Academy Journal of Social Sciences

Online ISSN: 2974-3532 • Volume 1; January 1; 2025

The Impact of Information Technology Governance on Reducing Cloud Accounting Information Systems' Risks: An Evidence form Egypt

Rana E. Elshorbagy[1], Ahmad A. Abu-Musa[2], Hatem M. El-Shishin[3], Laila Aladwey[4]

Received: 13 August 2024; Revised : 23 August 2024; Accepted : 9 September 2024; Published : 01 January 2025

Abstract

The study aims to investigate the possible contribution of Information Technolgy Governance (ITG) towards mitigating the risks associated with Cloud Accounting Information Systems (Cloud AIS). This goal has been accomplished by determining the categories and characteristics of the most significant potential risks associated with Cloud AIS; explaining how Cloud AIS raises potential risks that the Egyptian business environment faces, and outlining a proposed approach for ITG to lower those risks by putting in place an efficient ITG framework in the Egyptian business environment. A questionnaire-based field study is carried out to investigate how ITG can lower the risks associated with Cloud AIS. The questionnaires were sent to 215 respondents, including members of academic staff in the Egyptian uninveristies, accountants, Cloud implementation engineers, and IT risk managers. Nintiy-five valied and usable questionnaires are analyzed. The results indicated that risks facing the Egyptian business environment are increased by implementing Cloud AIS. Furthermore, the results demonstrated that implementing ITG lowers the possible risks associated with Cloud AIS in Egypt**Keywords**

Keywords: (Cloud AIS, Risks of Cloud AIS, IT governance, Field Study, Egypt)

To cite this paper:

Elshorbagy ,R., Abu-Musa,A., El-Shishin, H., Aladwey, L. (2025). The Impact of Information Technology Governance on Reducing Cloud Accounting Information Systems' Risks: An Evidence form Egypt. Academy Journal of Social Sciences. 3 (1), 70-111

[1] Demonstrator of Accounting Department, Faculty of Commerce, Tanta University
[2] Professor of Accounting Information Systems, Faculty of Commerce, Tanta University
[3] Professor of Cost Accounting, Faculty of Commerce, Tanta University
[4] Associate Professor in Accounting, Faculty of Commerce, Tanta University

1. Introduction:

Nowadays, Information Technolgy (IT) becomes essential to the survival of most organizations. This is because it facilitates corporate strategies and acts as a catalyst for modifying different organizations' business models. IT is a hardware and software combination that makes gathering, storing, and sharing knowledge, data, and information easier. For organizations, the use of IT has yielded significant benefits. However, there are significant costs, resources, time, and expertise associated with the setup and upkeep of IT. Some businesses are utilizing Cloud computing in their accounting information systems due to the difficulty in obtaining these requirements (Lioliou, 2019).

Cloud computing has emerged as an important strategy for enabling organizations around the world to enhance their competitiveness by gaining access to the distinctive expertise and technological competencies of Cloud service providers. The result of this trend is a significant upsurge in Cloud computing. The Cloud computing market is expected to reach a value of USD 864 billion by 2025 (Business wire, 2020).

Although Cloud computing has grown significantly in recent years and offers many potential advantages for an organization, there are risks associated with using Cloud computing (Abu-Musa, 2011). Risks are preventing organizations from achieving the goals or benefits of Cloud AIS through pointless and disappointing Cloud AIS engagements. Despite the advantages of Cloud AIS, there is a claim that if the project is not managed well, there could be serious risks involved (Abu-Musa, 2011). Consequently, Cloud AIS falls under the risk management system in organizations. The active involvement of Cloud AIS in decision-making regarding the involvement of third parties is implied by the implementation of the risk management system.

The Cloud makes data and software accessible online anytime, anywhere, from any device. In the case of Cloud accounting, you keep your business books online. That includes records of income and expenses, and assets and liabilities. The information is encrypted, much like a bank's, so only people with the login can view the data.

Implementing and training people in Cloud computing technology requires significant investments in time and resources. Organizations may decide to use Cloud computing in accounting information systems (AIS) for various reasons. These include cost savings, insufficient resources, lack of specialized knowledge, and the desire to focus on core activities.

Despite these potential benefits, implementing Cloud AIS has accompanying risks as well (Van Peursem and Jiang, 2008). Accordingly, Cloud AIS related benefits and associated risks should be weighed and carefully considered to ensure Cloud AIS implementation success. Because of the risks associated with Cloud AIS and the potential harm they could do to organizations, it is, therefore, necessary to conduct ongoing risk research and develop governance practices that offer practical frameworks for reducing the risks associated with these arrangements.

Because it is closely linked to the success of Cloud AIS, the governance of Cloud AIS is acknowledged in previous literature (Gorla and Somers, 2014) as having persistent strategic importance for practice. The rapidly changing global market necessitates updated knowledge on effective

governance for the evolving practice of Cloud AIS. As a result, a new term for governance—IT governance—has emerged to implement governance on Cloud AIS. High-level IT governance models are being developed, and IT governance is currently a top priority for many organizations.

IT governance refers to the set of guidelines, rules, and procedures that are used to coordinate IT and business efforts to maximise business value through the application of efficient IT performance, risk, and control management. Consequently, to help organizations effectively mitigate some of the potential risks associated with this arrangement, this study examines the risks associated with Cloud AIS and suggests an IT governance approach.

2. Research Problem:

Depending on the wide use of information technology which has become an essential part of conducting business for many small, medium, and large companies (Haynes & Li, 2016). Therefore, it has become natural to use Cloud computing in the accounting field which is called Cloud AIS to maintain business continuity and achieve competitive advantage. There are also advantages and benefits that drive the adoption of Cloud AIS, but there is a set of defects and risks that threaten organizations with failure and may expose them to exit the market.

In addition, there are risks and threats arising from Cloud AIS which affect the security, confidentiality, integrity, and reliability of information, so the ITG framework for information preservation must emerge, as shown in figure (1):

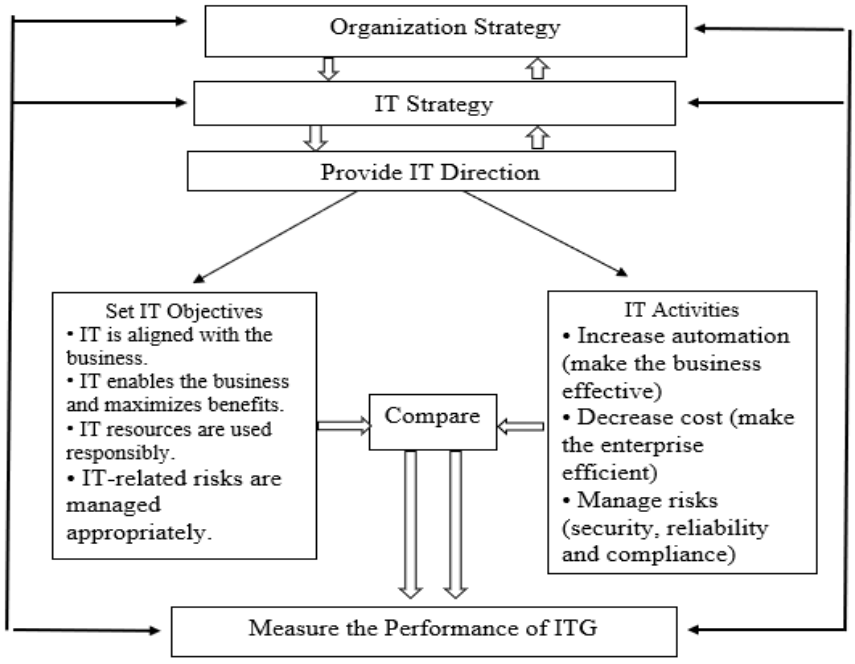

Figure (1): ITG Framework

Source: (Abu-Musa, 2007, P: 82)

3. Research Questions:

Based on the above, the main research question is: "Is there an impact for ITG in reducing Cloud AIS risks?". It is argued that COBIT 5 and COSO-ERM along with the alignment between business and IT strategies and performance have become the most important guidelines for information technology governance (ITG), which provide organizations with a useful tool to start evaluating their ITG systems (Abu-Musa, 2009). So, in this study, the researchers will examine the integration between COBIT 5 and COSO-ERM with business strategy and IT performance for enhancing ITG and reducing Cloud AIS potential risks.

This study examines impact of implementing ITG strategy on Cloud AIS risks to help organizations effectively reduce their potential Cloud AIS risks. The main research question is divided into the following sub-questions:

1. What are the most important potential risks of Cloud AIS?
2. What is the potential impact of implementing COBIT 5 on the risks of Cloud AIS?
3. What is the potential impact of implementing COSO-ERM 2017 on the risks of Cloud AIS?
4. Is it possible for implementing IT governance to reduce the potential risks of Cloud AIS?

4. Research Objectives:

The main research objective of the study is to identify the impact of implementing information technology governance (ITG) in reducing Cloud accounting information systems' risks. This objective can be achieved by the following sub-objectives:

1. Identifying the nature and types of the most important potential risks of Cloud AIS.
2. Examining the role of COBIT 5 in reducing the risks of Cloud AIS.
3. Examining the role of COSO-ERM with strategy and performance in reducing the risks of Cloud AIS.
4. Introducing a proposed approach for IT governance for reducing the risks of Cloud AIS through the integration between COBIT 5 and COSO-ERM with business strategy and IT performance.

5. Research Importance:

One can see from reviewing the prior studies on IT governance and Cloud AIS that the significance of this study comes from:

1. Organizations use IT developments at an ever-increasing rate. Additionally, there is an urgent need to lower the risks associated with Cloud AIS as an IT development. In modern accounting theory, this arrangement has taken on a special significance. The expansion of Cloud computing applications in the Egyptian environment, which emphasizes the significance of researching the risks to which organizations are exposed, is the reason for the research's significance.
2. To the best of the researcherss' knowledge, there is no comprehensive approach to IT governance that can be used to lower the risks associated with AIS in the Cloud. The integration of COBIT 5 and COSO-ERM with strategy and performance, which have been discussed in the literature to examine their role in reducing risks of Cloud AIS, is used in this research to close this gap since there aren't any studies about the potential function of this integration.

3. To the best of the researchers's knowledge, there is a dearth of research on the practical implementation of IT governance in developing countries in general and specifically in the Egyptian environment. The majority of prior studies were carried out in developed countries, and only a small number of studies concentrated on this topic.

6. Literature Review and Hypotheses Development:

The Study of Al-Wattar and AL-Shafeay (2023) aims to identify the aspects of (ITG) that may lower CAIS risks in Iraqi industrial enterprises. A snowball sample technique was employed in this study to gather data from 291 workers employed by Iraqi industrial firms. The findings demonstrated that the reduction of CAIS risks is strongly and favorably impacted by each of the (ITG) dimensions (Firm & Planning, Acquire & Implementation, Delivery & Support, Monitoring & Evaluation, Guidance & Control).

Furthermore, the study of Yau-Yeung et al. (2020); aims to show how Cloud computing has affected the practice of accounting. This empirical study applied transaction cost economics (TCE) to explore the risks of Cloud-based accounting systems and services in Australia and identified several risk mitigation strategies organizations adopt.

Based on interviews with accounting practices, amongst others, were classified according to the Technology-Organization-Environment framework. The findings suggested that Cloud accounting not only introduces specific risks to the "accounting process" but some of the known risks associated with other Cloud-based applications are more pronounced. While transaction-specific factors such as vendor selection and contractual arrangements were considered important as risk mitigation strategies, internal measures including policy development and staff training were seen as critical to Cloud accounting.

Moreover, the study of Liew and Abdul Hamid (2023) finds that universities must manage IT resources more efficiently as a result of the increasing integration of IT into the higher education system. Prior studies on the ITG of higher education institutions in Malaysia have shown a low level of general ITG awareness. Since top management continues to be the most influential group in determining the direction of IT in universities, this study aims to explore the role that top management plays in culture formation within ITG. As case study subjects, two technical universities with various ITG structures are selected. Five participants with a minimum of ten years of IT experience, each from two technical universities, are selected to serve as the main subjects of qualitative interviews.

For this study, the main technique for analysing both manifest and latent content is thematic analysis. Results show that top management's IT priorities have a significant impact on how ITG is implemented in universities. The deployment of ITG has been badly impacted by low IT priority. On the other hand, a university that places a high priority on IT can create an atmosphere that supports the development of a positive IT culture on campus. The results can help the university focus on clarifying the duties and responsibilities of upper management in relation to ITG in order to develop a long-lasting culture in ITG implementations.

In the same context, the study of Joshi et al. (2018) looks into the relationship between a firm's disclosure of its IT governance practices and the maturity of its IT governance processes. Additionally,

it looked at whether an industry's strategic use of IT causes a regular variation in the disclosure of IT governance.

Based on a content analysis of annual reports and a field survey on the maturity of the implementation of COBIT processes. The findings showed how IT governance frameworks can promote accountability and transparency by improving external reporting of pertinent IT information to external stakeholders, particularly in environments where IT plays a significant strategic role.

Additionally, the study of Abass et al. (2023) aims to evaluate the impact on corporate governance (CG) and audit risk (AR) of the integration of internal control frameworks under the Committee of Sponsoring Organizations (COSO) framework and information technology governance under the Control Objectives for Information and Related Technologies (COBIT) framework. Tools developed by earlier writers were used to measure the study variables. For the years 2019 through 2022, thirty Iraqi banks that are listed on the Iraq Stock Exchange were selected. The results of the study corroborate those of earlier investigations.

According to the study, COBIT has actively supported a range of banking operations and increased their effectiveness by utilising electronic devices and providing services promptly. Governance and audit readiness were significantly and favorably impacted by the integration of COBIT and COSO. The study's conclusions show how important regulatory frameworks are for improving banking performance.

Furthermore, the study of Gbadeyan et al. (2017) aims to determine the feasibility of Cloud computing being affected by security and privacy concerns. Failure to consider security and privacy issues could result in legal implications, reputational damage, financial problems, and a decrease in public trust in the healthcare provider.

This study used a case study conducted in Canada. In order to highlight Cloud computing risk assessment areas, this paper used Alberta's Privacy Impact Assessment (PIA) requirement and COBIT 5 for Risk as guidance. It also presents an IT governance and risk mitigation approach helpful for Cloud computing adoption in the healthcare industry. The results indicated that healthcare providers could make use of the proposed approach presented in this paper to reduce and continuously assess Cloud computing risks from an IT governance perspective.

In light of the findings provided in the previous literature, the following main hypothesis and three sub-hypotheses which are derived are suggested:

H_1: Adapting ITG has a significant positive impact on reducing the risks of Cloud AIS.

H_{11}: There is a significant positive impact of applying the COBIT5 framework on reducing the risks of Cloud AIS.

H_{12}: There is a significant positive impact of applying COSO-ERM 2017 on reducing the risks of Cloud AIS.

H_{13}: The integration between COBIT 5 and COSO-ERM 2017 has a positive impact on reducing the risks of Cloud AIS.

7. Research Method

The work presented in the current study combines theoretical and empirical work. The theoretical portion of this study used Analytical Descriptive Approach to study and analyze the risks associated with AIS in the Cloud, and it utilized COBIT 5 and COSO-ERM 2017 to determine the best IT governance strategy to reduce these risks. The Deductive Approach is also used to deduce the research hypotheses that will be empirically examined in the field study.

The empirical portion of this study used the Inductive Approach to conduct an applied study using a questionnaire to gather information about the risks associated with Cloud-based application integration services (AIS) and the role that IT governance would play in reducing those risks in the Egyptian environment. The questionnaire was sent out to a sample of academic staff members, accountants, IT risk managers, and Cloud implementation engineers.

8. The Study Population and Samples:

The researcherss' strategy is to conduct a field study, to explore and investigate the impact of ITG on reducing Cloud AIS. Therefore, the study population is represented in member of academic staff members, accountants, IT risk managers, and Cloud implementation engineers.

Accordingly, the study sample includes a selected number of different jobs in different sectors such as, universities, banks and companies. Thus, a total of 215 copies of the revised questionnaires were distributed to a selected number of different universities, companies and banks, the research ended with 95 valid and usable questionnaires representing 44.2% response rate after excluding incomplete and invalid questionnaires.

9. Data Collection:

The collection of data is the crucial operation in the execution of good research design. Data was collected using the final, developed, self- administered questionnaire (Appendix A) to investigate the impact of ITG on reducing Cloud AIS risks. A cover letter was used and attached with each questionnaire. The cover letter introduces the researcherss to the respondent and highlights the objectives of this survey. In addition, the respondents were promised anonymity and confidentiality to encourage them to participate in this survey.

Questionnaire (Appendix A) was divided into four main sections. The first section collects general information about the main characteristics of research sample and respondents' profiles. The second section of the questionnaire collects information regarding the potential threats and risks of Cloud AIS risks. The third section collects information related to some of main frameworks of ITG to reduce Cloud AIS risks; this section was divided into two parts, first: the role of COBIT 5 framework, and the second part related the role of COSO-ERM 2017. The last section collects information concerned with the integration between COBIT 5 and COSO-ERM 2017.

10. Results and Discussions:

Descriptive statistics of the collected data were analyzed for the purpose of understanding the main characteristics of the research variables. The main statistical results are presented in the following sections:

10-1. Descriptive Analysis

Statistical Package for Social Sciences (SPSS) version 26 has been used to analyse the data that was gathered. Since the arithmetic mean and standard deviation were used in the study, the researcherss employed descriptive statistics to perform a descriptive analysis of the field study data and this is shown in the following tables:

Table (1) Descriptive Statistics

Risks of Cloud AIS			
Variables	3.32	3.00	0.70
Lack of compliance with the service contract.	3.36	4.00	0.77
Conflicting between standards used in the accounting software and restrictions on software configuration maintenance.	3.31	3.00	0.62
Breaches continue to be an imposing threat to companies using the Cloud.	3.23	3.00	0.76
Lack of confidence in who provides Cloud computing service.	3.08	3.00	0.81
The risk of switching service providers.	3.26	3.00	0.70
Lack of confidence in the sustainability of the Internet.	3.28	3.00	0.74
The lack of full commitment by the organizations to launch mechanisms and legislations.	3.33	3.00	0.69
Unmanaged attack surface.	3.23	3.00	0.76
Insiders' abuse authorized access.	3.17	3.00	0.72
Lack of Visibility.	3.28	3.00	0.69
Insecure Interfaces/APIs (application programming interfaces).	3.36	3.00	0.70
External Sharing of Data.	3.14	3.00	0.78
Denial of Service (DoS) and Distributed Denial of Service (DDoS) Attacks.	3.33	3.00	0.69

Risks of Cloud AIS			
Variables	3.32	3.00	0.70
Phishing.	3.42	4.00	0.68
Malware.	3.18	3.00	0.73
Man-in-the-Middle (MitM) Attacks.	3.25	3.00	0.79
Advanced Persistent Threats (APTs).	3.22	3.00	0.83
Social Engineering.	3.16	3.00	0.72
Cryptojacking.	3.16	3.00	0.80
Zero-day Exploits.	3.32	3.00	0.70

It was clear from table (1) that the arithmetic mean values for risks of Cloud AIS ranged between 3.0842 to 3.4211, their standard deviation ranged between 0.62012 to 0.82744.

Table (2): Descriptive Statistics

COBIT 5 Processes suitable for reducing risks of Cloud AIS			
Variables	Mean	Median	Std. Deviation
Ensure Governance Framework Setting and Maintenance.	4.28	4.00	0.86
Ensure Risk Optimization.	4.32	4.00	0.66
Ensure Resource Optimization.	4.09	4.00	0.85
Manage strategy.	4.06	4.00	0.87
Manage service Agreements.	4.22	4.00	0.84
Manage Suppliers.	4.31	4.00	0.83
Manage Risk.	4.31	4.00	0.77
Manage Security.	4.28	4.00	0.83
Manage Programs and Projects.	4.06	4.00	0.97
Manage Changes.	4.07	4.00	0.98
Manage Service Requests and Incidents.	4.09	4.00	0.86

Manage Problems.	4.28	4.00	0.81
Manage Continuity.	4.06	4.00	0.93
Manage Business process controls.	4.16	4.00	0.93
Monitor, Evaluate and Assess Performance and Conformance.	4.03	4.00	0.89
Monitor, Evaluate, and Assess the System of Internal Control.	4.19	4.00	0.84

It was clear from table (2) that the arithmetic mean values for COBIT 5 Processes suitable for reducing risks of Cloud AIS ranged between 4.0316 to 4.3158 and their standard deviation ranged between 0.65661 to 0.98112.

Table (3) Descriptive Statistics

COSO-ERM 2017			
Variables	Mean	Median	Std. Deviation
Governance and Culture.	4.2211	4.0000	0.80131
Strategy and Objective Setting.	4.2316	4.0000	0.77806
Performance.	4.1579	4.0000	0.89104
Review and Revision.	4.2947	4.0000	0.7701
Information, Communication, and Reporting.	4.2	4.0000	0.69343

The table (3) indicated that the mean values for COSO-ERM 2017 ranged between 4.1579 to 4.2947 and its standard deviation ranged between 0.69343 to 0.89104.

Table (4) Descriptive Statistics

Integration between COBIT 5 and COSO-ERM 2017 in the light of reducing risks of Cloud AIS			
Variables	**Mean**	**Median**	**Std. Deviation**
There are many similar and different activities between the two frameworks.	1.0421	1.0000	0.52422
The two frameworks are compatible and complementary to each other.	1.1474	1.0000	0.58288

Reduce the risks of Cloud AIS.	0.9789	1.0000	0.5255
Eliminate several non-value-added activities.	1.0737	1.0000	0.55048
A reduction in costs and competitive advantages.	1	1.0000	0.63581
Achieve alignment of IT operations and goals with the organization's strategic objectives.	1.0421	1.0000	0.50352
Ensure IT delivers the expected benefits from the IT strategy to the organization along with cost optimization and adding value.	1.0421	1.0000	0.56334
Achieve optimal use of interest investments and suitable management of their crucial IT resources.	1.2	1.0000	0.55735
Enhance efficiency and effectiveness risk management processes.	1.0105	1.0000	0.5156
Achieve better performance measurement.	1.0632	1.0000	0.57999
Achieve benchmarking and information technology governance.	1.0526	1.0000	0.59014

Finally, table (4) showed the mean for Integration between COBIT 5 and COSO-ERM 2017 in the light of reducing risks of Cloud AIS ranged between 0.9789 to 1.2 and its standard deviation ranged between 0.50352 to 0.59014.

10-2. Reliability Analysis:

Using Cronbach's Alpha Test, which gauges internal consistency among scale items, the reliability of the scales was assessed. This will be presented in detail below.

10-2-1 Reliability Analysis for Risks of Cloud AIS:

As indicated in table (5) below, all Cronbach's Alpha if Item Deleted (ranged between .892 to .900) are less than overall Cronbach's Alpha (.901) which means that all questions are consistent and the data of questionnaire are valid.

Table (5): The Results of Reliability Analysis for Risks of Cloud AIS

Reliability Statistics

c

Cronbach's Alpha	N of Items
.901	20
Item-Total statistics	
	Cronbach's Alpha if Item Deleted
Lack of compliance with the service contract.	.896
Conflicting between standards used in the accounting software and restrictions on software configuration maintenance.	.898
Breaches continue to be an imposing threat to companies using the Cloud.	.900
Lack of confidence in who provides Cloud computing service.	.896
The risk of switching service providers.	.898
Lack of confidence in the sustainability of the Internet.	.898
The lack of full commitment by the organizations to launch mechanisms and legislations.	.897
Unmanaged attack surface.	.896
Insiders' abuse authorized access.	.896
Lack of Visibility.	.896
Insecure Interfaces/APIs (application programming interfaces).	.899
External Sharing of Data.	.896
Denial of Service (DoS) and Distributed Denial of Service (DDoS) Attacks.	.895
Phishing.	.898
Malware.	.898
Man-in-the-Middle (MitM) Attacks.	.892
Advanced Persistent Threats (APTs).	.893
Social Engineering.	.895
Cryptojacking.	.895
Zero-day Exploits.	.893

10-2-2. Reliability Analysis for COBIT 5 Processes Suitable for Reducing Risks of Cloud AIS:

As indicated in table (6) below, all Cronbach's Alpha if Item Deleted (ranged between .933 to .939) are less than overall Cronbach's Alpha (.939) which means that all questions are consistent and the data of questionnaire are valid.

Table (6): The Results of Reliability Analysis for COBIT 5 Processes Suitable for Reducing Risks of Cloud AIS

Reliability Statistics	
Cronbach's Alpha	**N of Items**
.939	16
Item-Total Statistics	
	Cronbach's Alpha if Item Deleted
Ensure Governance Framework Setting and Maintenance.	.938
Ensure Risk Optimization.	.939
Ensure Resource Optimization.	.934
Manage strategy.	.936
Manage service Agreements.	.936
Manage Suppliers.	.937
Manage Risk.	.937
Manage Security.	.935
Manage Programs and Projects.	.934
Manage Changes.	.932
Manage Service Requests and Incidents.	.935
Manage Problems.	.936
Manage Continuity.	.933
Manage Business process controls.	.935
Monitor, Evaluate and Assess Performance and Conformance.	.934
Monitor, Evaluate, and Assess the System of Internal Control.	.933

10-2-3 Reliability Analysis for COSO-ERM 2017:

As indicated in table (7) below, all Cronbach's Alpha if Item Deleted (ranged between .710 to .765) are less than overall Cronbach's Alpha (.775) which means that all questions are consistent and the data of questionnaire are valid.

Table (7): The Results of Reliability Analysis for COSO-ERM 2017

Reliability Statistics	
Cronbach's Alpha	**N of Items**
.775	5
Item-Total Statistics	
	Cronbach's Alpha if Item Deleted
Governance and Culture.	.765
Strategy and Objective Setting.	.710
Performance.	.736
Review and Revision.	.735
Information, Communication, and Reporting.	.722

10-2-4 Reliability Analysis for Integration between COBIT 5 and COSO-ERM 2017 in the light of Reducing Risks of Cloud AIS

As indicated in table (8) below, Cronbach's Alpha if Item Deleted of question 1 (.744) (in first analysis) is greater than overall Cronbach's Alpha (.739) and question 1 in (second analysis) (.745) is greater than overall Cronbach's Alpha (.744) which means that if these questions are deleted, the overall Cronbach's Alpha will be enhanced. Therefore, in third analysis, after deleting question 1 and question 2 from the analysis and re-estimate the Cronbach's Alpha.

Table (8): The Results of Reliability Analysis for Integration between COBIT 5 and COSO-ERM 2017 in the light of Reducing Risks of Cloud AIS

Reliability Statistics	
Cronbach's Alpha	**N of Items**
.739	11
Item-Total Statistics	

	Cronbach's Alpha if Item Deleted
There are many similar and different activities between the two frameworks.	.744
The two frameworks are compatible and complementary to each other.	.730
Integration will help organizations reduce the risks of Cloud AIS.	.733
Integration will help organizations eliminate several non-value added activities.	.717
Integration will result in a reduction in costs and competitive advantages.	.706
Integration will help organizations achieve alignment of IT operations and goals with the organization's strategic objectives.	.721
Integration will help organizations ensure IT delivers the expected benefits from the IT strategy to the organization along with cost optimization and adding value.	.716
Integration will help organizations achieve optimal use of interest investments and suitable management of their crucial IT resources.	.731
Integration will help organizations enhance efficiency and effectiveness risk management processes.	.715
Integration will help organizations achieve better performance measurement.	.698
Integration will help organizations achieve benchmarking and information technology governance.	.709

After the re-estimate (in the third analysis), the researcherss found that overall Cronbach's Alpha (.745), and there is no Cronbach’s Alpha for total-item statistics greater than overall Cronbach's Alpha (.745) which means that all questions are consistent and the data of questionnaire are reliable.

10-3. Correlations:

The researcherss used Pearson Correlation to analyze the correlation among Risks of Cloud AIS, COBIT 5, COSO-ERM 2017 and the Integration between COBIT 5 and COSO-ERM 2017 as follows:

Table (9): The Results of Correlation Matrix among Risks of Cloud AIS, COBIT 5, COSO-ERM 2017 and the Integration between COBIT 5 and COSO-ERM 2017

Correlations					
		Risks	COBIT 5	COSOERM 2017	Integration
Risks	Pearson Correlation	1	-.366**	-.299**	-.029
	Sig. (2-tailed)		.000	.003	.781
COBIT 5	Pearson Correlation	-.366**	1	.661**	.044
	Sig. (2-tailed)	.000		.000	.669
COSOERM 2017	Pearson Correlation	-.299**	.661**	1	.047
	Sig. (2-tailed)	.003	.000		.654
Integration	Pearson Correlation	-.029	.044	.047	1
	Sig. (2-tailed)	.781	.669	.654	
**. Correlation is significant at the 0.01 level (2-tailed).					

Based on the results of table (9), the researcherss found that a significant and negative correlation among risks of Cloud AIS, COBIT 5 and COSO-ERM 2017 at P-value ≤ 0.01 and coefficient of COBIT 5 and COSO-ERM 2017 are 3.66 and 0.299 respectively. However, the relationship between the risks of Cloud AIS and the integration between COBIT 5 and COSO-ERM 2017 is insignificant at P-value ≤ 0.01.

10-4 Regression Analysis:

10-4-1 The First Sub-Hypothesis:

Testing the first sub-hypothesis (H1-1) which is: **"There is a significant positive impact of applying the COBIT 5 framework on reducing the risks of Cloud AIS."** A simple regression analysis was used to test the first sub-hypothesis based on the collected data from the sample, the following table was obtained:

Table (10): The Impact of COBIT 5 on Reducing the Risks of Cloud AIS

Model	B	Std. Error	β	T	Sig T
COBIT 5	-.319	.084	.366	-3.794	.000

The previous table shows T-test, which is equal to -3.794 with a level of significance .000 < 0.005, that indicates this variable (COBIT 5) has statistical significance on the dependent variable (Risks of Cloud AIS).

The regression coefficient is negative, which means that there is a negative relationship between the independent variable (COBIT 5) and the dependent variable (Risks of Cloud AIS).

According to the previous results, the researcherss accepts the hypothesis, which means that there is a significant positive impact of applying the COBIT 5 framework on reducing the risks of Cloud AIS.

10-4-2\ The Second Sub-Hypothesis:

Testing the second sub-hypothesis (H1-2) which is: **"There is a significant positive impact of applying COSO-ERM 2017 on reducing the risks of Cloud AIS."** A simple regression analysis was used to test the second sub-hypothesis based on the collected data from the sample, the following table was obtained:

Table (11): The Impact of COSO-ERM 2017 on Reducing the Risks of Cloud AIS

Model	B	Std. Error	β	T	Sig T
COSO-ERM 2017	-.905	.300	.299	-3.017	.003

The previous table shows T-test, which is equal to -3.017 with a level of significance .003 < 0.005, that indicates this variable (COSO-ERM 2017) has statistical significance on the dependent variable (Risks of Cloud AIS).

The regression coefficient is negative, which means that there is a negative relationship between the independent variable (COSO-ERM 2017) and the dependent variable (Risks of Cloud AIS).

According to the previous results, the researcherss accepts the hypothesis, which means that there is a significant positive impact of applying COSO-ERM 2017 on reducing the risks of Cloud AIS.

10-4-3\ The Third Sub-Hypothesis:

Testing the third sub-hypothesis (H1-3) which is: **"The integration between COBIT 5 and COSO-ERM 2017 has a positive impact on reducing the risks of Cloud AIS."** A simple regression analysis was used to test the third sub-hypothesis based on the collected data from the sample, the following table was obtained:

Table (12): The Impact of the Integration between COBIT 5 and COSO-ERM 2017 on Reducing the Risks of Cloud AIS

Model	B	Std. Error	β	T	Sig T

The Integration	-.077	.278	.029	-.278	.781

The previous table shows T-test, which is equal to -.077 with a level of significance .781 > 0.005, that indicates this variable (The Integration) has statistical insignificance on the dependent variable (Risks of Cloud AIS).

The regression coefficient is negative, which means that there is a negative relationship between the independent variable (The Integration) and the dependent variable (Risks of Cloud AIS).

According to the previous results, the researcherss rejects the hypothesis, which means that there are valuable benefits resulting from the integration between COBIT 5 and COSO-ERM 2017 on reducing the risks of Cloud AIS.

10-4-4 The Main Hypothesis of the Study:

Testing the main hypothesis of the study which is**: "Adapting ITG has a significant positive impact on reducing the risks of Cloud AIS."** A simple regression analysis was used to test the main hypothesis based on the collected data from the sample, the following table was obtained:

Table (13): The Impact of ITG on Reducing the Risks of Cloud AIS

Model	B	Std. Error	β	T	Sig T
ITG	-.269	.069	.374	-3.885	.000

The previous table shows T-test, which is equal to -3.885 with a level of significance .000 < 0.005, indicates this variable (ITG) has statistical significance on the dependent variable (Risks of Cloud AIS).

The regression coefficient is negative, which means that there is a negative relationship between the independent variable (ITG) and the dependent variable (Risks of Cloud AIS). According to the previous results, the researcherss accepts the hypothesis, which means that adapting ITG has a significant positive impact on reducing the risks of Cloud AIS.

10-5 Kruskal-Wallis Test

The statistical findings of testing the research hypothesis are discussed and summarized in the following sub-sections as follows:

10-5-1 The Risks of Cloud AIS:

The results of the Kruskal-Wallis test shown in table (6.11) do not display any significant differences among different current jobs regarding the risks of Cloud AIS at a significant level (p = 0.05), except for seven variables: Lack of compliance with the service contract (.036); The risk of switching service providers (.044); The lack of full commitment by the organizations to launch mechanisms and

legislations(.023); Insiders abuse authorized access (.052); Denial of Service (DoS) and Distributed Denial of Service (DDoS) Attacks (.052); Cryptojacking (.012); Zero-day Exploits (.033).

It appears that there is a significant difference in opinions between members of the academic staff and cloud implementation engineers (52.66, 45.66 respectively) regarding the variable "Lack of compliance with the service contract." While the percentage of responses indicating this difference is not considerably high, the disparity in the ranks assigned to each group seems to have a substantial impact on the results. Similarly, the same applies between the groups of Accountants and IT Risk Managers with a difference in ranks of 35.09 and 29.75, respectively.

Next comes the variable "The risk of switching service providers," where the rank of the groups causing a significant difference in the results, using the mean rank, is as follows: Cloud Implementation Engineer (57.75), Member of Academic Staff (49.47), Accountant (34.41), IT Risk Manager (31.75). Similarly, the variable "The lack of full commitment by the organizations to launch mechanisms and legislations, "where the rank of the groups causing a significant difference in the results, using the mean rank, is as follows: Cloud Implementation Engineer (56.19), Accountant (50.86), Member of Academic Staff (48.14), IT Risk Manager (19.50).

In the same context, the variable "Insiders abuse authorized access, "where the rank of the groups causing a significant difference in the results, using the mean rank, is as follows: Member of Academic Staff (52.62), Cloud Implementation Engineer (45.47), Accountant and IT Risk Manager are almost similar in results (33.45, 33.67 respectively). Otherwise, the variable "Denial of Service (DoS) and Distributed Denial of Service (DDoS) Attacks, "where the rank of the groups causing a significant difference in the results, using the mean rank, is as follows: Cloud Implementation Engineer (53.50), Member of Academic Staff (50.72), Accountant (34.41), IT Risk Manager (30.17).

In the light of comments, the variable "Cryptojacking, "where the rank of the groups causing a significant difference in the results, using the mean rank, is as follows: Cloud Implementation Engineer (52.75), Member of Academic Staff (50.37), Accountant (44.91), IT Risk Manager (16.50). Finally, the variable "Zero-day Exploits, "where the rank of the groups causing a significant difference in the results, using the mean rank, is as follows: Member of Academic Staff and Cloud Implementation Engineer (51.33, 51.25), which do not make a significant difference in the result while Accountant (38.05) and IT Risk Manager (23.17) have made a significant difference.

Table (6.11): The Risks of Cloud AIS

Test Statistics[a,b]						
Variables	Current Job	N	Mean Rank	Kruskal-Wallis H	df	Asymp. Sig.
Lack of compliance with the service contract.	Member of Academic Staff	62	52.66	8.523	3	.036
	Accountant	11	35.09			
	IT Risk Manager	6	29.75			

c

Test Statistics[a,b]						
Variables	Current Job	N	Mean Rank	Kruskal-Wallis H	df	Asymp. Sig.
	Cloud Implementation Engineer	16	45.66			
	Total	95				
Conflicting between standards used in the accounting software and restrictions on software configuration maintenance.	Member of Academic Staff	62	50.79	4.306	3	.230
	Accountant	11	42.09			
	IT Risk Manager	6	30.67			
	Cloud Implementation Engineer	16	47.75			
	Total	95				
Breaches continue to be an imposing threat to companies using the cloud.	Member of Academic Staff	62	49.54	4.910	3	.179
	Accountant	11	53.23			
	IT Risk Manager	6	28.17			
	Cloud Implementation Engineer	16	45.88			
	Total	95				
Lack of confidence in who provides cloud computing service.	Member of Academic Staff	62	51.40	5.540	3	.136
	Accountant	11	36.18			
	IT Risk Manager	6	33.50			
	Cloud Implementation Engineer	16	48.38			
	Total	95				
The risk of switching service providers.	Member of Academic Staff	62	49.47	8.111	3	.044
	Accountant	11	34.41			
	IT Risk Manager	6	31.75			
	Cloud Implementation Engineer	16	57.75			
	Total	95				

Test Statistics[a,b]						
Variables	Current Job	N	Mean Rank	Kruskal-Wallis H	df	Asymp. Sig.
Lack of confidence in the sustainability of the Internet.	Member of Academic Staff	62	48.16	.485	3	.922
	Accountant	11	43.55			
	IT Risk Manager	6	48.67			
	Cloud Implementation Engineer	16	50.19			
	Total	95				
The lack of full commitment by the organizations to launch mechanisms and legislations.	Member of Academic Staff	62	48.14	9.547	3	.023
	Accountant	11	50.86			
	IT Risk Manager	6	19.50			
	Cloud Implementation Engineer	16	56.19			
	Total	95				
Unmanaged attack surface.	Member of Academic Staff	62	47.49	.745	3	.863
	Accountant	11	48.95			
	IT Risk Manager	6	41.83			
	Cloud Implementation Engineer	16	51.63			
	Total	95				
Insiders abuse authorized access.	Member of Academic Staff	62	52.62	7.737	3	.052
	Accountant	11	33.45			
	IT Risk Manager	6	33.67			
	Cloud Implementation Engineer	16	45.47			
	Total	95				
Lack of Visibility.	Member of Academic Staff	62	50.96	6.110	3	.106
	Accountant	11	31.86			

c

Test Statistics[a,b]						
Variables	Current Job	N	Mean Rank	Kruskal-Wallis H	df	Asymp. Sig.
	IT Risk Manager	6	40.67			
	Cloud Implementation Engineer	16	50.38			
	Total	95				
Insecure Interfaces/APIs (application programming interfaces).	Member of Academic Staff	62	47.13	3.378	3	.337
	Accountant	11	40.09			
	IT Risk Manager	6	62.00			
	Cloud Implementation Engineer	16	51.56			
	Total	95				
External Sharing of Data.	Member of Academic Staff	62	49.98	4.932	3	.177
	Accountant	11	37.64			
	IT Risk Manager	6	33.50			
	Cloud Implementation Engineer	16	52.88			
	Total	95				
Denial of Service (DoS) and Distributed Denial of Service (DDoS) Attacks.	Member of Academic Staff	62	50.72	7.728	3	.052
	Accountant	11	34.41			
	IT Risk Manager	6	30.17			
	Cloud Implementation Engineer	16	53.50			
	Total	95				
Phishing.	Member of Academic Staff	62	48.78	.509	3	.917
	Accountant	11	43.36			
	IT Risk Manager	6	46.00			
	Cloud Implementation Engineer	16	48.91			

Test Statistics[a,b]						
Variables	Current Job	N	Mean Rank	Kruskal-Wallis H	df	Asymp. Sig.
	Total	95				
Malware.	Member of Academic Staff	62	47.37	1.057	3	.788
	Accountant	11	43.32			
	IT Risk Manager	6	52.75			
	Cloud Implementation Engineer	16	51.88			
	Total	95				
Man-in-the-Middle (MitM) Attacks.	Member of Academic Staff	62	50.30	2.302	3	.512
	Accountant	11	40.09			
	IT Risk Manager	6	39.92			
	Cloud Implementation Engineer	16	47.56			
	Total	95				
Advanced Persistent Threats (APTs).	Member of Academic Staff	62	51.81	7.335	3	.062
	Accountant	11	36.27			
	IT Risk Manager	6	28.50			
	Cloud Implementation Engineer	16	48.59			
	Total	95				
Social Engineering.	Member of Academic Staff	62	47.88	.041	3	.998
	Accountant	11	48.23			
	IT Risk Manager	6	49.92			
	Cloud Implementation Engineer	16	47.59			
	Total	95				
Cryptojacking.	Member of Academic Staff	62	50.37	10.893	3	.012

c

Test Statistics[a,b]						
Variables	Current Job	N	Mean Rank	Kruskal-Wallis H	df	Asymp. Sig.
	Accountant	11	44.91			
	IT Risk Manager	6	16.50			
	Cloud Implementation Engineer	16	52.75			
	Total	95				
Zero-day Exploits.	Member of Academic Staff	62	51.33	8.755	3	.033
	Accountant	11	38.05			
	IT Risk Manager	6	23.17			
	Cloud Implementation Engineer	16	51.25			
	Total	95				
a. Kruskal Wallis Test						
b. Grouping Variable: Current Job						

6-8-5-2 COBIT 5 Processes Suitable for Reducing the Risks of Cloud AIS:

The results of the Kruskal-Wallis test shown in table (6.12) display significant differences among different current jobs regarding COBIT 5 processes suitable for reducing the risks of Cloud AIS at a significant level (p = 0.05), except for four variables: Ensure Governance Framework Setting and Maintenance; Ensure Risk Optimization; Manage Suppliers; Manage Security. Next comes the variable " Ensure Governance Framework Setting and Maintenance," where the rank of the groups causing a minor non-significant difference in the results, using the mean rank, is as follows: Member of Academic Staff (52.56), IT Risk Manager (40.50), Cloud Implementation Engineer (39.56), Accountant (38.64). Otherwise, the variable "Ensure Risk Optimization, "where the rank of the groups causing a simple non-significant difference in the results, using the mean rank, is as follows: IT Risk Manager (61.50), Member of Academic Staff (50.05), Accountant (40.82), Cloud Implementation Engineer (39.94).

As shown below in the table, the variable " Manage Suppliers," where the rank of the groups causing a non-significant difference in the results, using the mean rank, is as follows: Member of Academic Staff (50.10), IT Risk Manager (49.75), Accountant (45.45), Cloud Implementation Engineer (40.94). Furthermore, the variable " Manage Security," where the rank of the groups causing a non-significant difference in the results, using the mean rank, is as follows: Member of Academic Staff (51.00), IT Risk Manager (44.17), Accountant (43.59), Cloud Implementation Engineer (40.84).

Table (6.12): COBIT 5 Processes Suitable for Reducing the Risks of Cloud AIS

Test Statistics[a,b]						
Variables	Current Job	N	Mean Rank	Kruskal-Wallis H	df	Asymp. Sig.
Ensure Governance Framework Setting and Maintenance.	Member of Academic Staff	62	52.56	5.986	3	0.112
	Accountant	11	38.64			
	IT Risk Manager	6	40.50			
	Cloud Implementation Engineer	16	39.56			
	Total	95				
Ensure Risk Optimization.	Member of Academic Staff	62	50.05	4.861	3	0.182
	Accountant	11	40.82			
	IT Risk Manager	6	61.50			
	Cloud Implementation Engineer	16	39.94			
	Total	95				
Ensure Resource Optimization.	Member of Academic Staff	62	55.15	17.003	3	0.001
	Accountant	11	25.86			
	IT Risk Manager	6	47.25			
	Cloud Implementation Engineer	16	35.81			
	Total	95				
Manage strategy.	Member of Academic Staff	62	53.91	13.897	3	0.003
	Accountant	11	24.73			
	IT Risk Manager	6	37.00			
	Cloud Implementation Engineer	16	45.22			
	Total	95				
	Member of Academic Staff	62	54.02	14.024	3	.003

Test Statistics[a,b]						
Variables	Current Job	N	Mean Rank	Kruskal-Wallis H	df	Asymp. Sig.
Manage service Agreements.	Accountant	11	25.55			
	IT Risk Manager	6	49.92			
	Cloud Implementation Engineer	16	39.41			
	Total	95				
Manage Suppliers.	Member of Academic Staff	62	50.10	1.865	3	0.601
	Accountant	11	45.45			
	IT Risk Manager	6	49.75			
	Cloud Implementation Engineer	16	40.94			
	Total	95				
Manage Risk.	Member of Academic Staff	62	53.29	15.249	3	0.002
	Accountant	11	29.86			
	IT Risk Manager	6	62.25			
	Cloud Implementation Engineer	16	34.63			
	Total	95				
Manage Security.	Member of Academic Staff	62	51.00	2.692	3	0.442
	Accountant	11	43.59			
	IT Risk Manager	6	44.17			
	Cloud Implementation Engineer	16	40.84			
	Total	95				
Manage Programmes and Projects.	Member of Academic Staff	62	56.15	24.869	3	0.000
	Accountant	11	18.00			
	IT Risk Manager	6	29.92			

Test Statistics[a,b]						
Variables	Current Job	N	Mean Rank	Kruskal-Wallis H	df	Asymp. Sig.
	Cloud Implementation Engineer	16	43.84			
	Total	95				
Manage Changes.	Member of Academic Staff	62	55.66	15.898	3	0.001
	Accountant	11	32.45			
	IT Risk Manager	6	34.00			
	Cloud Implementation Engineer	16	34.25			
	Total	95				
Manage Service Requests and Incidents.	Member of Academic Staff	62	56.06	18.289	3	0.000
	Accountant	11	31.50			
	IT Risk Manager	6	29.42			
	Cloud Implementation Engineer	16	35.09			
	Total	95				
Manage Problems.	Member of Academic Staff	62	52.75	8.413	3	0.038
	Accountant	11	42.59			
	IT Risk Manager	6	48.42			
	Cloud Implementation Engineer	16	33.16			
	Total	95				
Manage Continuity.	Member of Academic Staff	62	57.52	26.369	3	0.000
	Accountant	11	21.59			
	IT Risk Manager	6	31.67			
	Cloud Implementation Engineer	16	35.38			
	Total	95				

c

Test Statistics[a,b]						
Variables	Current Job	N	Mean Rank	Kruskal-Wallis H	df	Asymp. Sig.
Manage Business process controls.	Member of Academic Staff	62	54.58	12.341	3	0.006
	Accountant	11	37.68			
	IT Risk Manager	6	28.92			
	Cloud Implementation Engineer	16	36.75			
	Total	95				
Monitor, Evaluate and Assess Performance and Conformance.	Member of Academic Staff	62	54.67	13.436	3	0.004
	Accountant	11	29.36			
	IT Risk Manager	6	32.00			
	Cloud Implementation Engineer	16	40.97			
	Total	95				
Monitor, Evaluate, and Assess the System of Internal Control.	Member of Academic Staff	62	53.81	9.697	3	0.021
	Accountant	11	37.77			
	IT Risk Manager	6	41.75			
	Cloud Implementation Engineer	16	34.84			
	Total	95				
a. Kruskal Wallis Test						
b. Grouping Variable: Current Job						

6-8-5-3 COSO-ERM 2017 Framework Components that can be applied to the Risks of Cloud AIS:

The results of the Kruskal-Wallis test shown in table (6.13) display significant differences among different current jobs regarding COSO-ERM 2017 Framework Components that can be applied to the Risks of Cloud AIS at a significant level (p = 0.05), except for two variables: Governance and Culture; Performance. As shown below in the table, the variable " Governance and Culture," where the rank of the groups causing a lightly non-significant difference in the results, using the mean rank, is as follows: IT Risk Manager and Member of Academic Staff (50.92, 50.24 respectively), and the variables were caused a relatively big non significant diference, using the mean rank, are as follows: Accountant (44.05),

Cloud Implementation Engineer (40.94). There were a big non-significant difference among groups under the variable "performance", by using the mean rank, are as follows: Member of Academic Staff (51.48), Cloud Implementation Engineer (49.00), IT Risk Manager (42.17), Accountant (30.14).

Table (6.13): COSO-ERM 2017 Framework Components that can be applied to the Risks of Cloud AIS

Test Statistics[a,b]						
Variables	Current Job	N	Mean Rank	Kruskal-Wallis H	df	Asymp. Sig.
Governance and Culture.	Member of Academic Staff	62	50.24	2.17	3	0.538
	Accountant	11	44.05			
	IT Risk Manager	6	50.92			
	Cloud Implementation Engineer	16	40.94			
	Total	95				
Strategy and Objective Setting.	Member of Academic Staff	62	54.23	10.88	3	0.012
	Accountant	11	33.86			
	IT Risk Manager	6	40.50			
	Cloud Implementation Engineer	16	36.38			
	Total	95				
Performance.	Member of Academic Staff	62	51.48	6.862	3	0.076
	Accountant	11	30.14			
	IT Risk Manager	6	42.17			
	Cloud Implementation Engineer	16	49.00			
	Total	95				

c

Test Statistics[a,b]						
Variables	Current Job	N	Mean Rank	Kruskal-Wallis H	df	Asymp. Sig.
Review and Revision.	Member of Academic Staff	62	52.85	8.103	3	0.044
	Accountant	11	32.59			
	IT Risk Manager	6	37.17			
	Cloud Implementation Engineer	16	43.84			
	Total	95				
Information, Communication, and Reporting.	Member of Academic Staff	62	52.23	8.657	3	0.034
	Accountant	11	30.64			
	IT Risk Manager	6	35.33			
	Cloud Implementation Engineer	16	48.31			
	Total	95				
a. Kruskal Wallis Test						
b. Grouping Variable: Current Job						

6-8-5-4 The Integration between COBIT 5 and COSO-ERM 2017

The results of the Kruskal-Wallis test shown in table (6.14) do not display any significant differences among different current jobs regarding the integration between COBIT 5 and COSO-ERM 2017 at a significant level (p = 0.05), except for three variables: The integration will help organizations reduce the risks of cloud AIS; The integration will help organizations ensure IT delivers the expected benefits from the IT strategy to the organization along with cost optimization and adding value; The integration will help organizations enhance the efficiency and effectiveness of risk management processes.

The variable " The integration will help organizations reduce the risks of cloud AIS "has a significant difference observed in the opinions of the groups, as follows: IT Risk Manager (67.00), Cloud Implementation Engineer (51.50), Member of Academic Staff (46.23), Accountant (42.55). On the other hand, the variable "The integration will help organizations ensure IT delivers the expected benefits from the IT strategy to the organization along with cost optimization and adding value "pointed to a significant difference which was ranked by responded groups using mean rank, as follows: Cloud Implementation

Engineer (57.81), IT Risk Manager (49.25), Member of Academic Staff (46.25), Accountant (42.91). Finally, the variable "the integration will help organizations enhance the efficiency and effectiveness of risk management processes", indicated that there was a high significant difference in the results due to the big differences in the responses of the target groups in the questionnaire, as the mean rank showed the following: Accountant (58.82), Member of Academic Staff (52.20), IT Risk Manager (33.83), Cloud Implementation Engineer (29.59).

Table (6.14): The Integration between COBIT 5 and COSO-ERM 2017

Test Statistics[a,b]						
Variables	**Current Job**	**N**	**Mean Rank**	**Kruskal-Wallis H**	**df**	**Asymp. Sig.**
There are many similar and different activities between the two frameworks.	Member of Academic Staff	62	46.23	6.207	3	0.102
	Accountant	11	42.55			
	IT Risk Manager	6	67.00			
	Cloud Implementation Engineer	16	51.50			
	Total	95				
The two frameworks are compatible and complementary to each other.	Member of Academic Staff	62	46.25	3.711	3	0.294
	Accountant	11	42.91			
	IT Risk Manager	6	49.25			
	Cloud Implementation Engineer	16	57.81			
	Total	95				
Integration will help organizations reduce the risks of cloud AIS.	Member of Academic Staff	62	52.87	10.684	3	0.014
	Accountant	11	33.91			
	IT Risk Manager	6	35.00			
	Cloud Implementation Engineer	16	43.69			
	Total	95				
	Member of Academic Staff	62	50.15	2.962	3	0.398

c

Test Statistics[a,b]						
Variables	**Current Job**	**N**	**Mean Rank**	**Kruskal-Wallis H**	**df**	**Asymp. Sig.**
Integration will help organizations eliminate several non-value-added activities.	Accountant	11	37.82			
	IT Risk Manager	6	45.08			
	Cloud Implementation Engineer	16	47.78			
	Total	95				
Integration will result in a reduction in costs and competitive advantages.	Member of Academic Staff	62	50.45	6.378	3	0.095
	Accountant	11	44.55			
	IT Risk Manager	6	60.67			
	Cloud Implementation Engineer	16	36.13			
	Total	95				
Integration will help organizations achieve alignment of IT operations and goals with the organization's strategic objectives.	Member of Academic Staff	62	50.83	3.793	3	0.285
	Accountant	11	46.36			
	IT Risk Manager	6	39.58			
	Cloud Implementation Engineer	16	41.31			
	Total	95				
Integration will help organizations ensure IT delivers the expected benefits from the IT strategy to the organization along with cost optimization and adding value.	Member of Academic Staff	62	52.02	12.009	3	0.007
	Accountant	11	53.82			
	IT Risk Manager	6	39.83			
	Cloud Implementation Engineer	16	31.50			
	Total	95				
Integration will help organizations achieve optimal use of interest investments and	Member of Academic Staff	62	46.46	1.166	3	0.761
	Accountant	11	52.23			
	IT Risk Manager	6	54.75			

Test Statistics[a,b]						
Variables	**Current Job**	**N**	**Mean Rank**	**Kruskal-Wallis H**	**df**	**Asymp. Sig.**
suitable management of their crucial IT resources.	Cloud Implementation Engineer	16	48.53			
	Total	95				
Integration will help organizations enhance efficiency and effectiveness risk management processes.	Member of Academic Staff	62	52.20	19.903	3	0.000
	Accountant	11	58.82			
	IT Risk Manager	6	33.83			
	Cloud Implementation Engineer	16	29.59			
	Total	95				
Integration will help organizations achieve better performance measurement.	Member of Academic Staff	62	49.21	1.132	3	0.769
	Accountant	11	45.27			
	IT Risk Manager	6	52.33			
	Cloud Implementation Engineer	16	43.56			
	Total	95				
Integration will help organizations achieve benchmarking and information technology governance.	Member of Academic Staff	62	50.23	3.365	3	0.339
	Accountant	11	46.18			
	IT Risk Manager	6	52.67			
	Cloud Implementation Engineer	16	38.84			
	Total	95				
a. Kruskal Wallis Test						
b. Grouping Variable: Current Job						

11 Conclusions and Recommandations:

11-1 Conclusions:

1- In this era of globalization, Cloud AIS has become one of the most popular and extensively used business strategies. Since 1999, companies in a wide range of industries have been adopting Cloud AIS. This trend began with basic information systems Cloud computing and progressed to strategic and transformational Cloud AIS, which involves strategic business functions.

2- Utilising the internet and IT improved already-existing procedures while also altering how businesses conduct business. To stay competitive, organizations are depending more and more on IT; one major effect of this increased reliance on IT is the adoption of Cloud AIS.

3- The literature review indicates that there are a variety of reasons why Cloud AIS was developed. Organizations can gain several benefits from Cloud AIS, including cost savings and increased flexibility that enable them to take advantage of economies of scale. As a result, decisions made regarding Cloud AIS have a direct impact on the cost structure of an organization. They may also have an impact on the organization's long-term competitive position and offer numerous opportunities that are not available internally.

4- While Cloud AIS offers numerous advantages and benefits if the risks are not properly addressed at the outset of the Cloud AIS arrangement, these potential benefits could easily be offset.

5- To properly manage and oversee Cloud AIS arrangement, benefits and risks need to be carefully weighed against one another. To do this, it was necessary to look for and implement various ITG frameworks.

6- All of the organizations participating in this IT investment must have a set of formalised standards, components, and processes for Cloud AIS to manage the risks associated with it and improve the effectiveness and quality of ITG.

7- ITG has changed in response to the growth of the IT environment and is now essential for tracking an organization's risk profile and pinpointing areas where the risk management procedure needs to be improved. Furthermore, IT took on a more active role in IT risk management.

8- Cloud AIS has a lot to offer businesses. Notwithstanding these advantages, this arrangement carries some risks.

9- To minimise the risks associated with Cloud AIS and optimise its benefits, organizations must seek out a suitable ITG framework.

10- To help decision-makers in the organization determine and manage the overall direction of IT, ITG is a collection of structures, procedures, policies, objectives, strategies, and responsibilities that are entrusted to them. Additionally, ITG is used to direct and control the organization toward achieving the organization's goals by adding value and balancing risks versus returns over IT and its processes.

11- To achieve flexibility in IT and the structuring of information systems operations, organizations must first achieve flexibility in IT. This is accomplished by enabling the role of management and control over IT activities within the organization, managing IT-related risks appropriately, raising awareness of the significance of IT for competitiveness, and reducingthe costs associated with IT investment. This highlights the importance of IT governance.

12- In addition to helping with financial management, Cloud AIS can also be used to lower carbon emissions, increase accessibility to accounting, and improve integration with current business

software and systems. Cloud AIS is extremely safe, and the majority of them include firewalls and 2-factor authentication in addition to extra encryption. For companies of all sizes and locations, Cloud AIS has a lot to offer.

13- The proposed approach of ITG to reduce the risks of Cloud AIS consists of the frameworks of ITG which are COBIT 5 and COSO-ERM 2017. These frameworks have a crucial role in reducing the previous risks.

14- A questionnaire-based field study is carried out to investigate ITG's possible contribution to reducingthe risks associated with Cloud AIS. A sample of academic staff members, accountants, IT risk managers, and Cloud implementation engineers were given the questionnaire. 215 questionnaires were sent by the researcherss. 95 respondents completed the usable questionnaires after these were collected.

15- The researcherss used the Alpha Cronbach's coefficient to measure the reliability of the study items to ascertain the reliability of the tool used to measure the responses of the items sampled. The Alpha Cronbach's coefficient for the questionnaire as a whole is equal to (0.922) and therefore can be depended on to measure the study’s variables of the questionnaire.

16- To test the first sub-hypothesis, the researcherss used a simple regression analysis based on the collected data from the sample. The T-test, which is equal to -3.794 with a level of significance .000 < 0.005, indicates COBIT 5 has statistical significance on risks of Cloud AIS. The regression coefficient is negative, which means that there is a negative relationship between independent COBIT 5 and the risks of Cloud AIS. According to the previous results, the researcherss accepts the hypothesis, which means that there is a significant impact of applying the COBIT5 framework on reducing risks of Cloud AIS.

17- To test the second sub-hypothesis, the researcherss used a simple regression analysis based on the collected data from the sample. The T-test, which is equal to -3.017 with a level of significance .003 < 0.005, indicates COSO-ERM 2017 has statistical significance on the Risks of Cloud AIS. The regression coefficient is negative, which means that there is a negative relationship between COSO-ERM 2017 and the Risks of Cloud AIS. According to the previous results, the researchers accepts the hypothesis, which means that there is a significant impact of applying COSO-ERM 2017 on reducing risks of Cloud AIS.

18- To test the third sub-hypothesis, the researchers used a simple regression analysis based on the collected data from the sample. The T-test, which is equal to -.077 with a level of significance .781 < 0.005, indicates the integration has statistical insignificance on the risks of Cloud AIS. The regression coefficient is negative, which means that there is a negative relationship between the integration and the risks of Cloud AIS. According to the previous results, the researchers rejects the hypothesis, which means that there are no valuable benefits resulting from the integration between COBIT 5 and COSO-ERM 2017 on reducing risks of Cloud AIS.

19- To test the main hypothesis, the researchers used a simple regression analysis based on the collected data from the sample. The T-test, which is equal to -3.885 with a level of significance .000 < 0.005, indicates ITG has statistical significance on the Risks of Cloud AIS. The regression coefficient is negative, which means that there is a negative relationship between the ITG and the risks of Cloud AIS. According to the previous results, the researchers accepts the hypothesis, which means that adapting ITG has a significant impact on reducing the risks of Cloud AIS.

11-2 Recommendations:

1. Establishing an efficient Information Technology Governance (ITG) framework is crucial for organizations to accomplish their goals and ensure that IT systems and business strategies are separated, IT resources are allocated appropriately, IT performance is tracked, and IT risks are minimized.

2. The researchers suggests that to lower the risks associated with Cloud AIS, it is imperative to implement the ITG-proposed approach since it incorporates some of the most suitable ITG frameworks.

3. Whether in graduate or postgraduate studies, the researchers suggests giving the ITG greater consideration at the various educational levels. Furthermore, since it is such a crucial issue, more attention as an observer and consultant should be given to the new era of Cloud AIS development.

4. The risk management of Cloud AIS must be positioned as a core function in organizations because it is a strategic function that facilitates objective realization. Further, organizations must invest in risk management capabilities (such as staff and tools) that will ensure the attainment of Cloud AIS objectives.

5. Information security governance concerns should be adopted by organizations to regularly review and monitor Cloud AIS service providers.

6. Whether they are service providers or client information systems auditors, CISA firms should enhance ITG by creating a suitable IT strategy and IT plan to direct the information systems auditor in carrying out technology-related tasks during the audit task.

References

Abass, Z.K., Al-Abedi, T.K. and Flayyih, H.H., 2023. Integration between cobit and coso for internal control and its reflection on auditing risk with corporate governance as the mediating variable. **International Journal of Economics and Finance Studies**, vol.15(2), pp.40-58.

Abu-Musa, A., (2011), "Exploring Information Systems/Technology Outsourcing in Saudi Organizations: An Empirical Study", Journal of Accounting, Business & Management, vol.18(2), pp.1-17.

Al-Wattar, Y. and AL-Shafeay, K., (2023), "The Role of (IT) Governance Framework's Dimensions in Limiting the Risks Of (CAIS): Applied to Industrial Firms in Iraq", ***World Bulletin of Social Sciences***, vol.26, pp.11-16.

Business Wire, (2020), "Global IT Outsourcing Market 2020-2025 - Growing Demand for Efficiency and Scalable IT Infrastructure".

ResearchAndMarkets.com, available at: https://www.businesswire.com/news/home/20200810005303/en/Global-IT-Outsourcing-Market-2020-2025

Gbadeyan, A., Butakov, S. and Aghili, S., (2017), "IT Governance and Risk Mitigation Approach for Private Cloud Adoption: Case Study of Provincial Healthcare Provider", ***Annals of Telecommunications***, vol.72, pp.347-357.

Gorla, N., and Somers, T., (2014), "The Impact of IT Outsourcing on Information Systems Success", ***Information & Management***, vol.51(3), pp.320-35.

Joshi, A., Bollen, L., Hassink, H., De Haes, S. and Van Grembergen, W., (2018), "Explaining IT Governance Disclosure through the Constructs of IT Governance Maturity and IT Strategic Role", ***Information & Management***, vol.55(3), pp.368-380.

Liew, C. and Hamid, N., (2023), "Information Technology Governance Implementation: Cultural Impact Caused by Top Management", ***International Journal of Engineering Trends and Technology***, vol.71(12), pp.107-118.

Lioliou, E. and Willcocks, L., (2019), "Global Outsourcing Discourse", Springer International Publishing, pp.1-292.

Van Peursem, K. and Jiang, L., (2008), "Internal Audit Outsourcing Practice and Rationales: SME Evidence from New Zealand", ***Asian Review of Accounting***, 16(3), pp.219-245.

Yau-Yeung, D., Yigitbasioglu, O. and Green, P., (2020), "Cloud Accounting Risks and Mitigation Strategies: Evidence from Australia", ***In Accounting Forum***, vol. 44(4), pp. 421-446. Routledge.

Appendix (A): Questionnaire

Required Definitions:

1- IT Governance (ITG):

It is a structure of relationships which links IT processes, IT resources, and information to organization strategies and objectives to direct and control the organization in order to achieve the organization's strategies and objectives. It also integrates best practices of planning and organizing, acquiring and implementing, delivering and supporting, and monitoring IT performance to ensure that the organization's IT resources are used responsibly, its risks are managed appropriately and its information and related technology are supporting its business objectives.

2- Control Objectives for Information and related Technology (COBIT5):

COBIT 5 is one of the most important ITG mechanisms and supporting tools that allow IT managers to communicate and bridge the gap between business risks, control needs, value creation, and technical issues. COBIT 5 is based on 37 high-Level IT Control objectives and on a structure that identifies three levels of IT activity: domains, processes, and activities. IT Control objectives are grouped into five domains that match the organizational area of responsibility. These domains are a grouping of IT processes and are defined as follows: evaluate, direct and monitor (EDM); align, plan and organize (APO); build, acquire and implement (BAI); deliver, service and support (DSS); and monitor, evaluate and assess (MEA).

3- COSO-ERM- Integrating with strategy and performance Framework:

It addresses the changes in ERM and how this affects the risk approach in the organization. It clarifies the importance of ERM in strategic planning and embedding it throughout the organization. In addition, this framework enhances alignment between performance and ERM to improve the setting of performance targets and understanding the impact of risk on performance, and accommodates expectations for governance and oversight. This framework contains five components: Governance and culture, Performance, Strategy & Objective-Setting, Review & Revision and Information, Communication & Reporting.

4- Cloud Accounting:

It is an online accounting information system based on Cloud computing and customer use the computer or other devices to achieve accounting and financial analysis functions. Cloud accounting software is similar to traditional, on-premises, or self-install accounting software, only the accounting software is hosted on remote servers, similar to the SaaS (Software as a Service) business model. Data is sent into "the Cloud," where it is processed and returned to the user.

First Section:

Listed below are some of the potential threats and risks of Cloud AIS. Please tick an appropriate box that expresses your opinion regarding the importance of each risk.

Risks of Cloud AIS	very Important	Important	Not Very Important	Not Important at All
1- Lack of compliance with the service contract.				
2- Conflicting between standards used in the accounting software and restrictions on software configuration maintenance.				
3- Breaches continue to be an imposing threat to companies using the Cloud.				
4- Lack of confidence in who provides Cloud computing service.				
5- The risk of switching service providers.				
6- Lack of confidence in the sustainability of the Internet, which poses a threat to the use of Cloud computing.				
7- The lack of full commitment by the organizations to launch mechanisms and legislations that help control the risk management sector for Cloud computing.				
8- Unmanaged attack surface includes subtle information leaks that lead to an attack.				
9- **Insiders abuse authorized access**. Because on-demand self-service makes easier unauthorized use.				
10- Lack of Visibility. An organization's Cloud-based resources are outside the corporate network and run on infrastructure the company does not own.				
11- Insecure Interfaces/APIs (application programming interfaces). This creates potential issues if a customer has not properly secured the interfaces for their Cloud-based infrastructure.				
12- External Sharing of Data. The shared link can be forwarded to someone else, stolen as part of a cyberattack, or guessed by a cybercriminal, providing unauthorized access to the shared resource.				
13- Denial of Service (DoS) and Distributed Denial of Service (DDoS) Attacks: These attacks aim to overwhelm a system or network with a flood of traffic, making it inaccessible to legitimate users. This means that a successful Denial of Service (DoS) attack against Cloud infrastructure is likely to have a major impact on a number of different companies.				
14- Phishing: It is a technique used to trick individuals into providing sensitive information such as usernames, passwords, or credit card details by disguising as a trustworthy entity via email, instant messaging, or fraudulent websites.				
15- Malware: It refers to malicious software designed to disrupt, damage, or gain unauthorized access to computer systems or networks. Examples include viruses, worms, Trojans, ransomware, and spyware.				
16- Man-in-the-Middle (MitM) Attacks: In MitM attacks, an attacker intercepts and alters communications between two parties without their				

Risks of Cloud AIS	very Important	Important	Not Very Important	Not Important at All
knowledge. This allows the attacker to eavesdrop, steal information, or manipulate data.				
17- Advanced Persistent Threats (APTs): APTs are sophisticated and targeted attacks aimed at gaining unauthorized access to systems or networks for a prolonged period. APTs typically involve multiple attack vectors and are carried out by skilled and persistent threat actors.				
18- Social Engineering: It involves manipulating individuals to divulge sensitive information or perform certain actions. It may include techniques like pretexting, baiting, or impersonation.				
19-Cryptojacking: It involves using someone's computing resources without their consent to mine cryptocurrencies. It can slow down systems, increase energy consumption, and impact performance.				
20- Zero-day Exploits: These exploits target vulnerabilities in software or systems that are unknown to the software developers or security community. Attackers exploit these vulnerabilities before a patch or fix becomes available.				

Second Section:

Listed below are some of the main frameworks of ITG to reduce the risks of Cloud AIS. Please tick an appropriate box that expresses your opinion.

First: Role of COBIT 5 Framework. The Following are the Most Suitable COBIT 5 Processes for Reducing Cloud AIS Risks:		Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
Domain	**Process**					
1-Evaluate, Direct, and Monitor (EDM):	**EDM01: Ensure Governance Framework Setting and Maintenance.** Analyze the requirements for the governance of enterprise IT, and maintain effective principles and practices, with clarity of responsibilities to achieve the enterprise's objectives.					
	EDM 03: Ensure Risk Optimization. Ensure that the enterprise's risk appetite and tolerance are understood, and that risk to enterprise value related to the use of IT is identified and managed.					
	EDM04: Ensure Resource Optimization. Ensure that adequate and sufficient IT-related capabilities (people, process, and technology) are available to support enterprise objectives effectively at optimal cost.					

First: Role of COBIT 5 Framework. The Following are the Most Suitable COBIT 5 Processes for Reducing Cloud AIS Risks:		**Strongly Agree**	**Agree**	**Neutral**	**Disagree**	**Strongly Disagree**
2- Align, Plan and Organize (APO):	**APO02: Manage strategy.** Provide a holistic view of the current business and IT environment, and the initiatives required to transfer to the desired future environment.					
	APO09: Manage service Agreements. Align IT-enabled services and service levels with enterprise needs and expectations, and monitoring of IT services, service levels, and performance indicators.					
	APO 10: Manage Suppliers. Manage IT-related services provided by suppliers to meet enterprise requirements, including management of contracts, and reviewing supplier performance for effectiveness and compliance.					
	APO 12: Manage Risk. Continually identify, assess and reduce IT-related risk within levels of tolerance set by enterprise executive management.					
	APO13: Manage Security. Define, operate and monitor a system for information security management.					

First: Role of COBIT 5 Framework. The Following are the Most Suitable COBIT 5 Processes for Reducing Cloud AIS Risks:		**Strongly Agree**	**Agree**	**Neutral**	**Disagree**	**Strongly Disagree**
3- Build, Acquire, and Implement (BAI):	**BAI 01: Manage Programs and Projects.** Manage all programs and projects from the investment portfolio in alignment with enterprise strategy and in a coordinated way.					
	BAI 06: Manage Changes. Manage all changes in a controlled manner, including standard changes and emergency maintenance relating to business processes, applications and infrastructure.					
4- Deliver, Service and Support (DSS):	**DSS02: Manage Service Requests and Incidents.** Provide timely and effective responses to user requests and resolution of all types of incidents.					
	DSS03: Manage Problems. Identify and classify problems and their root causes and provide timely resolution to prevent recurring incidents.					
	DSS04: Manage Continuity. Establish and maintain a plan to enable the business and IT to respond to incidents and disruptions.					
	DSS06: Manage Business process controls. Define and maintain appropriate business process controls to ensure that					

First: Role of COBIT 5 Framework. The Following are the Most Suitable COBIT 5 Processes for Reducing Cloud AIS Risks:		Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
	information processed by in-house or outsourced business processes satisfies all relevant information control requirements.					
5- Monitor, Evaluate and Assess (MEA):	**MEA 01: Monitor, Evaluate and Assess Performance and Conformance.** Collect, validate, and evaluate the business, IT, and process goals and metrics.					
	MEA 02: Monitor, Evaluate, and Assess the System of Internal Control. Continuously monitor and evaluate the control environment, including self-assessments and independent assurance reviews.					

Second: Role of COSO ERM-Integrating with Strategy and Performance framework 2017. The followings are the Components of COSO-ERM Framework that can be applied to Cloud AIS' Risks:	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
1- Governance and Culture: Board of directors understands Cloud computing, trends, and its potential impact on the organization and industry.					
2-Strategy and Objective Setting: The organization assesses the impact of different Cloud strategies (Cloud deployment models, Cloud delivery models, etc.) on the achievement of the strategy and business objectives.					
3- Performance: The organization prioritizes risks and risk responses to address Cloud computing risk.					
4-Review and Revision: The organization assesses internal and external changes and impact to business strategy and objects as well as the affect they will have on Cloud computing strategy or how Cloud computing can provide effective infrastructure to realize the changes.					
5- Information, Communication, and Reporting: The organization utilizes available and implements as appropriate additional platforms to leverage and consolidate Cloud computing information and technology data to support enterprise risk management.					

Third Section:

Listed below is the integration between COBIT 5 and COSO-ERM 2017. Please tick (√) in the appropriate box that expresses your opinion.

Integration between COBIT 5 and COSO-ERM 2017	**Yes**	**NO**	**I Don't Know**
1- There are many similar and different activities between the two frameworks.			
2- The two frameworks are compatible and complementary to each other.			
3- Integration will help organizations reduce the risks of Cloud AIS.			
4- Integration will help organizations eliminate several non-value-added activities.			
5- Integration will result in a reduction in costs and competitive advantages.			
6- Integration will help organizations achieve alignment of IT operations and goals with the organization's strategic objectives.			
7- Integration will help organizations ensure IT delivers the expected benefits from the IT strategy to the organization along with cost optimization and adding value.			
8- Integration will help organizations achieve optimal use of interest investments and suitable management of their crucial IT resources.			
9- Integration will help organizations enhance efficiency and effectiveness risk management processes.			
10- Integration will help organizations achieve better performance measurement.			
11- Integration will help organizations achieve benchmarking and information technology governance.			