence from a Single Case Study," *Computer Journal of Information System Research*, vol. 1, no. 1, pp. 69-94, 1997.

[5] COBiT, Executive Summary Frameworks, *Offman Estates*, 1998.

[6] Coen M. and Kelly U., "Information Management and Governance in UK Higher Education Institutions: Bringing IT in from the Cold," *Computer Journal of Perspectives*, vol. 11, no. 1, pp. 3-23, 2007.

[7] Colbert L. and Brown L., "A Comparison of Internal Controls: COBIT, SAC, COSO and SAS 55/78," *Computer Journal of IS Audit Control*, vol. 4, no. 4, pp. 26-35, 1996.

[8] Curtis M. and Borthick T., "Evaluation of Internal Control from a Control Objective Narrative," *Computer Journal of Information Systems*, vol. 13, no. 1, pp. 4-9, 1999.

[9] Hayale T. and Abu Khadra H., "Evaluation of the Effectiveness of Control Systems in the Computerized Accounting Information Systems: An Empirical Research Applied on Jordanian Banking Sector," *Computer Journal of Accounting Business and Management*, vol. 13, no. 2, pp. 39-68, 2006.

[10] Jarvenpaa S. and Ives B., "Executive Involvement and Participation in the Management of Information Technology," *Computer Journal of MIS Quarterly*, vol. 15, no. 2, pp. 205-227, 1991.

[11] Jurgen L., Monnoyer E., and Scherdin A., "Designing IT for Business: When Business and Computer People Put Their Heads Together, They Can Transfer a Company's IT Architecture," *Computer Journal of The McKinsey Quarterly*, vol. 54, no. 3, pp. 76-86, 2003.

[12] Klapper L. and Love I., "Corporate Governance Investor Protection and Performance in Emmerging Markets Working Paper," *Technical Report*, 2002.

[13] Kordel L., "IT Governance Hands-on Using COBiT to Implement IT Governance," *Information Systems Control Journal*, vol. 2, no. 1, pp. 157-164, 2004.

[14] Lainhart I. and John W., "COBIT: A Methodology for Managing and Controlling Information and Information Technology Risks and Vulnerabilities," *Computer Journal of Information Systems*, vol. 14, no. 1, pp. 79-91, 1995.

[15] Li C., Lim J., and Wang Q., "Internal and External Influences on IT Control Governance," *International Journal of Accounting Information Systems*, vol. 6, no. 8, pp. 225-239, 2007.

[16] Oak V., *Fund Report*, www.oakvaluefund.com, 2004.

[17] Oppenheim N., *Interviewing and Attitude Measurement,* Pinter Publishers, NY, 1992.

[18] Pauwels E., *Change Governance Series: Making Sense of Regulations and Best Practices*, Copyright Serena Software, 2006.

[19] Peterson R., "Crafting Information Technology Governance," *Computer Journal of Information System Management*, vol. 6, no. 4, pp. 167-173, 2004.

[20] Rau K., "Effective Governance of IT: Design, Objectives Roles and Relationships," *Computer Journal of Information System Management*, vol. 21, no. 2, pp. 21-40, 2004.

[21] Schwarz A. and Hirschheim R. "An Extended Platform Logic Perspective of IT Governance: Managing Perception and Activities of IT," *Computer Journal of Strategic Information Systems*, vol. 12, no. 2, pp. 129-166, 2003.

[22] Sohal A. and Fitzpatrick P., "IT Governance and Management in Large Australian Organizations," *International Journal of Production Economics*, vol. 75, no. 1, pp. 97-112, 2002.

[23] Syaiful A., Effective Information Technology Governance Mechanisims: An Australian Study Gadjah Mada," *International Journal of Business*, vol. 8, no. 1, pp. 69-102, 2006.

[24] Tuttle B., Vandervelde S. "An Empirical Examination of Cobit as an Internal Control Framework for Information Technology," *International Journal of Accounting Information Systems*, vol. 8, no. 4, pp. 240-263, 2007.

[25] Ulsch M. and Bamberger J., "Sound IT Governance Needs Requires Breadth and Depth," *Financial Executive*, 2006.

[26] Wallace R. and Mellor C., "No Response Bias in Mail Accounting Surveys: A Pedagogical Note," *Computer Journal of British Accounting Review,* vol. 20, no. 2, pp. 131-139, 1988.

[27] Weill P. and Ross J., *IT Governance: How Top Performers Manage IT Decision Rights for Superior Results*, Harvard Business School Press, UK, 2004.

[28] Weill P. and Ross J., "IT Governance on One Page", *Computer Journal of MIT Sloan Management*, vol. 43, no. 2, pp. 157-160, 2004.

[29] Weill P. and Ross J., *How Top Performers Manage IT Decision Right for Superior Results*, Harvard Business School Press, UK, 2004.

[30] Westerman G., "IT Risk Management: From IT Necessity to Strategic Business Value," *Research Paper 4658-07*, 2006.

Husam Abu Khadra received his BSc in accounting, Zarqa Private University, his MSc in accounting and financial from Arab Academy for Banking and Financial Sciences, and his PhD in accounting information system, Arab Academy for Banking and Financial Sciences.

Majdy Zuriekat received his BSc in accounting, Baghdad University, Iraq, his MBA from University of Jordan, and his PhD in accounting from University of Huddersfield, England.

Nidal Alramhi received his BSc in business sciences from Yarmok University, his MSc in accounting and financial from Arab Academy for Banking and Financial Sciences, and PhD in accounting information system, Arab Academy for Banking and Financial Sciences.