



**THE POWER OF IT GOVERNANCE WHEN APPLIED ON KEY
DIVISIONS IN FINANCIAL INSTITUTIONS
(I.T- I.S- RISK - AUDIT)**

Egyetemi doktori (PhD) értekezés

a szerző neve: Elias Radi Jriesat

témavezető neve: Dr. Jozsef Gall

DEBRECENI EGYETEM

Természettudományi és Informatikai Doktori Tanács

Informatikai Tudományok Doktori Iskola

Debrecen, 2019.

DOCTORAL (PhD) DISSERTATION

Elias Jriesat

Debrecen

2019

UNIVERSITY OF DEBRECEN

FACULTY OF INFORMATICS

Informatics Doctoral School

THE POWER OF IT GOVERNANCE WHEN APPLIED ON KEY
DIVISIONS IN FINANCIAL INSTITUTIONS (I.T- I.S - RISK - AUDIT)

The aim of this dissertation is to obtain a doctoral (PhD) degree
in the scientific field of “information technology”

Written by: Elias Jriesat..... certified

Doctoral final exam committee:

Name	academic degree
------	-----------------

President:	
------------	-------

Members:	
----------	-------

.....

.....

.....

Date of the doctoral final exam: 20.....

Reviewers of the dissertation:

Name, academic degree signature

.....

.....

Review committee:

Name, academic degree

signature

President:

Secretary:

Members:

.....

.....

.....

Date of defending the dissertation: 2019.

DECLARATION

I, the undersigned (name: Elias Jriesat, date of birth: 19/06/1982) declare under penalty of perjury and certify with my signature that the dissertation I submitted in order to obtain doctoral (PhD) degree is entirely my own work.

Furthermore, I declare the following:

- I examined the code of the Debrecen University's Doctoral School of informatics and I acknowledge the points laid down in the code as mandatory;
- I handled the technical literature sources used in my dissertation fairly and I conformed to the provisions and stipulations related to the dissertation;
- I indicated the original source of other authors' unpublished thoughts and data in the references section in a complete and correct way, considering the prevailing copyright protection rules;
- No dissertation which is fully or partly identical to the present dissertation was submitted to any other university or doctoral school for obtaining a PhD degree.

Debrecen, 31/10/2019.

Name: Elias Jriesat

Signature:

A handwritten signature in blue ink, appearing to read 'Elias Jriesat', with a stylized flourish at the end.

Contents

INTRODUCTION	1
1 TOPICS AND OBJECTIVES.....	5
1.1 THE AIMS OF THE DISSERTATION	5
1.2 THE MAIN RESEARCH TOPICS AND QUESTIONS.....	6
1.3 RESEARCH METHODOLOGY	8
1.3.1 IT GOVERNANCE METHODOLOGY.....	8
1.3.2 CLOUD COMPUTING	9
1.3.3 IT OPERATIONAL RISK.....	9
1.3.4 COBIT 5	10
1.4 STRUCTURE OF THE DISSERTATION	10
2 LITERATURE REVIEW.....	12
2.1 IT GOVERNANCE	12
2.1.1 INTERNAL CONTROLS DEFINITION.....	12
2.1.2 AUDITING / IT AUDIT.....	13
2.1.3 INFORMATION TECHNOLOGY ASSURANCE FRAMEWORK (ITAF).....	14
2.1.4 COMPUTERIZED ACCOUNTING INFORMATION SYSTEMS (CAIS).....	16
2.1.5 INFORMATION TECHNOLOGY GOVERNANCE (ITG).....	16
2.1.6 INFORMATION SECURITY GOVERNANCE (ISG).....	17
2.2 CLOUD COMPUTING	18
2.3 IT OPERATIONAL RISK.....	24
2.4 CONTROL OBJECTIVES FOR INFORMATION AND RELATED.....	32
3 METHODOLOGY	55
3.1 CONCEPTUAL FRAMEWORK.....	55
3.2 RESEARCH TOPICS – BRIEF DEFINITIONS.....	56
3.2.1 IT OPERATIONAL RISK.....	56
3.2.2 COBIT 5 FRAMEWORK	57
3.2.3 IT GOVERNANCE.....	57
3.2.3.1 VAL IT FRAMEWORK	58
3.2.3.2 INFORMATION TECHNOLOGY MANAGEMENT	60

3.2.4 CLOUD COMPUTING	61
3.3 MATERIAL AND METHODS.....	61
3.3.1 IT GOVERNANCE.....	62
3.3.2 CLOUD COMPUTING	65
3.3.3 IT OPERATIONAL RISK.....	70
3.3.3.1 DESIGN AND METHODS.....	70
3.3.3.2 RESEARCH POPULATION AND SAMPLE.....	72
3.3.4 COBIT 5.....	77
3.3.4.1 DESIGN AND METHODS	78
3.3.4.2 RESEARCH POPULATION AND SAMPLE.....	77
3.3.4.3 DATA ANALYSIS	80
4 RESULTS & RESEARCH FINDINGS.....	86
4.1 IT GOVERNANCE	86
4.1.1 DISCUSSION ON IT GOVERNANCE ERROR! BOOKMARK NOT DEFINED.	
4.1.2 RESULTS AND FINDINGS FINDINGS.....	89
4.2 CLOUD COMPUTING	97
4.2.1 DISCUSSIONS & COMPARISON STUDY	97
4.2.1.1 REGULATORY CONSIDERATIONS & INTERNATIONAL ST.....	98
4.2.1.2 RISK MANAGEMENT.....	99
4.2.1.3 DATA SECURITY AND DATA PROTECTION.....	100
4.2.1.4 EFFECTIVE ACCESS TO DATA & BUSINESS PREMISES.....	102
4.2.1.5 CHANGE MANAGEMENT AND CONTINUITY PLAN	104
4.2.1.6 EXIT PLAN.....	105
4.2.2 MATRIX: BSA GLOBAL CLOUD COMPUTING SCORECARD	106
4.2.2.1 DISCUSSION	106
4.2.2.2 ANALYSIS RESULTS:	108
4.3 IT OPERATIONAL RISK.....	113
4.3.1 DISCUSSIONS & COMPARISON STUDY	113
4.4 COBIT 5 FRAMEWORK.....	119
4.4.1 DESCRIPTIVE ANALYSES FOR POPULATION'S RESPONDENTS..	122
4.4.2 DESCRIPTIVE ANALYSIS ACCORDING TO THE GENDER	128

4.4.3	DESCRIPTIVE ANALYSES ACCORDING TO THE EDUCATIONAL	123
4.4.4	DESCRIPTIVE ANALYSIS ACCORDING TO THE PROFESSIONAL	123
4.4.5	DESCRIPTIVE ANALYSIS ACCORDING TO THE JOB TITLE:	124
4.4.6	DESCRIPTIVE ANALYSES FOR VARIABLES RELATION SHIPS :...	126
4.4.7	CORRELATIONS	132
5	CONCLUSIONS AND RECOMMENDATIONS.....	142
5.1	IT GOVERNANCE - CONCLUSION	142
5.2	CLOUD COMPUTING - CONCLUSION	144
5.3	IT OPERATIONAL RISK - CONCLUSION.....	150
5.4	COBIT 5 – CONCLUSION.....	152
6	REFERENCES.....	155
7	LIST OF PUBLICATIONS	175
8	LIST OF TABLES	178
9	ACKNOWLEDGMENTS	180
10	APPENDIX (A).....	183

INTRODUCTION

In recent years, IT experts have witnessed the growth of investments throughout the world of technology in various aspects. The era of innovation and investment in Information/Communication Technology has become increasingly sophisticated, especially in the business and the economic sectors. Nowadays, Information Technically is considered one of the areas that are most concentrated on, and one of the new technological trends in the market is Cloud Computing. The use of such a method of cloud services solidifies a positive role in facilitating business processes and simplifying information storage methods, as well as saving time/effort while enabling companies to reduce expenses allocated to cover the needs of the IT Department. However, this choice would roughly elevate the level of threats, and thus, lead focus on increasing the security level of controls that is highly essential in order to mitigate all risks. Nevertheless, both of the IT Audit and IT Risk topics have become crucially necessary in order to obtain a reasonable assurance level of risk mitigation by setting up high-level controls aligned with the related policies and procedures in any organization.

Abu Bakar and bin HJ Tasmin in their work [1] indicates, “The competition, globalization, and innovation related to technology, services, and product types which are offered to the customers in the banking industry affect their satisfaction and loyalty, besides it enhances institution’s profitability” . The papers [2,3] concentrated on the utilization of Information Technology and its functionality, clarifying that an effective utilization of IT could always lead the institutions to strengthen the inner system of work process and support the required controls in order to build and maintain new governance processes. Weidenmier M. L. and Ramamoorti, s. [4] stated that,

“The organizational risk could be increased with information technology; therefore, the organizations have to implement the control with a view to integrated controls and process linkages on IT”.

The large number of factors lately indicates the increasing expansion in Information Technology and in turn, desperately needs risk controls focusing on the growing demand of reducing risks and controlling IT costs. Recently, the control on the IT surroundings should be effective, designed particularly for the IT usage by stakeholders. In order to face the challenges in business and achieve the goals and objectives in information technology, the high-level executives must ensure the most efficient means of using IT (See in [5]). In either case, we are witnessing a dramatic era of rapid developments in some domains within the IT sector intended to facilitate work processes and procedures. For instance, “Cloud computing is known as a type of computing that relies on sharing computing resources rather than having local servers or personal devices to handle applications. Cloud computing is comparable to grid computing, a type of computing where unused processing cycles of all computers in a network are harnessed to solve problems too complex for any stand-alone machine” (See in [6]). It has now become commonplace for many institutions to use the implementation of Cloud Computing services.

Progressively, organizations become exposed to various operational risks related to the use of IT such as virus attacks, unauthorized access to data, breakdown of infrastructure, system and infrastructure contingency, and performance problems. Therefore, institutions should adopt the processes of identifying, analyzing, and evaluating potential IT related operational risks in order to prevent themselves from such massive risks (See in [7]).

In recognition of the fact that several financial worldwide establishments announced operational misfortunes, there has been a developing enthusiasm for Operational Risk Management. For instance, UBS (Swiss Multinational Investment Bank and Financial Services Company) confronted an operational misfortune/loss due to one of its dealer's deceitful conduct (Fraud), and also, Operational Losses were reported in 119 banks in the SIGOR (the Standards Implementation Group) totaling approximately €59.6 billion in 2008. In either case, the events of operational loss are complicated and vary in classifications between the internal and external categories to business intrusions caused by system breakdowns (See in [8]).

It is worth mentioning that the terms "SOX and EUROSIX" are considered essential regulations that protect the financial sectors worldwide from becoming vulnerable to any losses caused by the Operational Risk in the organizations. The European Parliament issued the EUROSIX, which was adopted by all EU members, whereas the US Government regulated SOX in the early of 2000's for their local market (See in [9]).

Furthermore, risks of every type related to roles of business require techniques to manage and control its utilization and to mitigate its negative effects in order to increase partner satisfaction. As a result, the concept of IT Governance was born in order to incorporate reception of control structures and best practices to encourage, monitor, and enhance critical IT activities to expand business esteem and reduce business risk according to business strategy.

In 1996, ISACA issued the primary adaptation of "The Control Objectives for Information and related Technology" (COBIT) which concentrated on

Audit, Control, and Management Concepts in the Enterprise. ISACA attempted to create COBIT until reaching COBIT 4.1 and then releasing the last form in COBIT 5 during early 2012, which concentrated mainly on merging the IT Management and the IT Governance concepts (See in [10]).

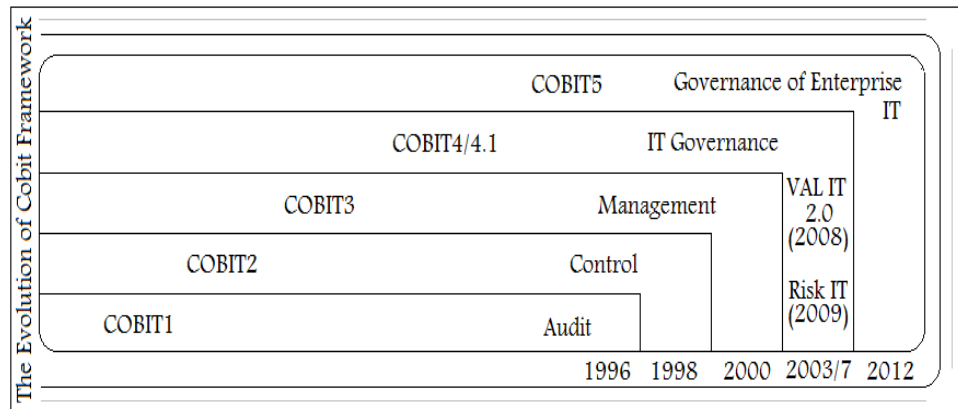


Figure 1: Evolution of COBIT framework

Source: prepared by the author

COBIT 5 is a complete, globally accepted framework for governing and managing Enterprise Information and Technology (IT) that supports enterprise executives and management in their definition and achievement of business goals and related IT goals. COBIT 5 describes five principles and seven enablers that support enterprises in the development, implementation, and continuous monitoring and improvement of good IT-related Governance and Management practices (See in [11]).

1 TOPICS AND OBJECTIVES

1.1 The aims of the dissertation

- The dissertation is focusing on four main subjects (IT Governance, Cloud computing, IT Operational risk and COBIT 5), targeting bunch of goals, the main aims of this dissertation are as follows:
- To clarify the major concept related to the IT governance.
- To prove that adopting IT Governance methodology might enhance the value of IT division in any institution.
- To Measure the level of knowledge and awareness in the “MENA” region related to the IT governance concept according to the international standards.
- To quantify the amount of studies in the MENA region related to the IT governance methodology.
- To Illuminate the overall perception of cloud computing.
- To measure UK’s, Germany’s, & Hungary’s rank in the cloud-computing domain according to the international BSA scorecard.
- To measure the awareness level of the Jordanian banks regarding the actual size of risks related to the IT division in all aspects.
- To prove that most of the professionals in the Jordanian banks are underestimating the value of capital reservation.
- To measure the maturity level of the Jordanian banks, regarding deploying COBIT 5 framework according to CBJ regulations.
- To measure the influence of COBIT 5 framework on the entire policies and procedures related to most of the departments in any institution.

- To estimate the level of correlation between the variables of COBIT 5 maturity level (as per each related department individually) and the annual financial variables of the banks.
- To estimate the level of correlation between the variables of COBIT 5 maturity level as per the whole organization and the annual financial variables of the banks.

1.2 The main research topics and questions

This dissertation designed in order to illuminate the absolute theory related to the IT governance concept, encompassing all of its aspects, according to the latest international standards, policies, and procedures adopted recently by most of the financial sectors in the local Jordanian and international markets. Additionally, it sheds light on the importance of cloud computing methodology, covering its general growth and expansion directed to simplify the execution practices and management methods related to Information Technology environment. Moreover, this dissertation is clarifying one of the essential concepts of (IT Operational Risk), that is considered as a crucial role in any risk division at any organization by concentrating only on three main event types based on Basel II international business standard clarifying its impact on the daily operational practices and role of work in any institution.

After all, the most recent important framework related to IT governance (COBIT 5) was included, where i exposed the general effect of this framework on the entire financial sector in the region. Such a huge framework is used to maximize the work controls and maintain simplicity of the daily work processes for all of the related Departments especially the IT division in any institution according to the international standards and regulations

stated by the authorities such as CBJ (Central Bank of Jordan), specifically in our case.

Several main questions derived from the main content of the whole research in order to shed light on the key major objectives obtained:

1. Does the MENA Region have sufficient contributions of publications in the fields of IT Governance, COBIT, IT Audit, and IT risk?
2. Does the amount of contributions reflect the current value of knowledge and awareness adopted recently in the MENA Region regarding the IT Governance concept?
3. How strong is the correlation between the main concept of IT Governance and the other suggested related topics (Cloud Computing, IT Operational Risk, and COBIT 5)?
4. What is the main concept of Cloud Computing and how would it generally affect the financial sector in any region?
5. What crucial points should the institutions take into consideration in case they are willing to apply Cloud-Computing Methodology and what security procedures should they adopt?
6. Are Germany, the UK, and Hungary considered as leading countries in the domain of Cloud Computing, and what legislative authorities are responsible for such legalizations and regulations in those countries?
7. Is the Jordanian banking sector fully aware of the volume of risks related to the IT sector, which surrounds its internal working policies and procedures?

8. Do the specialists in the Jordanian banks accurately estimate the allocation of capital (reserve) needed to afford the loss generated by event types related to IT Operational Risk?
9. What is the status of the Jordanian banking sector concerning COBIT 5?
10. How efficient and sufficient is the COBIT 5 framework concerning the improvement of the performance of the Jordanian Banks?
11. Does the implementation of COBIT 5 framework affect the related departments in the entire institution equally?
12. How valuable are the results of COBIT 5 Framework compared to the amount of money invested on implementing such a framework in any institution?
13. Does the maturity level of deploying COBIT 5 framework directly affect the profitability variables (ROA, ROE) of the banks in the Jordanian financial sector?

1.3 Research Methodology

As mentioned previously, this dissertation is focusing on for main topics (IT Governance, cloud computing, it operational risk and COBIT 5). I used several methodologies in order to conclude the needed understandings and targeted goals, as follows:

1.3.1 IT Governance Methodology

I have conducted a desk-based research targeting all the papers published between the years 2006 and 2016 that relates to IT governance topic or any other similar topic in most of the public, private, and governmental sectors in the 'MENA' region. In addition, I have used methods of content analysis to

get accurate results measuring the underlying development in the region focusing on IT governance / audit and COBIT frameworks and technologies used to mitigate IT operational risks, general and all other different types of risks related to it.

1.3.2 Cloud Computing

Moreover, I have prepared a comparison study targeting three European countries (Germany, Hungary, and U.K.), elucidating the main concepts of cloud computing theory, according to the most well-known regulations issued by several specialized European authorities. I clarified some major key points that must be taken into consideration in case of applying the cloud services in any sector. Also based on the 'BSA' global cloud-computing scorecard 2016 (of which Germany and U.K were a part of), I have prepared an assessment comparing between them, excluding the Hungarian data procured by surveying the specialists in the 'MNB' authority, in order to get relevant responses on the global 'BSA' survey.

1.3.3 IT Operational Risk

Furthermore, I have conducted a survey targeting all of the banks in the Jordanian sector in order to get some variables such as the "individual losses" and "maximum losses", in order to calculate the needed variables from the collected data such as (μ and σ). After all I have used Monte Carlo simulation in R code in order to measure the capital reservation of losses related to three specific event types correlated to IT (according to Basel II business standard).

1.3.4 COBIT 5

Finally, I have prepared a questionnaire targeting all of the Jordanian banks in the financial sector. The questionnaire contained One hundred and twenty-seven questions raised in the survey in order to measure the maturity level of the banks regarding adopting COBIT 5 Framework. I used SPSS analyses to get the accurate needed results.

1.4 Structure of the dissertation

The study is composed of five chapters as follows:

Chapter1: Describes the subject, aim and the objectives of dissertation, the field of research methodology, and the structure of the dissertation.

Chapter2: Includes a literature review related to the aim and objectives of the dissertation as follows:

- IT Governance topic trailed by the following: Internal Controls, Auditing/IT Audit, ITAF (Information Technology Assurance Framework), CCAIS (Computerized Accounting Information system), ITG (Information Technology Governance), and ISG (Information Security Governance).
- Cloud Computing theory and models
- IT Operational Risk
- COBIT (Control Objectives for Information and Related Technology)

Chapter3: Clarifies mainly the conceptual framework, methodologies, research variables, research populations, sampling, development and usage of questionnaires, and the techniques used for data analysis process is supported by the related validity and reliability analysis.

Chapter4: Discusses the findings, draws the conclusions of the results, and then suggests recommendations regarding useful solutions in the jordanian banking sector.

Chapter 5: The last chapter states the main conclusions and novelties of the research.

At the end of the study, appendixes, a list of figures, tables, list of publications, and references can be found.

2 LITERATURE REVIEW

2.1 IT Governance

This section is divided into six main sub-sections clarifying the most recent standards related to IT Governance.

2.1.1 Internal controls definition

The Committee of Sponsoring Organizations of the Tread Way Commission (COSO) has defined the internal control as a process affected by an organization's board of directors, management, and other faculties in order to provide assurance based on the achievement of objectives in the following categories: (See in [12]).

- Effectiveness and efficiency of operations
- Reliability of financial reporting
- Compliance with the applicable laws and regulations

Laudon and Laudon stated that managers rely on Information Systems in respect to the important role of the modern organization (See in [13]). Thus, the entire cash should be linked to Information System. The Banking Regulation and Supervision Board clarified that the internal control activities should be outlined and executed to tackle risks as an essential part of day-to-day operations in order to empower the monitoring of risks identified within a framework of risk assessment, as it should be involving:

- a) Policies and procedures related to the decision-making process
- b) Scope and implementation of risk management
- c) The process of setting and implementing limits and standards concerning risks
- d) Controls over the data processing infrastructure

- e) Financial and managerial reporting
- f) Personnel policy
- g) Identification of responsibilities
- h) Auditing prevention of fraud transactions (See in [14]).

Additionally, Haddad assured that internal control systems should be applicable and easily understood. Incentives and motivations should be given to employees who act in compliance with the internal controls defined and agreed upon in the organization (See in [15]).

Spira stated that the scope of internal audit procedures depends on the suitability, effectiveness, and efficiency of the work procedures (See in [16]).

2.1.2 Auditing / IT Audit

An audit role is defined as a systematic, documented, and independent process for obtaining audit evidence (records, statements of fact, or other information which is relevant and verifiable) and evaluating it objectively to determine the extent to which the audit criteria (set of policies, procedures, or requirements) is fulfilled. Several methodologies in audit may be employed to attain the audit purpose (See in [17]).

Allegrini and D'onza pointed out that operational audit, compliance, and other activities such as IT Audit, Fraud Investigation, Risk Assessment, and special projects form the total percentage of audit resources needed in the process of financial audit (See in [18]).

To examine the controls, effectiveness, operations, and security of critical systems in any organization, IT Audit is used internally so it would also identify opportunities for improvement in areas of weakness. Two primary

reasons for such attention to IT audit concepts are the increased IT dependence and spending for business operations, and the new professional requirements of these operations and legislation related to the audit. On the other hand, the demand to support key business activities by IT services has driven the level of IT spending globally to exceed approximately \$3.54 trillion and Banking and securities, insurance, and healthcare will be the fastest-growing segments in 2016 (See in [19]).

Multiple parties with various objectives could be served by IT audits within an organization; therefore, different definitions of IT audit quality have occurred. These definitions may include ideas such as completeness related to different standards, efficiency, cost, and impact. An important purpose of IT audits is to provide management with assurance that an automated process or system is meeting its objectives (See in [20]).

2.1.3 Information Technology Assurance Framework (ITAF)

The Information Technology Assurance Framework (ITAF) is a comprehensive and good-practice-setting reference model that provides guidance, tools, and techniques on the planning, design, conduct, and reporting of IS audit and assurance assignments. ITAF focuses on ISACA material and provides a single source of which Information Security audit and assurance professionals can seek guidance from research policies and procedures in order to obtain audit and assurance programs and to develop effective reports. ITAF 2nd edition was released in November 2013 and the 3rd edition in September 2014. The Information technology assurance framework (ITAF) pointed out that there are three main categories in ITAF IS audit and assurance standards:

- (1000's series) General standards of the operation process of IS assurance profession which are aligned the guiding principles.
- (1200's series) Performance standards which clarify several assignments, such as supervision and planning, materiality and risk, supervision and assignment management, scoping, audit and assurance evidence, and the exercising of professional judgment.
- (1400's series) Reporting standards, which address the regular type of means in communication and the information communicated.
 - The general standards include Audit Charter, Organizational independence, Professional independence, Reasonable expectation, Due Professional care, Proficiency, assertions, and criteria.
 - The Performance standards include engagement, planning of risk assessment, performance, and supervision, evidence, using the work of other experts, irregularity, and illegal acts.
 - The reporting standards include reporting and follow-up activities.

On the other hand, ITAF Information Security audit and assurance guidelines differed by its content from ITAF standards, but it consists of the same categories in the two sections of general guidelines and reporting guidelines without the addition of "Sampling" in the performance section. However, the two main sections of ITAF IS audit and assurance give a detailed illustration in demonstrating the guidelines and standards that should be pursued during IT audit process to get the maximum support in order to achieve a reasonable assurance of risk mitigations for all IT functions, processes, procedures, and applications (See in [21]).

2.1.4 Computerized Accounting Information Systems (CAIS)

The Data processed manually in the accounting information systems is a weak procedure and it is always subject to errors. Fortunately, the technology's improvements have accelerated the methods of collecting, processing, and retrieving data. In addition, computers decrease the likelihood amount of errors that could occur when processing data (See in [22]).

Thus, automated tools begin to occupy the highest positions in the market such as Computerized Accounting Information Systems (CAIS), which were integrated into the Information Technology systems field, and were mainly founded in order to help in improving the firm's control and related management issues in the Economic/Financial area. On the other hand, from a strategic point of view, the progress in technology has given us the ability to generate accounting information (See in [23]).

2.1.5 Information Technology Governance (ITG)

Weill and Ross explained, "Effective IT Governance is the single most important predictor of the value an organization generates from IT". Therefore, IT Governance is defined as the practice that helps in all IT investment decisions by establishing the accountability framework and allocating decision rights.

To deduce how governance decisions are made, it should be clarified that the most visible mechanisms of IT Governance are the organizational committees and roles that locate the responsibilities of decision-making according to intended archetypes. Assuring that without a better understanding of what processes are being implemented, how decisions are made, and what the desired outcomes are, IT Governance will never be effective enough to cover its role (See in [24]).

IT Governance is the responsibility of the directors' board and executive management. They are concerned regarding the IT's delivery of value added to the business and the mitigation of IT risks driven by strategic alignment of IT with the business, but by embedding accountability into the enterprise, both need to be supported by adequate resources and measured to ensure that the intended results are obtained (See in [25]).

In addition, IT Governance was described as a promising solution to the weak IT performance by some studies in the field. This is a well-known performance-strengthening tool that creates a control environment over business challenges and complexity of technology. Other research clarifies that the adoption of IT Governance helps to improve organizational accountability as well as increasing the Return on Investments (ROI) for any institution (See in [26]).

2.1.6 Information Security Governance (ISG)

ISG is an essential element of enterprise governance and consists of the organizational structures, leadership, and processes which are involved in the protection of informational assets. Therefore, institutions can address the issues of information security from a corporate governance perspective through what is called ISG, thereby optimizing certain outcomes. In terms of strategic alignment, in order to support organizational objectives, Information Security governance should enable institutions to align business strategy with security in order to support organizational objectives. ISG also supports the optimization of security investments in the support of business objectives and enables the firm to use security knowledge and infrastructure in the most efficient and effective manner possible. Finally, ISG better enables the

monitoring and reporting of security processes to ensure the achievement of objectives (See in [27]).

2.2 Cloud Computing

Several different standpoints regarding the concept of Cloud computing clarified by special authorities located in the three previous mentioned regions are as follows:

Financial Conduct Authority (FCA) (United Kingdom)

“Clouding could be defined as encompassing a range of IT services provided in various formats over the internet including private, public, or hybrid cloud as well as several domains such as Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS); Cloud services are constantly evolving” (See in [28]).

Hungarian National Bank (MNB) (Hungary)

“The computing cloud is a solution that enables network access to shared configurable computing resources on demand such as networks, servers, storage devices, applications, and services. It can be allocated quickly and achieve its goals with minimal management efforts or interaction from the service provider, who can serve several customers and allocates the various physical and virtual resources dynamically in line with user needs. Either way, this service could be used on demand, even on a self-serve basis. It could be accessed through the internet or a private network and it has the feature of fast reaction to changing capacity needs” (See in [29]).

Federal Office for Information Security (Germany)

“Cloud is understood as offering, using, and billing IT services dynamically adapted to the requirements via a network. These services are only offered and used by means of defined technical interfaces and logs. The range of the services offered within the cloud-computing framework covers the entire spectrum of information technology. Among other things, it includes infrastructure (e.g. computing power, storage space), platforms, and software; still, service could be obtained from public, private or hybrid cloud” (See in [30]).

In general, infrastructures, platforms, or services, which run on a distributed network using virtual resources and accessed by several internet protocols and network standards, are identified as Cloud-Computing (See in [31]).

Two main concepts of the Cloud that manage similar services, applications, and technology on the internet with the functionality of a self-service utility are clarified as follows:

- Virtualization: Systems are virtualized by pooling and sharing resources in cloud computing. Centralized infrastructure can provide systems and storage. The assessment of costs is on a metered basis, scaling resources by agility, and enabling a multi-tenancy concept.
- Abstraction: Applications run on physical systems that are not specified. Administration of systems is outsourced to others and access by users is ubiquitous. Cloud computing specifies the details of system implementation from users and developers, and the data stored in locations that are unidentified (See in [32]).

The main service models in cloud computing based on the definition of the National Institute of Standards and Technology (NIST) are as follows:

- Infrastructure as a Service (IaaS): the service provider offers virtual hardware and the user installs and operates all software on it.
- Platform as a Service (PaaS): the service provider offers virtual hardware and platform software (usually an operating system, database software, and web server), while the users install and operates their own business applications.
- Software as a Service (SaaS): the service provider offers a business solution operating on the virtual hardware and platform software. This is configured and partly operated by the user (e.g. user access management) (See in [33-35]).

The following figure shows the service models of cloud computing:

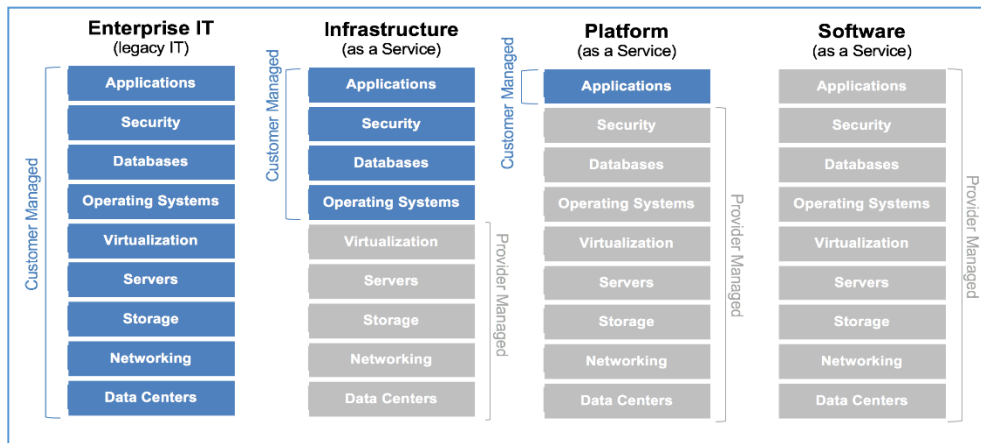


Figure 2: Cloud Computing Service Models (Cloud Computing) (See in [35]). Source: prepared by the author.

To explain Figure 2 simply, an analogy can be drawn to driving your own vehicle (Enterprise IT “legacy IT”), versus a rented vehicle (IaaS), versus riding a taxicab (PaaS), versus riding a bus (SaaS). The responsibility of

driving your own vehicle is all-inclusive, meaning the driver retains the duties of fueling, maintenance, driving, and decisions of desired destinations, etc. While driving a rented vehicle, the responsibility of repairing of said vehicle will not fall on the renter, but on the rental agency; the only duty of the renter is to keep an ample amount of fuel in the tank in order to reach any destination in mind. The same idea applies in “IaaS” model, the only requirement would be some configuration of system settings, maintenance of software, etc., and it would be able to be managed easily.

However, in the “PaaS” model, the analogy would slightly change, as if using a taxicab service. The choice of exact destination and direction remains applicable, however the decisions of the route, fuel management, and all other mechanical details are left to the driver of the taxicab. The same idea applies in the “PaaS” model since the customer will only be responsible of the application level in the cloud infrastructure and the rest will be managed by the service provider.

Regarding the “SaaS” model, the customer is not responsible for anything except for choosing directions and the rest will be completely managed by the service provider. As when choosing a bus for commuting to a destination in mind, the choice of which bus route and area of destination is the only decision needed by the commuter, while all the rest is left to the bus driver and predestined route he proceeds to take.

Whichever option willing to be used, special requirements for the outsourced options always apply to different kinds of institutions and determined separately by the function’s type (See in [36-37]).

Specific terms, with respect to outsourcing, are defined in regulations as follows:

- Critical or important – an operational function is being defined as critical or important if it has failures or defects in its performance resulting in weakening its compliance with obligations, regulations and terms either under its own authorization or any other regulatory systems, whether it affects the firm’s financial performance, or the continuity of the firm’s relevant services and activities (Senior Management Arrangements, Systems and Controls (SYSC 8.1.4R))
- Material outsourcing – defined as outsourcing of important services in which any fault or deficiency of such service can cause doubts of the firm’s continuing satisfaction of the threshold conditions or compliance with the Principles for Businesses (PRIN)
- Important operational functions – under the Electronic Money Regulations and the Payment Services Regulations, an operational function is important if a defect or failure in its performance would materially impair:
 - The authorized institution’s compliance with the regulations and any requirement of its authorization
 - The authorized institution’s financial performance
 - The authorized institution’s soundness or continuity (See in [38]).

Using Cloud computing may provide more flexibility to the services that any firm might receive, allowing for more innovation, and bringing more benefits to the firms, their customers, and the market. However, it can create new risks affecting the firm’s data security or control level as well as a slighter control for customers using the cloud over their providers; those new

identified risks need to be well recognized, observed and alleviated (See in [39]).

In other words, it is the institution's responsibility to identify the risks in all phases of the cloud service lifecycle and to implement proportionate protection measures. Others see that the cloud provider is responsible for the design, description, implementation and effective operations of organizational and operational measures (controls) with which the requirements are implemented at the cloud provider (See in [40]).

On the other hand, Georg assured that "Cloud Computing services exceeded the territorial borders. Providers nowadays are offering their services worldwide where they can target a larger market through global intermediaries and external subcontractors." Therefore, Georg concentrated on the contracting practices and conditions regarding cloud computing based on the EU private international law rules. He clarified that such international laws are protecting consumers taking into consideration the jurisdictional point of view and other applicable clauses of law, assuring that access to the EU courts for consumers would ensure the mandatory provisions enforcement of EU international or other national law (See in [41]). Cloud computing new standards and regulations have been raised at an extremely crucial period when companies needed solutions to reduce the load of administration and cost of operations. Such standards were published by IEC and ISO in 2014 (ISO/IEC 27018) entitled "Information technology (Security techniques) Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors". These standards were published in order to help Cloud service providers to meet the terms of their contracts' legal aspects when they process their own personal data, by acting as data

processor, creating cloud control mechanisms and other controls for clients (See in [42]).

In addition, the communication ‘Unleashing the potential of Cloud Computing in Europe’ was released in 2012 by the European commission to accelerate cloud growth throughout Europe. BZ examines eight countries in Europe and compares how they use cloud computing in E-Government. The results of the study showed a clarification that deployment of a cloud-computing model is also known as G-Cloud (Governmental Cloud), a community or private cloud particularly designed for the use of national government. However, no favored cloud service model has emerged; hence, all the standard models of cloud service like “Platform”, “Software”, and “Infrastructure” as a Service became adopted by most countries. Also, cloud computing had been anchored in half of the tested European countries in one of their national strategies of ICT (See in [43]).

2.3 IT Operational Risk

A few researchers have brought up that the scholastic writing on operational risks in the financial sector is commonly conflicting and sometimes seems as if it is open to interpretation. A few authors of the late 90's measured Operational Risk as the remainder that is not taken into consideration by credit or market Risk. In any case, this methodology was needlessly widespread and not precise enough (See in [44]).

During the recession of 2008, Operational Risk resulted in economic shocks, while presently, the most newsworthy Operational Risk involved large data breaches triggered by external attacks. In both examples, it appears that a series of process failures occurred compounding the risk such that what

appears to be an external event was actually a product of many poor or failed internal processes, meaning one risk can lead to another. That phenomena, although troublesome to the business, is a form of contagion, and requires an approach to ensure containment. Most susceptible to contagion are operations that affect customers. New regulation, the importance of consumer support, and the increased responsibility of governments in the financial sector have led to limitless lawsuits, large fines, and a new climate for reputational danger to financial firms. These new risks do not come from market/credit exposure directly, but rather occur from the way that firms adopt business and tighten customers' options (See in [45]).

Operational Risk does not involve a direct capital deployment with the opportunity of an investment gain. Losses from Operational Risk are not due to bad loans or holding volatile assets. The risk occurs because something undesirable resulted in an expense, fine, judgment, or other loss to the firm. Furthermore, there is no market/counterparty in Operational Risk, the loss cannot be renegotiated, and the payment cannot be prolonged. In fact, Operational Risks are often detected long after issues emerge and such issues are frequently intertwined and correlated, meaning that one form of Operational Risk increases the exposure of more risk (See in [46]).

Operational Risk is, at its core, a mistake/error, and a hazard. It is unfortunate that it has been embedded in how the enterprise functions and are often driven by people and IT systems that produce errors. Operational Risk is not strictly the product of an internal decision process, rather it is manifested through the complex web of employees, products, clients, systems, legal judgments, regulation, and fines (See in [47]).

Operational Risk is never really anticipated but firms must be prepared for it as part of an Enterprise Risk Management Strategy. Perhaps the most challenging feature of Operational Risk is that it is not necessarily easy to identify once it has happened. Decisions that involve the implicit acceptance of Operational Risk may not clearly expose the Operational Risk involved. Lastly, the most important reason when focusing on Operational Risk is that it remains costly to the enterprise, by directly affecting profitability and needed capital (See in [48]).

The term 'Operational Risk' is characterized as "the risk or hazard results from insufficient or unsuccessful inner process/procedures, individuals, and systems or from outside events. This definition covers legal risk but does not include reputational and strategic risk". At this point, it is imperative to notice that Operational Risks have three measurements: the reason/cause, the event/occurrence/incident, and the impact/ consequence/result. The Basel Committee of Banking Supervision categorizes Operational Risk depending on the incident impact and scope. However, the IT Operational Risk definition from Basel II does not mention strategic risks, which is considered inaccurate presently (See in [49]).

So far, little consideration has been given to the Data Innovation section in Operational Risks, which is mentioned in every event type in Basel II within the sections related to the IT Operational Risk. "Information related to IT Operational Risk is any risk affecting the privacy of information resources, which can result in the exposure, mistaken use/abuse, or damage of these assets. Also, the roles related to the Information technology Operational Risk are to mitigate any risk caused by accessibility/availability or to the reliability of practical IT assets" (See in [50]).

However, it is valid to accept risks in case such risks are included within the Risk Appetite Framework, keeping into consideration that Risk Management is all about finding a way to solve problems, which indeed reduces the impact and probability of risk occurrence to an acceptable level of the business aspect. Moreover, most of the listed risks accepted within the Risk Appetite Framework for any organization might be considered as the cost of doing business. Usually, small and medium enterprises prefer to utilize the “Threat-Based Approach” to secure their internal environment as much as possible since they cannot afford huge losses caused by risks. That is why Acceptable Risk Appetite Framework in SME’s is always smaller than the ones in the large institution. Such a methodology has two principal issues, as follows:

- Nearsighted: Centering on only a subset of the total amount of risks related to the portfolio - for those with innovation fixes
- Slowly and Receptive: Resulting in an expansion of device, tools, and services; each one is involved in a specific problem; with no essential cantered supervision, any IT team looking over the duties and working irresponsibly (See in [51]).

IT faces major clashes in Operational Risk, specified in the usual IT concerns ranging from different tool or hardware breakdowns through network worms and viruses to issues that are more familiar, for example, rejection of service attacks, as well as interruption efforts trying to gain access to the wireless network from outside the premises.

A large number of solutions for such issues would rely on technology, for instance implementing a standard assuring that moveable devices run solid firewalls and systems specialized with an antivirus tool become effectively

used. Such basic policies should remain ready to be utilized. Another standard could assure the existence of an obligation to forbid employees from installing their own uncontrolled and usually unprotected Wi-Fi nodes inside the work environment (See in [52]).

Some kinds of threats are harder to be controlled on the basis that technology cannot give any possible solutions. Solid policies and decent management are a key factor in decreasing the number and impact of these risks. Managerial staff should be well prepared to gain numerous management skills, on account of the assumption that any respectable employee is able to become a decent supervisor to become a manager is a typical mistake (See in [53]).

On the other hand, IT activities incorporate the establishment's capacity to process and store data in an opportune, solid, and secure way. IT tasks (commonly housed in a PC server farms with client associations through terminals) have turned out to be unique and may incorporate dispersed conditions, coordinated applications, media communications foundation, internet network, and a variety of PC working stages. More so, as the multifaceted nature of innovation develops, numerous establishments have expanded their dependence on merchants, collaborators, and other outsiders for an assortment of arrangements and services (See in [54]).

More to that point, regardless of whether Information systems are distributed, centralized internally, or externally outsourced, they are considered interdependent and interconnected. Management's ability of understanding and comprehending all of the risks is required in order to appropriately execute and deploy the strategic plan of the board, additional to the internal policies of the IT in any section. Any activity in the IT department

can generate many risks for all of the IT operational elements, therefore, the board must guarantee that higher-level management organize IT controls throughout the organization's working environment, involving any third-party arrangement and any external function usually outsourced. However, IT operational management should execute a hierarchical structure built by the HR, where proper, various working destinations exist for supporting the organization's business activities and exercises. The activities belonging to IT, whether centralized or decentralized, should always support functional operations, services, and products. Facilitating singular business units by MIS needs is one of the management roles. On the other hand, the responsibility of any Operational Risk Management concludes in data capturing, transaction processing, end user information process requirement, and data classification (See in [55]).

Similarly, powerful IT Management requires information and comprehension of the organization's IT condition. The documentation should be proper enough to indicate the way the system supports the related business processes and procedures. By utilizing technology assets of inventory, the higher-level management should perceive interdependencies of these tools and should be very aware of their relevance to the related business activities (See in [56]).

Additionally, management should be aware of data flow between and across all of the related systems. Any kind of documentation based on the data flow, in addition to infrastructure, will simplify choosing the optimal application of control and facilitate maintenance/support of information systems and assist in the risk identification process.

The management of any organization should take into consideration the security, infrastructure, and international standards in case any products or services are provided from an outside third party or external vendor (See in [57]).

The staff in the IT department also should have significant knowledge in the programs related to information security. In addition, in any organization, the IT team and the Information security team must protect the related processed and stored information. The management of the operations related to the IT should have secure controls classified as corrective, preventive, and detective controls. Access controls, incident response, and logs should be included in all respective logical control. However, in case it is needed, in order to recover all operations a general detailed Business Continuity Plan (BCP) should be existed addressing all the ordinary as well as extraordinary interruptions and disasters (See in [58]).

Pursuant to that, in order to obtain protected and maintained IT related systems, facilities, data, and media should implement an Information Security Management (ISM) tool, which should include any privacy programs related to the institution. This a requirement for the sake of protecting any identifiable personal data, remaining aware of the institution complexities. Yet, the main goal of the ISM is to enable the organization in order to meet all of the business goals easily by clarifying all of its related risks, as well as offering solutions. By this, we can assure mitigation of risks through obtaining several security objectives like availability, integrity of data or systems, confidentiality of data or systems, accountability, and assurance in order to achieve our security objective to measure, monitor, and identify all control security risks (See in [59]).

In the banking and financial services industry, the Basel Accords define Operational Risk as that risk coming from “inadequate or failed internal processes, people and systems, or from external events”. In order to permit a more comprehensive coverage of banking risks, as well as more risk-sensitivity, Basel II framework was initially published in 2004 intending to amend international banking that had controlled the amount of allocation (reserve) banks were required to hold in order to guard against the financial and operational risks they face. Three balancing and mutually reinforcing “pillars” are included; the first one consists of the basic minimum allocation requirements, the second one introduces the principle of a structured dialogue between banking institutions and supervisors and the last one focuses on transparency and market discipline.

Minimum requirements for allocation are set in “Pillar 1”. Its goal is to ensure that banks hold enough allocation to provide a minimum level of coverage for their credit risk, market risk, and operational risk.

“Pillar 2” set up a process of prudential supervision in order to strengthen and compliment the first pillar. It consists of the banks’ analysis of all of predicted risks, including those already covered by Pillar 1.

“Pillar 3” concentrates on market discipline, focusing on improving the transparency of the bank’s financial records by requiring disclosure of information needed by outside parties in order to form an accurate and comprehensive view of their capital/allocation adequacy (See in [60]).

In many ways, Operational Risk is driven by the firm’s operations, not the firm’s investments, or other deliberate deployments of capital/allocation to seek a profit. In many ways, that is true. This process is not separable from

the act of doing business, as it is also embedded in other activities undertaken by the enterprise. Operational Risk can also lead to additional regulatory and reputational harm, meaning that Operational Risk shows the dangerous feature of contagion, giving rise to new/additional risks. This is especially true when the Operational Risk in question is left unattended by management (See in [61]).

2.4 Control Objectives for information and related technology, (COBIT)

In 2012, COSO's internal COBIT 5 was released and a few years later, we witnessed initial eagerness only from a few associations. After much reluctance, moving forward from COBIT 4.1 to COBIT 5 was finally seen as the better move (See in [62]). The consideration remains in a general sense on IT procedures and impressively less on the more current features, for example, the standards, empowering agents, etc. Moreover, despite the way that few COBIT 5 and related productions are as of now accessible and can easily be distributed, the current reception rate in associations appears to be moving gradually, in any event all around the world (See in [63]).

This recent adaptation of this framework was released presenting essential highlights. One of those highlights is the advancement from COBIT 4.1 Maturity Model to COBIT 5 Process Capability Model. Therefore, after quite a long while of relative silence around COBIT, COBIT 5 was released, with a conveyance subtitled "A Business Framework for the governance and management of enterprise IT" (See in [64]). As of late, COBIT 5 demonstrates a basic essential extension development from the management of IT (v3) by methods of the governance of IT (v4/4.1) to a business framework for the large IT Institutions (See in [65]). ISACA claims that

COBIT 5 is an extensive framework for the entire affiliation and has, furthermore, joined and combined Val IT and Risk IT into COBIT5. De Haes and Van Greenberger clarify that “the enterprise IT Governance is a fundamental piece of corporate Governance, which contributes to the definition and utilization of procedures, social frameworks, and structure. Such a process should be done in association to enable both business and IT staff to fulfill their responsibilities and help the business/IT course of action (See in [66]). COBIT 5, the advanced equivalent of COBIT 4.1, offers a mapping apparatus that is easy to be implemented in order to map the strategic objectives of the association toward the related IT goals in order to accomplish the required model of governance (See in [67]).

Either way, finding out the major procedures and systems related to the administration overhauling, existing utilization of the COBIT 4.1 process will require minor changes, for example, joining existing methods and moving practices between various structures and forms (See in [68]).

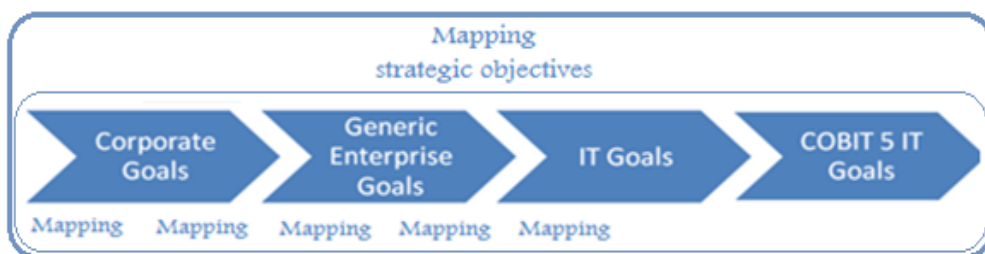


Figure3: Mapping objectives to IT Related Objectives
Source: prepared by the author

At any rate, the depiction in COBIT 5 also helps the usage from an operational perspective; COBIT 5 has extended the number of processes from 32 to 37 and has made a capability between 5 governance structures and 32 management execution forms.

The procedures have been changed and modified, while new processes have been introduced as well. The operational procedures (APO, BAI and DSS) are connected to the governance forms (EDM), additional to the control form of (MEA), underlining the arrangement among governance and administration here as well. Furthermore, the framework provides suggested metrics per process linking enterprise goals with IT related goals in order to be able to measure the performance of a process (See in [69]). Recently, ISACA did not change its correspondence outline by using the fundamental abbreviation of COBIT lately, yet the remarkable component of 'Control goals' has also gone, at any rate in given name and usual shape. Instead of that, COBIT 5 uses the term management practice (See in [70]). This is just to inform the outside world that another era has come, and the earlier period has been outdone! Despite the way that in COBIT 5, the methodology of clarifying the procedures specifically in details instead of presenting general processes, the IT frames material has been kept clear. The mix of the management practices with related activities can be used perfectly to derive the control goals and other necessary controls to fulfill the IT auditor requirements (See in [71]).

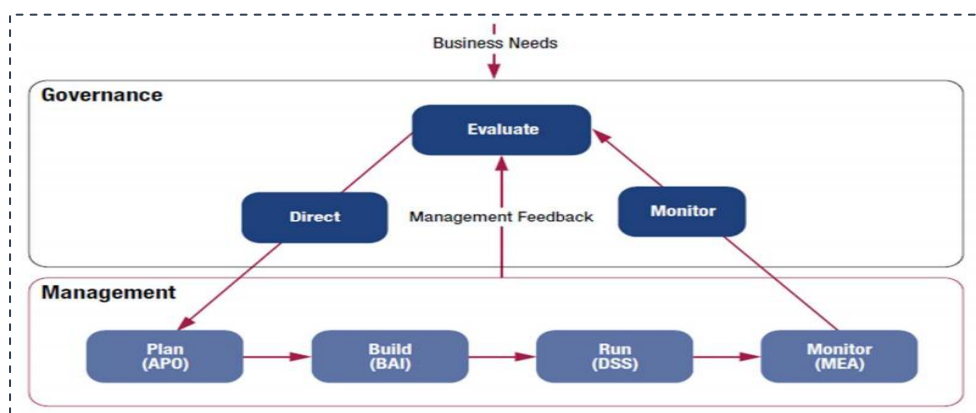


Figure 4: COBIT 5 Governance and Management Key Areas (COBIT 5) (See in [44]). Source: ISACA articles

However, the 5 main process domains are divided into one governance domain, additional to four management domains as shown in Figure 4; each domain consists of several numbers of processes, which allow it to achieve the main required objective(s). The governance of enterprise IT (EDM) domain contains five processes within each process presenting the “Evaluate, Direct, and Monitor” practices. The management of enterprise IT domains are in line with the responsibility areas of Plan, Build, Run, and Monitor (See in [72]). The 37 processes in the below Process-Domains are divided as the following:

- Align, Plan, and Organize (APO): thirteen processes
- Build, Acquire, and Implement (BAI): ten processes
- Deliver, Service, and Support (DSS): six processes
- Monitor, Evaluate, and Assess (MEA): three processes
- Evaluate, Direct, and Monitor (EDM): five processes (See in [73]).

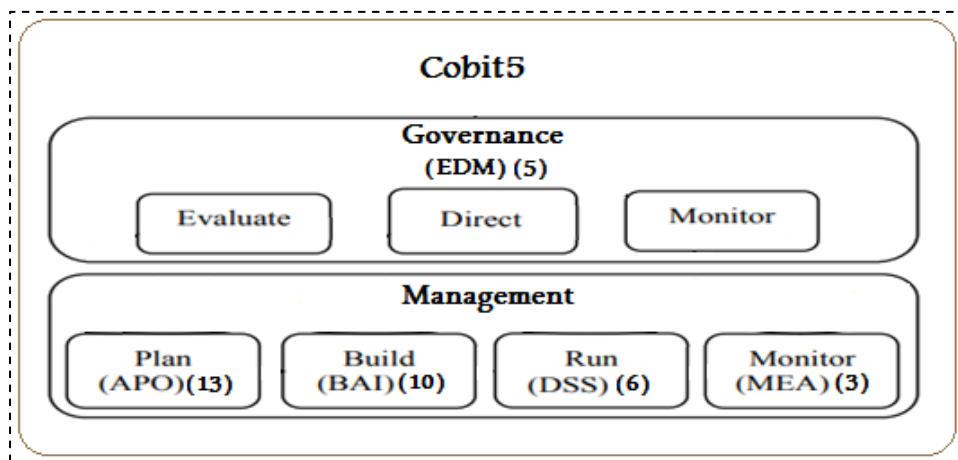


Figure 5: The five main processes in COBIT 5 Framework (COBIT 5)
Source: prepared by the author.

COBIT 5 is based on five main key principles designed for the governance and management of enterprise information technology. The following section

gives a semi-detailed overview of those five main key principles used in this framework: (See in [74]).

Principle 1: Meeting Stakeholder Needs

Enterprises exist to generate additional value for their partners (Stakeholders); therefore, the main governance objective for any institution is the value in creation to realize benefits at the best possible resource cost while reducing the risk.

Principle 2: Covering the Enterprise End-to-End

COBIT 5 combines the IT enterprise's governance into the general enterprise governance; therefore, it covers the whole organization, rather than just focusing on the IT role. Also, by using the basics effectively to integrate other international standards, frameworks and practices are capable to cover the whole enterprise end to end for all matters related to IT role.

Principle 3: Applying a Single Integrated Framework

Most of the best practices and international standards related to the IT are only concerned in IT roles and practices. On the contrary, COBIT is highly concerned in other related international frameworks and standards that make it a comprehensive framework related to the roles of management and governance of enterprise IT.

Principle 4: Enabling a Holistic Approach

Valuable management and governance which is effective for enterprise IT always require a comprehensive general approach to the IT domain. COBIT 5 uses enablers for that purpose to assure a comprehensive management and governance implementation of enterprise IT. Such enablers are considered as

a base that enables the institution to achieve its main goals and objectives.

Seven main categories of enablers are defined into COBIT 5 framework:

1. Principles, Policies, and Frameworks
2. Processes
3. Organizational Structures
4. Culture, Ethics, and Behavior
5. Information
6. Services, Infrastructure, and Applications
7. People, Skills, and Competencies

Principle 5: Separating Governance from Management

COBIT 5 framework clarifies specifically the differences between management practices and governance practices. These two domains essentially serve a different purpose; each one of them consists of different several types of behaviors, activities and requires different structuring in the organization.

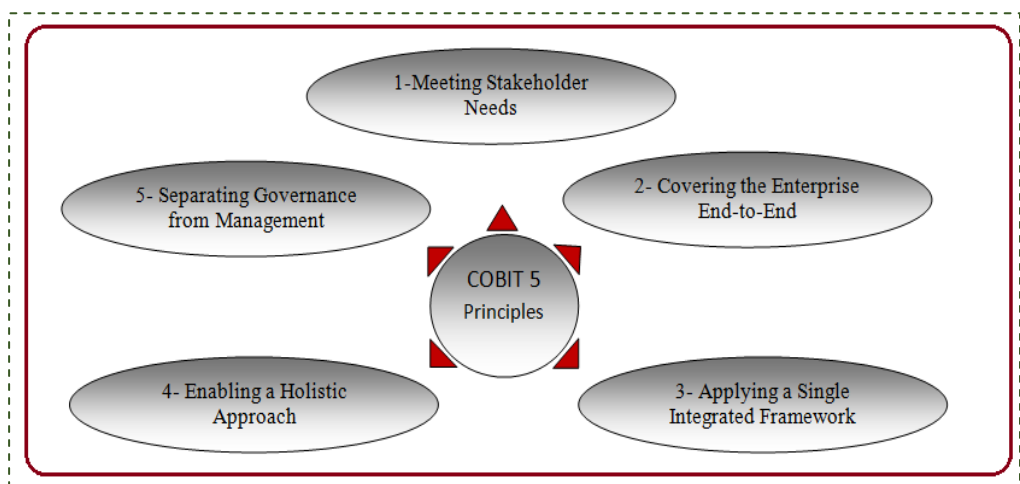


Figure 6: The 5 main Principles in COBIT 5 Framework (See in [105]).

Source: prepared by the author.

Therefore, governance process assures reaching all of the stakeholders' needs through the following:

- It assures that options and conditions are evaluated in order to achieve agreed and balanced institutional goals and objectives.
- It sets specified directions and instructions through prioritization and decision-making methods.
- It monitors the compliance and performance of the agreed instructions, directions, and goals (See in [75]).

On the other hand, the management processes are concerned in Planning, Building, Running, And Monitoring practices, and activities aligned with the instruction set by the governance body mentioned previously to achieve the general enterprise goals and objectives (PBRM) (See in [76]).

As discussed previously, the latest version of COBIT 5 has been built based on previous versions of the COBIT framework. IT has expanded on past variants of COBIT, Val IT, and Risk IT methods. Nevertheless, when executing COBIT 5, the association must figure out which partner interests have priority, what their desires are, what the IT capacities & capability to fulfill these desires are, and who is responsible for doing as such (See in [77]). The majority of the above-mentioned versions would require some additional knowledge regarding the basic processes and management systems that support the IT main functions and procedures in order to deliver the services and performance as expected. Keeping into consideration that in most of the cases, upgrading the existing COBIT version to a newer one might require major adjustments and a long procedure, since that might need both existing processes and moving practices between them or even adding new ones (See in [78]).

2.4.1. COBIT 5 Processes Descriptions

Simply, implementing COBIT 5 framework would require linking the 37 processes among the related departments inside any institution. The connections between the processes and the departments should be classified based on the description and purpose of each process. Processes should be linked to the department/departments based on its internal roles of work, policies, and procedures inside the institution.

Therefore, the below descriptions of the processes are based on the Pam book of the COBIT 5 framework, combined with my own experience in that field and reaffirmed by other trustworthy experts.

APO (13 Processes)

APO01: Manage the IT Management Framework

Process Owner: Information Technology Department

Process Description: In this process, the mission and vision of the enterprise should be maintained effectively and clarified simply. In addition, implementing and maintaining the mechanisms and authorities are important in order to be capable of managing the information as well as managing the IT usage in any enterprise to support the objectives of governance according to the internally agreed upon policies and procedures.

APO02: Manage Strategy

Process Owner: Information Technology Department

Process Description: This process should give a comprehensive overview of the present status of business and IT environments, required future instructions/directions, as well as required initiatives to move to the preferred future environment. The demanded reliable and effective responses might need powerful influenced institutional architecture, buildings, blocks, and

components with outsourced services and correlated capabilities in order to achieve the required strategic goals.

APO03: Manage Enterprise Architecture

Process Owner: Project Management Department

Process Description: A gathered set of business processes, applications, data, information, and layers of technological architecture would guide the establishment of an ordinary architecture for an organization. This may lead to the realization of both IT and general strategies, through generating some practices and key models to describe targeted strategies and specified baselines. On the other hand, this process is involved in specifying necessary demands for scientific classification, rules, procedures, guidelines, tools, and forms as well as providing strong logical relations between these components, while helping to increase agility, improve alignment and quality of information, with the addition of cutting cost through some useful methods such as building component re-usage.

APO04: Manage Innovation

Process Owner: Human Resources Department

Process Description: This process involves preserving a consciousness condition regarding the IT and other related service trends, also classifying modernized opportunities, as well as planning to get useful outputs from the innovation process aligned with the business needs. It also can improve the business using the existing tools and systems, services, or by using the enabled business innovation related to IT.

APO05: Manage Portfolio

Process Owner: Project Management Department

Process Description: Implementation of the strategic direction set for necessary investment, in accordance with the institutional architectural

vision, is used in addition to the required characteristics related to the value of investment and other correlated groups of services, while still considering several of investments, resources, and financial constraints. On the other hand, this process is involved in prioritizing and balancing all services and programs after the evaluation process is done. Additionally, constraints of funding and resources should be managed based on the strategic goals and Risk Appetite. Finally, performance monitoring is used for the whole portfolio of systems, programs, and services proposing necessary adjustments in service performance, and the priority of enterprise changing.

APO06: Manage Budget and Costs

Process Owner: Financial Department

Process Description: Implementing this process will affect the following:

- Manage IT related financial activities in the IT and business functions
- Manage covering cost
- Manage budget and the benefits of management. - Manage prioritized spending
- Manage reasonable system for allocating enterprise cost.
- Consult with related parties to recognize classify and control the expenses and revenues according to IT strategic plans

APO07: Manage Human Resources

Process Owner: Human resource Department

Process Description: A well-prepared approach should be provided in order to ensure best structuring, decisions, and human resources skills, keeping into consideration the importance of communicating responsibilities and roles as well as plans of growth defining the expected performance for measurement matters related to the motivated people.

APO08: Manage Relationships

Process Owner: Information Technology Department

Process Description: A formalized and transparent relationship between the IT and the business should be well managed in order to achieve goals agreed upon and aligned with the general strategic goals of the whole enterprise, according to the budget constraints and the Risk Appetite. Ownership and accountability for some key decisions should be taken according to the appropriate terms and procedures.

APO09: Manage Service Agreements

Process Owner: Information Technology Department

Process Description: This process is concerned with the service level agreement between the IT division and the related departments in the enterprise which takes into consideration the related department expectations and ensures the design, identification, publishing, and monitoring of all the services and performance indicators related to IT functions.

APO10: Manage Suppliers

Process Owner: Administration Department

Process Description: This process attends to the relationship between the enterprise and the external service provider. All of the outsourced provided services related to IT should meet the exact institution requirements, keeping into consideration the importance of managing the contracts and the relationship, as well as monitoring and reviewing the performance of suppliers to ensure their compliance with the points agreed upon in accordance with the contracts.

APO11: Manage Quality

Process Owner: Information Technology Department

Process Description: This process attends to the defined requirements of the quality of the process and the knowledge of communication, including all of the related procedures and enterprise outcomes, in addition to monitoring and controlling processes as well as any other related practices and processes, which ensure efficiency efforts and continuous improvements.

APO12: Manage Risk

Process Owner: Risk Department

Process Description: The process to conduct a survey often and mitigate IT-related risk within the acceptable level of Risk Appetite set by the executive level of management.

APO13: Manage Security

Process Owner: Information Security Department

Process Description: A system for managing the information security should be specified, activated to operate, and finally, be monitored.

BAI (10 Processes)**BAI01: Manage Programs and Projects**

Process Owner: Project Management Department

Process Description: This process clarifies that the project management department should be responsible for managing all types of projects and programs in the institution aligned with the general strategic goals. In addition, this process involves initiation, planning, controlling, executing, and closing all kinds of projects, especially the ones related to IT.

BAI02: Manage Requirements Definition

Process Owner: Information Technology Department

Process Description: This process attends to specifying and analyzing the requirements of any solution before getting involved in it. This step is taken in order to ensure its alignment with the general strategic enterprise requirements related to the defined information, application, infrastructure, and business processes, keeping into consideration that the financial overview is drawn according to the costs, benefits, and required approvals, while working around solutions and related risk analysis.

BAI03: Manage Solutions Identification and Build

Process Owner: Information Technology Department

Process Description: This process will build up and keep up distinguished solutions in accordance with the general enterprise requirements, keeping into consideration the roles of design and development as well as procurement process related to suppliers and vendors. On the other hand, managing configuration, managing testing, managing maintenance of business processes, data, and services are all essential and vital.

BAI04: Manage Availability and Capacity

Process Owner: Information Technology Department

Process Description: This process is concerned with balancing the “as is” and “to be” requirements related to the capacity, availability, and performance considering the cost-cutting. Such a process should include a detailed current situation analysis with a specified future forecasting based on the business requirements, impact, and pre-defined risks in order to ensure a logical plan of action to meet the exact needs.

BAI05: Manage Organizational Change Enablement

Process Owner: Project Management Department

Process Description: This process is involved with the successful implementation of wide organizational quick-change, while mitigating risk through the whole life cycle of any change process defining the exact affected parties related to IT and business.

BAI06: Manage Changes

Process Owner: Information Technology Department

Process Description: This process attends to any kind of change required from the business side on the IT systems. Such a process should include standards and procedures that control the whole change process including prioritization, impact assessment, authorization, reporting, tracking, documentation, and closure processes.

BAI07: Manage Change Acceptance and Transitioning

Process Owner: Information Technology Department

Process Description: In this process, arrangements and acceptance for new solutions should take place, keeping into consideration the importance of planning, data conversion, test acceptance, preparing releases, good communication, post implementation review, and production support.

BAI08: Manage Knowledge

Process Owner: Human resource Department

Process Description: This process concentrates on the importance of having a valid, reliable, and an up-to-date significant knowledge gained by the employees to ensure supporting the activities of processes and decision-making skills, while keeping into consideration the value of planning for the processes related to identification, maintenance, usage, and retirement of knowledge.

BAI09: Manage Assets

Process Owner: Information Technology Department | Related: Administration department.

Process Description: This process shares the ownership between the IT and the Administration department. The Administration department is responsible for managing all of the IT assets according to their work procedures while assuring the maximum usage needed with the least possible cost. This should be kept in consideration due to the importance of the physical protection for those assets, which are classified as critical in order to support important services considering its availability, capability, and reliability, ensuring that the needed software licenses are valid to the optimal required usage, according to the business needs as clarified clearly in the agreements.

BAI10: Manage Configuration

Process Owner: Information Technology Department

Process Description: This process clarifies the importance of characterizing and maintaining the mature relationships between the capabilities and key resources required to deliver enabled services related to IT, keeping into consideration the processes of baselines establishing information collecting, auditing configuration of information, and finally, updating the needed configuration for storage.

DSS (06 Processes)

DSS01: Manage Operations

Process Owner: Information Technology Department

Process Description: Organizing and implementing all of the policies and procedures related to IT, delivering internal and external services. This should be simultaneously aligned with the old procedures and the whole process should be monitored effectively.

DSS02: Manage Service Requests and Incidents

Process Owner: Information Technology Department

Process Description: This process includes incident solutions in order to concentrate on the efficiency and timely manners of the responding process in case any ticket is recorded on the related IT helpdesk system. On the other hand, such a tool should also handle the record of requests and the knowledge to restore normal service for any kind of additional diagnosis or investigation of the process of escalation and resolving of incidents.

DSS03: Manage Problems

Process Owner: Information Technology Department

Process Description: problems should be identified and classified, showing the root cause of appearances at hand and providing the suitable preventable solutions to require incidents, as well as recommending improvement options where and when needed.

DSS04: Manage Continuity

Process Owner: Risk Department | Related: Information Security Department

Process Description: A plan should be implemented and designed to enable IT and business processes to respond efficiently in case of any disruption and incidents occurring, so as to ensure the continuity of the critical business and IT processes operation and also to maintain the availability of information at an acceptable level based on the enterprise needs.

DSS05: Manage Security Services

Process Owner: Information Technology Department | Related: Information Security Department.

Process Description: This process involves the critical enterprise data protection and maintaining an acceptable level of information security and risk mitigation as per the internal policies related to the security while keeping in consideration the importance of keeping up an efficient security role and

access privileges related to critical information and data additional to the required security monitoring remains.

DSS06: Manage Business Process Controls

Process Owner: Risk Department

Process Description: Appropriate controls related to business should be defined and maintained to ensure that any in-house or external data business processes are relevant and comply with the applicable data control requirements, also managing controls to ensure the satisfaction of these requirements according to the mentioned information processes.

MEA (03 Processes)

MEA01: Monitor, Evaluate and Assess Performance and Conformance

Process Owner: Project Management Department

Process Description: All goals of the business procedures/policies and IT should be validated, gathered and assessed, in addition to the need of monitoring the performance and conformity of agreed upon goals and KPIs, keeping into consideration the importance of prompt reporting.

MEA02: Monitor, Evaluate, and Assess the System of Internal Control

Process Owner: Audit Department | Related: Operational risk department

Process Description: This process focuses on the importance of frequent evaluation and monitoring of environmental controls, including all of the assessment aspects and autonomous assurance reviews. It also focuses on enabling management to verify the deficiencies and inefficiencies related to the controls and to any other essential improvement on actions, while highlighting the importance of planning, organizing, and maintaining

standards needed for the assessment and assurance of the internal activities and controls.

MEA03: Monitor, Evaluate, and Assess Compliance with External Requirements

Process Owner: Compliance Department

Process Description: Ensuring that IT normal process and supported process are compliant with the contractual requirements and laws/rules regulated by authorized parties, such as the Central Bank of Jordan and the MNB, assuring that all of the internal mandates and requirements are well-identified and integrated with the overall enterprise compliance to the CBJ regulations, for instance.

EDM (05 Processes)

EDM01: Ensure Governance Framework Setting and Maintenance

Process Owner: Higher management | Related: General Manager.

Process Description: This process concentrates on the governance of enterprise IT requirements and the way it should be analyzed. It focuses on enabling principles, structures, procedures, responsibilities, and authorization in order to ensure achieving the goals and missions of the enterprise.

EDM02: Ensure Benefits Delivery

Process Owner: Higher management | Related: Project Management department

Process Description: This process is involved in optimizing contribution to business by IT services, assets, and business processes according to acceptable costs and is impacted by the current investments.

EDM03: Ensure Risk Optimization

Process Owner: Higher management | Related: Risk department.

Process Description: This process highlights the importance of understanding the Enterprise Risk tolerance processes and Risk Appetite, in addition to the importance of the communication and the significance/impact of risks related to the identified and managed usage of IT.

EDM04: Ensure Resource Optimization

Process Owner: Higher management | Related: Human Resource department.

Process Description: This process guarantees the capability of availability related to the IT sources such as procedures, resources, and used technologies to efficiently support the achievement of optimal objectives related to the enterprise.

EDM05: Ensure Stakeholder Transparency

Process Owner: Higher management | Related: Information technology department

Process Description: This process attends to the importance of being transparent in the performance and conformance measurement related to IT, to guarantee the approval of stakeholders concerning the corrective actions, agreed goals, and KPIs.

More clarifications can be found in Appendix (A) including Table 1 mapping all of the processes to the descriptions linked to their purposes.

However, at several examination points on the maturity model of the past adaptation of the COBIT structure, it was discovered that the new process capability approaches result in a change of the appraisal procedure, specifically in the formality/meticulousness of the evaluation. With this process capability, it became noteworthy that the reason for the procedures is actualized, creating a superior arrangement with the presently accepted

procedures, for example, ITIL and TOGAF (See in [79]). In COBIT 5, the Maturity Model has changed, allocating significantly more value to the processes. The task of the new process capability model is equivalent to the maturity model, yet the framework structure has differed. In regard to the maturity level, six levels of assessment of a procedure are shown, despite the fact that the name, the importance, and particularly the attributes for evaluating a procedure are not of much significance (See in [80]). Even though the two frameworks might appear similar, there are differences in scope and intent. The difference of intent between levels is linked to the significant focus on the achievement of the IT processes' purposes, and a more formal assessment is brought by the new framework (See in [81]). Moreover, COBIT 5 Process Capability Model contains six dimensions, which is indicated as follows: (See in [82])

Level 0: Incomplete process; the process is not set in place or it cannot achieve its targets/goals. At this level, the process has no goal to be accomplished. Thus, this level has no characteristics.

Level 1: Performed process; the process is set up in place and accomplishes its own reason of being. This level only received "Process Performance" as a process characteristic.

Level 2: Managed process; the process is executed and followed by a sequence of exercises and activities, for example, planning, modifying, and monitoring exercises. The results are set up, controlled, and kept up. This level has "Performance Management" and "Work Product Management" as process characteristics.

Level 3: Established process; the earlier level is now executed followed by a well-defined process that allows the accomplishments of the process outcomes. This level has “Process Definition” and “Process Deployment” as process characteristics.

Level 4: Predictable process; this level executes the processes according to a defined boundary that allows the accomplishments of the process outcomes. This level has “Process Management” and “Process Control” as process characteristics.

Level 5: Optimizing process; this level executes the processes in the way that assure the possibility of accomplishing relevant, current, and projected business goals. This level has “Process Innovation” and “Process Optimization” as process characteristics in order to achieve a given level of capability, this level must be completely accomplished.

Presently, Control Objectives for Information and related Technology (COBIT) has become a standout framework amongst the largest IT Governance (ITG) structures accessible and, furthermore, the most appropriate for audit as it gives exhaustive direction around IT forms and related business objectives (See in [83]).

Additionally, ISACA concentrates on two main important concepts through COBIT 5 Framework; COBIT for assurance and COBIT for risk. Using COBIT 5 for information security brings a number of information security-related capabilities to the enterprise, which can result in a number of enterprise benefits such as: (See in [84])

- Reduced complexity and increased cost-effectiveness due to improved and easier integration of information security standards, good practices and/or sector-specific guidelines, thus increasing user satisfaction with information security arrangements and outcomes
- Improved integration of information security in the enterprise
- Informed risk decisions and risk awareness
- Improved prevention, detection, and recovery
- Reduced impact of information security incidents
- Enhanced support for innovation and competitiveness
- Improved management of costs related to the information security function
- Better understanding of information security

Moreover, Risk Identification, assessment, and evaluation is involved with correctly determining the risk faced by the enterprise and providing recommendations to senior management on how to maintain risk effectively at an acceptable level, including but not limited to:

- Risk Identification, including emerging risk and risk associated with people, processes, technology, architecture, applications, information, natural factors and physical threats
- Assessing the risk levels associated with each threat, including anticipated risk likelihood and impact and the effectiveness of current and planned controls
- Calculating the risk levels using both quantitative and qualitative metrics and determining the impact of risk on the ability of the business to meet its goals and objectives

In recent times, organizations have an increasing number of patterns to automate their operational and hierarchical activities; thus, the speculation of data innovation (IT) keeps on expanding each year. In any case, great governance that can guarantee its arrangement and business procedure and acknowledged benefits from IT ventures has not been greatly affected by this expansion (See in [85]). Accordingly, IT Governance is then required as a reason for the nonstop change of the IT administrations. This examination is restored when delivering an instrument CAT5 in order to quantify the maturity level of IT Governance, hence facilitating the procedure of change within IT administrations. CAT5 depends on COBIT 5 framework and the plan used is the Unified Modeling Language. Through phases of data framework improvement, this examination results in an application for estimating the maturity level of IT Governance that can be utilized in surveying existing IT Governance (See in [86]).

3. METHODOLOGY

This chapter presents the research methodologies used in the four main sections (IT Governance, Cloud-Computing, IT Operational risk, and COBIT 5), through adopting the following: theoretical frameworks, operational definitions for the main variables, objectives, designs, research methods, research population - sample, research duration, data sources, data collection instrument as well as data analysis techniques.

3.1 Conceptual framework

The model in the figure below clarifies the dimensions of COBIT 5 framework affecting the financial performance in the banks sector.

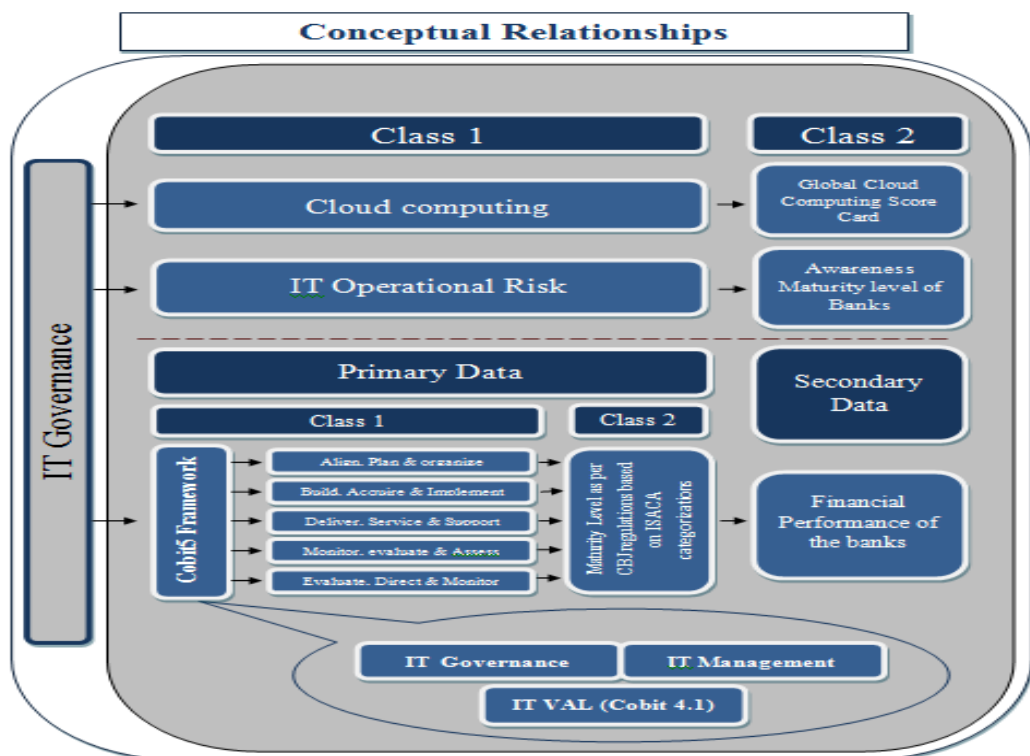


Figure 7: Thesis conceptual relationship.
Source: Prepared by the author.

3.2 Research Topics – Brief Definitions

3.2.1 IT Operational risk

Operational risk is known as the risk of a loss resulting from insufficient or failed inner processes, people, and systems or from external events. With exceptional technological and communications advancements and extent, all companies are facing innately greater operational risks. Such companies are financial services, which are concerned in both information and knowledge intensive, and are critically regulated with customers. Operational risk in financial establishments are classically a combination of a range of different sorts of risk.

It includes IT failure, interior, and external frauds, harms to physical assets, recruitment issues, and so on. It also includes cases that are an outcome of errors in institutional daily work process. Operational environments that require tight controls and maintenance tend to be subject to operational risks and counted as operational losses.

Financial establishments that are issue to operational risks consist of retail banks, commercial banks, investment banks, brokerage firms, asset management companies, and insurance organizations. In this thesis, we discuss the operational risk management troubles within the enterprises listed in the kinds of financial institutions described event types categorized by Basel II.

In the theses, IT operation risks are evaluated from three specific event types; we debate gaps in the previous literature as well as going further than to spotlight recent behaviors in the Jordanian bank institutions, focusing on the IT operational risk capital reserves related to the IT operational risk.

3.2.2 COBIT 5 Framework

The Information Systems Audit and Control Association (ISACA), and the IT Governance Institute (ITGI) created COBIT in early nineties. The first edition of COBIT concerning “Audit” was published in 1996; the second edition concerning “Controls” in 1998; the third edition concerning “Management” in 2000, and the on-line edition became available in 2003. The fourth edition of COBIT concerning IT Governance was issued in December 2005/7 (See in [87]). Finally, the fifth edition of COBIT concerning Governance and management of enterprise IT was issued in 2012; COBIT 5 integrates of all previous ISACA IT governance materials in COBIT 4, VAL IT, and RISKIT, concentrating on five core principles: (See in [88])

- 1) Meeting stakeholder needs
- 2) Covering the enterprise end-to-end
- 3) Applying a single, integrated framework
- 4) Enabling a holistic approach
- 5) Separating governance from management (ISACA 2007, 2009c, 2010)

COBIT 5 identifies “37” processes spread over governance and management domains. The five governance processes are the board’s responsibilities, covering the setting of the governance framework, responsibilities in terms of value, risks, and resources and providing transparency regarding IT to the stakeholders (See in [89]).

3.2.3 IT Governance

Weill and Ross argued, “Effective IT governance is the single most important predictor of the value an organization generates from IT”.

Therefore, IT governance is defined as the practice that helps in all IT investment decisions by establishing the accountability framework and allocating decision rights.

IT Governance was described as a solution to weak IT performance by some studies in the field, Also It is well known as a performance-strengthening tool, which creates a control environment over business challenges and complexity of technology. Other research found out that IT Governance adoption helps to improve organizational accountability, as well as increasing the “ROI” return on investments for any institutions (See in [26]).

3.2.3.1 Val IT Framework

Val IT was launched in March 2006 via ITGI. Second version of it -Val IT2.0- was launched in 2008 (See in [90]). Val IT is identified as the first inclusive framework to aid enterprise from the point of view of IT governance, with an emphasis on value. So, enabling firms to control their investments in IT-enabled changes such that they secure optimal value from IT-enabled business investments at a reasonable cost with an appropriate level of risk, can be viewed as Val IT’s typical goal.

The Val IT model is primarily based on three domains: Value Governance, Portfolio Management, and investment Management. The major focal point of Val IT domains is on delivering enterprise Value, through:

- Managing the typical funding portfolio to optimize value to the business enterprise (PM)

- Establishing governance strategy, the portfolio of IT- enabled investment packages that execute the strategy, and the portfolios of resulting IT services, property and different sources (VG)
- Managing the effects of individual investments programs, including business, process, people, technology, and organizational exchange enabled by using the enterprise and IT projects that create the need of the programs (IM) (See in [91]).

These three domains consist of 22 processes and 69 key management practices. Enterprise governance of IT highlights on the need for dynamic partnership between IT and business. Same as IT should be responsible for delivering the required technical ability. Likewise, business should be accountable for locating what technology abilities ought to be exchanged and for value transmission from those adjustments and abilities as well. To actualize that, COBIT framework that focuses on IT- related responsibilities, and Val IT framework that focuses on business- related obligation can be abridged.

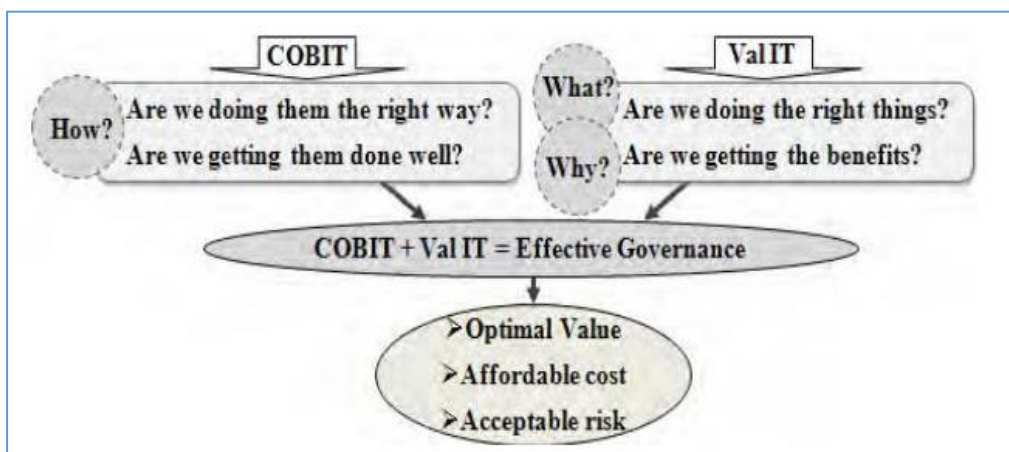


Figure 8: Effective governance through simultaneous use of COBIT and Val IT
Source: prepared by the author

3.2.3.2 Information Technology Management

The central objective of IT management is to generate value via the use of technology. To attain this, enterprise strategies and technology should be linked. IT management is distinct from management techniques tied to the automation or aid of human decision-making (See in [92]). IT management refers to IT related to management activities in any organization. MIS is concentrated ordinarily on the business phase, with strong input into the technology section of the business/organization. A fundamental center of attention of IT management is the value induction made feasible by technology (See in [93]). This requires the alignment of technology and business strategies while the value creation for an organization includes a community of relationships between inner and external environments, technology shows a necessary role in improving the inclusive value chain of an organization.

Yet, this augmentation requires enterprise and tech. management to work as an inventive, collaborative group rather of an only mechanistic length of control (See in [94]). Historically, one set of sources used to be dedicated to one precise computing technology, enterprise application, or line of business, and managed in a similar fashion. These resources supported a single set of necessities and processes and could not effortlessly be optimized or reconfigured to actual assist demand (See in [95]).

This directed technology carrier to construct out and accompaniment their product-centric infrastructure and management choices with United Infrastructure environments that link servers, storage, networking, security, management, and facilities (See in [96]).

The abilities of having this type of built-in and automated management surroundings and environment permit organizations to get

their applications up and running faster, with effortless manageability and maintenance, and allows IT to alter IT resources (such as servers, storage and networking) more rapidly to meet unforeseen enterprise demand (See in [97]).

3.2.4 Cloud Computing

Cloud computing recently developed computing technology that operates virtualization resources to deliver IT services through on-demand approach and the Internet technology (See in [98]).

Marston described cloud computing as “an information technology carrier model where computing offering (both hardware and software) are delivered on-demand to clients over a community in a self-service style, unbiased of tool and location (See in [99]).

The Operational model of information systems outsourcing is closely equivalent to that of cloud computing's, each practice tested the functionality of useful resource utilization, virtualization, scalability, and agility. Furthermore, National institute of necessities and technology (NIST) defined cloud computing as a model for enabling suitable on-demand network access to a shared pool of configurable computing resources that can be accepted manuscript hastily, provisioned and launched with minimal management effort or provider interaction. Based on NIST's classification, private cloud, community cloud, public cloud, and hybrid cloud are the four foremost patterns of cloud deployment (See in [100]).

3.3 MATERIAL AND METHODS

This section describes the overall methodologies that were adopted in this thesis. The following discusses research designs and methods, research

instruments, data collections, population & sampling, and finally data analysis. This chapter is mainly divided into four main sections as follows:

3.3.1 IT Governance

3.3.1.1 Design and Methods

A comparison study has been conducted in order to understand the current and previous studies targeting the Public, Private and governmental sectors in MENA region countries through a desk-based research method performed to analyze related articles focusing on IT Governance / Audit and COBIT frameworks and technologies used to mitigate operational, management and all other different types of risks.

MENA is an English acronym referring to the “Middle East and North Africa” region. The term MENA covers a wide region; it extends from Morocco to Iran and includes all Middle Eastern countries (Mashriq and Maghreb countries). This geographical acronym is roughly the same definition of the “greater Middle East”.

3.3.1.2 Research Population and Sample

While sampling hundreds of published articles, books, and conferences aiming to find related articles aligned with the goal of the study, the result showed 37 out of 150 related articles were found in the final total and are listed as the following:

NO.	Targeted Country	Targeted Sectors	Targeted Framework	Type of Research
1				
	Jordan	Banking	CAIS	Empirical
2				
	Jordan	Banking	ITG	Empirical
3				
	Jordan	Telecom	COBIT 5	Empirical

4	Jordan	Industrial	ITG	Empirical
5	Jordan	Banking	COBIT 5	Empirical
6	Jordan	Hospital	IS	Empirical
7	Algeria	Telecom	ITG	Empirical
8	Algeria	General	ITG	Theoretical
9	Egypt	Government	ITG	Theoretical
10	Egypt	Banking	COBIT/ IS	Empirical
11	Lebanon	Private	ITG	Empirical
12	Palestine	Audit Institutions	IT Audit	Empirical
13	Palestine	General	IT Risk/Audit	Empirical
14	Palestine	Government	ITG	Empirical
15	Saudi Arabia	General	COBIT/ITG	Empirical
16	Saudi Arabia	General	ITG	Empirical
17	Saudi Arabia	General	COBIT	Empirical
18	Saudi Arabia	General	ISG	Empirical
19	Saudi Arabia	Telecom	ICT Governance	Theoretical
20	Saudi Arabia	General	ITG/COBIT	Theoretical
21	Syria	Banking	COBIT	Empirical
22	Syria	Banking	ITG	Theoretical
23	Iraq	General	COBIT	Theoretical
24	UAE	General/SME's	IS Audit	Empirical
25	UAE	General	ITG	Theoretical
26	Saudi Arabia	General	ITG	Empirical

27	Jordan	General	ITG	Empirical
28	Bahrain	General	ITG	Theoretical
29	Bahrain	General	ITG	Theoretical
30	Bahrain	General	ITG	Theoretical
31	Bahrain	General	ITG	Empirical
32	Iraq/Mosul	Health	ISG	Empirical
33	Iran	Bank	COBIT	Theoretical
34	Iran	Bank/ Governmental	ITG	Empirical
35	Kuwait	General	ICT	Empirical
36	Morocco	General	ITG	Empirical
37	Oman	General	COBIT	Empirical

Table 1: Researches related to ITG- ICTG- ISG –COBIT -IT AUDIT frameworks.
Source: prepared by the author

3.3.1.3 Data Collection

Through my work, data has been collected targeting more than 150 different articles published in various academic and professional journals, periodicals, and conference papers including master's and PhD theses as well. Limited to the information provided through many online platforms, data has been filtered according to its scientific values, the relation to the targeted concept and the age of the publication, concentrating on the papers related to IT governance concept published in valuable magazines between 2006 through 2017.

3.3.1.4 Data Analysis

As per the interests of researchers focused on some sectors rather than others, as well as their contribution studies on IT Governance, COBIT framework and other related topics, sections have been divided according to sectors in the MENA region including but not limited to some general sectors; Banking, Governmental, Telecom, Health, and Industrial. (All of the above are shown in [101])

3.3.2 Cloud Computing

3.3.2.1 Design and Methods

This comparison study used meta-analysis design to elucidate the main concepts of cloud computing theory utilizing the most well-known regulations issued through a number of legislative authorities in three European countries (Germany, Hungary, and the UK) such as:

- 1- Financial conduct Authority (FCA), Prudential Regulation Authority (PRA), Data Act Protection (DAP), UK Government regulations, Bank of England.
- 2- Hungarian National Bank (MNB), Hungarian Financial Supervisory Authority (HFSA), National Authority for Data Protection & Freedom of Information in Hungary.
- 3- Federal Office for Information Security (BSI), German Federal Data Protection (BDSG)

Additionally, an assessment has been made based on the BSA Global Cloud Computing Scorecard 2016 (of which Germany and UK were a part of), excluding the data procured when specialists in the MNB authority (Hungary) were surveyed to gain relevant responses based on some main sections in the Global BSA survey,

The main reasons of sampling those three specific European countries are as follows:

- Germany and the UK are considered two of the top leaders in several areas, mainly in economics and regulations in Europe.
- In the Global Cloud Computing Scorecard classification, Germany has ranked in 3rd place and the United Kingdom has ranked in 9th place. Such a scorecard was classified by the leading advocate for the global software industry. This software is considered the first of its kind, ranking out of 24 countries representing 80 % of the global information and communications technology market, assessing seven sets of indicators: data privacy, cyber security, cybercrime, intellectual property, technology interoperability and legal harmonization, free trade, and IT infrastructure (See in [102]).
- UK's G-Cloud Strategy is the most fully elaborated cloud policy in Europe. It adopts a "public cloud first" approach for public procurement based on the public sector use of Information and Communications Technology (ICT).
- Germany is considered a great geographical location for cloud computing services comparing with others worldwide, as well as its restrictive laws that threaten to undermine the spirit of those same laws compared to other countries. For instance, by setting geographic restrictions on data that are neither needed to protect certain classes of data nor supported by law, practices in Germany could slow its own potential for any progress in the cloud (See in [103]).
- Hungary is a country that shows promise growing in the concept of clouding where many presiding authorities are concerned, especially the National Central Bank (MNB), which focuses on the applicability

of Cloud Computing in the financial sector. On the other hand, Hungary is one of the few generous countries that openly embraces and welcomes international students seeking further knowledge in specific degrees and graduate programs at its several universities, which I am fortunate to be a PHD scholar at present.

3.3.2.2 Research Population and Sample

Out of the available BSA (Global Cloud Computing Scorecard) of 24 different countries, I have sampled three European countries (Germany, Hungary, and the UK) according to their legislative authorities. This comparison study was conducted concentrating on the most six essential points that must be taken into consideration should one opt to apply Cloud computing services in any given sector. Additionally, through my work, 27 questions were derived based on the previously mentioned BSA Scorecard in order to measure the maturity level of readiness between the countries in question.

3.3.2.3 Data Collection

A large amount of data was collected and analyzed through my work according to the following six most important sections that have been considered in the comparison study due to their essential influence on cloud computing services implementation:

- Regulatory Considerations & International Standards
- Risk Management
- Data Security and Data protection
- Effective Access to Data & Business Premises
- Change Management and Continuity Plan
- Exit plan

On the other hand, based on the aforementioned fractional assessment (questionnaire) that was derived from the BSA 2016 Global Cloud Computing scorecard, some major questions were proposed in order to investigate the extent of aptitude, disposition, and inclination of those three EU pre mentioned countries in implementing and hosting Cloud computing services. Those questions were then divided into seven main fields as follows:

- Data privacy (8 questions)
- Security (3 questions)
- Cybercrimes (3 questions)
- Intellectual property rights (5 questions)
- Support for industry – led standards & international harmonization’s of rules (4 questions)
- Promoting free trade (3 questions)
- IT readiness broadband deployment (1 question)

3.3.2.4 Data Analysis

As my work shows, three main legislative authorities have been targeted in three European countries and with regulations prioritized, the six most important sections were focused on. A comparison study according to those regulations in said three European countries has been prepared based on those authorities resulting with the six sections mentioned above.

Appropriate solutions in several categories have been proposed in case cloud computing would be required.

Additionally, through my work, 27 questions were derived based on the previously mentioned BSA Scorecard in order to measure the maturity level of readiness between the countries in question. Those proposed questions

were divided into seven sections then weighted based on their importance and impact on cloud services.

As noticed earlier, each field of the seven listed previously contains several questions equaling different weights and subtotaled to equal 100% per section, calculated based on the following equations:

$$1^{\text{st}} \text{ Equation: } Qw = \frac{Im1 * Im2}{Tn}$$

Assuming that Qw stands for the Question's weight, Im1 stands for the value of Importance, Im2 stands for the value Impact and finally Tn stands for Total number of questions.

$$2^{\text{nd}} \text{ Equation: } R = \frac{Qw * L}{100}$$

Assuming that R stands for the Ratio, L stands for the Likert scale value based on three levels (Yes = "100", Partial = "50", No= "0").

As a pre -final step, each field has been weighted according to its importance and based on the BSA report with a combined sum of 100 % as follows:

- Data Privacy "10%",
- Security "10%",
- Cybercrime "10%",
- Intellectual Property Rights "20%",
- Support for industry-led standards "10%",
- Promoting Free Trade "10%",
- IT Readiness "30%"

As the final step, the sum of the above detailed values related to each country was calculated to identify the readiness, capability, and maturity level for each specific country in that regard.

3.3.3 IT Operational Risk

3.3.3.1 Design and Methods

Cooper and Schindler define research design as the blueprint for the collection, measurement, and analysis of data. Some studies adopted the cross-sectional descriptive research design. Cross-sectional studies are carried out once, which represent a snapshot at one point in time (See in [104]). Most of the survey designs provide an in-depth account of events, relationships, experiences/processes accruing in that particular instance (See in [105]).

This design was preferably adopted through my study because it offered the opportunity to collect data covering the IT operational risks in several private banks in the Jordanian financial sector at one point in time. It was also adopted as it allowed me to describe the phenomenon as it was, in its environment without any manipulation. It also allowed greater flexibility in terms of time and money, as well as the tendency to produce a high response rate. These reasons justified the use of this design in my study.

Based on the directions of both of the Central Bank of Jordan (CBJ) & the Association of Banks in Jordan (ABJ), a qualitative survey study was distributed in order to measure the current maturity of the local financial sector regarding the level of awareness related to these three main points as follows:

- Impact and criticality of risks caused by incidents related to Information Technology.
- Losses classified based on the three main particular event types related to IT Operational Risk according to Basel II accord.
- Annual allocation of a reasonable cash amount (reserves) based on the accurate estimation of losses caused by IT Operational risks and incidents.

3.3.3.1.1 Questioner Design

The Design consists of 6 Main sections as follows:

Section 1: Abstract specifying the targeted 3 main event types.

Section 2: Introduction clarifying the current situation of the market in that regards explaining the need of this questionnaire.

Section 3: Collecting General information of the participants limited to the following:

- Gender
- Job Title
- Professional Work Experience
- Name of Working Place

Section 4: Four Main Questions according to “External Fraud” event type

Section 5: Four Main Questions according to “Damage to physical Assets” event type

Section 6: Four Main Questions according to “Business disruption and systems failure” event type

The four main questions repeated for each one of the last three sections are limited to the following:

- What is the lower bound (JD) of a single loss caused by an IT Operational risk related to this “Event Type”?
- What is the annual average or expected frequency (repetition of occurrence/Likelihood) of IT operational risks related to this “Event Type”?
- What is the Average or expected amount (JD) of the individual loss for such “Event Types” (An Estimation)?
- What is the expected amount (JD) of the (Worst-Largest Loss) annually for such an “Event Type”?

3.3.3.2 Research Population and Sample

The sample is the portion or the subset of the research population, is selected to participate in a study, which represents the research population (See in [112]). My survey targeted all banks in the Jordanian financial sector asking several questions regarding three main event types related to the IT Operational risk role of work according to the Basel II accord and other international standards.

#	Jordanian Banks		
1	ABC Bank	12	Jordan Kuwait Bank
2	Al Rajhi Islamic Bank	13	National Bank of Abu Dhabi
3	Arab Jordan Investment Bank	14	Rafidain Bank
4	Bank al Etihad	15	Islamic International Arab Bank
5	Bank of Jordan	16	Societe Generale de Banque / Jordanie
6	Cairo Amman Bank	17	Standard Chartered
7	Capital Bank of Jordan	18	The Housing Bank for Trade & Finance
8	Citibank	19	National bank of Kuwait
9	Egyptian Arab land bank	20	Jordan Ahli bank
10	Arab Bank	21	BLOM BANK
11	Jordan Commercial Bank	22	Bank Audi

Table2: The targeted banks population in the study (IT Operational risk)
Source: prepared by the author

3.3.3.3 Data Collection

The questionnaire for the pilot test is like a draft that precedes the final report of which the purpose was to get problems out of the instrument so that the subject in my main study would not have trouble in completing the questionnaire. Therefore, to ensure validity and reliability of my data collection instruments, formulated questionnaires were pre-tested before they were administered to the respondents. The questionnaires were structured to address each of the research objectives.

Conclusively, for the main questionnaire results, the primary data was collected directly from the banks' administrators, IT systems' administrators, managers, and auditors. The data was collected by use of a closed-ended questionnaire with separate sections covering each of the objectives and event types. The initial three sections collected the general information related to the correspondents. The fourth section collected data on objective one (IT Operational risk / event type 1/ External Fraud). The fifth section collected data on objective two (IT Operational risk / event type 2/ Damage to Physical Assets). The last section collected data on objective two (IT Operational risk / event type 3/ Business Disruption and Systems Failures).

3.3.3.4 Data Analysis Design

Twenty-two responses from most of the targeted banks working in Jordan were received successfully and analyzed; results have been derived as shown in figure 9. Several methods are known to calculate the reserve needed for operational risk in the literature as well as in the regulations (see e.g. Basel II). I used the so-called Loss Distribution Approach, which is among the Advanced Measurement Approach in the Basel terminology. This method, among the most developed ones, gives a reserve highly depending on the

actual risk the institution has taken (since the Value at Risk is calculated for the total claim distribution). In the LDA, the total loss (or claim) distribution is modeled by a compound distribution, usually compound Poisson distribution, where the individual losses (claims), say, X_i for loss i , are independent and identically distributed, usually with positive loss distribution. Furthermore, the number of losses, also known as simply ‘frequency’, is a nonnegative integer valued random variable, say, N , and it is together with the individual losses is assumed to form an independent set of random variables. Thus, the total claim is clearly

$$S = X_1 + X_2 + \dots + X_N.$$

In this case, S is said to follow a compound distribution. If N has id Poisson distribution, then S has a compound Poisson distribution.

The most common choice for the individual loss distribution is the lognormal distribution. In operational risk, we often face the problem of small sample size from the last years. Hence, it is difficult to use sophisticated statistical methods for selection of distributions. The errors of the parameter estimations might also be rather large. Thus, as it is usual in the literature and in the practice, for such cases one can choose the compound Poisson model with lognormal individual loss distributions. Our calculations are also based on this choice for the same reasons.

Hence, based on the descriptive statistics of the survey we calculated the parameter estimates of the 3 parameters of the model. Clearly, the Poisson parameter is estimated by the average number of losses per a certain period. For the lognormal parameters (in what follows, they are referred as μ and σ) we used 2 statistics from the survey: the average size of the individual

losses and the ‘maximum’ loss they can imagine. The latter one - as usually done in practice - is identified by the 95% quintile of the lognormal distribution. Based on these two estimations we simply calculated the estimation for the two parameters. This was derived from the following equations:

- $\sigma_{1,2} = Z_{1-\alpha} \pm \sqrt{Z_{1-\alpha}^2 - 2 \ln \frac{q}{m}}$
- $\mu_{1,2} = \ln q - \sigma * Z_{1-\alpha}$
- $\text{Mean} = \exp\left(\mu + \frac{\sigma^2}{2}\right)$

Note that one could of course directly ask for the average individual loss and the variance or the standard deviation of the losses in the survey. That would be ideal from mathematical point of view since we could directly obtain the estimations of the first two moments of the individual loss distribution and then –as in the method of moments—just calculate the corresponding parameter estimates. However, it is not realistic that even experts are able to estimate the second moment based on their experience. It is much more realistic that they could estimate a kind of maximum loss.

Finally, as per the below figures and based on the fitted compound distribution, I calculate the Value of Risk (VaR) that will show the reserve needed at a certain confidence level. Since there is no formula for the quintile of the total loss, I apply Monte Carlo estimation to estimate the VaR.

Based on the above survey the following figure has been obtained.

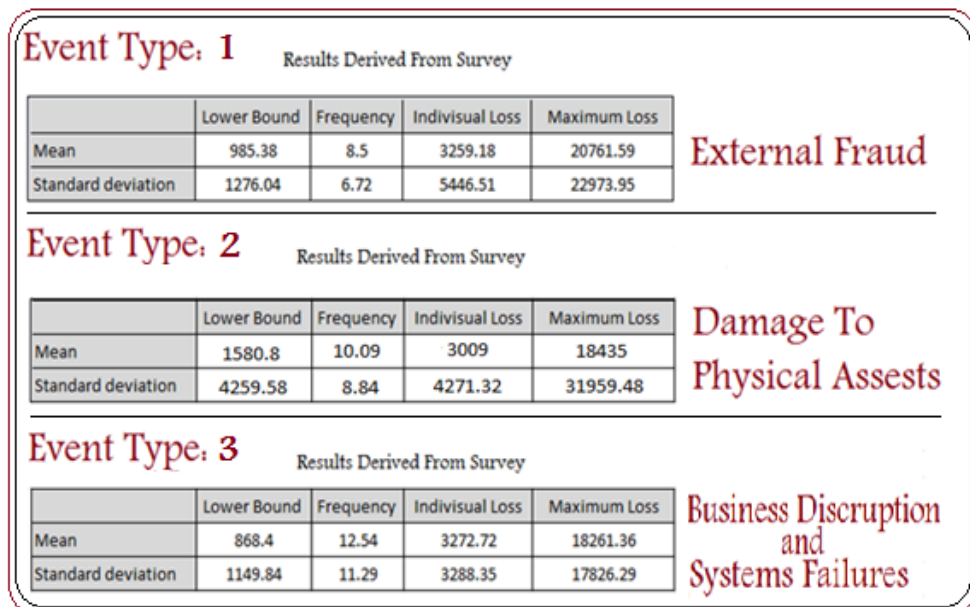


Figure 9: Results from Survey (IT operational risk)

Source: prepared by the author

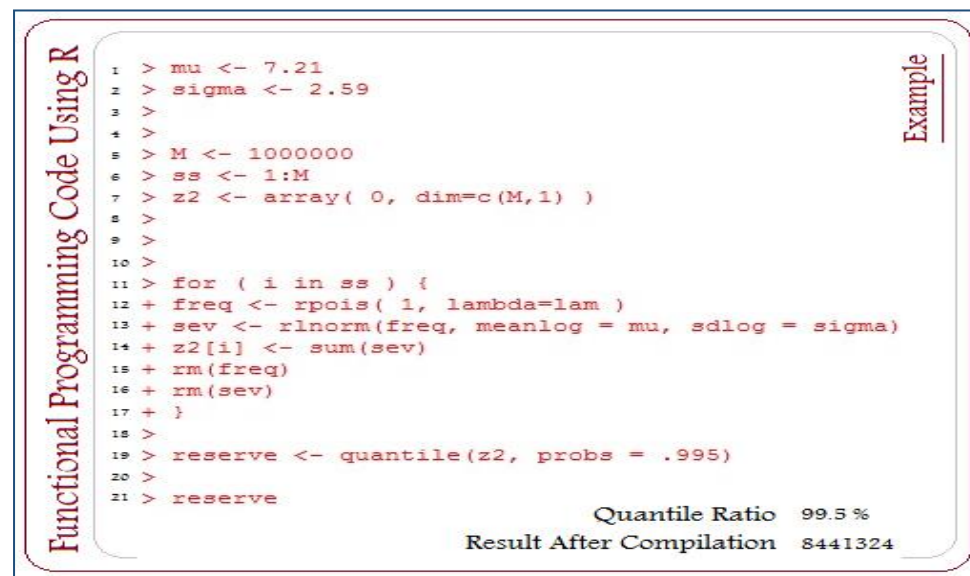


Figure10: Programming Code for R Functional Language (Monte Carlo method) (IT operational risk) Source: prepared by the author

3.3.4 COBIT 5

3.3.4.1 Design and Methods

My study uses the quantitative approach to an evaluation of the COBIT 5 framework. Burns and Grove underline that designing a qualitative study helps researchers to plan and implement said study in a way that will help them obtain the intended results, thus increasing the chances of acquiring the information that could be associated with the real situation (See in [106]). The use of my questionnaire was designed after some guidance and directions from professionals in ABJ (Association of Banks in Jordan) and reviewed by experts in CBJ (Central Bank of Jordan) based on some past-related studies that are adapted in order to partially meet the focus of this study. Said data is then collected directly from the respondents of the online questionnaire.

3.3.4.2 Research Population and Sample

Defining the target population, Sekaran clarifies a research population as the entire group of people, events, or things of interest that the researcher wishes to investigate. (See in [109]). A survey study was distributed on the 26 local and foreign banks in Jordan. The idea of this survey was supported by the Central Bank of Jordan (CBJ) as well as the Association of Banks in Jordan (ABJ). Such results are important to measure the current commitment value of the Jordanian banks regarding the CBJ regulations related to COBIT 5 Framework. Moreover, indicators highlight the maturity level in the Jordanian banks' sector regarding such international framework, particularly after passing more than 2 years since the first issuance and announcement of the CBJ regulations.

Jordanian Banks			
1	ABC Bank	13	Jordan Kuwait Bank
2	Al Rajhi Islamic Bank	14	National Bank of Abu Dhabi
3	Arab Jordan Investment Bank	15	Rafidain Bank
4	Bank al Etihad	16	Islamic International Arab Bank
5	Bank of Jordan	17	Societe Generale de Banque
6	Cairo Amman Bank	18	Standard Chartered
7	Capital Bank of Jordan	19	The Housing Bank for Trade &
8	Citibank	20	National bank of Kuwait
9	Egyptian Arab land bank	21	Jordan Ahli bank
10	Arab Bank	22	BLOM BANK
11	Jordan Commercial Bank	23	Bank Audi
12	Jordan Islamic Bank		

Table 3: Sample size of the targeted banks in Jordan

Source: prepared by the author

The process of selecting a` portion of the population to represent the entire population is known as sampling. A sampling process can be done through three steps that include identification of the population, identification of the sample size and selection of the sample (See in [113]). Simply, in this study I ran a survey on the Jordanian banks in the financial sector within the sample domain where the demographic criteria apply to regular employees, managers, and auditors, to measure their insights on how far their compliance is with the implementation of the COBIT 5 framework, where the sample of the respondents came to 23 banks.

3.3.4.3 Data Collection

My questionnaire was designed to gather information from the respondents of general managers, department managers, and audit managers etc. in banks operating in the Jordanian market using a questionnaire adapted from prior literature. Johnson and Turner clarify that data collection is “a method of gathering information from respondents about attitudes, knowledge, and beliefs” (See in [107]). Through my questionnaire, a Likert scale is used to

obtain the answers to the questions. Likert is a measurement of the metrics used to measure trends in the respondents' opinions. It implies a Likert scale of a five-degree answer to each interviewed question (ranging from not reached, slightly reached, partially reached, largely reached, and fully reached) which is represented numerically (1 to 5). To verify the veracity of the study tool, I presented the questionnaire to five experts, making the tool more accurate and objective as a measurement. The main determination of the questionnaire was to verify the following:

- The bank's awareness based on the international standards related to the IT Governance frameworks.
- The bank's compilation and maturity level regarding the CBJ regulations related to COBIT 5 framework.
- The indicators of financial performance in the Jordanian financial sector compared to the investments allocated for COBIT 5 Framework.

As known, the general goal of a pilot study is to provide information which can contribute to the success of the research as a whole [See in (111)]. The pilot study for this research was conducted with 3 respondents. They were randomly selected in order to validate the survey instrument.

Generally, a variety of methods is considered in order to form a research basis. In order to reach the objective for any research, the identification of an appropriate means of data collection is mandatory (See in [108]). In my research, I adopted two main types of data collection sources. The following sections explain data collection methods required for the research.

- Primary Data

The data is collected to obtain a sum of the study's objectives and research questions. The primary data is collected to provide the information that would produce answers to the research objectives, compared to secondary data that is used to develop contextual or confirmatory elements of research (See in [110]). In this study, the main instrument of data collection was the questionnaire. There are two phases involved in the data collection, the pilot phase, and the main study.

- Secondary Data

In this research, I used quantitative secondary data, which I obtained from journal articles and the annual banks' financial disclosures additional to the ABJ official annual reports.

3.3.4.4 Data Analysis

The data collected was analyzed using different statistical techniques, which were determined by the research objectives and goals. The data analyses of this study were defined into two phases. The first phase is the pilot study with just 4 respondents to test the reliability and content validity of the instrument designed using Statistical Package for Social Sciences (SPSS) software.

In the main analysis, for data analysis and hypothesis testing, SPSS was the software used, including the following analyses: descriptive statistics used to summarize and describe the key features of the sample data such as frequencies, percentages, means, standard deviations, and ranges. Descriptive analysis was carried out to present the raw data into a form that made it easily understood and interpreted. To present the response on the major variables

under investigation, a descriptive statistic (mean value and standard deviation) for all variables of interest were obtained.

- General Overview

Earlier on April/2016 the Central Bank of Jordan (CBJ) issued regulations concerning COBIT 5 Framework of which several phases and levels have been allocated in this project due to a number of milestones dependent on the plan included in the primary regulations.

Such a Project of COBIT 5 Framework implementation targeted the entire financial bank's sector located in Jordan, and as stated previously, the framework has been divided into five main key areas (APO, BAI, DSS, MEA, and EDM). They are also divided into 37 processes; each process had its own goals that should be measured continually. A gap assessment for the status of the Jordanian banks was completed comparing the current used practices to the global best practices shown in COBIT 5 Framework. Afterwards, a starting point of the project was defined as per the situation of each bank individually.

- COBIT Processes and related departments

In every bank, the (37) COBIT processes were divided on several related departments, with each department taking responsibility of managing its own related process/processes based on its role of work practices and procedures as the following:

REF #	Process	Process Name	Main Department	Related Parties
1	APO01	Manage the IT Management Framework	IT	/
2	APO02	Manage Strategy	IT	/
3	APO03	Manage Enterprise Architecture	PMO	/
4	APO04	Manage Innovation	HR	/
5	APO05	Manage Portfolio	PMO	/
6	APO06	Manage Budget and Costs	Finance	/
7	APO07	Manage Human Resources	HR	/
8	APO08	Manage Relationships	IT	/
9	APO09	Manage Service Agreements	IT	/
10	APO10	Manage Suppliers	Administration	/
11	APO11	Manage Quality	IT	/
12	APO12	Manage Risk	Risk	IS
13	APO13	Manage Security	IS	/
14	BAI01	Manage Programmes and Projects	PMO	/
15	BAI02	Manage Requirements Definition	IT	/
16	BAI03	Manage Solutions Identification and Build	IT	/
17	BAI04	Manage Availability and Capacity	IT	/
18	BAI05	Manage Organisational Change Enablement	PMO	/
19	BAI06	Manage Changes	IT	/
20	BAI07	Manage Change Acceptance and Transitioning	IT	/
21	BAI08	Manage Knowledge	HR	/
22	BAI09	Manage Assets	IT	/
23	BAI10	Manage Configuration	IT	/
24	DSS01	Manage Operations	IT	/
25	DSS02	Manage Service Requests and Incidents	IT	/
26	DSS03	Manage Problems	IT	/
27	DSS04	Manage Continuity	Risk	IT
28	DSS05	Manage Security Services	IT	/
29	DSS06	Manage Business Process Controls	Risk	Organize
30	MEA01	Monitor, Evaluate and Assess Performance and Conformance	PMO	/
31	MEA02	Monitor, Evaluate and Assess the System of Internal Control	AUDIT	/
32	MEA03	Monitor, Evaluate and Assess Compliance with External Requirements	Compliance	/
33	EDM01	Ensure Governance Framework Setting and Maintenance	Higher Management	GM
34	EDM02	Ensure Benefits Delivery	Higher Management	PMO
35	EDM03	Ensure Risk Optimisation	Higher Management	RISK
36	EDM04	Ensure Resource Optimisation	Higher Management	HR
37	EDM05	Ensure Stakeholder Transparency	Higher Management	IT

Table 4: 37 Processes related to the banks Department. (COBIT 5)

Source: Prepared by the author.

The survey contained 127 questions divided into 37 sections, each section representing one of the COBIT 5 processes aiming to measure the bank's compliance to the COBIT 5 Framework. All answers were collected and analyzed using (SPSS), then (R) Functional language for more certainty and accuracy.

The Processes Capability Model Defines a scale going from 1 to 5. Each maturity level is composed of expected objectives divided as per each level to assess the process level. To reach a specific level, all attributes and objectives should be at fully or at least largely achieved.

In level 1: The process does not exist or not performed at all

For level 2 to 5: Attributes for levels 2 to 5 are examined as per ISO/IEC 15504

The rating scale involves five implementation levels as follows:

Level 1	Not Implemented	The process is not implemented or fails to achieve its process purpose
Level 2	Slightly Implemented	The implemented process achieves its process purpose
Level 3	Partially implemented	The performed process is now implemented in a managed fashion.
Level 4	Largely Implemented	The managed process is now implemented using defined process.
Level 5	Fully Implemented	The established process is now operating within defined limits to achieve its process outcomes,

Table 5 Implementation rating scale (COBIT 5)

Source: prepared by the author

- Questionnaire Design

The Design consists of 11 Main sections as follows:

Section 1: The title and small abstract.

Section 2: Introduction clarifying the current situation of the market in that regards explaining the need of this questionnaire.

Section 3: Collecting Demographic characteristics for the participants limited to the following:

- Gender
- Academic Qualification
- List of the Professional Certificates Gained and related to this domain
- Professional Work Experience
- Job Title
- Organization sector
- Name of Working Place

Section 4: A Choice from a drop-down list contains all the Jordanian Banks.

- **Section 5:** A Choice form a drop-down list contains all of the Jordanian insurance companies.
- **Section 6:** Contains 44 questions divided into 13 APO processes - Likert scale from 1 to 5

Section7: Contains38 questions divided into (10) BAI processes - Likert scale from 1 to 5

Section 8: Contains 19 questions divided into (6) DSS processes - Likert scale from 1 to 5

Section 9: Contains 11 questions divided into (3) MEA processes - Likert scale from 1 to 5

Section 10: Contains 15 questions divided into (5) EDM processes - Likert scale 1 to 5

Section 11: Collect some main variable divided into 5 main questions limited to the following:

- The annual budget allocated for information technology department in the past two years.
- Any external or internal security breaches recorded in the organization during the last two years.
- Any security incident occurred, causing loss of sensitive data during the previous two years.
- External or internal frauds or financial robbery was detected on both electronic and manual levels in the institution during the past two years.
- The most three risky security breaches occurred during the past two years.

4 RESULTS & RESEARCH FINDINGS

4.1 IT Governance

All the results in this section are clarified in my paper [see (114)].

4.1.1 Discussion on IT Governance

Studies on IT governance and related subjects started early in 2006 in some Mena countries such as Jordan, Saudi Arabia and Algeria. Balgedom, S. [115] clarified that it is important to keep pace to technological development to achieve success and compete in such complex expansion in the Algerian market. Thus, Hayale et al [116] assured that Jordanian domestic banks are implementing effective fraud and error reduction controls, but still there is a need to other control systems such as DR, DS, and electronic controls. Also, they reveal that IT Governance in Saudi Arabia's public sector have been introduced in some main steps concluded by identifying what is meant by ITG and reviewing highlights in COBIT and its current state ensuring the future recommendation in that field.

4.1.2 Results and Findings

The below table highlights on all of the used material in the research focusing on many points especially the year of publishing, subject of the material, publishing country and domains that were mainly targeted in our study, keeping into consideration that all of the detailed results and findings are clarified and explained in Appendix 1.

NO.	Authors	Year	Country	Domains	Subject	Type of Research	Findings
1	Hayale & Abu-Khadra	2006	Jordan	Banking	CAIS	Empirical	Appendix A (Table 1)
2	Khadra	2009	Jordan	Banking	ITG	Empirical	Appendix A (Table 1)
3	Al- Skafy	2012	Jordan	Telecom	COBIT 5	Empirical	Appendix A (Table 1)
4	Al-Zwyalif	2013	Jordan	Industrial	ITG	Empirical	Appendix A (Table 1)
5	Al Ramahi	2014	Jordan	Banking	COBIT 5	Empirical	Appendix A (Table 1)
6	Al-Qudah	2012	Jordan	Hospital	IS	Empirical	Appendix A (Table 1)
7	Balgedom	2006	Algeria	Telecom	ITG	Empirical	Appendix A (Table 1)
8	Ayshosh & Wadih	2012	Algeria	General	ITG	Theoretical	Appendix A (Table 1)
9	Abu Hajar & Amineh	2014	Egypt	Government	ITG	Theoretical	Appendix A (Table 1)
10	Alber & mayval	2015	Egypt	Banking	COBIT/ IS	Empirical	Appendix A (Table 1)
11	Hejase	2016	Lebanon	Private	ITG	Empirical	Appendix A (Table 1)
12	Mahmoud Zgout	2016	Palestine	Audit Inst.	IT Audit	Empirical	Appendix A (Table 1)
13	Raeda Abu Etaiw	2012	Palestine	General	IT R./Audit	Empirical	Appendix A (Table 1)
14	Lubbard & Ashour	2014	Palestine	Government	ITG	Empirical	Appendix A (Table 1)
15	Abu -Musa	2009	Saudi Ar.	General	COBIT/ ITG	Empirical	Appendix A (Table 1)
16	Abu - Musa	2006	Saudi Ar.	General	ITG	Empirical	Appendix A (Table 1)
17	Abu - Musa	2008	Saudi Ar.	General	COBIT	Empirical	Appendix A (Table 1)
18	Abu - Musa	2010	Saudi Ar.	General	ISG	Empirical	Appendix A (Table 1)
19	Bin-Abbas & Bakry	2012	Saudi Ar.	Telecom	ICTG	Theoretical	Appendix A (Table 1)
20	Bakry & Alfantookh	2006	Saudi Ar.	General	ITG/COBIT	Theoretical	Appendix A (Table 1)
21	Zyoud, Lateef, Nsour, Reem	2014	Syria	Banking	COBIT	Empirical	Appendix A (Table 1)
22	Madian, Nazeer	2015	Syria	Banking	ITG	Theoretical	Appendix A (Table 1)
23	Karima Kadhim, Ahmad	2015	Iraq	General	COBIT	Theoretical	Appendix A (Table 1)
24	Vijaya Kumar & Ilangovan	2015	UAE	General/SME's	IS Audit	Empirical	Appendix A (Table 1)
25	Nicho & Mourad	2012	UAE	General	ITG	Theoretical	Appendix A (Table 1)
26	Waleed Afandi	2016	Saudi Ar.	General	ITG	Empirical	Appendix A (Table 1)
27	Firas Alkhaldi & Wraikat	2015	Jordan	General	ITG	Empirical	Appendix A (Table 1)
28	Harikrishnan, Zakareya	2014	Bahrain	General	ITG	Theoretical	Appendix A (Table 1)
29	Janahi. L. A. M.	2016	Bahrain	General	ITG	Theoretical	Appendix A (Table 1)
30	Griffiths, Janahi & Ammal	2014	Bahrain	General	ITG	Theoretical	Appendix A (Table 1)
31	Griffiths, Janahi & Ammal	2015	Bahrain	General	ITG	Empirical	Appendix A (Table 1)
32	Salim, Othman & Yahya	2012	Iraq	Health	ISG	Empirical	Appendix A (Table 1)
33	Yarifard & Gowda.	2010	Iran	Bank	COBIT	Theoretical	Appendix A (Table 1)
34	Ghazanfari, Fathian & Rais	2009	Iran	Bank/ Gov.	ITG	Empirical	Appendix A (Table 1)
35	Zaied,Khairalla & Rashed	2007	Kuwait	General	ICT	Empirical	Appendix A (Table 1)
36	Nakabi, Fadili & Sema.	2017	Morocco	General	ITG	Empirical	Appendix A (Table 1)
37	Shivasharikarapa, Smalov, et	2012	Oman	General	COBIT	Empirical	Appendix A (Table 1)

Table 6: Results of the conducted research (2006 -2017) (MENA Region)

Source: Prepared by the author.

According to the results above, the findings below were gathered into sections according to the annual dates of publications:

(2006-2008)

- From early 2006, Saudi Arabian researchers had begun publishing articles concentrating on the IT Governance theory revealing required facts in order to measure the awareness level in that regard.

- In 2007, two main studies have been carried out in Saudi Arabian and Kuwaiti institutions regarding ICT and IT Governance of which both studies concentrated on the readiness for deploying an electronic future. Abu Musa, A. [117] clarified that the IT Strategy should be aligned with the organizational strategy by the help of the IT resources in a responsible matter to achieve better governance.

- Zaied, A & Alrashed, W. [118] focused on the E-readiness of the organizations in Kuwait in order to adopt E-services and E- government and assured that most of the institution's infrastructure is ready by that time to host any coming E-services.

- Abu Musa, A. [119] clarified that COBIT is an important framework that should be adopted by the Saudi Arabian organizations. Despite the lack of trust in the efficiency of applying such processes, Abu Musa assured that the IT specialists and executive managers had valued the importance of COBIT processes the most. Moreover, he was confident that the banking sector had become prevalent with such frameworks more than the other sectors.

(2009-2011)

- In comparison between the Saudi Arabian, Iranian, and Jordanian published studies in the years 2009- 2011, Jordan lead in the first level of understanding and implementing IT Governance in several areas, especially

in the banking sector. Ghazanfari, M & Rais, S. [120] clarified that governmental banks in Iran lost their desire for hosting E-commerce due to the lack of competition in adopting mandatory rules and regulations of ITG in different sectors.

- Yarifard, R. & Gowda, k. [121] clarified that after applying COBIT framework in many banks of the region, the revelation showed that most of them did not exceed the third maturity level based on the processes' definition in the CMMI.

- Abu Musa, A. [122] clarified that the ITG COBIT processes and domains are neither audited nor formally conducted at several public Saudi Arabian organizations in that time.

- After some time, Abu Musa clarified that the majority of organizations in Saudi Arabia are aware of the importance of the ISG while they remained without any written IS policy statements nor clear information security strategies, nor plans for disaster recoveries for them including the roles and responsibilities of IS that are not communicated clearly or even defined.

- On the contrary, the Jordanian banks had effective extents in awareness/communication, responsibility, accountability, skills and expertise within the Jordanian domestic banks with some shortage in fully implementing other few dimensions such as plans, goal setting, and measurement (See in [123]).

(2012-2013)

- Afterwards, in 2012 and 2013 many studies were conducted targeting different sectors in several MENA countries such as Jordan, Oman, Iraq, UAE, Saudi Arabia, Algeria, and even Palestine. They focused on IT Governance and COBIT framework going through ICT Governance, IS, and IS governance (See in [124]).

-Salim, M et al [125] focused on the health sector in Mosul, Iraq and explored some critical points that influence the role of effective implementation of IS Governance in that country due to the lack of DR plans and BC plans, written information security policy, and risk assessment procedures.

- Al Skafy, H. & Althebeh, Z. [126] study focused on COBIT 5 framework used in Jordanian telecom sector revealing that most of COBIT principles are applied in a high degree in a particular telecom company.

-Bin Abbas, H. & Bakri, S. [127] clarified that the Saudi Arabian telecom sector should be aware that the new ICT Governance approach includes essential controls, incorporated knowledge, and management principles.

-Al Zwyalif, I. [128] clarified that IT Governance affects the value of accounting information through its direct effects on the AIS on the Jordanian industrial sector.

-Conversely, many Omani institutions in the public sector have realized the importance to provide comprehensive services to its citizens and thereby align to E-governance strategies (See in [129]).

-Ayshosh, R. et al [130] were concerned regarding the IT Governance various frameworks and models, measurement and maturity models, and implementation tools while they then tried to illustrate how IT Governance explains Solow's productivity paradox.

-Nicho, M. and Mourad, B [131] explained that structures, processes, and relational mechanisms are the three main IT Governance domains in the UAE public sector. Under each domain, there are correspondents that the ITIL domain provides relevant context in order to categorize the best practices.

-Raeda, I. [132] clarified that external auditors in Palestinian institutions face many risks. One of the most common risks is known as the Access Risk, while the Environmental Risk is the least common one known.

(2014-2015)

-A large group of researchers in the MENA region focused their studies on IT Governance and COBIT framework during 2014 to 2015 with belief of its importance in causing the success of any institution, especially after the expansion of using such frameworks, particularly after the release of last version of COBIT in 2012 (also known as COBIT 5).

-As Al Ramahi. N et al [133] focused on COBIT 5, he clarified that executives must ensure that information technology works with the greatest possible efficiency to help achieve strategic goals and objectives in Jordanian organizations.

-Zyoud et al [134] clarified that application level of IT Governance by using COBIT framework in Syrian banks reached the fourth maturity level according to the PAM book.

-Lubbad, R. Ashour, Y. [135] elucidated that the mechanics of IT Governance reduces risks to trim down the financial electronic manipulation while being mindful of application usage. Assuring that in order to improve the maturity of Governance, it is a requirement that concentration on the essential steps to move forward to the next level are taken. In addition, a requirement of an understandable plan and clear strategy for management and surveillance of all activities in IT Departments is met.

-Al Meida, R, Pereira and Da silva, M. [136] indicated that the mechanics of IT Governance is reducing these risks to reduce the financial electronic manipulation in light of the application of E-Government in the governmental units theoretically.

-Harikrishnan, S. & Zakareya, A [137] affirmed that the implementation of ISO 27001 standards in some Egyptian banks may affect indicators of profit as measured by return on capital, as well as the implementation of PCI-DSS standards may affect asset quality as in Non-performing loan ratio.

-Griffiths, M. Janahi, & Al-Ammal, H. [138] focused on the IT Governance rules and recommendations, and how to improve its maturity level in the local markets by processes that have been considered significant and necessary for implementing IT Governance framework considerable by respondents, concluding in managing all processes.

-Alber, N. & Nabil, M. [139] affirmed that studies concentrating on ITG and COBIT were conducted trying to explore the current situation for a better understanding of the current market situation regarding such theories.

-Madian, A. & Nazeer, M. [140] targeted the banks sector in Latakia, Syria and discovered that there is a commitment of using exercised IT Governance in the public banks of Latakia that ensures the control on this source trying to achieve the aim of these financial organizations.

-Kadhim, K. & Ahmad, J. [141] from Iraq, clarified that COBIT framework can be guided to develop regularly appropriate measures that achieve effective use of IT resources, infrastructure, skills, hardware, software, and several other components.

-Alkhaldi, F. & Wraikat, M. [142] examined the public sector in Jordan concentrating on ITG exploring that there is a relationship between IT Governance and IT Portfolio Management Pillars and organizations should take into consideration the importance of IT Governance and its accountability pillars, transparency, participation, and predictability in enhancing IT Portfolio Management.

-Furthermore, there are no significant variations in the Maturity Level Index scores between the four regions within the UAE (Abu Dhabi, Dubai, Sharjah and other Emirates) with the average of KPI scores between manufacturing trading and service sectors (See in [143]).

(2016-2017)

-Finally, during 2016-2017, several researchers in countries behind the online curve overwhelmingly felt responsible and continued to investigate IT Governance performance in their market (Lebanon, Bahrain, and Morocco). Then by conducting empirical studies on both public and private sectors arriving to the conclusion that IT directors and managers are more knowledgeable about COBIT, ITIL, ISO 17799, PAM Book, and Balanced Score Card approaches in comparison to employees in Lebanese organizations.

-IT structure in Bahrain public institutions requires reevaluation to improve the commonly known IT activities, leading to spread a cultural accountability by means of precise responsibilities and roles. Some organizations in Morocco are beginning to implement IT Governance practices and processes but IT frameworks are not applied, yet neither the other specific act like Service Level Agreements (SLA's), Activity Based Costing, ROI calculation, or measurements also are not widely practiced, so it might need more time and effort to be done.

-At the Palestinian institutions, IT usage in the completion stage of the audit process and reports issuance leads to improve quality of audit performance and documentation since this will insure more relevant evidence and objective results of audited items (See in [144]).

- Afandi, W. [145] agreed with Alkhaldi and assured that lately there are relationships between IT Governance, IT Portfolio Management, and their Pillars (such as accountability, transparency and PMOS, PMPS, PMRB) keeping into consideration that the relationship between IT Governance and IT Portfolio Management also strongly exists in the Saudi Arabian Organizations.

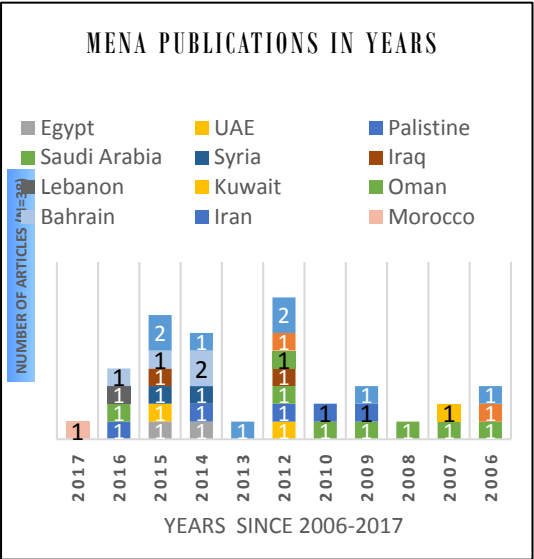


Figure 11: Publications according to MENA R.
Source: prepared by the author

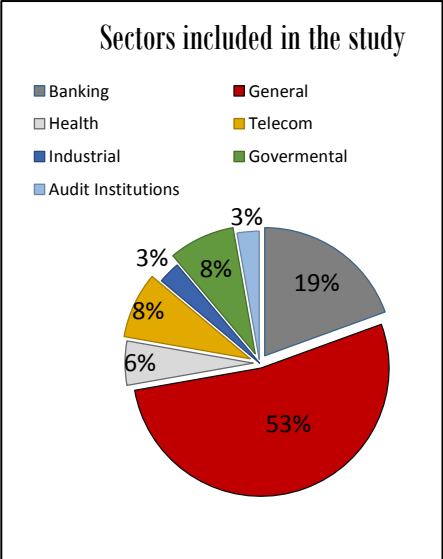


Figure 12: Sectors included in the study
Source: prepared by the author

Researchers' interests and their contribution studies on IT Governance and COBIT frameworks focused on certain sectors. As clarified in figure12 above, it is noticeable that the highest percentage, according to the sectors in the MENA region, showed that 53% of the studies represented the general sectors while the banking sector ranked second with 19%. Respectively, both Governmental and Telecom sectors ranked third with 8% for each, with the Health sector coming in fourth showing 6%. The remaining 6% were divided equally between the audit institutions and the industrial sector.

However, due to the largest sample that could be found on websites and electronic storage libraries, Figure 11 shows the total number of researches targeting various sectors in the MENA region, focused mainly on IT governance, and COBIT framework in all aspects.

It is perceivable that the total number of related articles found was 37 and the year 2012 was ranked first place with 21% of that total number. The year 2015 ranked second place with 18.4% targeting several sectors in MENA countries.

Furthermore, it is noticeable in the figure from 2012 and afterwards that the number of publications has been increased by almost three times, perhaps due to the release of COBIT 5 framework on 2012 by ISACA institutions. COBIT 5 (the governance and management of enterprise IT) was considered as a comprehensive framework that helped to spread awareness all over the region regarding its importance and motivated institutions in different sectors/countries to use such frameworks due to its importance to enhance work procedures and risk controls in any institution.

Continually, Figure 13 below shows that comparing between all of the countries in the MENA region, Jordan and Saudi Arabia had the highest rankings in contributions of publications related to IT Governance since 2006 until 2017. While Bahrain took third place contributing with the latest four publications, Algeria, Egypt, UAE, Syria, Iraq and Iran submitted the same number of publications which they had occupied the fourth rank in equal percentages. Unfortunately, the remaining countries resulted in modest contributions in the MENA region with the fact of the total absence of some of them.

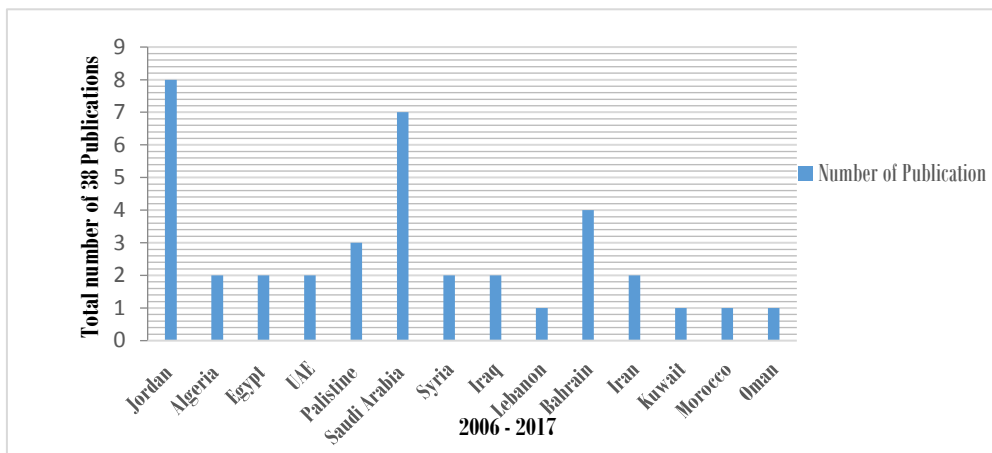


Figure 13: Contributions of MENA countries in Published studies related to ITG, IT Audit, ISG, and other similar studies. Source: prepared by the author

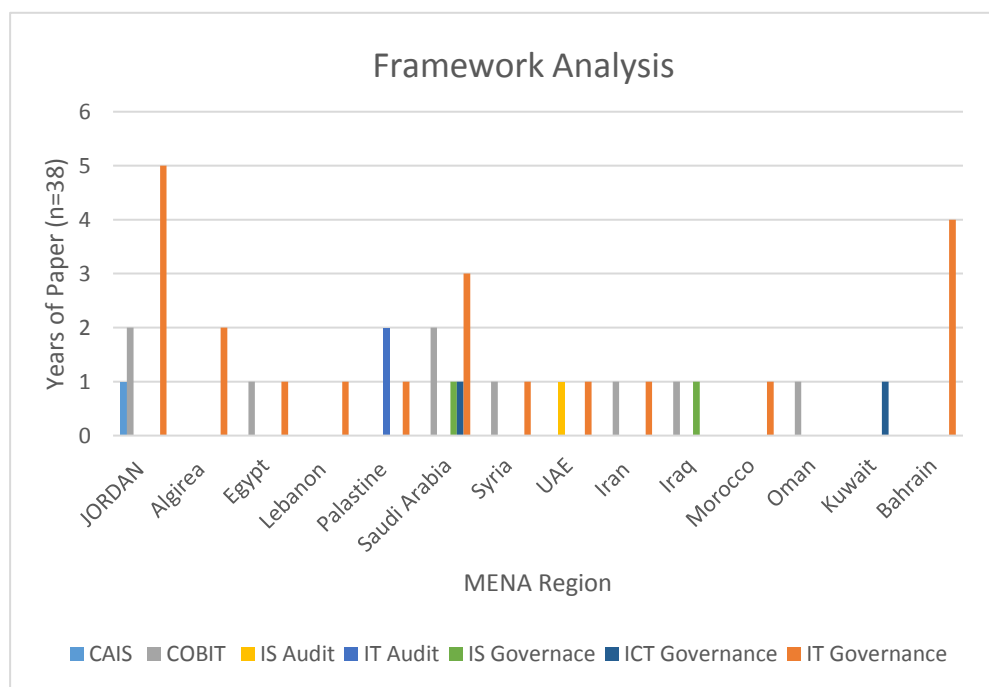


Figure 14: Topics of Publications used in MENA Region
Source: prepared by the author

Figure 14 shows several frameworks that have been targeted by researchers in order to investigate the Main ITG implementation in several institutions included in the MENA region. The aforementioned figure clarified that there are seven frameworks, which have been researched since 2006. There are uncertainties that the studies have demonstrated which are generally on the IT Governance and COBIT frameworks from different aspects such as CAIS, ICT Governance, IS audit, IT audit, and IS Governance. All the above-mentioned share the same affair by aiming to enhance work processes & procedures in order to mitigate risks and strengthen controls.

4.2 CLOUD COMPUTING

4.2.1 Discussions & Comparison study

As mentioned previously, legal information mentioned below are primarily gathered by regulation documents legislated by some main authorized parties in three European Countries.

1- Financial Conduct Authority (FCA), Prudential Regulation Authority (PRA), Data Act Protection (DAP), UK Government regulations, Bank of England (United Kingdom)

2- Hungarian National Bank (MNB), Hungarian Financial Supervisory Authority (HFSA), National Authority for Data Protection & Freedom of Information in Hungary (Hungary)

3- Federal Office for Information Security (BSI), and German Federal Data Protection (BDSG) (Germany)

The most six important sections that have been considered in the comparison study due to their essential influence on cloud computing services implementation are as follows: (See in [28-31] [38] [146-147])

4.2.1.1 Regulatory Considerations & International Standards

Initially, the British point of view is that institutions should have a documented business case to support the decision of outsourcing considering any relevant regulatory obligations, as well as probable risks and remain certain that the outsourced agreement will not worsen the firm's operational risk. Vital for regulation determination while keeping in mind this jurisdictional key point, the contract also should guarantee the auditors and regulators' effective access to data and business premises in case the service provider is located out of the U.K. On the other hand, adherence of the provider to the international standards is demanded, taking into account the importance of external assurance since it might be more relevant regarding the well-understood standards and stabilized assessed services in data centers.

Conversely, competent authorities in Hungary ensure the need of regulatory compliance before using the cloud services after assessing the detailed tasks in the decision-drafting phase. Besides the necessity of ensuring the essential controls and monitoring capabilities by the provider, it furthers more focus on complying with the regulations of "Act L of 2103" in electronic information security in case the systems are identified as an entity of key importance in the financial sector. Apart from this, they concentrate on monitoring the changes in the regulations of the EU as well as the Hungarian National Bank (MNB) regulations and international EU data privacy provisions and practices.

Additionally, in Germany, responsible parties see that in combination with the previous result, a high degree of trust in the cloud service provider is required before agreeing in contract with them. In addition, they consider the cloud computing compliance controls catalogue (C5) as the baseline that is intended to be an aid for the customer. Such a catalogue besides some international standards that should be taken into consideration such as ISO/IEC 27001:2013/ CSA3/ AICPA4/ IDW6 ERS FAIT 5 / BSI IT provides a better overview for a higher level of security and allowed us to avoid redundant audits.

4.2.1.2 Risk Management

Risk assessment is one of the serious aspects that firms should focus on. In fact, some parties in the UK ensure that firms should have a documented risk assessment and identification. Therefore, to generate further steps in order to mitigate risks while taking into consideration the main point of jurisdictional risk mentioned previously, for the reason of its significant impact on business procedures. Keeping in consideration the firm's responsibility in assessing and managing those operational risks and monitoring concentration risks, the business recovery overcomes in case the outsource provider failed, in addition of breaches notification.

Comparatively, other parties in Hungary strengthen the concept of the IT risk analysis to meet the requirements in cloud service security principles and phases of service's lifecycle. This would be achieved by operating controls either by the institution or by the service provider, as what was agreed upon by the signed contract, whereas the institution shall manage risks causing regulatory noncompliance with risk mitigation actions. This defines the level of required assurance according to the risk level of the areas involved.

However, Germans have a different perspective in this regard as some of the knowledgeable authorities see that policies and instructions for the general procedure applicable to the identification, analysis, assessment and handling of risks and IT risks. Specifically, they are documented, communicated, and provided according to (SA-01). The procedures for the identification, analysis, assessment and handling of risks, including the IT risks relevant to the cloud service, are done at least once a year in order to take internal and external changes and influencing factors into account. In addition, the identified risks should be comprehensibly documented, assessed, and provided with mitigating safeguards. Finally, top management parameters for the Risk Appetite and Risk Tolerances of the cloud provider must be included in the policy for the risk management.

4.2.1.3 Data Security and Data protection

UK experts believe that a security assessment and a data residency policy with the provider should be carried out by a firm, besides the provider's data loss and breach notification processes that should be aligned with the firm's risk appetite and legal / regulatory obligations.

Although, if public clouding is utilized, then data segregation and data sensitivity should be considered, keeping into account the appropriate steps to mitigate security risks as well as retaining an acceptable overall security exposure in the firm, in which general institutions should comply at the very least with the main principles of the DPA (Data Protection Authority).

Contrarily, Hungarian experts affirm that the institution should identify and apply security classification to the planned data in order to be outsourced by the cloud service provider in line with the legal regulations and its own data protection rules as specified in "NAIH" the Hungarian national authority

for data protection and freedom of information. Nonetheless, the data security requirements, stored data, and data transmission should be defined between the institution and the cloud, the resource and the cloud, and the cloud and other external service providers. All of them should be protected from unauthorized access and modification, recognizing that security incidents and their resolution should be declared, and the provider should support any regulated fraud's investigation. Moreover, institutions should support protection against malicious codes, including the installation, regular update, and central monitoring of security tools, as well as regular checking of the network and devices using an antivirus tool.

However, the institution is supposed to obtain assurance that the cloud service provider adheres to the relevant data protection rules and legal regulations (as mentioned previously) and identifies the differences between the data protection requirements relevant to the institution and the cloud service provider's data protection commitments, practices, and data reporting obligations relying on the contractual conditions.

Lastly, the assurance of safe handling and processing of personal data, banking data, insurance data, and confidential data classified by other sectorial laws is absolutely necessary, in compliance with the data protection regulation.

On the other hand, German experts reassure that the security of cloud services is an ongoing task so data of the cloud customer should only be processed, stored, and backed up outside the contractually agreed locations, only with the prior express written consent of the cloud customer. The cloud provider must use secure network protocols for the import and export of information as well as for the management of the service in order to ensure

the integrity, confidentiality, and availability of the transported data. Moreover, the requirements for the protection of personal data according to BDSG (German Federal Data Protection Act) or the EU Data Protection Directive boil down to the following: Legal permission/consent, Direct collection, Data minimization, Purpose limitation, Transparency, etc.

4.2.1.4 Effective Access to Data & Business Premises

Regulated firms should require effective access for the auditors, regulators, and relevant competent authorities to data related to its outsourced activities offered by service providers as UK expert parties advise. As such, regulated firms detect these notification requirements on accessing data and should be reasonable without restrictions on auditors and regulator's access, since they must treat any information disclosed in accordance with the confidentiality obligation set out in (FSMA)¹. Simultaneously, contracts should enable them to contact the service provider directly in case a firm cannot disclose data for any reason. In addition, in some cases, contracts must allow business premises' access relevant for the exercise of effective oversight, apart from that it is preferable to provide reasonable prior written notice before the time of this visit. This is valid except when there is an emergency or crisis situation at times when the scope of visit could be limited only to the services that are used by the firm's group.

¹The Financial Services and Markets Act is an Act to make provision about the regulation of financial services and markets; to provide for the transfer of certain statutory functions relating to building societies, friendly societies, industrial and provident societies and certain other mutual societies; and for connected purposes.

Complementary to the UK, Hungarian experts assure that data stored in the cloud should be protected from unauthorized access/modification and its availability ensured since sufficient logical data access controls is considered as one of the data security requirements within its scope of authority. Accordingly, the institution should establish a documented as well as approved user and access rights management procedure. Such procedures are at least on an equal level with the local procedure used for local systems, which should cover the processes for requesting approval, setting up access rights, regular review, and revocation. Although, privileged users are identified by a multifactor authentication, whereas the comprehensive and up-to-date record of authorized users and their access rights should be documented including user privileges. All the above mentioned should be monitored regularly. Similarly, the institution should obtain assurance that its resources located in the cloud are protected against unauthorized physical or logical access, damage, theft, and protection of the cloud service provider's data centers as much as the Physical access that is combined with environmental controls of physical resources (management of cryptographic keys).

German experts concentrate on the necessity of role and rights documentation, based on the business and security requirements of the cloud provider, as well as the policy for the management of the systems and data access authorizations. Such authorizations are responsible for rolling the granting and changing processes of data access authorizations for users under the responsibility of the cloud provider. At the same level, the perimeter of the premises/buildings, critical information, information systems, and other network infrastructure should be protected in a physically solid manner by means of appropriate security safeguards. In addition, structural, technical,

and organizational safeguards should protect sites from unwanted physical access or against natural threats such as fire, water, earthquakes, explosions, and civil disturbances.

4.2.1.5 Change Management and Continuity Plan

Commonly, risks can be introduced when changes are made to processes and procedures. UK expert authorities advise that firms should have a comprehensive change management process, establishing what provision has been made for making future changes to technology service provisions and how the testing of changes will be carried out. On the other hand, a firm should have arrangements to ensure that it can continue to function and meet its regulatory obligations if outsourced services are interrupted, considering the probability and impact of an unexpected disruption along with the importance of the documentation of the firm's strategy, including recovery from an event, plans for communicating, and regularly testing.

However, Hungarian authorities advise institutions to obtain regular assurance of the cloud service provider's compliance with the data security and protection requirements, which should be obtained at least annually or after any significant changes in the relevant business process, service, configuration or legal environment. Knowing that, some institutions might rely on independent third parties' audits or certifications for obtaining such kind of assurance.

German experts affirm the need to comply with the security targets in case of new developments and procurement of information systems. In case changes are made, the results should be categorized, prioritized, and subjected to tests during the development phase on the basis that a risk assessment is completed in order to obtain an appropriate authorization prior to making the

change available to the production environment. Furthermore, configuration of the objects, which might be affected by the change, should be assessed with regard to potential impacts not forgetting that emergency changes that should also be classified by the change manager who creates the change documentation before applying the change to the production environment. However, the main value concluded in the top management group who were identified as the process owners of the business continuity and contingency management also bear the responsibility for the establishment of processes in the company, as well as the compliance with the policies. Continually, they must ensure that adequate resources are available for an effective process. Based on the business impact analysis, a uniform framework for planning the business continuity and business plan should be introduced, documented, and applied in order to ensure that all plans are consistent

4.2.1.6 Exit plan

In the UK, experts clarify that firms need to ensure the capability of exiting plans of outsourcing without undue disruption to their provision of services or their compliance with regulatory regime. In that term, firms should have understandable, documented, and fully tested exit plans as well as termination agreement in order to maintain business continuity in case of transition to an alternative service provider. They should also consider obligations to ensure the outsourcing provider cooperate with the firm for a smooth transition and ensure the remote data from the service providers' systems on exit. Above all, it is imperative to monitor concentration risk and consider what actions should be taken in case of failure from the outsource provider.

Comparatively, Hungarian experts suggest that institutions should prepare an action plan and an exit strategy in order to mitigate risks, which in turn

should stipulate such service conditions allowing a facilitated exit from the cloud while providing the stored data in a format that can be interpreted and used irrespectively in the cloud service. This ensures and tests the operability of the impacted business processes in case the cloud service is discontinued with a risk proportionate method and frequency.

Finally, German experts advise that to maintain business continuity, the institutions should simply carry out the following several steps that should be defined in the action plan and exit strategy during the exit process:

- Installation of migration tools;
- Testing the downloading of the data in a test environment;
- Downloading the data in the production environment, and taking back the service based on the scripts;
- Validating based on the acceptance criteria; verifying the correctness of the data taken back; and closing the migration;
- Follow-up for fixing errors after migration;
- After the successful exit from the cloud, deleting the data at the service provider, including both live, backup, and archiving environments according to the contractual conditions

However, the service provider shall provide assurance (declaration) of deleting the data; Terminating the unnecessary IT and communication connections with the service provider.

4.2.2 Matrix: BSA Global Cloud Computing Scorecard (2016)

4.2.2.1 Discussion

The below matrix shows the response of the United Kingdom and Germany regarding several inquiries collected from the latest BSA survey study (2016) and merged with the Hungarian response which I have also collected from the Hungarian national bank authority through a survey and several meetings with the appropriate authorized personnel.

As observed in the table below, the first three sections display nearly similar responses among the three countries in various questions. Comparatively, noticeable differences occur in “Data Privacy” where data controllers are partially free from registration requirements in the UK, along with differences occurring in “Cyber Security” and “Intellectual Property Rights”, including “Cybercrime” (specifically the Budapest Convention consistency), particularly questioning law concerning cloud computing services and data transmission, additional to their policies, and criminal sanctions of copyrights on internet.

Questionnaire & Responses:

Nu	Question	UK	Germany	Hungary
Data Privacy				
1	Are there laws or regulations governing the collection, use, or other processing of personal information?	YES	YES	YES
2	Is the privacy law compatible with the Privacy Principles in the EU Data Protection Directive?	YES	YES	YES
3	Is the privacy law compatible with the Privacy Principles in the APEC Privacy Framework?	YES	YES	YES
4	Is an independent private right of action available for breaches of data privacy?	Available	Available	Available
5	Is there an effective agency (or regulator) tasked with the enforcement of privacy laws?	Sectorial Regulator	National Regulator	National Regulator
6	Are data controllers free from registration requirements?	Partial	Not Free	Not Free
7	Are cross-border transfers free from registration requirements?	YES	YES	YES
8	Is there a breach notification law?	Partial	Partial	Partial
SECURITY				
9	Is there a law or regulation that gives electronic signatures clear legal weight?	YES	YES	YES
10	Are ISPs and content service providers free from mandatory filtering or censoring?	YES	Partial	YES
11	Are there laws or enforceable codes containing general security requirements for digital data hosting and cloud service providers?	Limited coverage in legislation	Limited coverage in legislation	Limited coverage in legislation
CYBERCRIME				
12	Are cybercrime laws in place?	YES	YES	YES
13	What access do law enforcement authorities have to encrypted data held or transmitted by data hosting providers, carriers or other service providers?	Unlimited access	Access with a warrant	Not stated
14	Are cybercrime laws consistent with the Budapest Convention on Cybercrime?	YES	Partial	YES

INTELLECTUAL PROPERTY RIGHTS				
15	Is the country a member of the TRIPS Agreement?	YES	YES	YES
16	Have IP laws been enacted to implement TRIPS?	YES	YES	YES
17	Are criminal sanctions available for unauthorized making available (posting) of copyright holders' works on the Internet?	YES	Partial	Partial
18	Are there laws governing ISP liability for content that infringes copyright?	YES	YES	YES
19	Is there clear legal protection against misappropriation of cloud computing services, including effective enforcement?	Comprehensive protection	Comprehensive protection	Limited protection
Support for Industry-Led Standards & International Harmonization of Rules				
20	Are there laws, regulations or policies that establish a standard setting framework for interoperability and portability of data?	YES	YES	YES
21	Is there a regulatory body responsible for standards development for the country?	YES	YES	YES
22	Are international standards favored over domestic standards?	YES	YES	Partial
23	Does the government participate in international standards setting process?	YES	YES	YES
PROMOTING FREE TRADE				
24	Are cloud computing services able to operate free from laws or policies that mandate the use of certain products (including, but not limited to types of software), services, standards or technologies?	NO	YES	YES
25	Are cloud computing services able to operate free from laws or policies that establish preferences for certain products (including, but not limited to types of software), services, standards or technologies?	NO	Partial	Partial
26	Are "cloud computing" services able to operate free from laws that discriminate based on the nationality of the vendor, developer or service provider?	YES	YES	YES
IT READINESS, BROADBAND DEPLOYMENT				
27	Are there laws or policies that regulate the establishment of different service levels for data transmission based on the nature of data transmitted?	Regulation under consideration by government and extensive public debate	Regulation under consideration by government and extensive public debate	No

Table7: Global Cloud Computing Scorecard (2016)

Source: prepared by the author

4.2.2.2 Analysis Results:

The content of the basic questionnaire above was derived from the BSA 2016 Annual Global Cloud Computing Scorecard of which some major questions were collected to investigate the extent of aptitude, disposition, and inclination of those three EU countries for implementing and hosting Cloud computing services.

Questions have been weighted due to their importance and impact on cloud services. They have been divided into seven main fields, each of which containing several questions possessing different weights with a summation of 100% per section. Each field has its own different weight with a total of 100% based on COBIT 5 framework as the following: Data Privacy “17%”, Security “21%”, Cybercrime “22%”, Intellectual Property Rights “9%”, Support for industry led standards “9%”, Promoting Free Trade “8%”, and IT Readiness “14%”. See figures below.

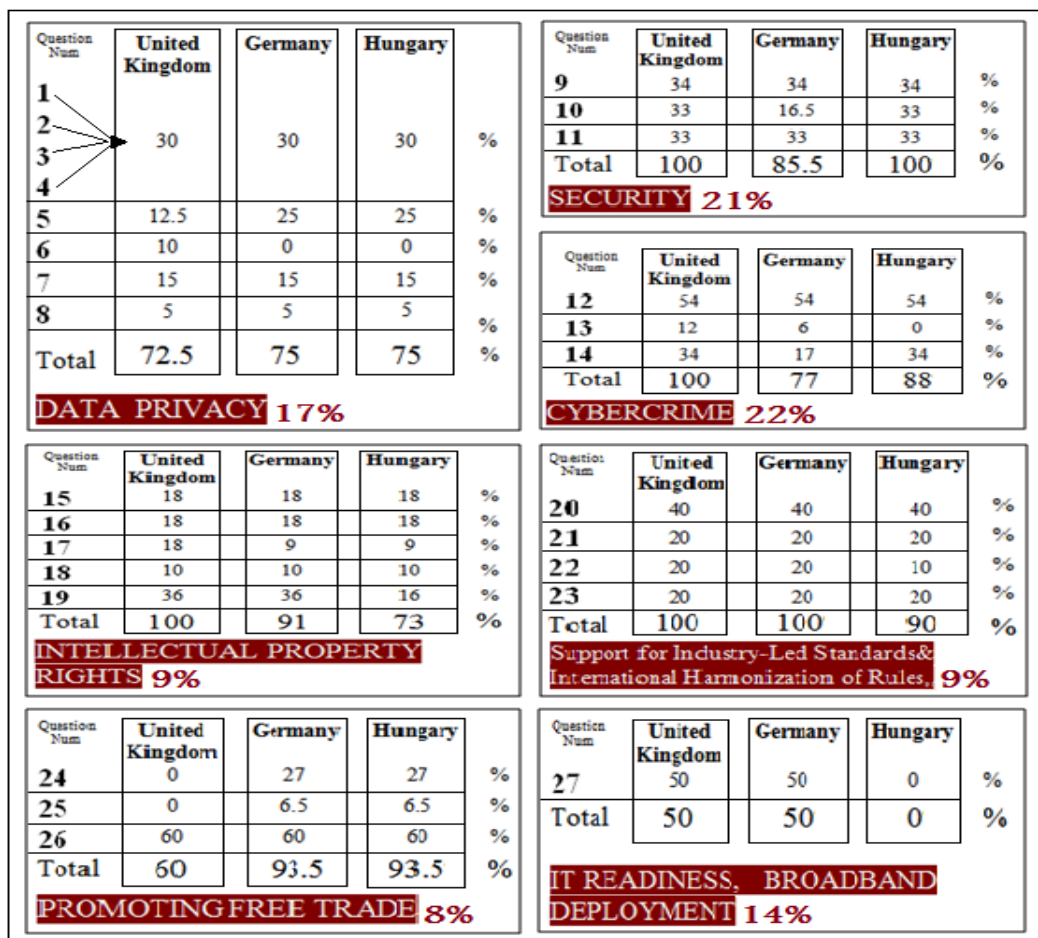


Figure 15: Cloud computing -Survey Results - 7 main fields
Source: prepared by the author

	United Kingdom				Germany				Hungary			
	weight	*	Importance	= Value	weight	*	Importance	= Value	weight	*	Importance	= Value
1. Data Privacy	72.5	*	17%	= 12.325	75	*	17%	= 12.750	75	*	17%	= 12.750
2. Security	100	*	21%	= 21	85.5	*	21%	= 17.955	100	*	21%	= 21
3. Cybercrime	100	*	22%	= 22	77	*	22%	= 16.940	88	*	22%	= 19.360
4. Intellectual Property Rights	100	*	9%	= 9	91	*	9%	= 8.190	73	*	9%	= 6.570
5. Support for Standards & international Rules	100	*	9%	= 9	100	*	9%	= 9	90	*	9%	= 8.10
6. Promoting Free Trade	60	*	8%	= 4.80	93.5	*	8%	= 7.480	93.5	*	8%	= 7.480
7. IT Readiness, BroadBand Deployment	50	*	14%	= 7	50	*	14%	= 7	0	*	14%	= 0
	Total Percentage % = 85.125				Total Percentage % = 79.315				Total Percentage % = 75.260			

Figure 16: Percentage of calculations - Cloud Computing

Source: prepared by the author

As a result, we can calculate the individual average for each section separately for each country aside, as follows:

- Germany total ratio = (79.315%)
- Hungary total Ratio = (75.260%)
- United Kingdom total ratio = (85.125%)

General Indicators	Germany	UK	Hungary
Population (millions) (2014)	83	63	9.8
Population Density (people per square km) (2014)	232	267	106
Per Capita GDP (US\$ 2014)	47.627	45.603	28,565
IT Service Exports (2014) (billions of US\$)	108.1	120.5	7.3
IT Readiness Indicators			
Internet Users (millions) (2014)	69	57	7.770
International Connectivity Score (2014) (Score is out of 10)	5.42	5.90	4.2
International Internet Bandwidth (2014) (bits per second per Internet user)	145.990	429.830	154,765
Fixed Broadband Subscriptions (millions) (2014)	29	23	2.8
Active Mobile Broadband Subscriptions per 100 inhabitants (2014)	64	89	41
Number of Active Mobile Broadband Subscriptions (millions) (2014)	53	56	4
Indicators values were collected from the BSA annual report merged with the values collected from the authorized parties in Hungary such as (MNB) the National Bank of Hungary			

Table 8: Important Indicators, IT Readiness (Germany, United Kingdom, Hungary) (cloud computing) (See in [23-25]). Source: prepared by the author

The above values show that United Kingdom is still considered as one of the leading countries concerning readiness and showing ability of implementing such cloud services. Nevertheless, Germany highly competes with the others in some major fields such as “Data Privacy” and “Promoting Free Trade”, where the country rises above the UK. Furthermore, it is also worth mentioning that “Data Privacy” is considered as one of the most important requirements for a healthy implementation process of Cloud solutions. Finally, due to the previous values, Hungary notably supersedes the other two competing countries in that regard, defeating Germany in two other fields (“Security” and “Cybercrime”).

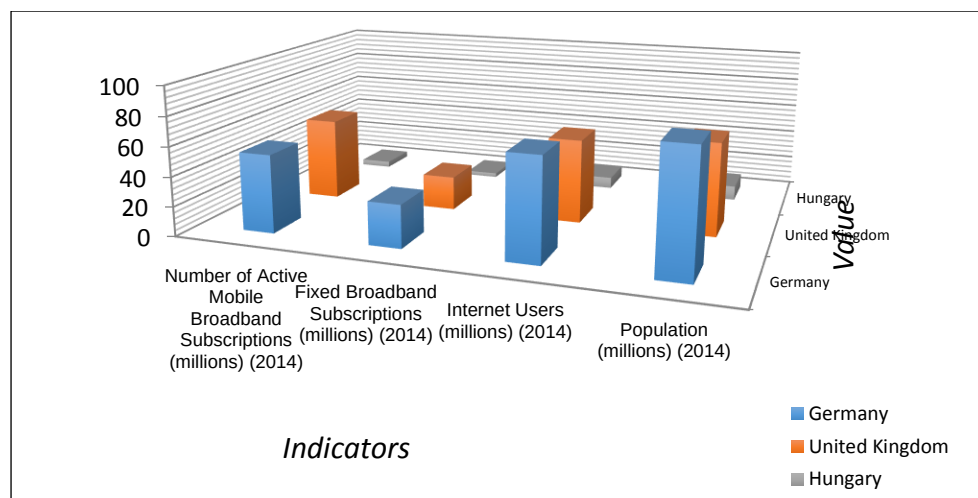


Figure 17: Population Indicator versus Internet (cloud computing)
Source: prepared by the author

The chart above (Figure 17) shows the population in the three countries mentioned earlier compared to the number of internet users, which represents almost one third of the total number of the internet users that are considered as fixed broadband subscribers, while nearly two-thirds of the total numbers of internet users are considered as mobile internet users of all types.

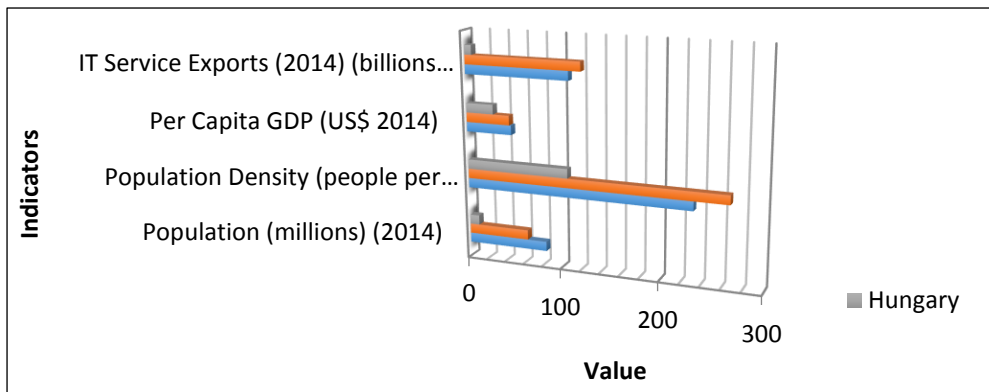


Figure 18: Population Indicator versus GDP (cloud computing)
Source: prepared by the author

As shown in the chart above (Figure 18), the population of each country compared to the population density per each square kilometer provides a general perception of the difficulty of delivering internet services according to the population sample while also maintaining the security of information without preventing penetration. Furthermore, the graph shows the differences in the expected growth of the average real GDP per capita compared to the total annual export volume for 2014 in IT services, taking into account the services of cloud computing, which is considered one of the leading services in recent years.

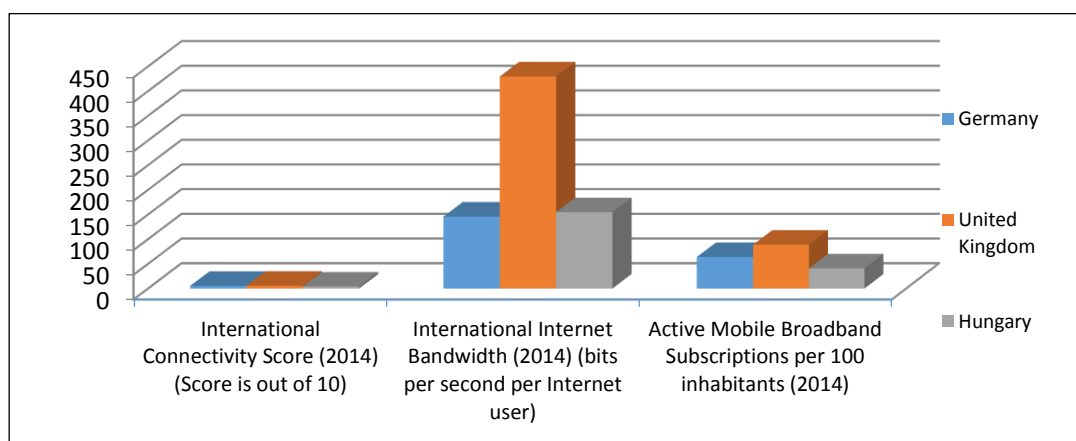


Figure 19: International Internet Bandwidth versus Connectivity score
Source: prepared by the author

The chart above (Figure 19) clarifies the total active mobile broadband subscription percentage as per each country showing that the United Kingdom ranked in first place by having the largest number of active mobile broadband subscriptions. Additionally, it had the first rank by adopting the highest international internet bandwidth as well as the international connectivity score in 2014, which gives us an indication regarding the reason of why the UK is considered one of the top leading countries in the matter of regulating and implementing such cloud computing services.

4.3 IT Operational risk

4.3.1 Discussions &Comparison study

The previously conducted survey, related to the IT Operational Risk topic, targeted 26 banks in the Jordanian financial sector asking several questions regarding three main event types related to the operational risk role of work according to Basel II and other international standards’ instructions. Twenty-two banks answered and their responses were received and collected successfully, as seen in the prepared figures and results below:

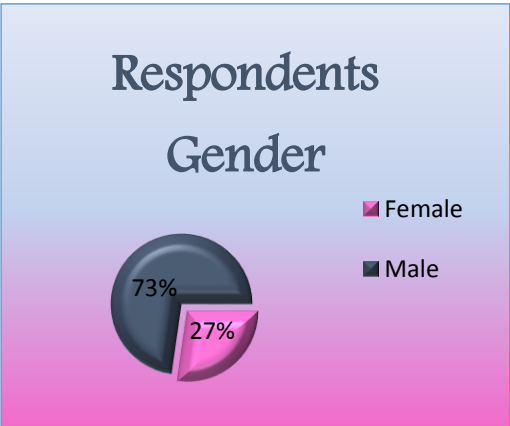


Figure 20: Respondents ‘gender
Source: prepared by the author



Figure 21: Respondents’ job titles
Source: prepared by the author

As shown above (Figure 20), more than 75% of the respondents were of the male gender opposed to 27% of the female gender. Furthermore, 18.2 % of the respondents hold a managerial position with 6-10 years of experience. Adversely, the largest amount of the respondents represents managers with experience of approximately 11-15 years. Finally, this figure assures that most of the interested participants were regular employees with experience from 3-5 years.

Data were Collected from my survey which targeted all of the Jordanian Banks covering the period from (2016 -2018)

Event Type: External Fraud

	Lower Bound	Frequency	Individual Loss	Maximum Loss
Mean	985.38	8.5	3259.18	20761.59
Standard deviation	1276.04	6.72	5446.51	22973.95

Log-normal distribution
Results

Calculation	Greater
σ_1 2.34	2.34
σ_2 1.58	
μ_1 5.36	6.85
μ_2 6.85	

Event Type: Damage To Physical Assests

	Lower Bound	Frequency	Individual Loss	Maximum Loss
Mean	1580.8	10.09	3009	18435
Standard deviation	4259.58	8.84	4271.32	31959.48

Calculation	Greater
σ_1 2.42	2.42
σ_2 1.5	
μ_1 5.08	6.88
μ_2 6.88	

Event Type: Business Disruption and Systems Failures

	Lower Bound	Frequency	Individual Loss	Maximum Loss
Mean	868.4	12.54	3272.72	18261.36
Standard deviation	1149.84	11.29	3288.35	17826.29

Calculation	Greater
σ_1 2.59	2.59
σ_2 1.33	
μ_1 4.74	7.21
μ_2 7.21	

The below Data were Collected from a Hungarian study targeting most of the Hungarian banks and covering the period from 2009 - 2012 / Reference: PHD Thesis – University of Debrecen – Gabor Nagy

Event Types	Mean	Standard Division	Median	Maximum loss
External Fraud	11468	93684	562	1247836
Damaged to Physical Assets	982	2670	504	58952
Business Disruption & System Failures	3671	23658	421	325248

Figure 22: Results derived from survey - Log-normal distribution (IT Op. Risk)
Source: prepared by the author (See in [148])

As observed from Figure 22, some main results have been concluded as the following:

- For the first event type “External Fraud”, the figure highlights that the (Average) mean value of the lower bound is derived by a calculation completed by all of the banks equaling 985.38 JODs. This clarifies that the Jordanian banks do not acknowledge a loss incident less than the average of 985.38 JODs. Given that, the standard deviation value comes to 1276.04 JODs indicating an estimation showing large differences in loss values as the banks have different regulations.
- Regarding the “Frequency” column, it is defined as the number of occurrences repeated in a specific event type where it shows that the Mean value (as per the estimation by the specialist overlooking the “External Fraud” event type) equals 8.5 with a standard deviation value of 6.7, which represents the normal case in most of the Jordanian banks.
- Regarding the “Individual Loss” column, it is defined as the average expected amount of individual losses related to a certain event type. Specifically, in our case, we can conclude that the mean value (as per the estimation of specialists regarding this specific event type) equals 3259.18 JODs, while the standard deviation value equals 5446.51 JODs which clearly shows a large value of standard deviation; proving a large difference in the estimated values related to this section remain.
- Regarding the “Maximum Loss” column, it is defined as the expected amount of the worst / largest loss. In our case, 20761.59 JODs is equal to the largest loss related to the “External Fraud” event type.
- The highest mean value (as per the estimation of specialists) based on the expected annual values of lower bound belongs to the “Damaged to

- Physical Assets” event type with a large standard deviation value equal to 4259.58 JODs.
- The lowest mean value estimated annually for the lower bound is related to the “Business Disruption and System Failure” event type. This gives a direct indicator that the Jordanian banks concentrate on the importance of this specific event type including any other losses or incidents related to this event type due to its high sensitivity and impact on the daily work process in any institution.
 - Furthermore, the highest mean value estimated for the annual frequency segment (as per the estimation of the specialists) belongs to the “Business Disruption and System Failure” event type due to its lowest values of estimation linked to the “Lower Bound “segment which gives more chance to count additional incidences related to this event type.
 - Vice versa, while keeping in consideration what was indicated in the external fraud section, the “Damage to Physical Assets” event type has been ranked in the middle range between both previously mentioned event types.
 - Thus, it is evident that all of the estimations of the specialists, regarding the “Individual Loss” and “Maximum Loss” segments, are similar in values. Despite the minor differences in the maximum loss related to the “External Fraud” event type equaling 20761.59 JOD’s, it proves that most of the banks grade the losses of this event type as one of the most expensive losses based on the large amount of fraud occurring recently in the Jordanian market, especially the ones related to the IT operations.
 - Moreover, one of the lowest estimated mean values of the individual loss segment relates to the “Damage of the Physical Assets” event type

clearly clarifying that such incidences are less harmful and less expensive than the others are.

larger Result		Lower Estimation		Higher Estimation	
External Fraud					
Monte Carlo		Monte Carlo		Monte Carlo	
lam	8.5	lam	7	lam	15
mu	5.36	mu	5.36	mu	5.36
sigma	2.34	sigma	2.34	sigma	2.34
M	1000000	M	1000000	M	1000000
Quantile	99.90%	Quantile	99.90%	Quantile	99.90%
Reserve	1226619	Reserve	1056908	Reserve	1638737
Damage To Physical Assests					
Monte Carlo		Monte Carlo		Monte Carlo	
lam	10.09	lam	8.99	lam	17
mu	5.08	mu	5.08	mu	5.08
sigma	2.42	sigma	2.42	sigma	2.42
M	1000000	M	1000000	M	1000000
Quantile	99.90%	Quantile	99.90%	Quantile	99.90%
Reserve	1331915	Reserve	1252993	Reserve	1807299
Business Disruption and Systems Failures					
Monte Carlo		Monte Carlo		Monte Carlo	
lam	12.54	lam	10	lam	20
mu	4.74	mu	4.74	mu	4.74
sigma	2.59	sigma	2.59	sigma	2.59
M	1000000	M	1000000	M	1000000
Quantile	99.90%	Quantile	99.90%	Quantile	99.90%
Reserve	2033095	Reserve	1774688	Reserve	2773473

Figure 23: Main events types results (IT Operational Risk)

Source: prepared by the author

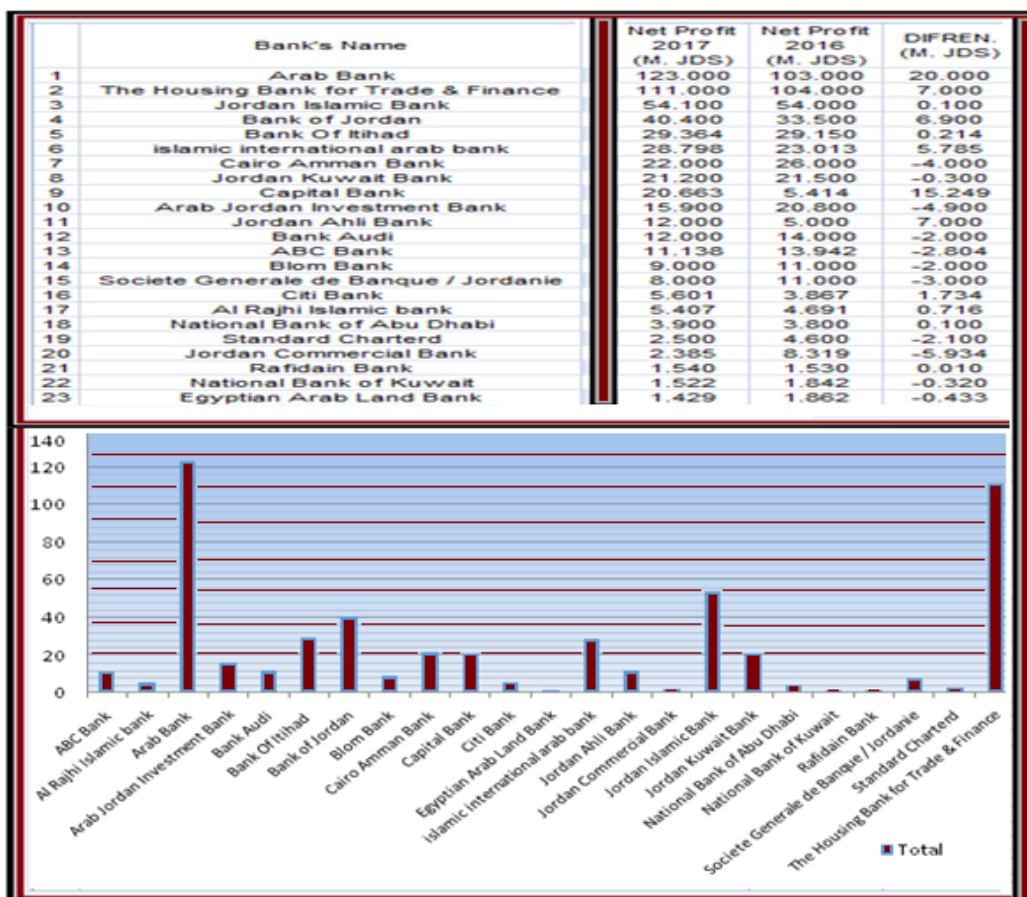


Figure 24: Jordanian banks net profit after Tax (in Million JODS)

Source: prepared by the author

- As shown above in Figure 23, the average amount of Capital (Reserve) linked to the “Business Disruption and Systems Failures” event type in all of the Jordanian banks has been estimated by specialists totaling the amount of “2,033,095” JODs.
- In order to keep confidentiality for the Jordanian banks, it was prevented by the security protocols to expose the specific values of reserves related to each bank individually. Therefore, it was allowed only to show the total of the estimated values related to all of the Jordanian banks.

For retaining more acute results, I assumed that the specialists have underestimated the values of losses related to the previously mentioned event types and based on that, similar calculations were completed using the same variables but changing the LAM (Frequency) value with a lower estimation on one side and a higher estimation on the other, resulting with the following:

- By estimating the LAM (frequency) segment with a lower value, the reserves slightly change with low effect on the essential calculation; but in contrast, the high estimation of the LAM (frequency) segment will significantly be affected with a higher value of needed reserves.
- Consequently, there is a definite risk when underestimating the volume of loss caused by such event types since such an act would result in a massively negative effect on the business role inside any institution, while noting that a high level of awareness is highly needed in that topic.

4.4 COBIT 5 Framework

As mentioned previously, the conducted survey focused on representing the 37 main suppositions derived from the five main processes (APO - BAI - DSS – MEA - EDM) and divided into 127 questions measuring the Jordanian bank's compliance to the CBJ regulations related to the COBIT 5 Framework, as well as its reflection on the financial performance of all the Jordanian banks. All answers were collected and analyzed using SPSS tool for more certainty and accuracy. Results showed the following: -

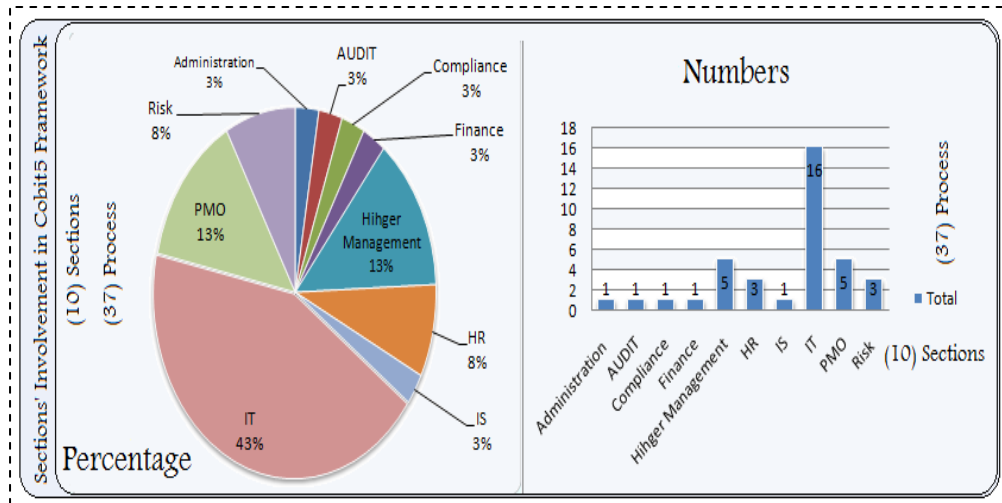


Figure 25: Bank's Related Departments throughout COBIT 5's implementation phase. Source: prepared by the author

- Noticeably in the COBIT 5 framework, the Information Technology is one of the most involved departments inside any institution during the implementation phase. Accordingly, 43% of the processes in COBIT 5 framework are related to the IT division (as shown above in Figure 25).
- Additionally, some institutions in the Jordanian banks' sector considered the Project Management Department as the second most involved department due to its essential role that would affect the whole work process in any organization. Keeping in consideration that the board/higher management also holds a larger responsibility according to the Governance processes (EDMs) related to the COBIT 5 framework, which is due to its genuine relation with the IT Governance committee including all of the related executives and stakeholders, headed by the general manager of the firm.

Gender	Bank Name	Academic Qualification	Professional Work Experience	Job Title
Female	AB #####	Bachelor degree	11 - 15 Years	Risk Department - IT Operational Risk Manager
Female	Ca #####	Bachelor degree	11 - 15 Years	Risk Department - IT Operational Risk Manager
Female	Eg #####	Master Degree	11 - 15 Years	Risk Department - IT Operational Risk Manager
Female	Na #####	Bachelor degree	11 - 15 Years	Risk Department - IT Operational Risk Manager
Female	So #####	Master Degree	21 - 25 Years	Risk Department - IT Operational Risk Manager
Female	Is #####	Bachelor degree	6 - 10 Years	Risk Department - IT Operational Risk Manager
Male	Jo #####	Bachelor degree	21 - 25 Years	IT Department - Manager
Male	Sa #####	Bachelor degree	6 - 10 Years	IT Department - Manager
Male	St #####	Bachelor degree	16 - 20 Years	IT Department - Executive Manager
Male	Th #####	Bachelor degree	16 - 20 Years	IT Department - Executive Manager
Female	Bl #####	Master Degree	21 - 25 Years	IT Department - Executive Manager
Male	Ar #####	Bachelor degree	21 - 25 Years	IS Executive Manager
Female	In #####	Bachelor degree	11 - 15 Years	IS Department - Manager
Male	Na #####	Master Degree	11 - 15 Years	IS Department - Manager
Male	Jo #####	Master Degree	16 - 20 Years	IS Department - Manager
Male	Ba #####	Bachelor degree	3 - 5 Years	Information Security Senior Officer - Risk Department
Male	Ci #####	Bachelor degree	3 - 5 Years	Information Security Senior Officer - Risk Department
Male	Ba #####	Master Degree	11 - 15 Years	Information Security and QA Unit Head
Male	Jo #####	Bachelor degree	21 - 25 Years	I.T Consultant
Male	Ca #####	Bachelor degree	11 - 15 Years	Audit Department - IT Auditor
Male	Jo #####	PhD Degree	16 - 20 Years	Audit Department - IT Auditor
Male	Ar #####	Bachelor degree	6 - 10 Years	Audit Department - IT Auditor
Male	Ba #####	Bachelor degree	6 - 10 Years	Audit Department - IT Auditor

Table 10: Survey participant's information (COBIT 5)

Source: prepared by the author

Based on Figure 10 above, the table shows results with some detailed information related to the respondents of the 23 banks surveyed, showing that the total number of banks in Jordan are 26, divided into local, foreign, and Islamic banks. Therefore, it is worth mentioning that all of the banks' names had been encoded and not specified in some parts of the analysis due to the privacy agreements with the legislative authorities.

4.4.1 Descriptive Analyses for Population's Respondents

The characteristics of the respondents in the selected population were found within the research conducted on 26 Banks operating effectively at the level of the Hashemite Kingdom of Jordan, where all the banks operate under the umbrella of the Central Bank of Jordan.

4.4.2 Descriptive Analysis according to the Gender:

Gender			
			Percentage
Valid	Male		65%
	Female		35%
	Total		100%

Table 11: Respondents to gender (COBIT 5)

Source: Prepared by the author based on SPSS analysis outputs

The table above describes the respondents' gender; with males representing a percentage of 65% that have responded to the questionnaire opposed to the number of female respondents with a percentage of 35%.

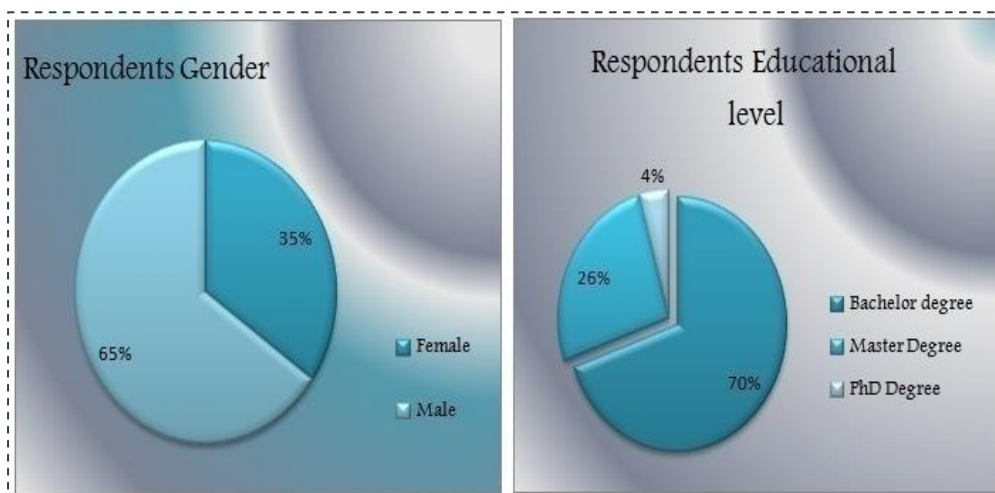


Figure 26: Respondents to Educational level & Gender (COBIT 5)

Source: prepared by the author

4.4.3 Descriptive Analyses according to the Educational Levels:

Academic Qualification		
		Percentage
Valid	Bachelor's degree	70%
	Master's degree	26%
	PhD Degree	4%
	Total	100%

Table 12: Respondents to Academic Qualification (COBIT 5)
Source: Prepared by the author based on SPSS analysis outputs

Table 12 describes the number of respondents according to their academic qualification with the majority of them representing approximately 70% holding bachelor's degrees, respondents holding a master's degree with 26%, and a PhD Degree with 4%.

4.4.4 Descriptive Analysis according to the Professional Work Experience:

Professional Work Experience		
		Percentage
Valid	11-15 Years	35%
	16-20 Years	17%
	21-25 Years	22%
	3-5 Years	9%
	6-10 Years	17%
Total		100%

Table 13: Respondents to professional work experience (COBIT 5)
Source: Prepared by the author based on SPSS analysis outputs

Table 13 shows that the largest group of respondents represented 11-15 years of professional experience as a group of 35%, followed by a group of 22% representing professional experience of 21-25 years.

Job Title		
		Percentage
Valid	Audit Department - IT Auditor	17%
	I.T Consultant	4%
	Information Security and QA Unit Head	4%
	Information Security Senior Officer - Risk Dep.	8%
	IS Department – Manager	13%
	IS Executive Manager	4%
	IT Department - Executive Manager	13%
	IT Department - Manager	8%
	Risk Department - IT Operational Risk Manager	29%
Total		100%

Table 14: Respondents to job title (COBIT 5)

Source: Prepared by the author based on SPSS analysis outputs

4.4.5 Descriptive Analysis according to the Job Title:

Table 14 above shows that the largest number of respondents according to the job title belongs to the Risk Department - IT Operational Risk Manager representing 29% of the respondents, which indicates that according to the researcher's knowledge, the most concerned sect are the managers related to the Risk Department.

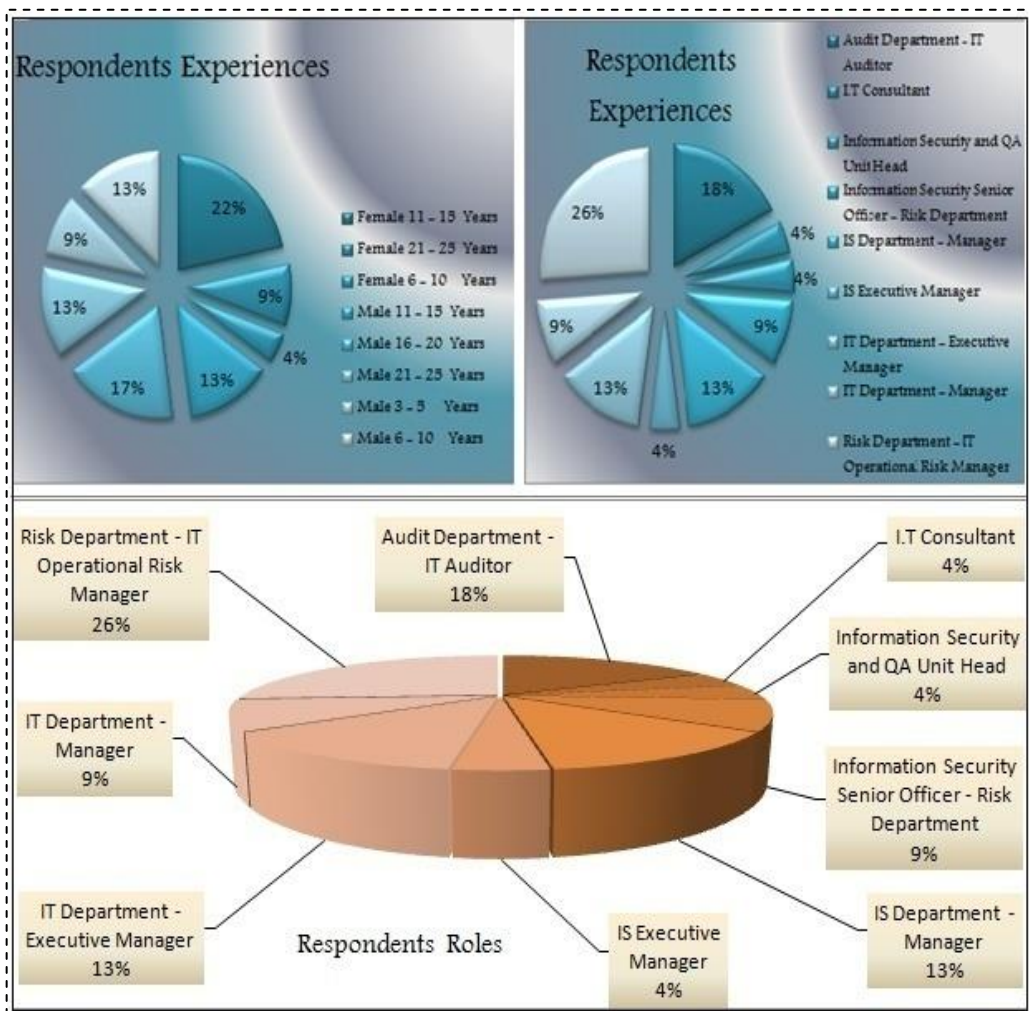


Figure27: Respondents Work Experiences, Professions & Positions (COBIT 5)
Source : Prepared by the author

Figure 27 shows that the most interested respondents that participated in such a survey from the banks' employees were females with an experience ranging between 11-15 years of work, followed by males with an experience ranging between 16-20 years of work. Recognizing that the percentage of the female employees in the Jordanian bank's sector exceeded 38% according to the latest declaration from the ABJ (The Association of Banks in Jordan), it

is clear that the above representation of 26% of the interested respondents were from the Risk Departments who are in turn responsible for the IT Operational Risk Division, followed by the Information Security Department, and finally the Information Technology & Audit Departments.

4.4.6 Descriptive Analyses for Variables Relation ships :

- The Banks and ROE / ROA

	Bank's Name	ROA 2017	ROA 2016	DIFREN.	ROE 2017	ROE 2016	DIFREN.	Net Profit 2017 (M. JDS)	Net Profit 2016 (M. JDS)	DIFREN. (M. JDS)
1	Arab Bank	1.350%	1.140%	0.210%	12.740%	10.770%	1.970%	123.000	103.000	20.000
2	The Housing Bank for Trade & Finance	1.600%	1.530%	0.070%	11.500%	11.090%	0.410%	111.000	104.000	7.000
3	Jordan Islamic Bank	1.300%	1.370%	-0.070%	15.090%	16.520%	-1.430%	54.100	54.000	0.100
4	Bank of Jordan	1.920%	1.727%	0.193%	9.930%	8.902%	1.028%	40.400	33.500	6.900
5	Bank Of Itihad	1.120%	1.180%	-0.060%	8.730%	9.770%	-1.040%	29.364	29.150	0.214
6	islamic international arab bank	1.400%	1.200%	0.200%	17.400%	15.600%	1.800%	28.798	23.013	5.785
7	Cairo Amman Bank	1.080%	1.270%	-0.190%	7.550%	14.400%	-6.850%	22.000	26.000	-4.000
8	Jordan Kuwait Bank	0.840%	0.860%	-0.020%	4.800%	4.970%	-0.170%	21.200	21.500	-0.300
9	Capital Bank	1.150%	0.300%	0.850%	7.870%	2.125%	5.745%	20.663	5.414	15.249
10	Arab Jordan Investment Bank	0.940%	1.300%	-0.360%	8.800%	10.600%	-1.800%	15.900	20.800	-4.900
11	Jordan Ahli Bank	0.480%	0.200%	0.280%	4.020%	1.580%	2.440%	12.000	5.000	7.000
12	Bank Audi	1.500%	1.620%	-0.120%	11.560%	13.700%	-2.140%	12.000	14.000	-2.000
13	ABC Bank	1.010%	1.320%	-0.310%	7.550%	9.630%	-2.080%	11.138	13.942	-2.804
14	Blom Bank	1.100%	1.330%	-0.230%	10.100%	12.710%	-2.610%	9.000	11.000	-2.000
15	Societe Generale de Banque / Jordanie	0.590%	0.870%	-0.280%	6.000%	8.740%	-2.740%	8.000	11.000	-3.000
16	Citi Bank	1.620%	1.130%	0.490%	8.440%	5.990%	2.450%	5.601	3.867	1.734
17	Al Rajhi Islamic bank	1.220%	1.060%	0.160%	9.230%	8.410%	0.820%	5.407	4.691	0.716
18	National Bank of Abu Dhabi	1.180%	1.030%	0.150%	6.100%	6.300%	-0.200%	3.900	3.800	0.100
19	Standard Chartered	0.590%	1.090%	-0.500%	3.030%	5.480%	-2.450%	2.500	4.600	-2.100
20	Jordan Commercial Bank	0.200%	0.568%	-0.368%	1.680%	6.070%	-4.390%	2.385	8.319	-5.934
21	Rafidain Bank	1.100%	1.100%	0.000%	2.100%	2.200%	-0.100%	1.540	1.530	0.010
22	National Bank of Kuwait	0.530%	0.610%	-0.080%	1.770%	2.200%	-0.430%	1.522	1.842	-0.320
23	Egyptian Arab Land Bank	0.420%	0.540%	-0.120%	2.370%	3.220%	-0.850%	1.429	1.862	-0.433

Table 15: Financial performance ratios for Jordanian banking sector (2016-2017)
Source: prepared by the author

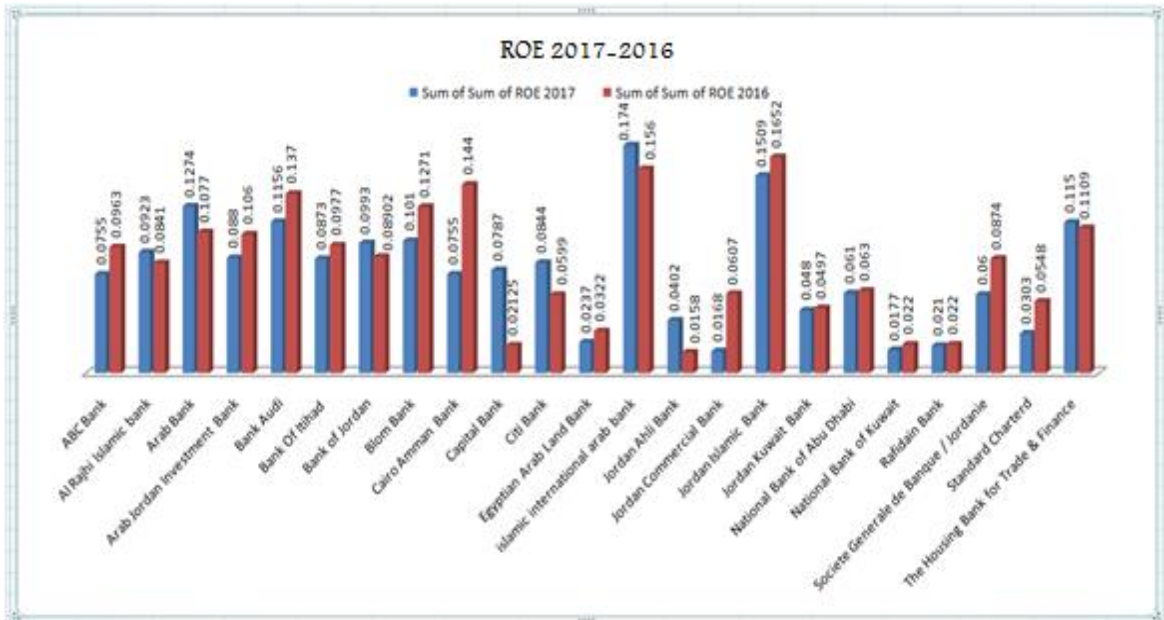


Figure 28: ROE Compared results according to 2016 – 2017
Source: prepared by the author

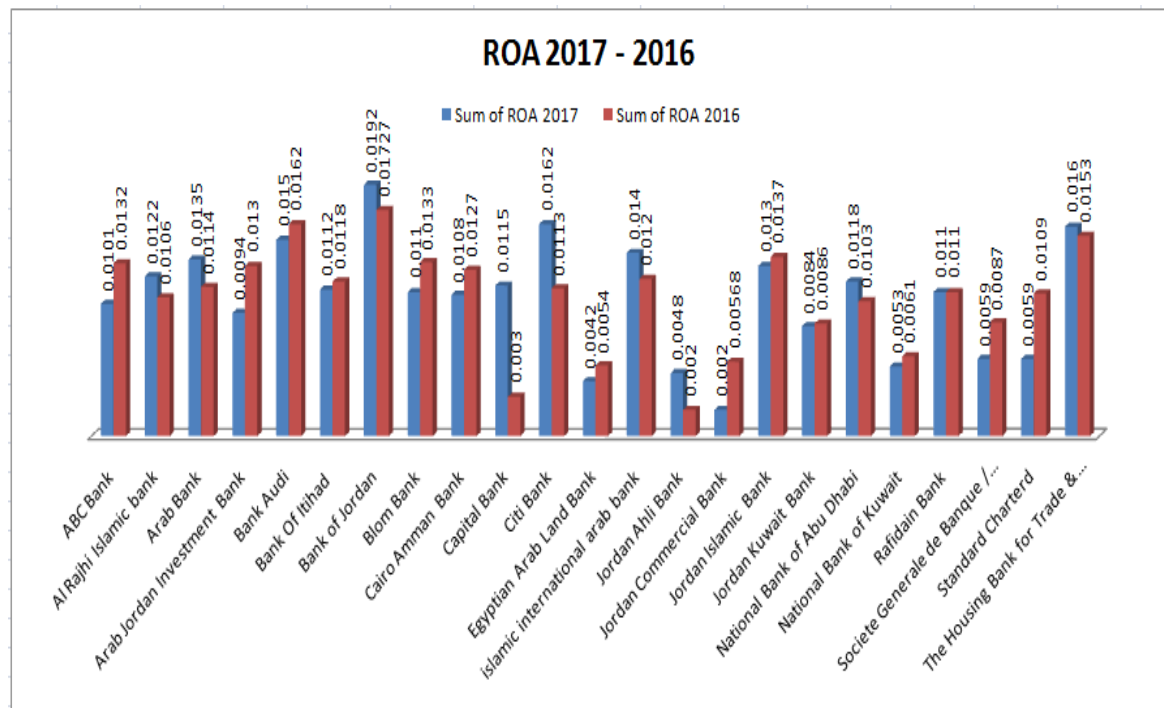


Figure 29: ROA Compared results according to 2016 – 2017
Source: prepared by the author

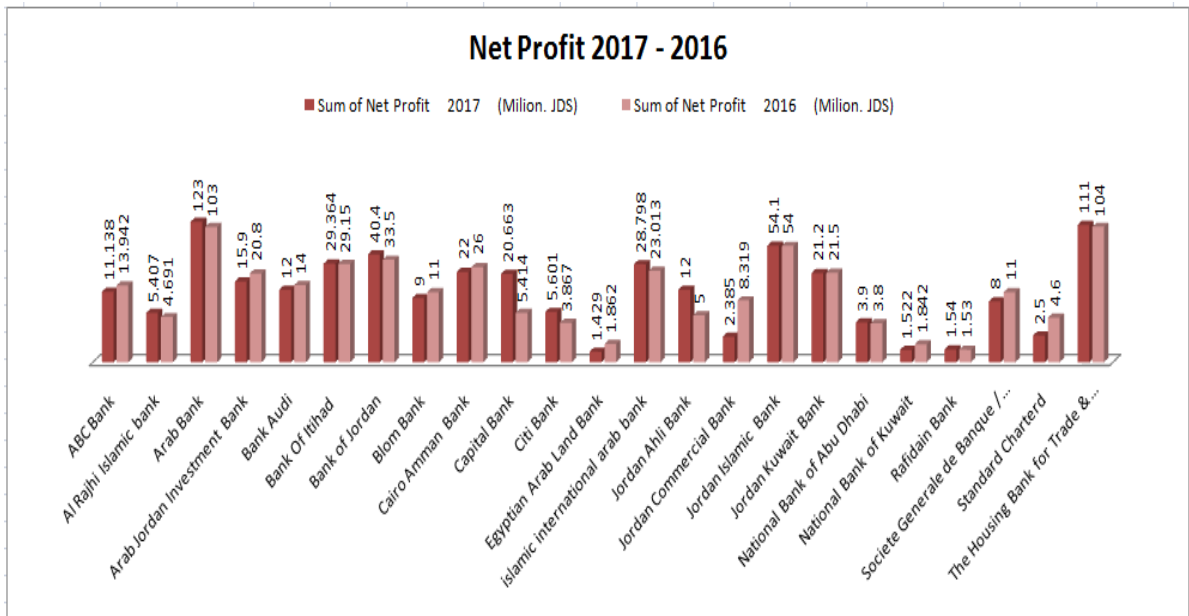


Figure 30: Net Profit Compared results according to 2016 – 2017

Source: prepared by the author

According to the figures above (28,29,30) and based on the CBJ and ABJ accurate financial statements, only 8 out of 23 ROEs' results related to the Jordanian banks had increased during 2017. In turn, only 9 out of 23 ROAs' results related to this exact sample increased in 2017, and 11 out of 23 Jordanian Banks enlarged its Net Profit values in 2017.

Table 16 below shows the results of the previously conducted survey indicating the deployment's maturity level of the COBIT 5 framework in the Jordanian banks' sector. It clarifies the mean values (Maturity levels) for the 37 processes divided into 5 main sections (APO, BAI, DSS, MEA, and EDM).

Process Name	APO01	APO02	APO03	APO04	APO05	APO06	APO07	APO08	APO09	APO10	APO11	APO12	APO13	APO	
														Total	
AVG	2.8	3.2	2.8	2.9	2.9	3.0	3.1	3.1	3.1	3.0	2.9	2.8	2.9	3.0	
Median	2.5	3.0	2.8	3.0	2.8	3.0	3.0	3.0	3.0	3.0	3.0	2.8	2.7	2.9	
SD	0.539	0.557	0.454	0.428	0.460	0.439	0.608	0.410	0.411	0.501	0.518	0.591	0.435	0.5	
Process Name	BAI01	BAI02	BAI03	BAI04	BAI05	BAI06	BAI07	BAI08	BAI09	BAI10					BAI
											Total				
AVG	3.0	3.1	2.9	2.9	3.0	2.7	3.0	3.0	2.9	2.7	2.9				
Median	3.2	3.0	2.8	2.7	3.0	2.8	3.0	3.0	3.0	3.0	2.9				
SD	0.529	0.423	0.548	0.489	0.501	0.655	0.402	0.357	0.443	0.448	0.5				
Process Name	DSS01	DSS02	DSS03	DSS04	DSS05	DSS06 <td colspan="8"></td> <th>DSS</th>									DSS
						Total									
AVG	2.9	2.9	2.7	3.0	3.0	2.9	2.9								
Median	3.0	3.0	3.0	3.0	3.0	2.7	2.9								
SD	0.432	0.413	0.558	0.396	0.388	0.356	0.4								
Process Name	MEA01	MEA02	MEA03 <td colspan="11"></td> <th>MEA</th>												MEA
			Total												
AVG	2.7	2.7	3.1	2.8											
Median	2.8	2.8	3.0	2.9											
SD	0.670	0.664	0.397	0.6											
Process Name	EDM01	EDM02	EDM03	EDM04	EDM05 <td colspan="9"></td> <th>EDM</th>										EDM
					Total										
AVG	2.8	3.0	3.1	2.8	2.9	2.9									
Median	3.0	3.0	3.0	2.7	3.0	2.9									
SD	0.548	0.355	0.392	0.409	0.477	0.4									

Table 16: COBIT 5 Processes (AVG, Mean, SD) Table - Jordanian Banks' Sector. (COBIT 5). Source: prepared by the author.

Table 16 above shows the results of the previously conducted survey indicating the deployment's maturity level of the COBIT 5 framework in the Jordanian banks' sector. It clarifies the mean values (Maturity levels) for the 37 processes divided into 5 main sections (APO, BAI, DSS, MEA, and EDM).

The right section of the table clarifies the 5 main values of maturity levels separated into the main sections of the COBIT 5 framework according to the 23 banks responses, as previously mentioned. The table clearly shows that the higher value belongs to the APO main process, while the lowest value belongs to the MEA main process. Conclusively, in the initial stage of the project the majority of the Jordanian banks are concentrating on deploying the APO (practical) part of the COBIT 5 framework (Align, Plan, and Orgnize) rather than the MEA (control) part of the framework process (Monitor, Evaluate, and Assess).

							Process Level		Department Level	
#	ID	Process Name	Responsible Department	Shared Responsibility	No.	Participant Percentage	Mean	SD	Av. Mean	Av. SD
1	APO10	Manage Suppliers	Admin Dep.	IT	1	2.70%	3.0	0.501	3.00	0.50
2	MEA02	Monitor, Evaluate and Assess the System of Internal Control	AUDIT	OP Risk	1	2.70%	2.7	0.664	2.70	0.66
3	MEA03	Monitor, Evaluate and Assess Compliance with External Requirements	Compliance	N/A	1	2.70%	3.1	0.397	3.10	0.40
4	APO06	Manage Budget and Costs	Finance	N/A		2.70%	3.0	0.439	3.00	0.44
5	EDM01	Ensure Governance Framework Setting and Maintenance	Higher Management	GM	5	13.51%	2.8	0.548	2.92	0.44
	EDM02	Ensure Benefits Delivery		PMO			3.0	0.355		
	EDM03	Ensure Risk Optimization		Risk			3.1	0.392		
	EDM04	Ensure Resource Optimization		HR			2.8	0.409		
	EDM05	Ensure Stakeholder Transparency		IT			2.9	0.477		
6	APO04	Manage Innovation	HR	PMO	3	8.11%	2.9	0.428	3.00	0.46
	APO07	Manage Human Resources	HR	N/A			3.1	0.608		
	BAI08	Manage Knowledge	HR	N/A			3.0	0.357		
7	APO13	Manage Security	IS	N/A		2.70%	2.9	0.435	2.90	0.44
8	APO01	Manage the IT Management Framework	IT	N/A	15	40.54%	2.8	0.539	2.91	0.48
	APO02	Manage Strategy	IT	N/A			3.2	0.557		
	APO08	Manage Relationships	IT	N/A			3.1	0.410		
	APO09	Manage Service Agreements	IT	N/A			3.1	0.411		
	APO11	Manage Quality	IT	N/A			2.9	0.518		
	BAI03	Manage Solutions Identification and Build	IT	N/A			2.9	0.548		
	BAI04	Manage Availability and Capacity	IT	N/A			2.9	0.489		
	BAI06	Manage Changes	IT	N/A			2.7	0.655		
	BAI07	Manage Change Acceptance and Transitioning	IT	N/A			3.0	0.402		
	BAI09	Manage Assets	IT	Admin Dep.			2.9	0.443		
	BAI10	Manage Configuration	IT	N/A			2.7	0.448		
	DSS01	Manage Operations	IT	N/A			2.9	0.432		
	DSS02	Manage Incidents and Service Requests	IT	N/A			2.9	0.413		
	DSS03	Manage Problems	IT	N/A			2.7	0.558		
	DSS05	Manage Security Services	IT	IS			3.0	0.388		
9	APO03	Manage Enterprise Architecture	PMO	N/A	6	16.22%	2.8	0.454	2.92	0.51
	APO05	Manage Portfolio	PMO	N/A			2.9	0.460		
	BAI01	Manage Programs and Projects	PMO	N/A			3.0	0.529		
	BAI02	Manage Requirements Definition	PMO	N/A			3.1	0.423		
	BAI05	Manage Organizational Change Enablement	PMO	N/A			3.0	0.501		
	MEA01	Monitor, Evaluate and Assess Performance and Conformance	PMO	N/A			2.7	0.670		
10	APO12	Manage Continuity	Risk	IS	3	8.11%	2.8	0.591	2.90	0.45

Table 17: Responsibility of departments according to COBIT 5 framework
Source: prepared by the author

As shown in Table 17 above, the basic information of relations between the 37 processes and the related departments according to its role in deploying COBIT 5 framework, clarifying several main issues as follows:

- The ID and the process name introduce each process individually.
- The columns “Responsible Department” and “Shared Responsibility” define the associated departments linked to the related processes according to its roles.
- The column “Number of Processes” defines the total associated processes to each department individually.
- The column “Participant Percentage” defines the percentage of related processes out of 37 processes divided as per the related department.
- The sectional column “Process Level” defines the mean and standard deviation as per each process individually.
- The column “General Department Level” defines the average mean and average standard deviation as per the department level.

4.4.7 Correlations

Basic forms of correlation coefficients (Pearson) were calculated to examine the strength and direction of the relationship between each set of variables. Correlation analysis is used to describe the strength and direction of the linear relationship between two variables. The Pearson correlation coefficient (r) can take on only values from -1.00 to +1.00. A correlation of +1.00 indicates a perfect positive correlation (i.e. as one variable increases, so too does the other) and a value of -1.00 indicates a perfect negative correlation (i.e. as one variable increases, the other decreases). Conversely, a correlation of zero indicates no linear relationship at all. I have tested the correlation connection between the independent variable revealed by the

COBIT Maturity level of the related departments in the banks (Admin, Audit, Compliance, Finance, Higher management, HR, IS, IT, PMO) and the dependent variable revealed by the financial performance indicators accredited by ABJ (Association of banks in Jordan) and CBJ (Central bank of Jordan) using SPSS.

Correlations Tables:

		Admin	Audit	Compliance	Finance	HM	HR	IS	Risk	PMO
Admin	Pearson Correlation		,633**	,477*	,636**	,790**	,722**	,620**	,728**	,677**
	Sig. (2-tailed)		,001	,021	,001	,000	,000	,002	,000	,000
	N		23	23	23	23	23	23	23	23
Audit	Pearson Correlation			-,006	,711**	,812**	,684**	,588**	,890**	,877**
	Sig. (2-tailed)			,980	,000	,000	,000	,003	,000	,000
	N			23	23	23	23	23	23	23
Compliance	Pearson Correlation				,098	,294	,271	,480*	,337	,249
	Sig. (2-tailed)				,658	,173	,212	,021	,116	,252
	N				23	23	23	23	23	23
Finance	Pearson Correlation					,746**	,598**	,416*	,696**	,637**
	Sig. (2-tailed)					,000	,003	,048	,000	,001
	N					23	23	23	23	23
Higher Management	Pearson Correlation						,576**	,590**	,841**	,848**
	Sig. (2-tailed)						,004	,003	,000	,000
	N						23	23	23	23
HR	Pearson Correlation							,773**	,733**	,688**
	Sig. (2-tailed)							,000	,000	,000
	N							23	23	23
IS	Pearson Correlation								,754**	,749**
	Sig. (2-tailed)								,000	,000
	N								23	23
IT	Pearson Correlation	,742**	,770**	,467*	,552**	,729**	,778**	,879**	,904**	,894**
	Sig. (2-tailed)	,000	,000	,025	,006	,000	,000	,000	,000	,000
	N	23	23	23	23	23	23	23	23	23

Table 18: Correlation between departments (COBIT 5)

Source: prepared by the author

The correlation shows that the Admin, Audit, Compliance, Finance, Higher management, HR, IS, IT, PMO, and Risk departments are

insignificantly correlated with ROA, ROE, and net profit related to the Banks Financial Performance in 2017. This is ordinary and expected since COBIT 5 Framework mainly affects some major set of policies and procedures related to IT or other related departments in any institution. Therefore, the revenue of implementing such a framework on any institution will not take place in the immediate foreground of the financial performance especially in the case of individual process application. Yet, it requires sufficient time in order to reap the results of applying the whole set of altered procedures that will affect the daily work practices of the related departments.

Keeping in consideration that such an act would lead to generate major outputs of work products and KPIs, they would yet to be measured depending on the actual performance and deliverables of each related department.

**. Correlation is significant at the 0.01 level (2-tailed).

*. Correlation is significant at the 0.05 level (2-tailed).

In addition, Table 18 concludes some of the relationship between the independent variables based on the IT Department is concluded as follows:

IT and admin

The correlation shows that IT is significantly and positively associated with the admin department. The statistical results indicate that there is a significant correlation (r) between the variables, (0.742).

IT and audit

The correlation shows that IT is significantly and positively associated with the audit department. The statistical results indicate that there is a significant correlation (r) between the variables, (0.770).

IT and compliance

The correlation shows that IT is significantly and positively associated with the compliance department. The statistical results indicate that there is a significant correlation (r) between the variables, (0.467).

IT and finance

The correlation shows that IT is significantly and positively associated with the Finance department. The statistical results indicate that there is a significant correlation (r) between the variables, (0.552).

IT and higher management

The correlation shows that IT is significantly and positively associated with the Higher Management. The statistical results indicate that there is a significant correlation (r) between the variables, (0.729).

IT and HR

The correlation shows that IT is significantly and positively associated with the HR department. The statistical results indicate that there is a significant correlation (r) between the variables, (0.778).

IT and IS

The correlation shows that IT is significantly and positively associated with the IS department. The statistical results indicate that there is a significant correlation (r) between the variables, (0.879).

IT and PMO

The correlation shows that IT is significantly and positively associated with the Project Management department. The statistical results indicate that there is a significant correlation (r) between the variables, (0.894).

IT and Risk

The correlation shows that IT is significantly and positively associated with the Risk department. The statistical results indicate that there is a significant correlation (r) between the variables, (0.904).

Furthermore, three main tables are included in the analysis part as follows (Paired Samples Statistics table, Paired Samples Correlations table, and Paired Samples Test table) showing descriptive statistics such as Mean, Sample Size, Standard Deviation, and Standard Error for each variable entered. Notably, the sample size here is 23 banks.

The implemented paired T-test can only use cases that have non-missing values for both variables while the Paired Samples Correlations shows the bivariate Pearson correlation coefficient (with a two-tailed test of significance) for each pair of variables entered.

Paired Samples Correlations (ROE, ROA, Net Profit)

Correlations

		Admin	Audit	Compliance	Finance	High - Mang.	HR	IS	IT	PMO
ROA_2017	Pearson Correlation	,197	-,165	,391	,155	,074	-	,170	,150	-,003
	Sig. (2 tailed)	,368	,452	,065	,479	,738	,931	,438	,496	,990
	N	23	23	23	23	23	23	23	23	23
ROA_2016	Pearson Correlation	-,010	-,031	,055	,118	,063	-,154	,052	,124	,098
	Sig. (2- tailed)	,964	,889	,802	,593	,776	,483	,814	,573	,656
	N	23	23	23	23	23	23	23	23	23
DIF_ROA	Pearson Correlation	,293	-,194	,484*	,067	,023	,174	,174	,051	-,132
	Sig. (2- tailed)	,174	,375	,019	,761	,916	,428	,426	,817	,549
	N	23	23	23	23	23	23	23	23	23
ROE_2017	Pearson Correlation	,196	-,073	,304	,266	,236	-,067	,130	,110	,106
	Sig. (2- tailed)	,370	,741	,158	,219	,278	,762	,554	,618	,630
	N	23	23	23	23	23	23	23	23	23
ROE_2016	Pearson Correlation	,094	,089	,067	,320	,280	-,072	,118	,177	,253
	Sig. (2- tailed)	,669	,685	,763	,137	,195	,745	,592	,420	,245
	N	23	23	23	23	23	23	23	23	23
DIF_ROE	Pearson Correlation	,157	-,273	,382	-,118	-,098	,015	,008	-,126	-,263
	Sig. (2- tailed)	,474	,207	,072	,592	,655	,946	,969	,568	,225
	N	23	23	23	23	23	23	23	23	23
Net_Profit_2017	Pearson Correlation	,171	,190	,020	,228	,264	,104	,136	,204	,223
	Sig. (2- tailed)	,435	,386	,929	,295	,223	,636	,537	,351	,306
	N	23	23	23	23	23	23	23	23	23
Net_Profit_2016	Pearson Correlation	,132	,219	-,069	,246	,275	,092	,122	,201	,247
	Sig. (2- tailed)	,550	,315	,756	,258	,203	,675	,579	,359	,257
	N	23	23	23	23	23	23	23	23	23
DIF_Profit	Pearson Correlation	,284	-,021	,417*	,055	,107	,116	,144	,138	,025
	Sig. (2- tailed)	,190	,926	,048	,802	,628	,597	,512	,531	,909
	N	23	23	23	23	23	23	23	23	23

Table 19: Paired Samples Correlations (ROE, ROA, Net Profit) (COBIT 5)

Source: prepared by the author

The Paired Samples Correlation table highlight the information that departments score as significantly positive correlated pointing out that the highest correlation found was between the IT Department and Risk Department showing a value of ($r = .904$).

Paired Samples Test (1)

Paired Departments		Paired Differences					t	Df	Sig
			Std. Deviation	Std. Error Mean	95% Confidence Interval of the Difference				
					Lower	Upper			
Pair 1	IT - Admin	,1156	,3384	,0706	-,0308	,2619	1,638	22	.116
Pair 2	IT - Audit	-,2504	,4582	,0955	-,4485	-,0522	-2,621	22	.016
Pair 3	IT - Compliance	,1953	,3827	,0798	,0298	,3608	2,447	22	.023
Pair 4	IT - Finance	,0866	,3783	,0789	-,0770	,2502	1,097	22	.284
Pair 5	IT - High. Management	-,0076	,2479	,0517	-,1148	,0996	-,148	22	.884
Pair 6	IT – HR	,0800	,2302	,0480	-,0195	,1796	1,668	22	.110
Pair 7	IT – IS	-,0439	,2122	,0442	-,1356	,0479	-,991	22	.332
Pair 8	IT – PMO	-,0117	,1726	,0360	-,0863	,0629	-,325	22	.748
Pair 9	IT – Risk	,0231	,1661	,0346	-,0487	,0949	,667	22	.512

Table 20: Paired Sample test based on IT Dep. (COBIT 5)

Source: prepared by the author

Paired Samples Test (2)

#	Paired Dep.	Sig. (2-tailed)
Pair 1	Audit - Admin	,003
Pair 2	Audit - Compliance	,012
Pair 3	Audit - Finance	,002
Pair 4	Audit - High Management	,014
Pair 5	Audit - HR	,004
Pair 6	Audit - IT	,016
Pair 7	Audit - PMO	,003
Pair 8	Audit - Risk	,007
Pair 9	Compliance - High Management	,037
Pair 10	Compliance - IS	,013
Pair 11	Compliance - IT	,023
Pair 12	Compliance - Risk	,030
Pair 13	HR - IS	,043

Table 21: Paired Sample of Most significant T-tests (COBIT 5)

Source: prepared by the author

Determinately, there is a significant statistical difference between the departments clarifying that the work role obviously differs among paired departments.

The following figure shows the survey results maturity levels related to the COBIT 5 Framework.

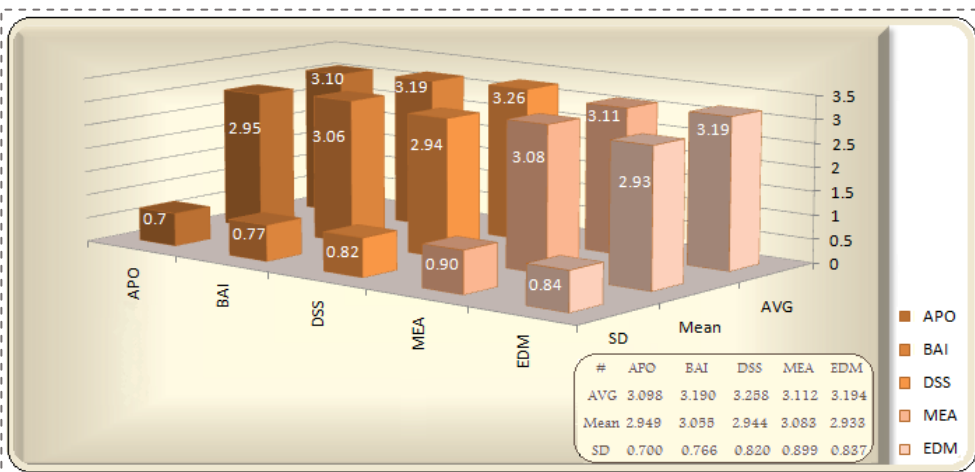


Figure 31: COBIT 5 Processes (AVG, Mean, SD) Chart - Jordanian Banks' Sector

Source: prepared by the author .

Based on Figure 31 above, which is mainly derived from the essential results of the survey tht targetted the banks in the Jordanian market.ome interesting results were exposed as the following:

- The lowest mean value belongs to the MEA Group of Processes showing that most of the banks did not give the needed attention for this kind of process or that they might have faced serious difficulties in implimenting such a process, knowing that the group of processes are mainly owned by the control departments additional to the PMO division, even though the SD gives an indicator that there are major differences between the banks' responses dissimilar to each other in this regard.
- The highest number between all of the average/means calculations belongs to the APO group of processes equaling the value of 3, clarifying that the majority of banks in Jordan highly comply with these types of processes implimentation in all aspects of APO (Align, Plan, and Organize) found in the COBIT 5 framework, knowing that the largest part of this group of processes are mainly owned by the IT Department while the rest are related to the PMO, HR, Finance, IS and Administration Departments.
- High Standard Deviation values clarify large dissimilarities according to the specialists' responses based on the maturity level of the banks, as they have different assumptions regarding the recent achieved levels of processes' implementation. Nevertheless, the above figure clarifies that the MEA (Monitor, Evaluate and Assess) group of processes calculated the highest value of SD equaling 0.6 degrees, clarifying that most of the banks differ in their responses indicating that they slightly

differentiate in their maturity level of implementing and complying with COBIT 5 regulations related to the MEA practices in all aspects.

- The APO02 process (Manage Strategy), owned by the IT department, retains the highest value of 3.2 degrees average, which might clarify that the most mature department during the implementation process of COBIT 5 framework would be the IT division in most of the banks based on being familiar with such standards since their role of work usually should depend on a well managed IT strategy aligned with the general strategy of the institution.
- The APO03 process (Manage Enterprise Architecture), owned by the project management department in some financial institutions, would be considered as the lower value of the average. This would be convenient in most of the cases since this process is usually built based on the general strategic plan of the institution, and implementing such a process would be complicated most of the time, which would be the reason why most of the banks are facing difficulties to deploy such a process.
- The APO04 process (that manages innovation) has received the lowest value of SD indicating that most of the banks' responses are highly similar in that regard, making it the smoothest and most comprehensive process concerning an implementation phase.
- Finally, it is evident the MEA01 process (Monitor, Evaluate and Assess Performance and Conformance) has received the higher value of SD which indicates that majority of the banks had different viewpoint concerning this process since it measures the performance and conformance in the institution which would slightly vary by the bank's standard methods.

5. CONCLUSIONS AND RECOMMENDATIONS

Through this thesis, some theoretical frameworks were adopted to explore the importance of the IT Governance concept such as the Cloud Computing method, IT Operational Risk Conception and COBIT 5 Framework. In order to clarify the conclusion, results were gathered in sections as the following:

5.1. IT Governance - Conclusion

After conducting an empirical comparison study in order to analyze the scientific content of the previous and current scientific researches targeting the public, private, and governmental sectors in the MENA region, I concluded the following:

- The theoretical studies contribution in the MENA region targeting the IT Governance sector was concluded by 11 theoretical studies against 27 empirical studies in that regard.
- Since early 2006, several studies precisely targeted the IT Governance topic, but many researchers in the MENA region also paid early attention towards similar topics of this framework. The majority of those studies have been conducted empirically focusing on several types of sectors such as the banking sector with a percentage of 19% of all the targeted studies, additional to 8% representing the percentage of participation related to the governmental and telecom sectors.
- Jordan ranked first due to concentrating on the value of maturity interconnected with their awareness level, as well as their aim in deploying the IT Governance concept in several areas especially in the banking sector with 21% of all participant studies. Saudi Arabia ranked

second with 18.4% in all types of research, and Bahrain placed third with 10.5% of the total participant studies.

- Several MENA region researchers concentrated on the IT Governance topic and concluded with participant studies equaling 57.8%, with 26.3% of the participants focused on COBIT articles, while the rest were counted with other related topics.
- A massive absence of participation by several countries such as Tunis, Yemen, and Libya occurred due to their economic instability and political situation.
- As a result of insufficient awareness and knowledge in the research field, it is extremely important to spread the cultural awareness in the MENA region regarding the importance/impact of the role that research plays, especially in the field of IT Governance due to its huge effect on the development process in any institution.
- Extra effort should be placed in publishing scientific articles related to IT Governance and COBIT Frameworks targeting the Industrial and Health sectors in the MENA region.
- The COBIT 5 Framework is strongly linked to the IT Governance framework by reason of concentrating on the value of integrating the management and governance utilities in order to reach to the extreme values of adopting IT techniques, policies, and procedures aligned with the general strategic plan of any institution.
- The remaining two subjects (Cloud Computing and IT Operational Risk) are partially connected to the IT Governance concepts, confirming their importance and sequential necessity for providing awareness of multiple types of threats/risks that might surround the IT

division giving a chance for preparing a suitable IT environment and focusing on needed methods that mitigate risk and strengthen controls.

5.2. Cloud computing - Conclusion

By preparing and reviewing the majority of publications and scientific articles related to the subject, several points had been focused on in order to clarify the importance and accuracy of using the Cloud Computing method, since it is considered as an essential and valuable trend in recent years, yet most of the users underestimate its risk. The following are the main results:

- Cloud Computing is divided into several well-known types, such as Public Cloud, Private Cloud, and Hybrid Cloud.
- Public cloud is possibly represented by the “Software as a Service” model (SaaS) in which the service provider controls all the elements in the cloud model.
- Hybrid cloud is possibly represented by the “Infrastructure as a Service” model (IaaS) and “Platform as a Service” model (PaaS) in which the institution and service provider share the responsibility of controlling the cloud elements
- Private cloud is considered as the most secured cloud option since it is completely managed by the institution itself.
- Community cloud is one of the most important and recent competing trends in the market, ensuring effectiveness and added security yet has not currently achieved one of the key goals of assuring reduction of expenses while using cloud services.

Regarding the Cloud Computing conducted research, I discovered that there are some key points that the majority of legislative authorities in several countries agreed on in order to help institutions ensure constant and secure

work procedures for the use of cloud computing services, specifically the outsourced ones, concluding in the following sections:

1. Regulatory Considerations and International Standards of cloud computing require these common objectives to be met:
 - Relevant Regulatory obligations peculiar to Cloud computing services, focusing on Jurisdiction as where the service provider is located should be considered.
 - An assurance of the effective access to Data and Premises by the authorized people/controllers, specifically on data related to the outsourced activities offered by service providers, should be guaranteed.
 - Contracts should guarantee the rights of direct communication with the service provider in case beneficiary firms cannot disclose data for any reason and ensure access allowance to business premises that are relevant to the practice of “Effective Oversight” if needed.
2. Risk Management in cloud computing requires these common objectives to be met:
 - Risk Assumption, Risk Avoidance, Risk Retention, Risk Transfer, and any other related strategy or related combination of strategies should be used and managed properly in similar institutions taking into account the Business recovery tactic in case of outsource provider failure, without neglecting any notification of breaches in the possible event of any unwelcome intruders.
 - The roles of Risk Assessment and Risk Control are two of the most critical phases considered to be as an on-going task, which should be

applied at least once annually due to its high effect on the success of the cloud service lifecycle regardless of which type of cloud service is used.

3. Data Security and Data Protection methods in cloud computing requires these common objectives to be met:
 - Security Assessment and a Data Residency policy with the provider should be carried out by a firm, however, in case of using public clouding, data segregation and data sensitivity should be considered.
 - The identification and appliance of security classification to data that is planned to be outsourced to the cloud service provider should be prepared accurately by the institution in line with the legal regulations with its own data protection rules.
4. Effective Access to Data and Business Premises in cloud computing requires these common objectives to be met:
 - The institution is required to obtain an assurance that the cloud service provider adheres to the relevant data protection rules and legal regulations that are set by the legislative authorities in various countries in order to make new provisions for the regulation of processing of information related to individuals, including the obtaining, holding, usage, or disclosure of such information.
5. Change Management policy and Continuity Plan in Cloud Computing requires these common objectives to be met:
 - A regular assurance of the cloud service provider's full compliance of the data security and protection requirements is required at least annually or after any significant changes are made to the relevant business process, service, configuration, or legal environment.

- In order to maintain well-functioning and healthy related work procedures, the Continuity Plan should be reviewed and adopted by higher level management in case of any disturbance in work flow, unexpected trouble, or failure of the service provider.
- It is essential for firms to have a comprehensive Change Management Policy establishing what provisions must be made for making future changes to technology service and methods of testing changes tasked to be carried out.

6. Exit plan in cloud computing

- It is essential to have a documented and fully tested Exit Plan to ensure the capability of exiting outsourcing plans without unexpected disruption to the firm's provision of services or unexpected compliance with regulatory regime in case of termination or transition to an alternative service provider.
- Focus should place on the importance of the obligations in the termination agreement that ensure the outsourcing provider cooperate with the firm for a smooth transition.

Additionally, based on the conducted survey derived from the BSA global list, the following was concluded on my behalf:

- The UK is still considered one of the leading countries concerning readiness and ability of implementing such cloud services.
- Germany highly competes with the other countries in some major fields such as "Data Privacy" and "Promoting Free Trade", where Germany rises above the UK in these regards.
- The "Data Privacy" section is still considered one of the most important requirements for a healthy implementation process of Cloud computing

solutions, and notably, Hungary defeats the competing countries in that regard, also superseding Germany in two other fields (Security and Cybercrime).

- I discovered that Germany ranked third place on the BSA global list, while the UK ranked in ninth place, considered as leaders due to their infrastructure, flexibility, and readiness for adopting such a concept in most of the sectors. Unfortunately, Hungary did not place on this list, compared to the first 24 mentioned leading countries worldwide in cloud computing domain.
- On the other hand, I discovered that Hungary also competes on the level of regulations, assuring that most of the essential regulations related to Cloud Computing usage and methods are available and approved by the responsible authorities in Hungary.
- Public Cloud users should be aware that their information could be stored in a shared infrastructure. For this purpose, I propose that cloud service providers should contractually agree to bear a financial burden in case of fraud occurrence according to their oversight or non-adherence to the regulations agreed upon, as well as a security assessment and data residency policy with the provider always carried out by the firm.
- I propose that different moderated rules should exist in place in order to regulate these cloud trends and in my opinion, a partnership be made among all European countries to act as an official unified party, which would be responsible for the creation of the regulations and standards that would suit the EU region. Such regulations would serve a better facilitation of cloud computing services due to the EU's unity,

geographical proximity, and possible need to exchange such services among the EU countries.

- A classification and ranking for past/present cloud service providers should be completed based on their sufficient compliance to related regulations and standards in order to facilitate a process for the beneficiary organizations to choose the best match of cloud service providers for contracting matters. Also, it is worth mentioning that the risk of Jurisdiction location of the service provider is an essential matter in this case focusing on the sensitivity of data used by the governmental sector rather than the private sector while applying cloud computing.
- Extreme caution should be taken in the event that data belonging to the governmental sector might be used, transmitted, or stored, since such data is crucially sensitive and would affect the general safety standard in a country.
- A classification of the data that will be used in cloud services should be applied before the implementation phase regardless of what kind of cloud model that will be used.
- Finally, I suggest using a community cloud-computing model that groups institutions who share the same classification, business model, infrastructure, and community with common concerns, whether managed internally or by a third party, and either hosted internally or externally.

5.3. IT Operational Risk - Conclusion

The following shows results related to the IT Operational Risk conducted survey which targeted all of the Jordanian banks, Knowing that after comparing the size and values of the collected data in this Jordanian study with a previous Hungarian study in 2012 which targeting most of the Hungarian banks, we found that the size of data in Hungary were 4 times larger than the Jordanian ones, based on that the following was concluded:

- Most of the Jordanian banks have gained sufficient awareness specifically related to the three important event types with a high maturity level in the related work procedures.
- I concluded that the "Business Disruption and Systems Failures" event type requires a capital (reserve) with an estimated total of 2.03 million JODs. This event type is considered vital, as it would affect the main role of businesses directly, possibly causing a detrimental collapse/termination of the daily work processes in case of high probabilities of occurrence.
- The estimation of Capital (Reserve) related to the two event types (External Fraud and Damage to Physical Assets) calculate lower than the third event type (Business Disruption and Systems Failures). This possibly portrayed a history of less harmful outcomes while the estimation of occurrence of the first and second event types (Frequency) resulted in a lower average than the third event type, in all of the Jordanian banks.
- The estimated net profit during 2017 for the 22 banks targeted in my survey totaled approximately 514 million JODs, as per the recent declaration of the Association of Banks in Jordan (ABJ). Therefore,

when comparing the results of their Allocation (Reserves), it is apparent that the specialists in the financial sector are too optimistic regarding the financial risks, especially during the years when the economical market was on the rise.

- The volume of needed Allocation (Reserve) related to the three specific event types previously mentioned are grossly being underestimated by the banks' specialists.
- My study reveals that there is a high probability of achieving similar results in adjacent countries. Therefore, it is my proposition that such a survey should be completed by similar banks in the MENA region to ascertain the necessary data that can yield actions required in the financial sectors in order to avoid massive losses related to such event types.
- The Jordanian banking sector pays careful attention to event types of IT Operational Risk as per the Basel II classification, keeping in consideration the differences between such event types. The following order of these event types is in accordance to their importance based on the concluded results:

1st Business Disruption and Systems Failures

2nd Damage to Physical Assets

3rd External Fraud

In my opinion, it should be necessary for the Jordanian banks to give additional attention towards the expected IT Risk event types, especially the "Damage to Physical Assets" and "External Fraud" event types due to their critical impact on the business role in any institution.

5.4. COBIT 5 – Conclusion

Based on the conducted Cobit 5 survey which targeted all the Jordanian banks and covering the period from (2016-2018) the following were concluded:

- COBIT 5 Framework is considered as a comprehensive practice that includes 37 processes affecting more than 60 policies and 140 work procedures in any institution.
- Most of the related policies and procedures are linked to the IT services and activities, guaranteeing that nine departments are commonly related to the COBIT 5 Framework summarized by the IT, IS, RISK, HR, Administration, Compliance, Organizational, Finance, and Audit departments, additional to the higher-level management.
- This framework retains several major roles and responsibilities that should be clearly defined using the RACI model. Such a deployment requires continual practical improvements with small steps toward stabilization and effectiveness, assuring maximum focus on changing and improving the people's behavior by scheduling professional training sessions, such as ITIL in order to increase the knowledge base of the related stakeholders and increasing their awareness regarding COBIT 5 processes, practices, and activities.
- Tasking such a project for applying the COBIT 5 framework in any institution requires commitment and effort from all of the related stakeholders/departments. This is dependent on a very detailed plan and specified milestones to measure achievements periodically in order to assess current situations and immediately correct the direction if

necessary, since losing the road map of such a project might lead to some irreparable problems and even more conflicts.

While conducting my research within the period of 2 years after the CBJ (Central Bank of Jordan) regulations were declared related to the COBIT 5 Framework, my research concluded the following:

- Many significant indicators showed an acceptable level of awareness within the Jordanian banks regarding the importance of deploying such a framework and standards for the projected longevity of their current infrastructure and the health of their institutions.
- The majority of the Jordanian banks had faced several difficulties in the initial stages of the COBIT 5 implementation project. I have derived that the relationship between the COBIT 5 processes and financial performances of the Jordanian banks portrayed an insignificant relationship. This result is not in line with (Alramahi Nidal, Barakat Abdallah, Hossam Haddad (2014))
- It was through my research that a discovery of the total value of the COBIT 5 maturity level related to all of the Jordanian banks reached a level of 2.9 out of 5. This indicates that the majority of these banks are complying with their best efforts in the deployment process of the COBIT 5 Framework striving to achieve the required maturity level according to the CBJ regulations.
- The possibility of a positive correlation between the COBIT 5 Framework and the financial performance indicators related to the Jordanian banks is remarkably promising, given sufficient time for the results of implementing the related enhanced policies and procedures to come to fruition.

- My research reveals that the financial performance and profitability ratios of the majority of related Jordanian banks still demonstrate some bad indicators of “ROA”, “ROE”, and “Net Profits after tax” when being compared between the years of 2016 and 2017.
- Through my research, I have discovered that the most affected department while adopting the COBIT 5 Framework was the IT group concluding that approximately 40.5% of the practices were directly related to this division.
- Notably, my results of this analysis showed strong correlations between the IT and the other involved departments, which indicated that most of the affected departments are related to each other sharing several concerns and responsibilities during the implementation process of the COBIT 5 Framework.

It is my proposition that this survey should be replicated/conducted annually targeting the whole sample of Jordanian banks or in any interested comparable countries in the region, in order to assure the increased awareness of the maturity level in the importance of deploying and understanding such a framework.

Finally, I strongly propose that the researchers in this field should continue studying and examining the COBIT 5 Framework further in several sectors in order to increase the value and volume of the academic contribution in that regard, clarifying the advantages of merging the concepts of management and governance within the IT sector.

Optimistically, it is my belief that such indicators of awareness regarding the IT Governance topic will increase dramatically, especially with the recent release of the new COBIT 2019 regulations.

6. REFERENCES

1. Alhaji Abu bakar Aliyu, Rosmaini Bin HJ Tasmin (2012), The Impact of Information and Communication Technology on Banks' Performance and Customer Service Delivery in the Banking Industry, *International Journal of Latest Trends in Finance & Economic Sciences*, Vol-2 No. 1, pp 80-90.
2. Flowerday, S., & Von Solms, R. (2005). Real-time information integrity = system integrity + data integrity + continuous assurances. *Computers & Security*, Vol-24 No. 8, pp 604-613.
3. Hamaker, S., & Hutton, A. (2004). Principles of IT governance. *Information Systems Control Journal*, No. 2, pp 47-50.
4. Weidenmier, M. L., & Ramamoorti, S. (2006). Research opportunities in information technology and internal auditing. *Journal of Information Systems*, Vol-20 No. 1, pp 205-219.
5. Lunardi, G. L., Becker, J. L., Maçada, A. C. G., & Dolci, P. C. (2014). The impact of adopting IT governance on financial performance: An empirical analysis among Brazilian firms. *International Journal of Accounting Information Systems*, Vol-15 No.1, pp 66-81.
6. P. Joshi, (2016). Clouds and big data: A compelling combination. In 2016 3rd International conference on Computing for Sustainable Global Development (INDIACom), New Delhi, India, pp. 2113-2118.
7. N. Gupta and S. Thakur (2014). the factors affecting adoption of cloud computing technology in education institutions. *International Journal of Advanced Research in Computer and Communication Engineering*. Vol-3 No.6, pp. 7229-7235.

8. Pakhchanyan, S. (2016). Operational risk management in financial institutions: A literature review. *International Journal of Financial Studies*, Vol-4 No. 4, pp.20-28.
9. Knahl, M. H. (2009). A Conceptual Framework for the Integration of IT Infrastructure Management, IT Service Management, and IT Governance. *World Academy of Science, Engineering and Technology*. No. 52, pp. 438-443.
10. Anonymus, ed., Isaca (2012). COBIT 5: A business framework for the governance and management of enterprise IT. ISACA and IT Governance Institute. pp. 1-94.
11. Santoro, F. M., & Baião, F. A. (2017). Knowledge-intensive process: A research framework. In *International Conference on Business Process Management*. pp. 460-468. Springer, Cham.
12. Lutz, J. (2014). Committee of Sponsoring Organizations of the Treadway Commission: Internal Control – Integrated Framework in special consideration of the changes in the new edition 2013. *University of applied sciences*. Pp. 1-78
13. Laudon, K. C., & Laudon, J. P. (2000). *Management information system: organization and technology in the networked enterprise*, 4th ed. Upper Saddle River, NJ Prentice Hall International in. U.S. Pearson Custom Publishing.
14. The Banking Regulation and Supervision Board (2001). “Regulation on Banks’ Internal Control and Risk Management Systems”, general provisions, pp. 1-26.
15. Haddad, Hossam (2016) Internal Controls in Jordanian Banks and Compliance Risk, *Research Journal of Finance and Accounting*, Vol.7, No.24, pp. 17-31

16. Spira, L. F., & Page, M. (2003). Risk management: The reinvention of internal control and the changing role of internal audit. *Accounting, Auditing & Accountability Journal*, Vol-16 No.4, pp. 640-661.
17. The International Organization for standardization (ISO) 19011, (2011). Guidelines for auditing management systems. Available on: <http://asq.org/learn-about-quality/iso-19011/> [Accessed on September, 21th 2017]
18. Allegrini, M., D'onza, G. (2003). Internal auditing and risk assessment in large Italian companies: an empirical survey. *International Journal of Auditing*. Vol-7 No.3, pp. 191-208.
19. Stamford, Conn. (2016). Gartner Says Worldwide IT Spending is Forecast to Grow 0.6 Percent in 2016. Available on: <https://www.gartner.com/en/newsroom/press-releases/2016-01-18-gartner-says-worldwide-it-spending-is-forecast-to-grow-1-percent-in-2016> [Accessed on 2017, Jun 12]
20. Stoel, D., Havelka, D., & Merhout, J. W. (2012). An analysis of attributes that impact information technology audit quality: A study of IT and financial audit practitioners. *International Journal of Accounting Information Systems*. Vol-13 No. 1, pp. 60-79.
21. ITAF, (2014). a Professional Practices Framework for IS Audit/Assurance, 3rd Edition. Provided by ISACA. Available on: http://m.isaca.org/Knowledge-Center/Research/Documents/ITAF-3rd-Edition_fmk_Eng_1014.pdf. [Accessed on 2017, Sep 23].
22. DALCI, İlhan, and Veyis Naci TANIŞ (2004). Benefits of computerized accounting information systems on the JIT production

- systems. Çukurova Üniversitesi Sosyal Bilimler Enstitüsü Dergisi. Vol-13, No. 1, pp. 21-36.
23. Urquía Grande, E., Pérez Estébanez, R., & Muñoz Colo MENA, C. (2011). The impact of Accounting Information Systems (AIS) on performance measures: empirical evidence in Spanish SMEs. *The international journal of digital accounting research*. No.11, pp. 25-43.
 24. Weill, P., & Ross, J. W. (2004). Ten principles of IT governance. Excerpted from *IT Governance*. Harvard Business school (HBSWK Publications). pp. 6.
 25. Barbosa, S. C. B., Rodello, I. A., & Pádua, S. I. D. D. (2014). Performance measurement of information technology governance in Brazilian financial institutions. *JISTEM-Journal of Information Systems and Technology Management*, Vol-11 No.2, pp. 397-414.
 26. Wessels, E., & Logger Enberg, J. V. (2006, September). IT governance: theory and practice. In *Proceedings of the conference on information technology in tertiary education*, Pretoria, South Africa. pp. 18-20.
 27. Johnston, A. C., & Hale, R. (2009). Improved security through information security governance. *Communications of the ACM*, Vol-52 No.1, pp. 126-129.
 28. Financial Conduct Authority, (2016). FG16/5: Guidance for firms outsourcing to the ‘cloud’ and other third-party IT services. Available online: <https://www.fca.org.uk/publications/finalised-guidance/fg16-5-guidance-firms-outsourcing-%E2%80%98cloud%E2%80%99-and-other-third-party-it> (Accessed on 15 November 2016)
 29. A Magyar Nemzeti Bank 2/2017. (I.12.) számú ajánlása a közösségi és publikus felhőszolgáltatások igénybevételeéről “On the Usage of

- Social and Public Cloud Services”. Available online: <http://www.mnb.hu/en/publications> (Accessed on 10 October 2016)
30. Federal Office for Information Security (2013). Cloud Computing Controls Catalogue C5. Available on: [https://www.bsi.bund.de/EN/Topics/CloudComputing/Compliance Controls Catalogue/Compliance Controls Catalogue.html](https://www.bsi.bund.de/EN/Topics/CloudComputing/Compliance%20Controls%20Catalogue/Compliance%20Controls%20Catalogue.html) (Accessed on 1 December 2016)
 31. European Commission, (2012). opinion 05/2012 on Cloud Computing. Available Online: <https://www.technethics.com/assets/Opinion-05-2012-on-Cloud-Computing.pdf> (accessed on 11 November 2016)
 32. Barrie Sosansky (2011). Cloud Computing Bible, 1st ed; Wiley Publishing, Inc. Indianapolis, Indiana. pp. 1 – 500, ISBN: 978-0-470-90356-8.
 33. National Institute of standard and technology (2011). The NIST Definition of Cloud Computing, Special Publication 800-145. Available online: <http://faculty.winthrop.edu/domanm/csci411/Handouts/NIST.pdf> (Accessed on 15 October 2016)
 34. Caixa Bank, (2015). Cloud Financial Services. Available online: <http://www.eba.europa.eu/documents/10180/1228702/Session+2++Mario+Maawad+-+Cloud+Financial+Services.pdf> (accessed on 28 November 2016)
 35. Data Protection Act (2012). Guidance on the Use of Cloud Computing. Available online: <https://ico.org.uk/media/about-the-ico/documents/1042330/cloud-computing-guidance-for-organisations.pdf> (Accessed 14 October 2016)

36. Chris Mitchell, C.S, (2014). Outsourcing personal data processing in the cloud. Royal Holloway University of London, pp. 1-6, in press.
37. European Banking Authority, (2015). Cloud Security Strategies. Available Online : <https://eba.europa.eu/sites/default/documents/files/documents/10180/1228702/8a0b90bc-1ad4-4780-9c01-8590bc2ef6c9/Session%20%20%20-%20Fabio%20Gianotti%20-%20Cloud%20Security%20Strategies.pdf> (Accessed on 17 December 2016)
38. Bird and Bird, (2014). Cloud Computing & Your Legal Questions Answered. Available online: <https://www.twobirds.com/~//media/PDFs/Expertise/IT/Cloud%20computing%20law%20interactive.pdf> (Accessed on 17 November 2016)
39. Carlin, C. S.; Curran, C.K. (2011). Cloud Computing Security. International Journal of Ambient Computing and Intelligence. Vol-3 No.1, Pp. 14-19, 10.4018/jaci.2011010102.
40. Bank of England (2015). Outsourcing Functions of Cloud. Available online: <https://www.bankofengland.co.uk/prudential-regulation/publication/2015/report-on-outsourcing-functions-to-the-cloud-1> (accessed on 22 September 2016)
41. Haibach, G.H. (2015). Cloud computing and European Union private international law. Journal of Private International Law. Vol-11, No.2, pp. 252-266, 17441048.2015.1067994.
42. Paul, P.D.H; Vagelis, V.P; Irene I.K (2014). The new cloud computing ISO/IEC 27018 standard through the lens of the EU legislation on data protection. Brussels privacy hub working paper, Vol-1, No.2, pp. 1-26.

43. Zwattendorfer, B.Z.; Stranacher, K.S.; Tauber, A.T.; Reichstädter, P.R. (2013). Cloud computing in e-government across Europe. In International Conference on Electronic Government and the Information Systems Perspective. Vol-8061, pp. 181-195, 10.1007/978-3-642-40160-2.
44. Bauer, S. (2012). A literature review on operational it risks and regulations of institutions in the financial service sector. The Role of Information Security Awareness for Promoting Information Security Policy Compliance in Banks, No.19.
45. Walker, R. (2015). The Increasing Importance of Operational Risk in Enterprise Risk Management. Enterprise Risk Management, No.82.
46. Basel Committee. (2011). Principles for the Sound Management of Operational Risk. Basel, Switzerland: Bank for International Settlements Communications.
47. Birindelli, G., & Ferretti, P. (2017). The Operational Risk: An Overall Framework. In Operational Risk Management in Banks. Palgrave Macmillan, London, pp. 9-35.
48. Wu, D. D., & Olson, D. (2010). Enterprise risk management: a DEA VaR approach in vendor selection. International Journal of Production Research, Vol-48 No.16, pp. 4919-4932.
49. Chaudhuri, A., & Ghosh, S. K. (2016). Quantitative modeling of operational risk in finance and banking using possibility theory. Springer International Publishing.
50. Ahlan, A. R., & Arshad, Y. (2012). Understanding Components of IT Risks and Enterprise Risk Management. In Risk Management for the Future-Theory and Cases. InTech.

51. Saint-Germain, R. (2005). Information security management best practice based on ISO/IEC 17799. *INFORMATION MANAGEMENT JOURNAL-PRAIRIE VILLAGE-*, Vol-39 No.4, pp. 60.
52. Dirk Paessler. (2008). The Role of Network Visibility in IT Operational Risk Management, Paessler: PRTG Network Monitor, Pp.1-8
53. Thach, L., & Woodman, R. W. (1994). Organizational change and information technology: Managing on the edge of cyberspace. *Organizational Dynamics*, Vol-23, No.1, pp. 30-47.
54. Lorenzi, N. M., & Riley, R. T. (2000). Managing change: an overview. *Journal of the American Medical Informatics Association*, Vol-7, No.2, pp.116-124.
55. Federal Housing Finance Agency, (2017). Information Technology Risk Management Program [Pdf]. Available on: https://www.fhfa.gov/SupervisionRegulation/Document/Information_Technology_Risk_Management_Program_Module_Final_Version_1.1.pdf (Accessed on 21 Sep 2016)
56. Laudon, K. C., & Laudon, J. P. (2016). Management information system. Pearson Education India. Global Edition (30th).
57. Georgakopoulos, D., Hornick, M., & Sheth, A. (1995). An overview of workflow management: From process modeling to workflow automation infrastructure. *Distributed and parallel Databases*, Vol-3 No.2, pp. 119-153.
58. Bollinger, A. S., & Smith, R. D. (2001). Managing organizational knowledge as a strategic asset. *Journal of knowledge management*, Vol.5, No. 1, pp. 8-18.

59. Hong, K. S., Chi, Y. P., Chao, L. R., & Tang, J. H. (2003). An integrated system theory of information security management. *Information Management & Computer Security*, Vol-11 No.5, pp. 243-248.
60. Thoraval, P. Y. (2006). The Basel II framework: the role and implementation of Pillar 2. *Financial Stability Review*, No.9, pp. 117-132.
61. Sands, P., Liao, G., & Ma, Y. (2018). Rethinking operational risk capital requirements. *Journal of Financial Regulation*, Vol-4, No.1, pp. 1-34
62. Pasquini, A., & Galiè, E. (2013). COBIT 5 and the Process Capability Model. Improvements Provided for IT Governance Process. In *Proceedings of FIKUSZ'13 Symposium for Young Researchers*, pp. 67-76.
63. Dey, M. (2007). Information security management-a practical approach. In *AFRICON 2007*, pp. 1-6. IEEE.
64. Buckby s., best p. And steward j. (2009). The current state of information technology governance literature. In *information technology governance and service management: frameworks and adaptations*. Aileen cater-steel (university of southern queens land australia), australia, pp.1-43.
65. Musson, d., 2009. IT governance: a critical review of the literature. In *information technology governance and service management: frameworks and adaptations*. Aileen cater-steel (university of southern queens land australia), australia, pp. 44-62.
66. De Haes, S., Van Grembergen, W., & Debreceeny, R. S. (2013). COBIT 5 and enterprise governance of information technology: Building

- blocks and research opportunities. *Journal of Information Systems*, Vol-27 No.1, pp. 307-324.
67. International monetary fund (2012), JORDAN 2012 ARTICLE IV CONSULTATION, International Monetary Fund Washington, D.C., imf country report 12/119, pp.1-70.
 68. Van grembergen, g., de haes, s. (2008). Analysing the relationship between IT governance and business/ IT Alignment Maturity. In: proceedings of the 41st hawaii international conference on system science, IEEE computer society, waikoloa, hi, pp. 428.
 69. Menevse, A., Mr. (2011). Toward Better IT Governance With COBIT. Available on: <http://m.isaca.org/Knowledge-Center/COBIT/Documents/COBIT-Focus-Toward-Better-IT-Governance-with-COBIT-5.pdf> (Accessed on January 17th 2016)
 70. Cartlidge, A., & Hanna, A. (2007). The IT Infrastructure Library An Introductory Overview of ITIL® V3 Version 1.0. Retrieved January. 2019 from http://thuvienso.vanlanguni.edu.vn/handle/Vanlang_TV/2384
 71. Todd Fitzgerald, C. I. S. S. P., Bonnie Goins, C. I. S. S. P., & Rebecca Herold, C. I. S. S. P. (2005). Information security and risk management. Official (ISC) 2® Guide to the CISSP®-ISSEP® CBK®, 1. Isaca 2012.
 72. Mangalaraj, G., Singh, A., & Taneja, A. (2014). IT governance frameworks and COBIT-a literature review.
 73. Moeller, R. R. (2013). Executive's guide to IT governance: improving systems processes with service management, COBIT, and ITIL. John Wiley & Sons

74. Bartens, Y., De Haes, S., Lamoen, Y., Schulte, F., & Voss, S. (2015). On the way to a minimum baseline in IT governance: using expert views for selective implementation of COBIT 5. In 2015 48th Hawaii International Conference on System Sciences, IEEE, pp. 4554-4563.
75. Nugroho, H. (2014). CONCEPTUAL MODEL OF IT GOVERNANCE FOR HIGHER EDUCATION BASED ON COBIT 5 FRAMEWORK. Journal of Theoretical & Applied Information Technology, Vol-60, No. 2.
76. Galiè. (2013). COBIT 5 and the Process Capability Model / Improvements Provided for IT Governance Process. Conference Proceedings compilation @ Obuda University Keleti Faculty of Business and Management. Pp.67-76.
77. Radovanovic, d., lucic, d., radojevic, t. And sarac, m. (2011). Information technology governance –COBIT model. Proceedings of the 34th international convention, opatija, pp.1426 – 1429.
78. Parvizi, R., Oghbaei, F., & Khayami, S. R. (2013). Using COBIT and ITIL frameworks to establish the alignment of business and IT organizations as one of the critical success factors in ERP implementation. In The 5th Conference on Information and Knowledge Technology, IEEE, pp. 274-278.
79. Ridley, g., j. Young, and p. Carroll, (2008). studies to evaluate COBIT's contribution to organizations: opportunities from the literature. Australian accounting review, Vol-18, No. 4, pp. 334-342.
80. Gantman, S., &Fedorowicz, J. (2016). Communication and control in outsourced IS development projects: Mapping to COBIT domains. International Journal of Accounting Information Systems, Vol-21 No. 32, pp. 63-83.

81. The UK's leading provider of expert services for IT professionals (2006). IT governance developing a successful governance strategy. The National Computing Centre, pp. 1-71.
82. Preittigun, A., Chantatub, W., & Vatanasakdakul, S. (2012). A Comparison between IT governance research and concepts in COBIT 5. International Journal of Research in Management & Technology, Vol-2 No. 6, pp. 581-590
83. Koutoupis, a.g. and a. Tsamis (2009). Risk based internal auditing within Greek banks: a case study approach. Journal of management and governance, Vol-13 No.1, pp. 101-130.
84. Khanyile, S., & Abdullah, H. (2011). COBIT 5: an evolutionary framework and only framework to address the governance and management of enterprise IT. unisa. ac. Za.,pp.1-7.
85. Selig, G. J. (2018). IT Governance—An Integrated Framework and Roadmap: How to Plan, Deploy and Sustain for Competitive Advantage. In 2018 Portland International Conference on Management of Engineering and Technology (PICMET) IEEE, pp. 1-15.
86. Youssfi, K., Houssaini, S., Boutahar, J. (2016). CAT5: A Tool for Measuring the Maturity Level of Information Technology Governance Using COBIT 5 Framework. International Journal of Advanced Computer Science and Applications, Vol. 7, No. 2, pp. 385-391.
87. Kanellou, a. And c. Spathis (2011), auditing in enterprise system environment: a synthesis. Journal of enterprise information management, Vol-24, No. 6, pp. 494-519.
88. Nabiollahi, a. And bin sahibuddin, s. (2008). Considering service strategy in itilv3 as a framework for it governance, information technology international symposium 1, august 2008, ieee computer society, kualalumpur, pp.1-5.

89. Liu, h., zhu, y. (2009). Measuring effectiveness of information security management. International symposium on computer network and multimedia technology. wuhan, pp. 1-4.
90. Voon and J. Salido, (2009). MOF to COBIT/Val IT Comparison and Cross-Implementation Guide, Institut Teknologi Telkom, pp.1-50.
91. IT Governance Institute (2008). Enterprise Value: Governance of IT Investments, The Val IT Framework 2.0., USA: ITGI, pp. 1-32.
92. O'Brien, J (2001). Management Information Systems: Managing Information Technology in the Internetworked Enterprise. Boston: Irwin McGraw-Hill. ISBN 0-07-112373-3
93. Bird, M. (2010). Modern Management Guide to Information Technology. Collection of Articles. (Book) Pp. 1-300.
94. Talbot, Chris, (2011). HP Adds to Converged Infrastructure Lineup. Channel Insider, pp. 5-25.
95. Gardner, D. (2010). Converged Infrastructure Approach Paves Way for Improved Data Center Productivity, Butts," IT Business Edge
96. Huff, Lisa, (2011). The Battle for the Converged Data Center Network, Data Center Knowledge.
97. Oestreich, Ken, (2012). "Converged Infrastructure," CTO Forum, at the Way back Machine.
98. D.C. Chou, (2015). Cloud computing: A value creation model, Comput. Stand. Interfaces No.38. pp.72–77.
99. S. Marston, Z. Li, S. Bandyopadhyay, J. Zhang, A. Ghalsasi, (2011). Cloud computing - the business perspective, Decis. Support. Syst. No. 51, pp. 176–189.

100. National Institute of Standards and Technology (2012). Cloud Computing Program. Available on: <http://www.nist.gov/itl/cloud/> 2012 (Accessed November 01, 2012).
101. Jreissat, E., Jozsef, G., (2018). The Influence of IT Audit, ITG / ISG and Cobit Frameworks on Institutions in “MENA” Region. Jour of Adv Research in Dynamical & Control Systems, Vol. 10, No. 04, Special Issue, 2, pp. 637-646.
102. BSA Report (2016). Global cloud computing scorecard. Available on: <http://cloudscorecard.bsa.org/2016/> (Accessed on 18 November 2016)
103. HM Government, (2011). Government Cloud Strategy. Available on: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/266214/government-cloud-strategy_0.pdf (Accessed on 9 November 2016)
104. Cooper, J., & Schindler, M. (2008). Perfect Sample Size in Research. New Jersey
105. Liebetrau, C., & Schindler, K. (1999). U.S. Patent No. 5,988,930. Washington, DC: U.S. Patent and Trademark Office.
106. BURNS, N. G., & Grove, S. SK (2001). The practice of nursing research: conduct, critique and utilization.
107. Johnson, B., & Turner, L. A. (2003). Data collection strategies in mixed methods research. Handbook of mixed methods in social and behavioral research, pp. 297-319.
108. Marshall, B., Cardon, P., Poddar, A., & Fontenot, R. (2013). Does sample size matter in qualitative research? : A review of qualitative interviews in IS research. Journal of Computer Information Systems, Vol- 54, No. 1, pp. 11-22.

109. Sekaran, U. (2003). *Research Methods for Business, A Skill Building Approach*, John Willey & Sons. Inc. New York.
110. Hox, Joop J., and Hennie R. Boeijs. (2005). Data collection, primary versus secondary. pp. 593-599.
111. Hassan, Z. A., Schattner, P., & Mazza, D. (2006). Doing A Pilot Study: Why Is It Essential?. *Malaysian family physician : the official journal of the Academy of Family Physicians of Malaysia*, Vol-1, No.2-3, pp. 70-3.
112. Uma, S., & Roger, B. (2016). *Research methods for business: A skill building approach*. John Wiley & Sons. book.
113. Zikmund, W. G., Babin, B. J., Carr, J. C., & Griffin, M. (2013). *Business research methods*. Cengage Learning
114. Jreissat, E., Jozsef, G., (2018). A Review of IT Audit, Information Technology Governance, Information security Governance and COBIT Frameworks on Institutions. *International Journal of pure and applied Mathematics*. Vol.119 No. 18. pp. 525-540.
115. Balgedom, Sabah (2006), the impact of ICT on the strategic management of Economies firms, Master Thesis, Qusentina University, pp.1-318.
116. Hayale Bakry, S. H., & Alfantookh, A. (2006). IT-governance practices: COBIT. *Applied Computing and Informatics*, Vol-5, No.2, pp. 53-61.
117. ABU-MUSA, A. A. (2007): "Exploring Information Technology Governance (ITG) in Developing Countries: An Empirical Study", *The International Journal of Digital Accounting Research*, vol. 7, n.13: 71- 117.

118. Zaied, A. N. H., Khairalla, F. A., & Al-Rashed, W. (2007). Assessing e-Readiness in the Arab Countries: Perceptions towards ICT Environment in Public Organisations in the State of Kuwait. *Electronic Journal of E-government*, Vol.5, No.1.
119. Abu-Musa, A. (2008). Exploring the importance and implementation of COBIT processes in Saudi organizations: An empirical study. *Information Management & Computer Security*, Vol-17, No.2, pp. 73-95.
120. Ghazanfari, M., Fathian, M., & Rais, S. M. (2009). COBIT a Suitable Framework for Measuring IT Governance in Organizations (Case Study for Governmental Banks of Iran). *Iranian Communication and Information Technology*. Vol.1, pp.1-2,
121. Yarifard, R., & Gowda, K. N. (2010). Applying CMMI to Determine the Stages of the COBIT Domains in the Banking Sector of Iran. *Asian Journal of Development Matters*, Vol-1, pp. 164-169.
122. Abu-Musa, A. A. (2009). Exploring COBIT processes for ITG in Saudi organizations: an empirical study. *The International Journal of Digital Accounting Research*. Vol.9 No.10, pp.99-126.
123. Abu-Musa, A. (2010). Information security governance in Saudi organizations: an empirical study. *Information Management & Computer Security*, Vol-18, No.4, pp. 226-276.
124. Al-Qudah, H. S. S., Saaty, A. S. A., & Al-Momani, A. A. M. (2012). Impact of Information Technology on Management Control at Al Bashir Public Hospital: A Case Study of Jordan. *International Journal of Business and Management*, Vol-7, No.2, pp. 260.

125. Salim, M., Othman, M., & Yahya, H. (2012). An Investigation of ISG Status in Mosul Health Sector. In the Symposium on IT Governance, Management & Audit. Pp. 1-5.
126. Al Skafy, H., & Al-Theebbeh, Z. A. H. (2012). The level of information technology governance in KULACOM-Jordan Company. Available on:
<https://basicresearchjournals.org/business/abstract/Al%20Skafy%20and%20Al-theebbeh.html>. (Accessed on: October, 10th 2016)
127. Bin-Abbas, H., & Bakry, S. H. (2012). Assessment of ICT governance in three different Saudi institutions using an integrated approach. International Journal of Arab Culture, Management and Sustainable Development, Vol-2, No. 2-3, pp. 255-272.
128. Al-Zwyalif, I. M. (2013). IT governance and its impact on the usefulness of accounting information reported in financial statements. International Journal of Business and Social Science, Vol-4, No.2.
129. Sarayrih, M. A., & Sriram, B. (2015). Major challenges in developing a successful e-government: A review on the Sultanate of Oman. Journal of King Saud University-Computer and Information Sciences, Vol-27, No. 2, pp. 230-235.
130. Ayshosh Riad, Wadih Fawaz, (2012) IT Governance: competitive advantage within knowledge economy. Available on:
<http://iefpedia.com/arab/wp-content/uploads/2012/05/حوكمة-تكنولوجيا-المعلومات-ميزة-استراتيجية-في-ظل-اقتصاد-المعرفة.pdf> [Accessed on Sep 20,2017]
131. Nicho, M., & Mourad, B. A. (2012). Success factors for integrated ITIL deployment: An IT governance classification. Journal of

- Information Technology Case and Application Research, Vol-14, No.1, pp. 25-54.
132. Raeda I. abu Etaiwy, (2012). Impact of the use of Information Technology Risks in Organizations Subject to Auditing on External Auditors' Job Quality in Gaza Strip. Available on: <http://library.iugaza.edu.ps/thesis/106713.pdf> [Accessed on September, 25th 2017]
 133. Alramahi Nidal, Barakat Abdallah, Hossam Haddad (2014) Information Technology Governance Control Level in Jordanian Banks Using: Control Objectives for Information and Related Technology (COBIT 5), European Journal of Business and Management, Vol.6, No.5, pp.194-206 .
 134. Zyoud, Lateef, Nsour, Reem Mohammad, (2014). Determining the level of IT governance applicable Commercial Bank of Syria in Lattakia according to a framework (COBIT). Economic and Legal Sciences, Series ISSN: 2079-3073, Vol-36 No.2.
 135. Lubbad, R. R., & Ashour, Y. (2014). Towards An Abbreviated Model of IT governance for Palestinian government sector According to COBIT 5 framework. The Islamic University of Gaza. pp. 1-117. Available on: <http://library.iugaza.edu.ps/thesis/113542.pdf> [Accessed on 2017 Sep. 26th]
 136. Almeida, R., Pereira, R., & da Silva, M. M. (2013). IT governance mechanisms: a literature review. In International Conference on Exploring Services Science (pp. 186-199). Springer, Berlin, Heidelberg.

137. Harikrishnan S., Zakareya A. K., (2014). Bahrain Governance Framework: Towards Efficient Use of IT. Journal of Inspiration Economy. Econ.1 No. 1 Pp.1-16.
138. Griffiths, M., Janahi, L., & Al-Ammal, H. (2014). IT Governance from Theory to Practice: The Importance of Accountability. In BCS International IT Conference. Available On: <https://pdfs.semanticscholar.org/4027/3024ef0522922077fbcfb4022b707d171030.pdf> [Accessed on October 7th, 2017]
139. Alber, Nader and Nabil, Myvel, (2015) The Impact of Information Security on Banks' Performance in Egypt, International Journal of Economics and Finance Vol. 7, No. 9.
140. Dr. Madian A.& Dr. Nazeer M. (2015). تكنولوجيا المعلومات في فروع المصارف العامة في مدينة اللاذقية (دراسة ميدانية). سلسلة العلوم الاقتصادية والقانونية Print ISSN: 2079-3073, Online ISSN: 2663-4295, Vol.2, No. 37.
141. Karima A. Kadhim, Ahmad J. Hamoudi, (2015). IT governance procedures: A proposed model in the light of COBIT's framework objectives, Journal of administration and economics. pp. 243-259.
142. Firas Alkhaldi, Minwer Wraikat, (2015). Portfolio Management and IT Governance: An Empirical Investigation Using PLS Path Analysis. International Journal of Scientific Knowledge, Vol. 6, No.3, pp. 1-20
143. Vijayakumar, U., & Ilangoan, D. (2015). A Quantitative Approach to Information Systems Audit in Small and Medium Enterprises. Informatica Economica, Vol.19, No.3, pp. 89.
144. Mahmoud y. Zgout, (2016). The Effectiveness of using Information Technology (IT) in Auditing and its impact on improving the quality of Auditing service in the Gaza Strip, The Islamic University–Gaza

- pp. 1-17. Available on: <http://library.iugaza.edu.ps/thesis/119448.pdf>
[Accessed on 2017 sep. 25]
145. Afandi, W. S. (2016). Information technology governance role in enhancing IT portfolio management: a case study on Saudi Arabia private sector. *International Journal of Research and Reviews in Applied Sciences*, Vol-26, No.1, pp. 47.
 146. National Authority for Data Protection and Freedom of Information of Hungary, Opinion on Data Processing by Drones. Available On: https://www.naih.hu/files/opinion_data_processing_by_drones_2015_02_04.pdf (Accessed on 20th, November 2016).
 147. Hungary- Financial Supervisory Authority Issues Circular for Hungarian Financial Institutions on the Use of Cloud Computing Technologies. Available online: <https://iapp.org/news/a/2012-08-08-hungary-financial-supervisory-authority-issues-circular-for-hung/> (Accessed on 10th, December 2016).
 148. Nagy Gábor (2015). Kockázati mérések és mértékek instabilitása Szerző. Available on : https://dea.lib.unideb.hu/dea/bitstream/handle/2437/216190/Nagy_Gabor_disszertacio.pdf?sequence=1&isAllowed=y (Accessed on: December 20th 2018)

7. LIST OF PUBLICATIONS

✓ The Influence of IT Audit, ITG, ISG and COBIT Frame work on institutions in “MENA” Region.

Journal of Advanced Research in Dynamical and Control Systems (JARDCS)
ISSN 1943-023X.

Coauthors: Elias Jriesat¹, Jozsef Gall²

✓ Cloud Computing Regulations and Readiness: Comparison Study (United Kingdom, Germany and Hungary) (Accepted to be published in Feb/ 2020).

EPJ Data Science. IP Factor: 3.262

ISSN: 2193-1127 | Journal no. 13688.

Coauthor: Elias Jriesat

✓ A Review of IT Audit, Information Technology Governance, Information security Governance and COBIT Frameworks on Institutions.

International Journal of pure and applied Mathematics.

ISSN: 1134-3395 - VOL. 119 - No. 18.

Coauthors: Elias Jriesat¹, Jozsef Gall², Mohamed Doheir³

▪ COBIT 5 Framework’s Essentials, Efficiency and Impact on the Banking Sector.

Working Paper.

Coauthor: Elias Jriesat

▪ IT Operational Risk endeavors and event’s impact on the Jordanian banking Sector.

Working Paper.

Coauthors: Elias Jriesat¹, Jozsef Gall²

Jreissat Elias közleményei (2019.08.14)

2020

1. Elias, R. Jreissat Cloud Computing Regulations and Readiness: Comparison Study (United Kingdom, Germany and Hungary) EPJ DATA SCIENCE 9 : 1 p. m.a. (2020) Közlemény:30765171 Jövőbgyott Forrás Folyóiratokk (Szakokk)

2018

2. Elias, R Jreissat ; Jozsef, M Gall The Influence Of IT Audit, ITG / ISG and Cobit Frameworks on Institutions nn "MENA" Region JOURNAL OF ADVANCED RESEARCH IN DYNAMICAL AND CONTROL SYSTEMS 10 : special issue_4 pp. 637-646. , 10 p. (2018) Teljes dokumentum Közlemény:3371631 Admin láttamozott Forrás Folyóiratokk (Szakokk)
3. Elias, R. Jreissat ; Jozsef, M. Gall ; Mohamed, Doheir A Review of IT Audit, ITG/ISG and Cobit Frameworks on Institutions in "MENA" Region INTERNATIONAL JOURNAL OF PURE AND APPLIED MATHEMATICS 119 : 18 pp. 525-541. , 17 p. (2018) Teljes dokumentum Közlemény:30765179 Admin láttamozott Forrás Folyóiratokk (Szakokk)

1. Elias, R. ;Jreissat
Cloud Computing Regulations and Readiness: Comparison Study (United Kingdom, Germany and Hungary)
EPJ DATA SCIENCE 9 : 1 p. m.a. (2020)
Folyóiratcikk/Szakcikk (Folyóiratcikk)/Tudományos
[30765171] [Jóváhagyott]

2. Elias, R ;Jreissat ; Jozsef, M ;Gall
The Influence Of IT Audit, ITG / ISG and Cobit Frameworks on Institutions nn "MENA" Region
JOURNAL OF ADVANCED RESEARCH IN DYNAMICAL AND CONTROL SYSTEMS 10 : special issue_4 pp. 637-646. , 10 p. (2018)
 Teljes dokumentum
Folyóiratcikk/Szakcikk (Folyóiratcikk)/Tudományos
[3371631] [Admin láttamozott]

3. Elias, R. ;Jreissat ; Jozsef, M. ;Gall ; Mohamed, Doheir
A Review of IT Audit, ITG/ISG and Cobit Frameworks on Institutions in "MENA" Region
INTERNATIONAL JOURNAL OF PURE AND APPLIED MATHEMATICS 119 : 18 pp. 525-541. , 17 p. (2018)
 Teljes dokumentum
Folyóiratcikk/Szakcikk (Folyóiratcikk)/Tudományos
[30765179] [Admin láttamozott]

8. LISTOF TABLES

Table 1: Research related to ITG - ICTG- ISG - COBIT -ITAUDIT frameworks. (ITG)

Table 2: The targeted banks population in the study. (IT O.R)

Table 3: Sample size of the targeted banks in Jordan (COBIT 5)

Table 4: 37 Processes related to the banks Department. (COBIT 5)

Table 5: Implementation rating scale (COBIT 5)

Table 6: Results of the conducted research (2006- 2017) (MENA Region) (ITG)

Table 7: Global Cloud Computing Scorecard (2016) (Cloud computing)

Table 8: Important Indicators, IT Readiness (Germany, United Kingdom, and Hungary)

Table 9: Jordanian Banks Profit after Tax in Million JDS

Table 10: survey participant's information (COBIT 5)

Table 11: Respondents to Gender (COBIT 5)

Table 12: Respondents to Academic Qualification (COBIT 5)

Table 13: Respondents to Professional Work Experience (COBIT 5)

Table 14: Respondent's to Job Titles (COBIT 5)

Table 15: Financial performance ratios for Jordanian banking sector (2016-2017)

Table 16: COBIT 5 Processes (AVG, Mean, SD) Table -Jordanian Banks' Sector

Table 17: Responsibility of departments according to COBIT 5 framework

Table 18: correlation between departments (COBIT 5)

Table 19: Paired Samples Correlations. (ROE, ROA, Net Profit) (COBIT 5).

Table 20: Paired Sample test based on IT Dep. (COBIT 5)

Table 21: Paired Sample of Most significant-tests (COBIT 5)

7. LIST OF FIGURES

Figure (1): Evolution of COBIT framework (COBIT 5)

Figure (2): Cloud Computing Service Models (cloud computing)

Figure (3): Mapping objectives to IT Related Objectives (COBIT 5)

Figure (4): COBIT 5 Governance and Management Key Areas (COBIT 5)

Figure (5): The five main processes in COBIT 5 framework (COBIT 5)

Figure (6): The 5 main Principles in Cobti5 Framework (COBIT 5)

Figure (7): Thesis Conceptual relationship

Figure (8): Effective governance through simultaneous use of COBIT and Val IT

Figure (9): Results from Survey (IT O.R)

Figure (10): Programming Code for R Functional Language (Monte Carlo method)

Figure (11): Publications according to MENA Region (ITG)

Figure (12): Sectors included in the study (ITG)

Figure (13): Contributions of MENA countries in Published studies related to ITG, IT Audit, ISG and other similar studies. (ITG)

Figure (14): Topics of publications used in MENA region (ITG)

Figure (15): Cloud computing- survey results - 7 main field (Cloud computing)

Figure (16): percentage of calculations – cloud computing survey (Cloud computing)

Figure (17): Population Indicator versus Internet (cloud computing)

Figure (18): Population Indicator versus GDP (cloud computing)

Figure (19): International Internet Bandwidth versus Connectivity score

Figure (20): Respondents ‘gender (IT O.R)

Figure (21): Respondents job titles (IT O.R)

Figure (22): Results Derived from Survey– Log-normal distribution (IT O.R)

Figure (23): Main Events types Results (IT O.R)

Figure (24): Jordanian Banks Net profit after Tax (in Million JDS)

Figure (25): Bank’s related departments throughout COBIT 5 implementation phase.

Figure (26) Respondents’ to Educational level & Gender (COBIT 5)

Figure(27): Respondents Work Experiences, Professions & Positions (COBIT 5)

Figure (28): ROE Compared results according to 2016 – 2017

Figure (29): ROA Compared results according to 2016 – 2017

Figure (30): Net Profit Compared results according to 2016 – 2017

Figure (31):COBIT 5 Processes (AVG, Mean, SD) Chart -Jordanian Banks’ Sector

9. ACKNOWLEDGMENTS

I would like to express my deepest appreciation to all those who provided me the possibility to complete this thesis. A special gratitude I give to my supervisor, Dr. Gall Jozsef, whose contribution in stimulating suggestions and encouragement, helped me to coordinate my PHD study and to script this thesis.

Furthermore, I would like also to acknowledge with much love and appreciation the crucial role of my family, specifically to my father and mother who gave me the strength to reach forward towards my dream.

Words do not express in thanking my best friends, Hossam and Loai, for their unlimited support and help in the past years of my study. Special thanks go to my lovely work colleagues, Mr. Samir, Ms. Hiba, and Ms. Farah for helping to ease this long journey during my work hours, also no words would be enough to thank my cousin Kevin and his family for his effort and aiding me in reaching the close of my thesis.

May God bless you, my beloved ones.

10 Appendix (A)

- To Check IT Operational Risk Survey, please use the below link:

<https://docs.google.com/forms/d/1j0qX6GXpivL8bVEDb-rkuQBPE0ngjjC0m0U8g5fTKC8/edit>

- To check Cobit Survey, Please Use Below link:

<https://docs.google.com/forms/d/1y8Z515Aqg2vJqnWTRaWMnvu5HneiuBfPJ6skvLWPsNQ/edit>

- The below shows the full version of the used table in the IT Governance study which was used in order to conclude the above related results.

Table (1):

No.	Author	Year	Country	Sector	Framework	Type of research
1	Hayale and Abu Khadra	2006	Jordan	Banking	CAIS	Empirical
Title	Evaluation of The Effectiveness of Control Systems in Computerized Accounting Information Systems: An Empirical Research Applied on Jordanian Banking Sector					
Findings	The Jordanian domestic banks are using effective fraud and error reduction controls, there is a need for the application other control system, such as: data security, disaster recovery, communication level and electronic controls.					
No.	Author	Year	Country	Sector	Framework	Type of research
2	Balgedom	2006	Algeria	Telecom	IT Governance	Empirical
Title	The impact of ICT on the strategic management of Economics firms					
Findings	The most important focus in the conclusion on the need to keep pace with technological development because of its role in the activation of the strategic management of organizations to cope with the pressures of modern complex competitive environment and achieve successes and advantages allow them to confrontation and survival. It is what Algerian economic institutions must strive for, and in particular Algeria Telecom company MOBILIS					
No.	Author	Year	Country	Sector	Framework	Type of research
3	Bakry, S. H., & Alfantookh, A.	2006	Saudi Arabia	Public	IT Governance / Cobit	Theoretical
Title	IT-governance practices: COBIT					
Findings	IT governance is introduced in main four steps, 1 st the review which identifies what is meant by ITG, then presenting main organization concerned with its development. 2 nd review highlights COBIT. 3 rd current state of Cobit and finally recommendations and comments of the future of IT governance developments.					
No.	Author	Year	Country	Sector	Framework	Type of research
4	ABU-MUSA, A. A	2007	Saudi Arabia	Public	IT Governance	Empirical
Title	Exploring Information Technology Governance (ITG) in Developing Countries: An Empirical Study					
Findings	Ensuring alignment of IT strategy with overall organizational strategy and supporting it as well as using the IT resources in a responsible manner, managing their IT- related risks appropriately to get the most of the IT development for business success, the entire above is only done by achieving better governance in the Saudi organizations.					
No.	Author	Year	Country	Sector	Framework	Type of research
5	Zaied, A. N. H., Khairalla, F. A., & Al-Rashed, W	2007	Kuwait	Public	ICT	Empirical
Title	Assessing e-Readiness in the Arab Countries: Perceptions Towards ICT Environment in Public Organisations in the State of Kuwait					
Findings	The overall e-Readiness of the public organizations for applying e-Government is only 54%. Ninety percent of the public organizations have adopted ambitious plans to deliver their e-Services within the 10 coming years, while others have seen a more unstructured development. In addition, 50% of the information technology employees in these organizations agreed that the network backbone technologies and infrastructure that connect their organizations to the public network is ready for applying the e-Government and they satisfied about the performance of their organization towards applying e-Government.					
No.	Author	Year	Country	Sector	Framework	Type of research
6	Abu-Musa, A.	2008	Saudi Arabia	Public	Cobit	Empirical
Title	Exploring the importance and implementation of COBIT processes in Saudi organizations: An empirical study"					

Findings	Employees in public sector realize COBIT process and domains impertinence, also lower percentage trust that such processes are satisfactorily implemented in their organization, keeping into consideration that banks service organizations and financial institutions show more concern and application of Cobit processes, also internal auditors, IT specialists and executive managers are the most who appreciated the importance of Cobit processes.					
No.	Author	Year	Country	Sector	Framework	Type of research
7	Ghazanfari, M., Fathian, M., & Rais S. M	2009	Iran	Banking / Government	IT Governance	Empirical
Title	Cobit a suitable frame work for measuring IT Governance in Organizations (Case Study for Governmental Banks Of Iran)					
Findings	For IT Governance in Iran, the average maturity level in the governmental banks is (1. 60), which means that Maturity level is not high enough regarding the importance of the adaptation of strategies of business with strategies of IT and the effective usage of IT that would benefit the institutions and helps to achieve strategic goals, also by losing the competition spirit in the banks industry and the satisfaction by applying just the mandatory rules and regulations, governmental banks desire for hosting E-commerce in business as a strategic tool has been vanished .					
No.	Author	Year	Country	Sector	Framework	Type of research
8	Khadra et al.	2009	Jordan	Banking	IT Governance	Empirical
Title	An Empirical Examination of Maturity Model as Measurement of Information Technology Governance Implementation.					
Findings	Local banks in Jordan applied effective awareness and communications, responsibility and accountability, and skills and expertise dimensions, on other hand, there is a shortage with others dimensions (tools and automation, "goal setting and measurement", and "policies, plans, and procedures")					
No.	Author	Year	Country	Sector	Framework	Type of research
9	Abu-Musa, A. A.	2009	Saudi Arabia	Public	Cobit \ IT Governance	Empirical
Title	Exploring COBIT processes for ITG in Saudi organizations: an empirical study					
Findings	IT is the responsibility of IT departments in Saudi organization to implement ITG COBIT process and domains and such process are neither audited nor formally conducted in the organizations. Useful information for senior management accountants, auditors, IT managers should be spelled out to clarify the implementation phase and the impact of Cobit on ITG in Saudi organizations.					
No.	Author	Year	Country	Sector	Framework	Type of research
10	Abu-Musa, A.	2010	Saudi Arabia	Public	IS Governance	Empirical
Title	Information security governance in Saudi organizations: an empirical study					
Findings	Even if the Saudi organizations majority are aware of the ISG's importance as a competence factor for the success of IT and corporate governance but still most of them do not have any written IS policy statements nor clear information security strategies nor plans for disaster recoveries , even roles and responsibilities of IS are not defined and communicated clearly, above all the alignment between ISG and the organization's overall business strategy is relatively poor also risk assessment procedures are not effectively nor adequately implemented, finally performance measurement system or properly functioning ISG processes are not found in the majority of Saudi organizations.					
No.	Author	Year	Country	Sector	Framework	Type of research
11	Yarifard, R., & Gowda, K. N.	2010	Iran	Banking	Cobit	Theoretical
Title	Applying CMMI to Determine the Stages of the COBIT Domains in the Banking Sector of Iran					
Findings	In most of the banking sectors, after the process of adopting Cobit framework, it appeared that Three Cobit domains (Planning and Organizing), (Acquisition and Implementation), and (Delivery and Support) - were at the stage of "Defined Processes. On the other hand the (Monitoring) domain was at the "Repeatable" stage in the Capability Maturity Model Integration "CMMI".					
No.	Author	Year	Country	Sector	Framework	Type of research
12	Al-Qudah, et al,	2012	Jordan	Hospital	IS	Empirical
Title	Impact of Information Technology on Management Control at Al Bashir Public Hospital: A Case Study of Jordan"					
Findings	Directors shall execute many training courses to enable the process of control connotation among staff members, and other growth segments in the field of information systems and mere latest technology at this topic.					
No.	Author	Year	Country	Sector	Framework	Type of research
13	Ayshosh and Wadih	2012	Algeria	Public	IT Governance	Theoretical
Title	IT governance: a strategic advantage in a knowledge economy					
Findings	IT Governance and it's various frameworks and models, measurement and maturity models, and related implementation tools, and its roles in ensuring the performance of the organization also tries to describe how IT Governance explains Solow's productivity paradox					
No.	Author	Year	Country	Sector	Framework	Type of research
14	Raeda I. abu Etaiwiy	2012	Palestine	Public	IT Risks Audit	Empirical
Title	Impact of the use of Information Technology Risks in Organizations Subject to Auditing on External Auditors' Job Quality in Gaza Strip					
Findings	External auditors usually faces a lot of risks, but one of the most well known risks in organizations is called the "ACCESS RISK", while "Environmental RISK" is the least one usually, the most measures affected by IT are efficiency and skills, on the otherhand both new clients' admission and retention of old ones are the least.					
No.	Author	Year	Country	Sector	Framework	Type of research

15	Bin-Abbas, H., & Bakry, S. H	2012	Saudi Arabia	Government/Telecom	ICT Governance	Theoretical / compare study
Title	Assessment of ICT governance in three different Saudi institutions using an integrated approach					
Findings	New ICT governance approach includes essential controls, incorporated knowledge management principles, structured according to a comprehensive scope and assessment measures including importance weights assessment indicators and implementation grades , assessing those three main Saudi institutions providing useful results and focus on problems that require attentions and finally presenting views on the control's importance derived the ICT staff opinions.					
No.	Author	Year	Country	Sector	Framework	Type of research
16	Nicho, M., & Mourad, B. A.	2012	UAE	Public ITG/ITIL	IT Governance	Theoretical
Title	Success factors for integrated ITIL deployment: An IT governance classification					
Findings	Structures, processes, relational mechanisms are the 3 IT Governance domains, under each one of them there are correspondent ITIL domain provide relevant context to categorize the best practices. The difference between "process and "relational mechanisms" contexts in ITG were mostly clear in the factor of "people" especially in "Organizational" and "communications" factors.					
No.	Author	Year	Country	Sector	Framework	Type of research
17	Salim, Othman, & Yahya	2012	Iraq /mosusl	Health	ISG	Empirical
Title	An Investigation of ISG Status in Mosul Health Sector					
Findings	Several facts regarding the Most of Mosul hospitals in Iraq: They are aware of the importance of ISG; they do not have disaster recovery plan or business continuity plan (BCP), neither have written information security policy nor security awareness program. There is no effective risk assessment procedures; implementation. Majority of Mosul hospitals do not have performance measuring systems or even a suitable working ISG processes.					
No.	Author	Year	Country	Sector	Framework	Type of research
18	Shivashankarappa, Smalov, Anba.	2012	Oman	Public	Cobit	Empirical
Title	Implementing it governance using COBIT: A case study focusing on critical success factors					
Findings	Many public sector enterprises in Oman have realized the importance of integration to provide comprehensive services to its citizens and thereby align to e-governance strategies. Many Organizations identified the critical success factors and then proposed a novel framework for achieving ITG.					
No.	Author	Year	Country	Sector	Framework	Type of research
19	Al Skafy et al.	2012	Jordan	Telecom	Cobit 5	Empirical
Title	The level of information technology governance in KULACOM-Jordan Company					
Findings	Moderate average of ITG is founded in Kulakom Jordan company, (E, D, and M), (BAI) COBIT principles are applied in highly degree in the company. The rest of COBIT principles such as: (A, P, O.), (D, S, S), (M, E, A) are applied in moderate degree.					
No.	Author	Year	Country	Sector	Framework	Type of research
20	Al-Zwyalif	2013	Jordan	Industrial	IT governance	Empirical
Title	IT Governance and its Impact on the Usefulness of Accounting Information Reported in Financial Statements					
Findings	IT governance affects the usefulness of accounting information and AIS. However, this usefulness is significantly influenced by the AIS. IT governance affects the usefulness of accounting information through its direct effects on the AIS.					
No.	Author	Year	Country	Sector	Framework	Type of research
21	Al Ramahi et al.	2014	Jordan	Banking	COBIT 5	Empirical
Title	Information Technology Governance Control Level in Jordanian Banks Using: Control Objectives for Information and Related Technology (COBIT 5)					
Findings	Executives must ensure that information technology works with the greatest possible efficiency to help achieve goals and objectives. Growing competitive advantage, ensuring compliance and continuity, security and privacy are essential in order to achieve effective management for Information Technology related risks as well as maximal benefits in technology investment.					
No.	Author	Year	Country	Sector	Framework	Type of research
22	Abu Hajar and Amineh	2014	Egypt	Government	IT governance	Theoretical
Title	The role of IT governance mechanisms in reducing information security risks to cut Of electronic financial manipulation in government units as a result of government system					
Findings	The mechanics of IT Governance is reducing these risks to reduce the financial electronic manipulation in light of the application of E-Government in the governmental units theoretically					
No.	Author	Year	Country	Sector	Framework	Type of research
23	Lubbad, R. R., & Ashour, Y	2014	Palestine	Government	IT Governance	Empirical
Title	Towards An Abbreviated Model of IT governance for Palestinian government sector According to COBIT 5 framework					
Findings	13 processes has high significant and necessary for implementing IT governance framework considerable by respondents concludes in Managing all process such as (Solutions Identification and Build, Strategy, Security Services, Relationships, Security, Assets, Continuity, the IT Management Framework, Problems, Operations, Business Process Controls), then					

	(Monitor, Evaluate and Assess Performance and Conformance), finally Ensure Benefits Delivery. The entire above are to be independent of context (international or national) and organizational settings.					
No.	Author	Year	Country	Sector	Framework	Type of research
24	Zyoud, Lateef, Nsour, Reem Mohammad	2014	Syria	Banking	Cobit	Empirical
Title	Determining the level of IT governance applicable Commercial Bank of Syria in Lattakia according to a framework (COBIT)					
Findings	The level of application of IT governance in the Commercial Bank of Syria Lattakia according to the framework (COBIT) is the four dimensions of the average level.					
No.	Author	Year	Country	Sector	Framework	Type of research
25	Harikrishnan, Zakareya,	2014	Bahrain	Public	IT Governance	Theoretical
Title	Bahrain Governance Framework: Towards Efficient Use of IT					
Findings	Bahrain enterprise architecture and governance is long term, continuous effort and is an "living" entity with many parts, it is a model of organization's enterprise and its future direction, enterprise architecture value to business operation should be more than simply information technology investment decision management, it is a main tool to reduce the response time for impact assessment, tradeoff analysis, reduce time-to-market, strategic plan redirection and tactical reaction, enterprise architecture and governance is not the end but a continuous journey.					
No.	Author	Year	Country	Sector	Framework	Type of research
26	Griffiths, Janahi, & Al-Ammal	2014	Bahrain	Public	IT Governance	Theoretical
Title	IT Governance from the theory to Practice: The importance of accountability					
Findings	Improving the Governance maturity needs to refocus on what is necessary to move beyond the current level and requires a clear strategy or plan for the oversight and management of IT activities. IT Governance is mainly related to IT decision-making authority. Accountability is an important part in IT Governance. Although organizations share more or less the same characteristics, they have different IT Governance maturity levels. IT Governance is specific for the organization and is the responsibility of the board and senior executives to give direction and control over IT					
No.	Author	Year	Country	Sector	Framework	Type of research
27	Alber and mayval	2015	Egypt	Banking	COBIT / IS	Empirical
Title	The impact of information security on banks in Egypt					
Findings	Implementation of ISO 27001 standards may affect profitability indicators as measured by "Return on Capital", while implementation of PCI-DSS standard may affect asset quality as measured by "Non-Performing Loan Ratio"					
No.	Author	Year	Country	Sector	Framework	Type of research
28	Madian A., NAzeer M.	2015	Syria	Banking	IT Governance	Theoretical
Title	IT in Public banks Branches in Latakia City (A Field Study)					
Findings	There is commitment of the public banks in Latakia city using exercising of IT governance that ensures the control on this resource, as well as, making sure that it enhances achieving wished fit with the strategy and aims of these organizations.					
No.	Author	Year	Country	Sector	Framework	Type of research
29	Karima A. Kadhim, Ahmad J. Hamoudi	2015	Iraq	Public	Cobit	Theoretical
Title	IT governance procedures: A proposed model in the light of Cobit's framework objectives					
Findings	General concept of information technology reflects the group elements interact with each other in order to perform specific tasks. And that the adoption of these techniques requires the provision of an appropriate environment to understand the hardware and software and provide adequate resources for the information technology, infrastructure and the skills required. COBIT framework can be guided to develop appropriate regulatory measures that achieve effective use of those components.					
No.	Author	Year	Country	Sector	Framework	Type of research
30	Vijayakumar, U., & Ilangoan, D.	2015	UAE	Public / SME's	IS AUDIT	Empirical
Title	A Quantitative Approach to Information Systems Audit in Small and Medium Enterprises					
Findings	This study focused on measuring the effectiveness of the IS audit functions in selected small and medium enterprises. The variations in KPI scores between (manufacturing, trading and services sectors) sectors in India and UAE for the SMEs. The Study found There are no significant variations in the Maturity Level Index scores, between the sectors in India. In addition, There are significant variations in the Maturity Level Index scores, between the sectors in the UAE. Furthermore, There are no significant variations in the Maturity Level Index scores, between the four regions (Abu Dhabi, Dubai, Other Emirates and Sharjah), in both countries India and UAE. There is no significant interaction between the two factors sector and region, in the determination of Maturity Level Index scores, in both the countries. Therefore, the auditor should examine the Information System policies and standards followed in an SME.					
No.	Author	Year	Country	Sector	Framework	Type of research
31	Dr. FIRAS M. ALKHALDI Dr. MINWER M. WRAIKAT	2015	Jordan	Public	ITG Governance	Empirical

Title	Portfolio Management And IT Governance: An Empirical Investigation using PLS Path Analysis					
Findings	There is a direct relationship between IT Governance and IT Portfolio Management Pillars; the Technique to Execute Organization Strategy (PMSE), Optimizing Resource Allocation across Projects (PMOS), Projectification of Business Strategy (PMPS), and Risk Balance (PMRB). Firms should take into considerations the importance of IT governance and its pillars accountability, transparency, participation and predictability in enhancing IT Portfolio Management.					
No.	Author	Year	Country	Sector	Framework	Type of research
32	Janahi, L., Griffiths, M., & Al-Ammal, H.	2015	Bahrian	Public	ITG	Empirical
Title	<i>A conceptual model for IT Governance: A case study research</i>					
Findings	Study enables public sector organizations to adopt an IT Governance model in a simple and dynamic manner. The model provides a basic structure of a concept; for instance, this allows organizations to gain a better perspective on IT Governance processes and provides a clear focus for decision-making attention. IT Governance model also forms as a basis for further research in IT Governance adoption models and bridges the gap between conceptual frameworks, real life and functioning governance.					
No.	Author	Year	Country	Sector	Framework	Type of research
33	Hejase et al,	2016	Lebanon	public	IT governance	Empirical
Title	Information technology governance in Lebanese organizations					
Findings	IT middle management represented by IT directors and IT managers are more knowledgeable about COBIT, ITIL, ISO 17799, PMBok and Balanced Score Card approaches in comparison to employees. IT structure / strategy are aligned with the corporate structure / strategy. Implementing IT governance at their organizations will affect their job responsibilities, IT investments in their organization are taken in consultation with the board. IT structure/strategy are aligned with the corporate structure/strategy.					
No.	Author	Year	Country	Sector	Framework	Type of research
34	Mahmoud y. Zgout	2016	Palestine	Audit institutions	IT Audit	Empirical
Title	The Effectiveness of using Information Technology (IT) in Auditing and its impact on improving the quality of Auditing service in the Gaza Strip					
Findings	IT is important in planning phase, control tests' execution and process test phases. Important role played by IT in the analytical audit implementation phase and balance examination is based on assessment of the client's ability to continue and comparing real results with the planned ones. IT usage in completion stage of audit process and report's issuance leads to improve quality of audit performance and documentation since this will assure more relevant evidence and objective result of audited items.					
No.	Author	Year	Country	Sector	Framework	Type of research
35	Waleed S. Afandi	2016	Saudi Arabia	Private	ITG	Empirical
Title	INFORMATION TECHNOLOGY GOVERNANCE ROLE IN ENHANCING IT PORTFOLIO MANAGEMENT: A CASE STUDY ON SAUDI ARABIA PRIVATE SECTOR					
Findings	1st there is an existence of the relationship between IT Governance and its Pillars: accountability, transparency, participation, and predictability. 2nd there is an existence of the relationship between IT Portfolio Management and its Pillars: a Technique To Execute Organization Strategy accountability, transparency,, Optimizing Resource Allocation across Projects (PMOS), Projectification of Business Strategy(PMPS),and Risk Balance (PMRB). 3rd there is a relationship between IT Governance and IT Portfolio Management.					
No.	Author	Year	Country	Sector	Framework	Type of research
36	Janahi, L. A. M.	2016	Bahrain	Public	ITG	Theoretical
Title	<i>The importance of accountability in IT governance practice in the public sector: a case study of the Kingdom of Bahrain</i>					
Findings	IT structure in public sector organizations needs revisiting to enable to better disseminating of IT activities , therefore lead into promoting an accountability culture through definite roles and responsibilities. In addition, the researcher pointed to the enacting forces and the importance of IT-related laws in defining internal controls and protecting the organization's assets from IT related risks.					
No.	Author	Year	Country	Sector	Framework	Type of research
37	Nakabi, N., Tadili, H., & Semaa, A.	2017	morocco	Public	ITG	Empirical
Title	The state of IT Governance in Moroccan Public Sector					
Findings	IT governance based on decisive factors namely: (i) setting up an IT leadership authority that must be granted to the CIO with a clear definition of his authorities and responsibilities. (ii) Defining organization's structure in terms of IT functionality and IT subordinates and describing limits and separations between Business/IT functions. (iii) Definition of clear decision-making processes in terms of portfolio management, the necessary IT investments. Decision-making in the public sector is an important challenge Many organizations are beginning to implement IT Governance practices. We note that IT Governance Structures are implemented in the main cases. For IT Governance Processes, we note that IT frameworks are not applied and specific processes like Service Level Agreements (SLAs), Activity Based Costing, ROI calculation, and measurements are not widely practiced.					

- The below shows the full version of the table used in the cloud computing study which was used in order to conclude the above related results.

Table (2) (UK) – United Kingdom (HU) – Hungary (GER) – Germany

1	Risk Management
UK	*Documented Risk assessment, Identification, and steps to mitigate. *Support the decision making by identifying good practices including (data and information security management system requirements, cyber risks, rules & guidance. Considerateness legal and regulatory risks of providing or using services in different jurisdictional. *Assess & manage operational risks of regulated services which are under the firm's responsibility. *Monitor concentration risk & consider actions after outsource provider fail. * Detailed breach's Notification & business recovery arrangements. *Ensure that remediation of breaches is included in the contract.
HU	*The institution's IT risk analysis covers the options for meeting the requirements in cloud service security principles, and phases of service's lifecycle. *To meet these requirements the institution either operates its own controls or stipulates in the contract that the service provider operates the controls and the institution obtains assurance of the operation thereof. *The management of the institution ensures that risk mitigating action plans are prepared. *The institution shall manage risks causing regulatory noncompliance with risk mitigation actions. *The institution defines the level of required assurance according to the risk level of the areas involved in order to maximize the assurance obtained focusing on the availability of the required cloud security and the existing of audit expertise.
GER	*Policies and instructions for the general procedure applicable to the identification, analysis, assessment and handling of risks and IT risks in particular are documented, communicated and provided according to SA-01.2 *The procedures for the identification, analysis, assessment and handling of risks, including the IT risks relevant to the cloud service are done at least once a year in order to take internal and external changes and influencing factors into account. *Identified risks are comprehensibly documented, assessed and provided with mitigating safeguards. *Top management parameters for the risk appetite and risk tolerances of the cloud provider are included in the policy for the risk management. *Top management is informed of the status of the identified risks and mitigating safeguards at least once every three months and in an appropriate form. *pointing on different jurisdictional problem, If the cloud provider is a German (AG) [public limited company] or a German (KGaA) [partnership limited to shares], § 91 Para. 2 AktG [German Public Companies Act] is applied.
2	International standards
UK	*Firms may wish to take account of the provider's adherence to international standards. *Assurance obtained from international standards for the delivery of critical or important operational functions or material outsourcing could be insufficient on its own, so firms should take account of any external assurance that has already been provided when conducting their own due diligence, since external assurance might be more relevant to firms consideration regarding well-understood standards, stabilized assessed services in data

	center , Uniformed service among the customer base, finally external audit is specific to the service a firm proposes to use.
HU	It is important to continuously monitor the changes in the regulations of the EU affecting cloud computing services, practices and best practice recommendations. * It is also essential to keep an eye on the Hungarian and EU data privacy provisions and practices—in particular to practices and resolutions concerning cross-border data transfers or data transfers to third countries. *Institutions are expected to comply with the national bank’ s previous recommendations on the safety of financial services provided online and on information system protection.
GER	The following standards were taken into account: •ISO/IEC 27001:2013 •CSA3 - Cloud Controls Matrix 3.01 (CSA CCM) •AICPA4 - Trust Services Principles Criteria 2014 (TSP) •ANSSI5 Référentiel Secure Cloud v2.0 (version intermédiaire validée du 20/03/2015, not published yet) •IDW6 ERS FAIT 5 (draft of a statement on accounting: "Grundsätze ordnungsmäßiger Buchführung bei Auslagerung von rechnungslegungsrelevanten Dienstleistungen einschließlich Cloud Computing" [Generally accepted accounting principles for the outsourcing of accounting-related services including cloud computing], version of 4 November 2014) •BSI IT-Grundschutz Catalogues, 14th version 2014 •BSI SaaS Sicherheitsprofil 2014 [BSI SaaS security profiles 2014]

3	Oversight of service provider
UK	Institutes retain full accountability for discharging all of their responsibilities under the regulatory system so they should be clear about the provided services and where the firm’s V.S the Service provider’s responsibility begins and ends. Also, responsibility for the day-to-day and strategic management of the service provider should be allocated. * Ensure staff skilled and resourced to test outsourced activities, identify, monitor and mitigate against arising risks, and manage an exit a service provider.
HU	*The institution obtains a high level of assurance about the protection of the cloud service provider’s data centers, computing and communication devices, and of ensuring the high availability thereof; * assurance about the separation of the cloud service provider’s clients and systems depending on the cloud service model such as Physical access and environmental controls of physical resources, Logical access controls and security settings of the virtualization infrastructure, operating systems, middleware, databases and applications * The institution obtains assurance of the service provider’s information security governance system, processes and the operating of respective controls * The institution obtains assurance of the controlled operation of the service provider’s IT operational processes.
GER	Roles and responsibilities of the cloud provider and the cloud customer, including the duties to cooperate and corresponding controls at the cloud customer should be described in the system description and documented without putting cloud provider at risk by this documentation. In service level agreements *The cloud provider should provide comprehensible and transparent specifications regarding its jurisdiction as well as with respect to data storage, processing and backup locations. *The cloud provider provides comprehensible and transparent specifications regarding applicable disclosure and investigatory powers of government agencies which allow access to data of the cloud customer. *The specifications must allow an expert third party to assess the general suitability of the cloud service for the customer application. * regarding available and valid certifications and certificates of independent third parties, which allow an expert third party to assess the general suitability of the cloud service for the customer.

4	Data security
UK	A security assessment should be carried out by a firm. * Data residency policy with the provider which sets out the jurisdictions in which the firm’s data can be stored processed and managed. * Provider’s data loss & breach notification processes are aligned with the firm’s risk appetite and legal or regulatory Obligations. *In case of using public clouding consider data segregation. * mitigate security risks. * Data sensitivity how it is transmitted stored and encrypted. (agree a data residency policy with the provider upon commencing a relationship with them, which sets out the jurisdictions in which the firm’s

	data can be stored, processed and managed. This policy should be reviewed periodically ● understand the provider's data loss and breach notification processes and ensure they are aligned with the firm's risk appetite and legal or regulatory obligations ● consider how data will be segregated (if using a public cloud) ● take appropriate steps to mitigate security risks so that the firm's overall security exposure is acceptable ● consider data sensitivity and how the data are transmitted, stored and Encrypted, where necessary 9.)
HU	The institution should identify and applies security classification to the data that is planned to be outsourced to the cloud service provider in line with the legal regulations and its own data protection rules and then defines data security requirements. * Assurance regularly of the cloud service provider's full compliance with data security is required at least annually. * Data transmission between the institution and the cloud, between the resources in the cloud, and between the cloud and other external service providers is protected from unauthorized access and modification. * The data stored in the cloud is secured from unauthorized access and modification, and its availability is ensured. * Management and reporting of security incidents. The institution should be immediately informed of security incidents and their resolution; * Fraud investigation. The institution expects the service provider to support such investigation, and a regulated fraud investigation process; * Protection against malicious codes, including the installation, regular update and central monitoring of security tools, as well as regular antivirus checking of the network and devices;
GER	*It should be noted that the security of cloud services is an ongoing task. *The cloud provider provides comprehensible and transparent specifications regarding its jurisdiction as well as with respect to data storage, processing and backup locations, which allow an expert third party to assess the general suitability of the cloud service for the customer application. *Data of the cloud customer shall only be processed, stored and backed up outside the contractually agreed locations only with the prior express written consent of the cloud customer. * The cloud provider uses secure network protocols for the import and export of information as well as for the management of the service in order to ensure the integrity, confidentiality and availability of the transported data. * Assuring a consistent and comprehensive approach regarding the monitoring, recording, assessment, communication and escalation of security incidents. * Policies and instructions with technical and organizational safeguards are documented, communicated and provided according to SA-01 in order to ensure a fast, effective and proper response to all known security incidents

5	Data Protection Act (DPA)
UK	A firm should comply with the eight principles of the DPA and any associated guidance. 1. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless (a) at least one of the conditions in point 2 is met, and (b) In the case of sensitive personal data, at least one of the conditions in point 3 is also met. 2. Personal data shall be obtained only for one or more specified and lawful purposes and shall not be further processed in any manner incompatible with that purpose or those purposes. 3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed. 4. Personal data shall be accurate and, where necessary, kept up to date. 5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes. 6. Personal data shall be processed in accordance with the rights of data subjects under this Act. 7. Appropriate technical and organizational measures shall be taken against unauthorized or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data. 8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

HU	* The institution obtains assurance that the cloud service provider adheres to the relevant data protection rules and legal regulations. (implementation) a) The institution identifies the differences between the data protection requirements relevant to the institution and the cloud service provider's data protection commitments, practices and data reporting obligations. When identifying these differences, the institution: ⊗ Compares the service provider's data handling and data processing practices with the requirements relevant to the institution; ⊗ Assesses when and how the service provider is obliged to provide data to authorities (e.g. based on regulations effective in the service provider's country), and what notification the service provider undertakes to provide when performing such obligations; ⊗ Assesses when and how the service provider's subcontractors, other business partners as well as data subjects can access the data, and if the institution deems it risky, the institution does not allow the use of respective subcontractor or other third party at its discretion. b) The institution applies contractual conditions that manage the differences identified, thereby ensuring full compliance. *The institution ensures the safe handling and processing of personal, banking and insurance data, as well as data classified as secret by other sectorial laws, in compliance with the data protection regulation.
GER	* Legally, regulatory and statutory prescribed requirements, as well as the procedure to comply with these requirements and regulations must be identified, documented and updated regularly by the cloud provider for the cloud service related to the respective application. * Requirements for the protection of personal data (e. g. according to BDSG [German Federal Data Protection Act] or EU Data Protection Directive). *Preventing violations against statutory or contractual duties with respect to information security. * data protection principles: • Legal permission/consent. Processing personal data is prohibited unless the data subject has given consent, or the processing is permitted by law. • Direct collection. Personal data must be collected directly from the data subject. • Data minimization. Only data required for the specific operation can be processed. Processing systems must be designed with the aim of collecting, processing and using as little personal data as possible. In particular, personal data is to be aliased or rendered anonymous as far as possible. • Purpose limitation. Data collected for a specific purpose cannot be used for other purposes. Data must be deleted or anonymized as soon as it is no longer necessary for the purpose for which it was collected or processed. • Transparency. The data controller must provide comprehensive information about the identity of the data controller, the purpose of the collection/processing/use of the data and the categories of recipients. • Access. A data subject must be given access to his personal data stored by the data controller. • Accuracy. Personal data must be accurate. Incorrect data must be corrected. • Data security. Technical and organizational measures must be taken against unauthorized or unlawful processing of personal data and against accidental loss/destruction/damage of personal data.

6	Effective access to data
UK	Firms should require effective access to data related to the outsourced activities for regulated firms, their auditors, regulators and relevant competent authorities. *Ensure notification requirements on accessing data are reasonable. * No restrictions on the number of requests to access or receive data by auditors or regulators. *Ensure that regulators will treat any information disclosed in accordance with the confidentiality obligation set out in (FSMA). * Contract enables regulator or auditor to contact service provider directly in case firm cannot disclose data for any reason. *Ensure jurisdictions allowance of stored data access for UK regulators.
HU	* The data stored in the cloud is protected from unauthorized access and modification, and its availability is ensured. * establishing sufficient logical data access controls is considered one of the data security requirements within its scope of authority. * The institution restricts access to the cloud service to the necessary

	and sufficient level in line with the relevant business requirements, by using suitable identification, authentication and authorization solutions. * a) The institution establishes a documented and approved user and access rights management procedure, which is at least at an equal level with the procedure used for local systems in order to control access to the cloud service; b) The user and access rights management procedure cover the processes for requesting, approval, setting up access rights, regular review and revocation; c) Privileged users are identified by multi-factor authentication, their activities related to the service are logged, the logs are regularly reviewed, and the institution is also entitled to review; d) The institution defines conflicting roles and accesses in connection with the cloud service; e) The institution has comprehensive and up-to-date records of authorized users and their access rights, including privileged, technical and external / remote users, which can be compared with the actual system settings; f) User and access rights management activities are regularly monitored (who requested, Authorized, set, reviewed or revoked what right for whom). * Assesses when and how the service provider's subcontractors, other business partners as well as data subjects can access the data, and if the institution deems it risky, the institution does not allow the use of respective subcontractor or other third party at its discretion.
GER	* A role and rights concept based on the business and security requirements of the cloud provider as well as a policy for the management of system and data access authorizations are documented, communicated and provided according to SA-01 and address the following areas: • Granting and change (provisioning) of data access authorizations on the basis of the "least-privilege principle") and as is necessary for performing the required tasks ("need-to-know principle"), • Separation of functions between operative and controlling functions (also referred to as "separation of duties"), • Separation of functions in the administration of roles, approval and granting of data access authorizations, • Regular review of granted authorizations, • Withdrawal of authorizations (de-provisioning) in case of changes to the employment relationship, • Requirements for the approval and documentation of the management of system and data access authorizations. * System access authorizations for users under the responsibility of the cloud provider (internal and external employees) are granted in a formal procedure. * Granting and change of data access authorizations for users under the responsibility of the cloud provider comply with the policy for the management of system and data access authorizations. - Data access authorizations comply with the "least-Privilege principle"). - Formal approval is given by an authorized person, before the data access authorizations are set up - Technically assigned data access authorizations which do not exceed the formal approval. * Data access authorizations of users under the cloud provider's responsibility (internal and external employees) are withdrawn in the case of changes to the employment relationship (dismissal, transfer, longer period of absence/sabbatical/parental leave) promptly, Data access authorizations of users under the cloud provider's responsibility (internal and external employees) are reviewed at least once a year in order to adjust them promptly to changes to the employment relationship

7	Access to business premises
UK	For some firms' contracts must allow business premises' access, which are relevant for the exercise of effective oversight. * This does not necessarily require access to all business premises; Data centers might have limit access to it. * Provide reasonable prior written notice of this visit, except when there is an emergency or crisis situation. * Internal assigned auditor could undertake the visit. *scope of visit could be limited only to the services that are used by the firm' group. *If the regulator deems it necessary and required under applicable

	legal and regulatory requirements to make a visit and outsource provider should cooperate in working hours or in short not in case of emergency
HU	* The institution obtains assurance that its resources (processing and storage capacities) located in the cloud are protected against unauthorized physical or logical access, damage and theft. * The institution obtains a high level of assurance about the protection of the cloud service provider's data centers, computing and communication devices, and of ensuring the high availability thereof; * The assurance covers at least the following, depending on the cloud service model: 1. Physical access and environmental controls of physical resources; * The technical separation of resources belonging to different clients, with special attention to management interfaces (e.g. web-based administrative interfaces, application programming interfaces – APIs); 5. Management of cryptographic keys, including the use of HSM (Hardware Security Module).
GER	The perimeter of premises or buildings which house sensitive or critical information, information systems or other network infrastructure are protected in a physically solid manner and by means of appropriate security safeguards * Access to the premises or buildings which house sensitive or critical information, information systems or other network infrastructure is secured and monitored by means of physical site access controls in order to avoid unauthorized site access. * Structural, technical and organizational safeguards are taken to protect premises or buildings which house sensitive or critical information, information systems or other network infrastructure against fire, water, earthquakes, explosions, civil disturbances and other forms of natural threats and threats caused by humans.

8	Change Management
UK	Risks can be introduced when changes are made to processes and procedures. *Firms should have a comprehensive change management process. *establishing what provision has been made for making future changes to technology service provision. *establishing how the testing of changes will be carried out.
HU	The institution obtains assurance regularly of the cloud service provider's full compliance with data security and protection requirements – at least annually, or after significant changes in the relevant business process, service, configuration or legal environment. The institution also relies on independent third parties' audits or certifications for obtaining assurance. The institution obtains assurance of the controlled operation of the service provider's IT operational processes / Change and version management; configuration management;
GER	Complying with the security targets in case of new developments and procurement of information systems as well as changes The procedures for the identification, analysis, assessment and handling of risks, including the IT risks relevant to the cloud service are done at least once a year in order to take internal and external changes and influencing factors into account. Policies and instructions with technical and organizational safeguards for the proper management of changes to information systems for the development or operation of the cloud service, including middleware, databases, operating systems and network components are documented, communicated and provided according to SA-01 The principal of a change performs a risk assessment beforehand. All configuration objects which might be affected by the change are assessed with regard to potential impacts. The result of the risk assessment is documented appropriately and comprehensively. All changes are categorized on the basis of a risk assessment (e. g. as insignificant, significant or far-reaching impacts) in order to obtain an appropriate authorization prior to making the change available to the production environment. All changes are prioritized on the basis of a risk assessment (e. g. as low, normal, high, emergency) in order to obtain an appropriate authorization prior to making the change available to the production environment.

	All changes to the cloud service are subjected to tests (e. g. for integration, regression, security and user acceptance) during the development and before they are made available to the production environment. The tests are carried out by adequately qualified personnel of the cloud provider. According to the service level agreement (SLA), changes are also tested by the customers (tenants) suitable for this. Personnel of the cloud provider. According to the service level agreement (SLA), changes are also tested by the customers (tenants) suitable for this. Before a change is released to the production environment, it must be reviewed by an authorized body or a corresponding committee whether the planned tests have been completed successfully and the required approvals are granted. Emergency changes are to be classified as such by the change manager who creates the change documentation before applying the change to the production environment. Change management procedures include role-based authorizations in order to ensure an appropriate separation of duties regarding the development, release and migration of changes between the environments.
--	--

9	Continuity and business planning
UK	Firm should have arrangements to ensure that it can continue to function and meet its regulatory obligations if outsourced services are interrupted. *Likelihood and Impact of an unexpected disruption should be considered. * document Firms strategy, including recovery from an event, plans for communicating and regularly testing. * put in place arrangements to ensure the regulator has access to data in case of disruption.
HU	When a business need for cloud services is identified, the institution examines the viability of using a cloud service in view of the business needs, costs and risks of cloud services, security requirements and legal requirements. Preparation for decision and planning shall be done as follows. The institution assesses, already in the decision drafting phase, the detailed tasks to achieve compliance with each relevant legal regulation³. By using cloud services, the responsibility for operating in compliance with regulations remains with the institution, therefore the institution assesses beforehand how it can meet its obligations, and how the cloud service provider ensures the necessary controls and monitoring capabilities. Before using cloud services, the institution ensures that full regulatory compliance can be achieved for the cloud services. A declaration, contractual obligation, or liability insurance by the service provider (a medium level of assurance); ● Audit reports issued by third parties that were engaged by the service provider, and certificates to international standards (a medium or high level of assurance 5); ● Tests or certifications performed directly by the institution or by accredited certification entities that were engaged by the institution (a medium or high level of assurance 6).
GER	The top management is specified as the process owner of the business continuity and contingency management and bears the responsibility for the establishment of the process in the company and compliance with the policies. They must ensure that adequate resources are made available for an effective process. Policies and instructions for determining impacts of possible malfunctions of the cloud service or company are documented, communicated and provided according to SA-01. Based on the business impact analysis, a uniform framework for planning the business continuity and business plan is introduced, documented and applied in order to ensure that all plans are consistent. The business impact analysis as well as the business continuity plans and contingency plans are verified, updated and tested at regular intervals (at least once a year) or after essential organizational or environment-related changes.

10	Exit plan
UK	Firms need to ensure that they are able to exit outsourcing plans without undue disruption to their provision of services or compliance with regulatory. * understood, documented and fully tested exit plans. * maintain business continuity even if transition to an alternative service provider. *obligations to ensure outsourcing provider cooperate with firm for smooth transition. * how to remove data from the service provider's systems on exit. * monitor concentration risk and consider what action it would take if the outsource provider failed.

Ger	The institution must assess and manage the risks of abandoning (exiting) a cloud service, including the possibility of an unexpected, unplanned exit. The institution prepares an exit strategy and an action plan in order to lower the risks.
HU	The institution stipulates such service conditions that allow the exit from the cloud without Difficulty especially the providing of the stored data in a format that can be interpreted and used irrespectively of the cloud service; Ensures and tests the operability of the impacted business processes in case the cloud service is discontinued with a risk proportionate method and frequency. In the preparation phase, the institution provides the required personnel, assets and technology for the exit, as well as the required legal and contractual conditions - The infrastructure required for taking back the data and operating the service so that the business processes relying on the affected systems can operate without interruption, or with a level of disruption that can still be tolerated by the business needs; - The expertise and project team necessary for exiting from the cloud service and resuming local operations, or transferring the service to another provider; - The detailed exit implementation plan, including the scheduling of the exit, IT and security requirements, the tools to be used, test cases and scripts, as well as the acceptance criteria for the testing and for the service taken back or migrated to another service provider; - A detailed step-by-step time schedule, defining milestones and resources, assigning responsibilities, including a worst-case scenario; - The cooperation obligations, tasks and responsibilities of the entities involved in discontinuing the service; - The scheduling and the conditions of providing the service and the availability and transfer of data during the exit. The institution carries out the steps defined in the exit strategy and action plan during the exit: - Installation of migration tools; - Testing the downloading of the data in a test environment; - Downloading the data in the production environment, and taking back the service based on the scripts; - Validating based on the acceptance criteria; verifying the correctness of the data taken back; and closing the migration; - Follow-up for fixing errors after migration; - After the successful exit from the cloud, deleting the data at the service provider, including both live, backup and archiving environments according to the contractual conditions. The service provider shall provide assurance (declaration) of deleting the data; - Terminating the unnecessary IT and communication connections with the service provider.

11	Legal and regulatory considerations
UK	*The Firm should have a documented business case in support of the decision to use one or more service providers. *Ensure service is suitable and considering any relevant legal or regulatory obligations. *Ensuring that outsource agreement will not worsen the firm's operational risk and considering the risk of using such services. *knowing which jurisdiction, the service provider business' premises are located in to identify by which law it is governed thus if it is out of UK the firm should ensure effective access to data and business premises for auditor and relevant regulator and maintain an accurate record of contracts.
HU	*The institutions should ensure that full regulatory compliance can be achieved for the cloud services before they are used, and the cloud service provider should ensure the necessary controls and monitoring capabilities. *Complying with the relevant provisions of act L of 2013 electronic information security in state is compulsory if the institution/systems are identified as an entity of key importance in the financial sector.