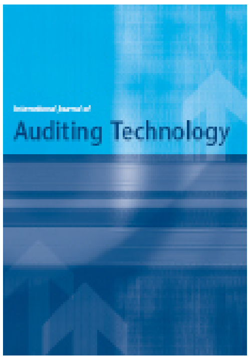
INDERSCIENCE PUBLISHERS
Linking academia, business and industry through research



International Journal of Auditing Technology

ISSN online: 1757-8760 - ISSN print: 1757-8752
https://www.inderscience.com/ijaudit

Assurance and consultancy internal audit roles in information technology risk management

Reda Elazab, Ismail Gomaa

DOI: 10.1504/IJAUDIT.2022.10054517

Article History:

Received:	02 July 2021
Accepted:	27 September 2021
Published online:	09 March 2023

Assurance and consultancy internal audit roles in information technology risk management

Reda Elazab*

Department of Accounting,
Faculty of Commerce,
AlAlamein International University,
Damnhour University, Egypt
Email: relazab@aiu.edu.eg
Email: reda.elazab@com.dmu.edu.eg
*Corresponding author

Ismail Gomaa

Department of Accounting,
Faculty of Commerce,
Alexandria University, Egypt
Email: ismail.gomaa@alexu.edu.eg

Abstract: The study explores the extent of internal audit involvement in information technology (IT) risk management. Hence, the paper proposes new assurance and consultancy internal audit roles in IT risk management. Using the data collected from 75 internal auditors through an exploratory study in Egypt, a framework of internal auditing roles in IT risk management is identified. The collected assurance and consultancy internal audit roles in IT risk management might help different parties such as management, audit committee, IT professionals to be more adaptable in assessing and monitoring IT risks. This study's contributions have important implications for exploring the extension of the internal audit profession in IT risk management. The paper is also one of the first to deal with the assurance and consultancy internal audit roles in IT risk management.

Keywords: assurance and consultancy roles; internal audit; information technology; risk management.

Reference to this paper should be made as follows: Elazab, R. and Gomaa, I. (2022) 'Assurance and consultancy internal audit roles in information technology risk management', *Int. J. Auditing Technology*, Vol. 4, No. 4, pp.241–265.

Biographical notes: Reda Elazab is an Assistant Professor of Accounting and Auditing at the AlAlamein International University and Damnhour University. His research interest areas are auditing and financial accounting with a specific interest in accounting information systems, internal control, information technology risk management, and the impact of information technology on auditing.

Ismail Gomaa is a Professor of Accounting and Auditing at the Alexandria University. His research interest areas are auditing, accounting information systems, data security, forensic accounting, and the impact of information technology on financial and managerial accounting.

1 Introduction

Internal audit is the first defence line in the risk management process and has value-added and economic benefits to firms (Jiang et al., 2019; Marshall, 2020). Also, Breger et al. (2020) found that the external audit relies on internal audit work in the risk management process. Moreover, the amendments made by the Institute of Internal Auditors (IIA) on the internal audit definition in 1999 and 2014 dramatically shifted the internal auditors' responsibilities to provide consulting and assurance services in the field of internal control, risk management, and corporate governance (IIA, 1999, 2004).

With growing IT infrastructure, real-time accounting in business operations, many companies are struggling with IT challenges. Traditionally, IT risks include data integrity, security, privacy, and application processing (Hermanson et al., 2000). Recently, new IT risks have been generated, such as cybersecurity, information security, mobile computing, emerging technologies, and social media (GTAG, 2012). The real-time shift of accounting information will need new internal and external audit functions, *which this paper motivates*.

By this extended duty, internal auditors can provide management and audit committees with recommendations, advice, and consultations about the internal control system's effectiveness, which adds value to companies' operations and timeliness (IIA, 1999, 2004). Although there are numerous auditing and IT guidelines that present new duties to internal auditors in the IT environment, this paper is the first to explore specific internal audit roles in IT risk management. Also, our paper divides the suggestion roles into assurance and consultancy roles and examines them in the real world by the design science methodology.

There is a lack of literature focusing on the internal auditor's role in IT risk management. Hermanson et al. (2000) and Burton (2000) agreed that internal auditors perform a core role in IT risk management without identifying the proposed roles that internal auditors might do in the different IT risk dimensions. Harb (2020) found a significant impact of internal audit functions on the efficiency of accounting information technology of the public joint-stock pharmaceutical industries sector.

The exploration presented in our study is a critical, premiere step in developing extension functions related to the IT internal audit roles. For the practical side of this paper, exploratory data is collected from internal auditors' sample selection in Egypt in the same line with Hermanson et al. (2000) and Burton (2000). Regarding Egypt, the Egyptian Institute of Directors (EIOD) in the Ministry of Investment and International Cooperation issued the Egypt Code of Corporate Governance in 2005. Updated EIOD (2016) has requested from the board of directors to establish systems that ensure compliance with the laws and the adequacy of internal control procedures.

Egypt's development requires scientific studies to establish new controls and procedures to ensure this new environment's success in Egypt. The exploratory research in this paper has a significant practical contribution. It outlines the linkage between management, IT professionals, audit committee, and internal audit in the IT risk management process. Moreover, our findings may be useful for regulators, companies' management, standard setters, internal auditors, and audit committees to create guidance for the internal audit roles in the IT risk management process and the IT risk areas that internal audit should involve as well.

The remainder of this paper is structured as follows: Section 2 provides a brief theoretical framework of the internal audit roles in IT risk management. Section 3 presents the proposed assurance and consultancy internal auditing roles in IT risk categories. Section 4 presents the method used in this paper. Section 5 presents the findings. Section 6 presents the conclusion and identifies future research.

2 Theoretical framework

Few studies have searched the internal audit involvement in IT risk management. In the initial stages, traditional internal auditing roles have focused only on accounting issues and operations processing in companies. Over time, companies depend on IT in most of their activities, including several new risks. Thus, management needs to accommodate these several risks by extending internal auditing roles in IT risk management (Hermanson et al., 2000; Bailey et al., 2017).

Hermanson et al. (2000) and Burton (2000) agreed that internal auditors give various attentions to IT risk types. More concern and emphasis are on common IT controls, such as IT asset safeguarding, application processing, data integrity, and data security. However, they found that internal auditors place moderate attention on system maintenance and continuity of processing. Finally, the least attention is to systems implementation and operating systems.

To involve the internal audit functions in the IT business environment, specific guidelines developed by groups such as IIA COBIT, Big 4, or ISACA may assist in identifying certain internal audit roles in IT risk management. The IIA commissioned the Global Internal Audit Common Body of Knowledge (CBOK) to study internal auditing development over the world. The CBOK engages researchers from around the world in understanding internal auditing practice better. Also, Information Systems Audit and Control Association (ISACA) presented *Control Objectives for Information and Related Technology (COBIT) (5)*, which provides a series of potential checklists and controls (Kahyaoglu and Caliyurt, 2018). Finally, the insights of Ernst & Young on governance, risk, and compliance produce a useful guideline for assurance and consultancy internal auditing services.

Figure 1 presents the structure of the proposed internal audit roles in IT risk management. *Scope 1* presents the objectives of the proposed IT internal audit framework. The main objective is to identify the possible internal audit roles and in IT risk management. Beyond the previous objective, the proposed framework has a lot of potential contributions such as:

1 Providing an approach for internal auditors' roles to be involved in several types of IT risks.

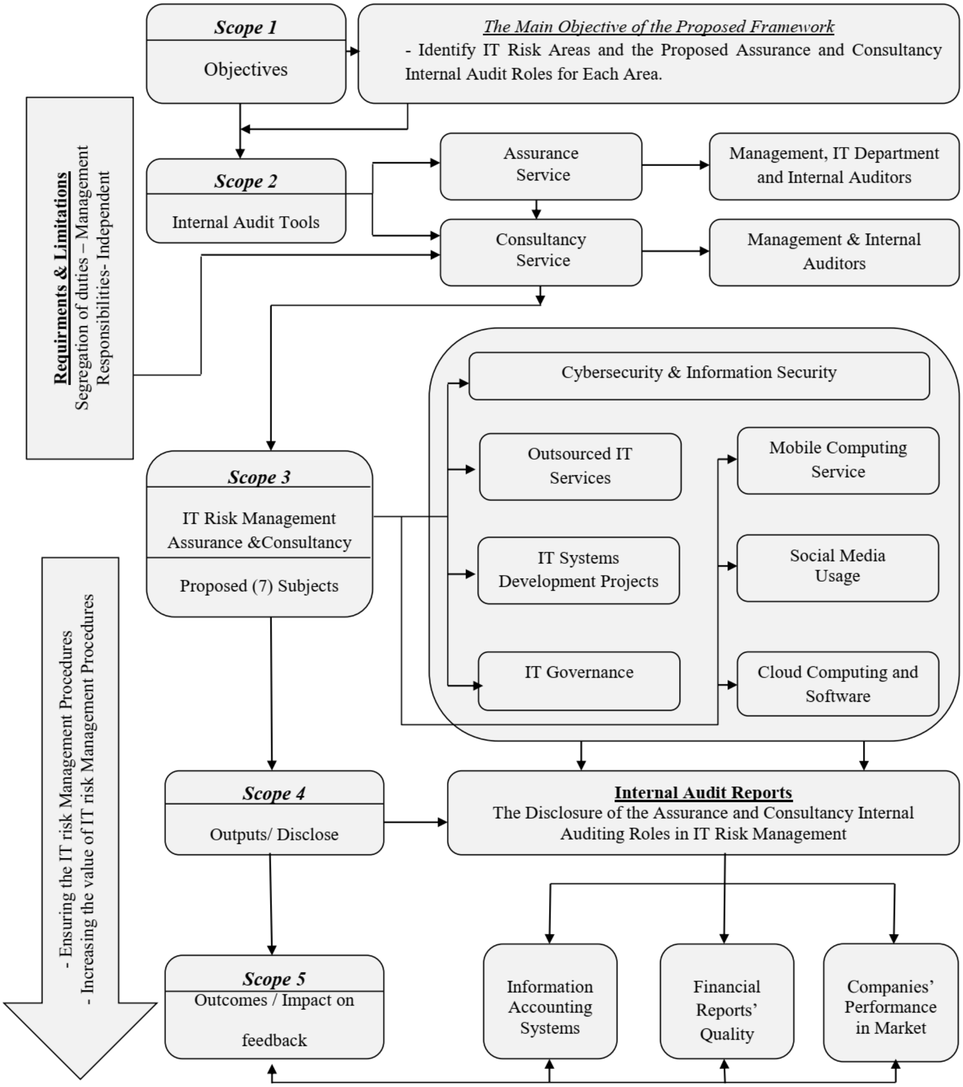
2 Increasing collaboration between management, IT experts, internal audit departments, boards of directors, and audit committees.

3 Increasing IT awareness and IT knowledge levels for employees, internal auditors, boards of directors, and audit committee members.

4 Giving more attention regarding IT issues.

5 Enhancing the awareness of IT standards and instructions, such as IT governance, COBIT, and information security governance.

Figure 1 Internal audit framework


Scope 1
Objectives
The Main Objective of the Proposed Framework
- Identify IT Risk Areas and the Proposed Assurance and Consultancy Internal Audit Roles for Each Area.
Requirments & Limitations
Segregation of duties – Management Responsibilities- Independent
Scope 2
Internal Audit Tools
Assurance Service
Consultancy Service
Management, IT Department and Internal Auditors
Management & Internal Auditors
Cybersecurity & Information Security
Outsourced IT Services
Mobile Computing Service
IT Systems Development Projects
Social Media Usage
IT Governance
Cloud Computing and Software
Scope 3
IT Risk Management Assurance &Consultancy
Proposed (7) Subjects
- Ensuring the IT risk Management Procedures
- Increasing the value of IT risk Management Procedures
Scope 4
Outputs/ Disclose
Internal Audit Reports
The Disclosure of the Assurance and Consultancy Internal Auditing Roles in IT Risk Management
Scope 5
Outcomes / Impact on feedback
Information Accounting Systems
Financial Reports' Quality
Companies' Performance in Market

Scope 2 presents the updated audit roles types. The paper depends on both assurance and consultancy internal audit roles in the IT risk management process (*scope 2*). By using both roles, the IT framework achieves the benefits of the traditional assurance services besides the value-added of the consulting services as well. Most important, internal auditors should not perform any management responsibilities or positions to maintain their independence and objectivity (Roussy and Perron, 2018).

Scope 3 shows the proposed IT risk subjects. This study offers (7) subjects of IT risks: cybersecurity, IT systems development projects, IT governance, outsourced IT services, mobile computing, social media use, and cloud computing. Scope 4 presents the consequences of the new IT internal audit roles in the financial reports (*system's outputs*). There is a new concept that will be generated, which is 'the disclosure of the assurance and consultancy internal audit roles in IT risk management'. This new concept might be new possible future research.

Finally, Scope 5 presents the (*system's outcomes*) of revealing the IT internal audit information, which probably enhances companies' accounting information systems and increases financial reports' quality.

3 The proposed assurance and consultancy internal auditing roles in IT risk management

This section presents the second stage of the proposed IT internal audit roles in IT risk management. The second stage suggests the assurance and consultancy internal audit roles upon the professional resources in IIA, COBIT, and Big 4. The paper suggests (7) IT risk categories as follows: cybersecurity, IT systems development projects, IT governance, IT outsourced services, mobile computing, social media use, and cloud computing.

3.1 Cybersecurity risks

In today's digital world, businesses cannot afford to be held back by cyber-risks, and internal auditing is one of the essential defence lines from cyber-attacks. Cybersecurity is one of the highest-priority items on business agendas (IIA, 2018; Islam et al., 2018). According to the 2008 report of the Centre for Strategic and International Studies (CSIS) Commission on Cybersecurity for the 44th presidency, Cybersecurity is one of the most security challenges in the USA (Borgman et al., 2015).

To face cyber-attacks, companies need internal control security controls to protect information systems not just from technical issues but also from internal control issues (Borgman et al., 2015). Conklin and White (2006) concluded that cyber-attacks, such as malware, denial of service, and phishing harm companies' security and disrupt regular businesses.

Also, when companies have a data breach (*cybersecurity risks*), they increase the control procedures by assigning information technology governance roles to the audit committee (Lankton et al., 2021). Far behind that, Rosati et al. (2020) found that cybersecurity risks can represent a significant issue to financial reporting quality.

Cybersecurity is a comprehensive concept that includes information assurance and information security (Gyun No and Vasarhelyi, 2017). Studies found a positive relationship between internal audit function and information security management (Steinbart et al., 2014a, 2014b, 2013, 2012). Islam et al. (2018) concluded that the internal audit function in cybersecurity is positively associated with internal audit competence related to governance, risk, and control.

Based on IT and internal control guidelines and the previous discussion, the paper develops the internal auditing roles in cybersecurity risk management into two objectives. The first objective identifies whether an attack is occurring or not. Also, assuring that companies have the appropriate procedures and simulation exercises to manage cyber-attacks and information security risks (*assurance roles*).

Second, internal audit should add value to the cybersecurity management process by providing internal control consultations, recommendations, and training to management (*consultancy roles*). Table 1 presents the proposed internal audit roles in cyber risk management.

Table 1 Proposed internal auditing role in cybersecurity risks

N	*Internal auditors' proposed role*
Role type: assurance role	
1	*Ensure* that the company conducts an annual independent vulnerability scan and a penetration test of external networks.
2	*Ensure* that the company has a management crisis plan in case of an actual IT incident or cyber-attack and (*if this plan exists*) internal auditors should ensure it is updated over time.
3	*Ensure* that the company has simulation exercises concerning crisis management.
4	*Ensure* that network architecture coincides with the internal auditing plan.
5	*Evaluate* procedures, policies, and tools for a recent incident and compare it with planned systems.
6	*Confirm* that the company has an IT incident team and *making* sure that they know their roles and responsibilities.
7	*Review* all third parties who have access to the company's data.
8	*Review* the activity of privileged users and *verify* that only authorised users have privileged capabilities.
9	*Perform* a scan for weaknesses in the IT internal network.
Role type: consultancy role	
10	Provide *training* about cyber internal control procedures for IT professionals.
11	Give *recommendations* about policies regarding financial/non-financial confidential data.
12	Provide *consultations* to the IT incident team regarding IT policies.
13	Give *recommendations* about internal control procedures for the Sarbanes-Oxley Act 2002 (*SOX*)/(*COBIT*)
14	*Suggest* risk-based and objective-driven penetration assessments tailored to measure the company's ability to respond to threats.
15	*Provide* information security awareness training programs to increase the success rate.
16	Provide *training* about data loss prevention and information privacy.

3.2 IT systems development projects (IT investments projects)

Due to the fast-growing IT development, companies develop and update their IT systems. As a result, many IT budgets spend on patents and system development projects (Ashurst et al., 2008). Internal auditors can play an active role in IT system development projects' risks in two main objectives as shown in Table 2. The first objective evaluates the procedures that manage IT programs (*assurance roles*). The second objective motivates internal auditors to add value to the internal control procedures in IT projects and programs (*consultancy roles*).

3.3 IT governance

IT governance guidelines create trust in transactions between companies and stakeholders in the IT environment (Debreceny, 2013). Héroux and Fortin (2013) noted that internal auditing can identify IT risks, evaluate IT security plans, define privacy procedures, and data integrity. Wilkin and Chenhall (2020) found that IT governance improves organisational capability and performance.

Table 2 Proposed internal auditing roles in IT systems development projects

N	*Internal auditors' proposed role*
Role type: assurance role	
1	*Evaluate* key IT systems development projects throughout their lifecycles (contract compliance, project management, costs, and benefits).
2	*Conduct* cost-benefit analysis for IT systems development projects.
3	*Assess* the company's project management methodology regarding IT investments.
4	*Ensure* that IT systems development projects are consistent with the company's methodology.
5	*Ensure* that the users are involved in changes in the IT project scope and deliverables.
6	*Review* the user satisfaction study after the IT Project/System is completed.
7	*Confirm* that there are feedback/impact systems related to IT systems development projects in order to use it for future IT investments.
Role type: consultancy role	
8	Provide *training* about cost-benefits analysis for IT systems development projects.
9	Provide *consultation* about acceptance/rejection procedures of a new IT systems development project.
10	Provide *consultation* about internal control assessments for IT systems development projects.
11	Provide a *recommendation* about a user satisfaction study.

Table 3 Proposed internal auditing roles in IT governance

N	*Internal auditors' proposed role*
Role type: assurance role	
1	*Evaluate* that the company has adequate IT governance procedures.
2	*Evaluate* IT governance procedures, performance measures, service-level agreements (SLAs), and customer service.
3	*Evaluate* periodically whether the IT functions align with the company's strategic priorities or not.
4	*Evaluate* that the company has adequate procedures to assess and manage IT risks
5	*Evaluate* whether the company performs IT risk management periodically or not.
6	*Evaluate* the effectiveness of IT resources and performance management reports.
Role type: consultancy role	
7	Provide *training* about internal control procedures related to IT risks.
8	Provide *consultations* about (COBIT) and (COSO) internal control procedures.
9	Provide *consultations* about internal control governance procedures for IT risk management.

The suggested IT internal audit develops two new missions for the internal auditors in IT governance. The first mission is to ensure that companies have effective IT governance procedures with clear IT risk management objectives (Héroux and Fortin, 2013). Additionally, internal auditors should ensure/confirm that the senior management retains control of IT operation responsibility.

The second mission is to add value to the IT control procedures through giving consultations and recommendations. As a first try to explore IT internal audit roles in IT governance, Table 3 presents the proposed roles.

3.4 IT outsourcing services

IT outsourcing refers to a paid contract of IT functions or services, strategic advantages, as well as cost benefits (Samantra et al., 2014). IT outsourcing uses external service providers to help companies with IT services for the business process, IT application services, and infrastructure solutions for business outcomes (González et al., 2016). Lacity et al. (2009) determined IT outsourcing risks, such as the possibility of weak management, inexperienced staff, business uncertainty, old technology skills, endemic uncertainty, hidden costs, innovative capacity loss, eternal triangle, and technology indivisibility.

Dhillon et al. (2017) noted that internal auditing should be involved in the IT outsourcing process to assure that the proper administration of the client (*company*) and supplier (*vendor*). Brandas (2010) clarified that internal auditing reviews IT outsourcing contracts, evaluate system security, and assess service level agreements (SLA) for both client/Supplier areas.

Hence, this paper proposes that the audit assurance side can ensure the initial contract monitoring, auditing, physical, logical security, and outsourcing decision process comply with its outsourcing strategy. Moreover, the consultancy internal auditing roles should provide recommendations, training, and guidance to help manage business continuity plans, disaster recovery, and reporting. The proposed functions are presented in Table 4.

3.5 Social media use

Social media is a new paradigm on the internet. It provides online social media networking, such as Twitter, Facebook, MySpace, and YouTube, for users, whether people or companies communicate. Today, social media networking is considered a proper tool to network with people and companies sharing similar business interests (French e al., 2018).

Today, IT is densely connected to social media strategies in coordination with marketing strategies. He (2012, 2013) found that companies do not have internal control procedures for social media risks. Additionally, both studies concluded that companies should mitigate social media risks by increasing monitoring employees' internet activity, increasing training programs, and developing a social media control plan.

The most famous example of social media risks is 'behalf risks' when users are communicating on behalf of companies. Users in sites like (Twitter, Facebook and LinkedIn) create pages or profiles to communicate with customers on behalf of companies through these channels. This interfering creates a lot of legal and regulatory problems (He, 2012).

This paper suggests the IT audit roles social media risks in stages. Firstly, internal auditors collaborate with IT professionals to re-assess the company's information content available on social media sites. Secondly, internal auditors evaluate threats of using social media websites on the company's information security. Finally, internal auditors evaluate the design of policies and procedures in place to manage social media risks within companies. As a first try to develop new IT internal audit roles in social media risk management, this paper offers Table 5.

Table 4 Proposed internal auditing roles in IT outsourcing

N	*Internal auditors' proposed role*
Role type: assurance role	
1	*Evaluate* that the contractual terms are clearly defined by taking samples of client/supplier informational systems.
2	*Evaluate* the data security that is outsourced by taking samples of client/supplier information systems.
3	*Evaluate* the outsourcing decision *process/contract* complies with the company's strategy.
4	*Evaluate* a sample of third-party vendors and review their service-level agreements.
5	*Ensure* in coordinating with IT professionals that all source codes delivered by the outsourcer are scanned and cleaned from any malware.
6	*Evaluate* the decision-making process around what elements of IT that should be outsourced.
7	*Evaluate* the current risk assessment procedures related to IT outsourcing services before selecting vendors.
Role type: consultancy role	
8	Provide training related to internal control procedures on IT outsourcing processes/contracts.
9	Provide *consultations* about the appropriate steps where noncompliance occurred from vendors.
10	Provide *recommendations* for accepting/rejecting IT outsourcing agreements/contracts.
11	Provide *consultations* about the decision-making process around what elements of IT that should be outsourced.

3.6 Mobile computing

The proliferation of mobile devices in companies, whether private or public, creates a new IT challenge called 'mobile computing usage'. The primary type of *mobile computing risks* is mobile device risks, such as laptops, tablet PCs, and smartphones, which are in widespread use in most companies until IT became an integral part of how people accomplish tasks.

This research divides three objectives for the internal audit roles to cover Ernst and Young's mobile computing risks. The first objective is the monitoring of the inventory process of mobile computing devices. Second, the review processes for policies that manage stolen or lost mobile computing devices and rules that organise using personal employees' equipment at work. Finally, internal auditors check all types of information that can be stored on mobile devices. The IT internal audit roles that achieved all previous objectives are presented in Table 6.

Table 5 Proposed internal auditing roles in IT outsourcing

N	*Internal auditors' proposed role*
Role type: assurance role	
1	*Evaluate* that the contractual terms are clearly defined by taking samples of client/supplier informational systems.
2	*Evaluate* the data security that is outsourced by taking samples of client/supplier information systems.
3	*Evaluate* the outsourcing decision process/contract complies with the company's strategy.
4	*Evaluate* a sample of third-party vendors and review their service-level agreements.
5	*Ensure* in coordinating with IT professionals that all source codes delivered by the outsourcer are scanned and cleaned from any malware.
6	*Evaluate* the decision-making process around what elements of IT that should be outsourced.
7	*Evaluate* the current risk assessment procedures related to IT outsourcing services before selecting vendors.
Role type: consultancy role	
8	Provide training related to internal control procedures on IT outsourcing processes/contracts.
9	Provide *consultations* about the appropriate steps where noncompliance occurred from vendors.
10	Provide *recommendations* for accepting/rejecting IT outsourcing agreements/contracts.
11	Provide *consultations* about the decision-making process around what elements of IT that should be outsourced.

Table 6 Proposed internal auditing roles in mobile computing

N	*Internal auditors' proposed role*
Role type: assurance role	
1	*Assess* the inventory process of mobile computing devices.
2	*Ensure* that the company has adequate procedures for lost or stolen devices.
3	*Ensure* that the company has an *auditing/checking* process for the usage of employees' devices during work.
4	*Ensure* that the company has adequate procedures for reviewing the stored information on internal mobile devices.
5	*Evaluate* types of stored information on mobile devices (sensitive information – not sensitive information).
6	*Ensure* that the stored information on mobile devices is encrypted.
Role type: consultancy role	
7	Provide *consultations* on the internal control inventory process of mobile computing devices.
8	Conduct *training* or provide *recommendations* about the type of information that can be stored on mobile devices.

3.7 Cloud computing and software

Cloud computing is an emerging internet-based computing technology that provides various platforms on-demand and pay-as-you-go (Chen and Yoon, 2010). Growing companies' infrastructure and traditional applications to the cloud means that the in-house control shifts to a third party, such as Amazon, Microsoft, and Google. Many challenges appear, such as privacy problems, security issues, information availability, and performance. Thus, internal auditing should involve in cloud computing risk management to ensure that companies have adequate procedures for potential risks and add value to the risk management process.

Table 7 Proposed internal auditing roles in cloud computing and software

N	*Internal auditors' proposed role*
Role type: assurance role	
1	*Ensure* that the company has procedures for cloud computing risks.
2	*Evaluate* the company's cloud computing strategy (*if it exists*).
3	*Evaluate* information security practices and procedures for cloud computing.
4	*Ensure* that the information security procedures coincide with the company's strategy.
5	*Ensure* that there are internal security measures to protect the stored company's data in the cloud.
6	*Evaluate* service level agreements (SLAs) in cloud computing contracts, including legal, governance, compliance, security, and privacy.
7	*Ensure* that the information within the company's cloud is encrypted.
8	*Ensure* that there are contingency plans in case of failure, liability agreements, and extended support.
9	*Review* all internal software licenses, update, and renew.
10	*Review* internal software contracts.
Role type: consultancy role	
11	Provide *consultations* in information security practices and procedures for cloud computing.
12	Provide *consultations* on cloud computing contracts between the company and the provider.
13	Provide *recommendations* about opportunities for software/cloud cost reductions/timing.
14	Provide internal control *training* in internal control for cloud computing and software contracts.

Software and IT programs, this research focuses on IT cost reduction for establishing new IT projects (*software-updated program*). Importantly, internal software licenses currently account for about 20% of IT costs. Therefore, companies try to mitigate IT costs by reducing software' license-related expenses, limiting potential reputational risks associated with license violations, improving internal software to be more efficient, strengthening IT services, and improving overall operating efficiencies (KMPG, 2017).

Upon the previous discussion, this paper proposes a set of new IT assurance and consultancy internal auditing roles in cloud computing and usage of software/programs, as follows in Table 7. This suggestion may help for better control of companies' cloud, information, software, and IT programs.

In conclusion, the suggested internal audit functions can be considered as a guideline for IT risk management. These motivated outcomes are tested in more detail in the next section. Specifically, the method used to collect data and the validity of these new IT internal audit roles in the real world is outlined.

4 Method

By the design science methodology, the paper examines IT internal audit's framework validation in the real world, which adds high external validity. The paper conducted an exploratory study with a group of an expert sample of internal auditors in Egypt.

4.1 The exploratory study design

To conduct the exploratory study in Egypt, this paper developed a *checklist* of all proposed assurance and consultancy internal auditing roles in IT risk categories. By the *checklist*, the participant can value and evaluate the proposed assurance and consultancy internal auditing role for each IT risk category individually by five *Likert-scale*. This exploration survey is also supported by an online interview and comments obtained during these interviews.

Table 8 All cases, activity distribution

	Frequency	*Percent*	*Valid percent*
Banks	9	12.0	12.0
Commercial	9	12.0	12.0
Constructions	7	9.3	9.3
Consultation	6	8.0	8.0
Government	4	5.3	5.3
Hospital	2	2.7	2.7
Manufacturing	3	4.0	4.0
Natural gas	3	4.0	4.0
Pharmaceutical	3	4.0	4.0
Telecommunicate	9	12.0	12.0
Universities	15	20.0	20.0
Others	5	6.7	6.7
Total	*75*	*100.0*	*100.0*

4.2 Data collection

The field research was carried out in Egypt. Data were collected from one source, which is an exploration survey with highly experienced internal auditors in Egypt from different sectors. Participants are *75* internal auditors with non-missing data from different industry and service sectors in Egypt. The participants received no monetary compensation for completing the study but were given the option to request a report of the results. Table 8 illustrates the number of cases processing summary and also the activity diversity.

Table 9 Chi-square goodness of fit/KMO and Bartlett's test

A: Cybersecurity and IT investments projects: test statistics					
	MEANCyber	*MEANCCyber*	*MEANAITD*	*MEANCITD*	
Chi-square	26.000^{a}	32.213^{b}	37.200^{e}	57.720^{d}	
df	14	10	16	13	
Asymp. sig.	0.026*	0.000*	0.002*	0.000*	
B: IT governance and IT outsourcing: test statistics					
	MEANAITGOV	*MEANCITGOVE*	*MEANAITOUTS*	*MEANCITOUTS*	*MEANASOCIAL*
Chi-square	51.933^{c}	62.427^{b}	40.413^{c}	48.933^{b}	46.333^{f}
df	15	10	15	10	19
Asymp. sig.	0.000*	0.000*	0.000*	0.000*	0.000*
C: Social media, mobile computing, and IT software: test statistics					
	MEANCSOCIAL	*MEANAMOBILE*	*MEANCMOBILE*	*MEANASOFT*	*MEANCSOFT*
Chi-square	109.253^{g}	35.600^{a}	65.280^{h}	47.867^{i}	59.560^{j}
df	12	14	8	18	11
Asymp. sig.	0.000*	0.001*	0.000*	0.000*	0.000*
D: Sampling adequacy test					
Kaiser-Meyer-Olkin measure of sampling adequacy				0.863**	
Bartlett's test of sphericity		Approx. Chi-square		480.854	
		df.		45	
		Sig.		0.000**	

Notes: ^{a,b,c}MEANCyber, MEANCCyber averages for cybersecurity, MEANAINF, MEANCINF averages for information security, MEANAITD, MEANCITD averages for IT Development, MEANAITGOV, MEANCITGOV averages for IT Governance, MEANASOFT, MEANCSOFT averages for software, MEANAITOUTS, MEANCITOUTS averages for outsourcing, MEANASOCIAL, MEANCSOCIAL averages for social media, and MEANAMOBILE, MEANCMOBILE averages for mobile computing (*significant).

As a description of the sample, 50% of the sample participants are between 30–40 years old. They have between 5–11 years of audit experience. We conducted a robust check that the participant (*internal auditors*) must have at least 1–5 years of experience. Another robust condition is that the participant has a *certified internal auditor* (*CIA*) or is in progress.

4.3 Data analysis

The data analysis procedure focused on a descriptive analysis of all the proposed IT internal auditing roles (Stoel et al., 2012). As an organised procedure, I coded all the proposed IT assurance and consultancy internal audit roles, for example, *ITinvest_A_1* (*abbreviation of the IT risk category name – A for Assurance or C for consultancy – number of the role*). As an additional validity procedure, we computed a set of new variables as averages of all proposed roles, whether it is assurance or consultancy in each IT category. In this case, the exploratory study includes seven types of IT risk. We created fourteen new average variables for each set of roles (*for example, MEANACyber – MEANCCyber*). This coded data is beneficial for differentiating the internal audit assurance and consultancy roles groups in the analysis process.

4.4 Data check

A reliability test was conducted for the sample. The objective is to test the credibility of the suggested IT internal auditing roles in the proposed checklist. As a highly consistent response, the reliability test results showed that responses of the sample of internal auditors are reliable with 97.9% (Cronbach's alpha = 0.979). This indicator singles good reliability, as good Cronbach's Alphas for the sample are higher than the minimum 0.7.

Before doing the data analysis, the *Chi-square goodness of fit test* was conducted to determine how well the theoretical distribution fits the empirical distribution. Table 9 – A, B and C show an almost *P-value* = 0.000 for all variables, which means a significant difference between the observed sample distribution and the expected probability distribution. Consistently, panel D presents the *Kaiser-Meyer-Olkin test result*, which measures the sampling adequacy value. The result was *more significant than 50%*, giving a good indicator for measuring and observing the proposed roles.

5 Results and discussion

According to the nature of the exploratory study, descriptive analysis is used. Table 10 illustrates the descriptive analysis of sample responses for the importance of assurance and consultancy internal auditing roles in cybersecurity risks. *MEANACyber* and *MEANCCyber* indicate that all proposed assurance and consultancy internal auditing roles in cybersecurity risks are important *Mean* = 4.31 for assurance roles set and Mean = 4.01 for consultancy setting (*more than 3*). The descriptive analysis indicates that all the suggested roles are significant and useful for the IT risk management process.

Table 10 Descriptive statistics for cybersecurity risks

	N	*Minimum*	*Maximum*	*Mean*	*Std. deviation*
Cyber_A_1	75	2	5	4.41	0.680
Cyber_A_2	75	3	5	4.51**	0.685
Cyber_A_3	75	2	5	4.16	0.789
Cyber_A_4	75	1	5	4.01	0.780
Cyber_A_5	75	2	5	4.23	0.764
Cyber_A_6	75	2	5	4.23	0.815
Cyber_A_7	75	2	5	4.40	0.771
Cyber_A_8	75	2	5	4.35	0.762
Cyber_A_9	75	1	5	4.49	0.778
Cyber_C_1	75	2	5	4.16	0.772
Cyber_C_2	75	2	5	4.19**	0.748
Cyber_C_3	75	1	5	3.77	0.831
Cyber_C_4	75	1	5	3.97	0.822
Cyber_C_5	75	1	5	4.01	0.830
Cyber_C_6	75	1	5	3.97	0.854
Cyber_C_7	75	1	5	4.01	0.908
MEANACyber	75	3	5	4.31*	0.535
MEANCCyber	75	3	5	4.01*	0.607
Valid N (listwise)	75				

Notes: [a]From A_1 to A_8 are the internal auditing assurance roles in cybersecurity risks, From C_1 to C_7 are the internal auditing consultancy roles in cybersecurity risks, MEANACyber, MEANCCyber are the averages of the aggregations of assurance roles and consultancy roles individually. ***Higher Means*. *Average.

The most critical proposed assurance role is ‘ensure that the company has a management crisis plan in case of an actual IT incident or cyber-attack and (if this plan exists) ensure it is updated over time’ (*Mean* = 4.51 and 0.685, *std. deviation*). Compares to ‘give recommendations about new policies and procedures related to confidential data’ is a significant consultancy role in cybersecurity risks.

The previous result is consistent with Lankton et al. (2021) about increasing the control procedures for *cybersecurity risks* by assigning information technology governance roles to the audit committee. The accepted internal audit roles in *cyber-attack* are significant at the same line as Lois et al.’s (2020) findings that the data protection against cyber-attacks and employees’ skills and training are significant.

Table 11 shows that the essential internal auditing assurance roles in IT development and investments risks are ‘evaluate key IT systems development projects throughout their lifecycles (contract compliance, costs, and benefits) and review the user satisfaction study after the IT project/system is completed’ (*Mean* = 4.15/4.09 and 0.748/0.800 *std. deviation*). On the other hand, ‘provide consultation about internal control procedures for new IT systems development projects’ is the most potent consultancy role in IT investment risks. *MEANAITD* and *MEANCITD* specify that all proposed assurance and consultancy internal auditing roles in IT development and investment risks are needed with a *Mean of 4.09* for assurance set and *4.04* for consultancy roles.

Table 11 Descriptive statistics for IT development and investment risks

	N	*Minimum*	*Maximum*	*Mean*	*Std. deviation*
ITinvest_A_1	75	2	5	4.15*	0.748
ITinvest_A_2	75	2	5	4.11	0.746
ITinvest_A_3	75	2	5	4.03	0.788
ITinvest_A_4	75	2	5	4.12	0.770
ITinvest_A_5	75	1	5	3.89	0.815
ITinvest_A_6	75	1	5	4.15**	0.800
ITinvest_A_7	75	1	5	4.11	0.798
ITinvest_C_1	75	2	5	3.99	0.814
ITinvest_C_2	75	1	5	3.93	0.777
ITinvest_C_3	75	2	5	4.09**	0.720
ITinvest_C_4	75	2	5	4.03	0.753
MEANAITD	75	2	5	4.07*	0.597
MEANCITD	75	2	5	4.01*	0.618
Valid N (listwise)	75				

Notes: [a]From A_1 to A_7 are the internal auditing assurance roles in IT development and investment risks. From C_1 to C_4 are the internal auditing consultancy roles in information security risks. MEANAITD, MEANCITD are the averages of the aggregations of assurance roles and consultancy roles individually. ***Higher Means*. **Average*.

Table 12 Descriptive statistics for IT governance

	N	*Minimum*	*Maximum*	*Mean*	*Std. deviation*
ITGovernance_A_1	75	1	5	4.29**	0.785
ITGovernance_A_2	75	2	5	4.21	0.759
ITGovernance_A_3	75	2	5	4.20	0.771
ITGovernance_A_4	75	3	5	4.29	0.749
ITGovernance_A_5	75	2	5	4.21	0.776
ITGovernance_A_6	75	2	5	4.11	0.709
ITGovernance_C_1	75	2	5	4.15**	0.748
ITGovernance_C_2	75	2	5	4.03	0.870
ITGovernance_C_3	75	2	5	4.00	0.788
MEANAITGOV	75	3	5	4.21*	0.641
MEANCITGOV	75	2	5	4.06*	0.663
Valid N (listwise)	75				

Notes: [a]From A_1 to A_6 are the internal auditing assurance roles in IT governance. From C_1 to C_3 are the internal auditing consultancy roles in IT governance. MEANAGOV, MEANCGOV are the averages of the aggregations of assurance roles and consultancy roles individually. ***Higher Means*. **Average*.

Table 13 Descriptive statistics for IT outsourcing

	N	*Minimum*	*Maximum*	*Mean*	*Std. deviation*
ITOutsourcing_A_1	75	1	5	4.28*	0.781
ITOutsourcing_A_2	75	3	5	4.24	0.654
ITOutsourcing_A_3	75	2	5	4.12	0.753
ITOutsourcing_A_4	75	3	5	4.05	0.613
ITOutsourcing_A_5	75	3	5	4.09	0.619
ITOutsourcing_A_6	75	3	5	4.19	0.672
ITOutsourcing_A_7	75	2	5	4.23	0.709
ITOutsourcing_C_1	75	2	5	4.11*	0.628
ITOutsourcing_C_2	75	2	5	4.04	0.743
ITOutsourcing_C_3	75	1	5	4.07	0.794
ITOutsourcing_C_4	75	1	5	4.08	0.784
MEANAITOUTS	75	3	5	4.16*	0.510
MEANCITOUTS	75	2	5	4.09*	0.601
Valid N (listwise)	75				

Notes: [a]From A_1 to A_7 are the internal auditing assurance roles in IT outsourcing risks. From C_1 to C_4 are the internal auditing consultancy roles in IT outsourcing risks. MEANAOUTS, MEANCOUTS are the averages of the aggregations of assurance roles and consultancy roles. ***Higher Means*. **Average*.

As expected, both proposed assurance and consultancy internal auditing roles related to IT governance are significant with a higher means (*4.21 and 4.06*, Table 12). The results show that the 'evaluate that the company has adequate (effective) IT governance procedures.' is the higher significant assurance role with a mean of 4.29. The previous results are consistent with Carle et al. (2020) that found IT governance improves companies' capability, controlling, monitoring outcomes, and performance. Moreover, the significant consultancy is 'Provide training about internal control procedures related to IT risks' with a mean of = *4.15*. This result is consistent with previous practical results about the importance of internal auditors' training recommendations recognised by Hoos et al. (2017).

Internal audit assists managers in evaluating IT outsourcing decisions. Averages for assurance and consultancy internal audit roles show that the proposed assurance and consultancy internal auditing roles in the IT outsourcing process are important and influential (*4.16 and 4.09*).

Regarding the contractual terms, the results show that the most significant assurance role is to 'evaluate that the contractual terms are clearly defined and compiled by taking samples of client/supplier informational systems' (*Mean* = 4.28). Additionally, the most significant consultancy role is 'provide training related to internal control procedures on IT outsourcing processes/contracts' (*Mean* = 4.11) (Table 13).

The results in Table 14 show that all proposed assurance and consultancy internal audit roles in social media risks are significant (*Means* = 4.04 and 4.01). The suggested assurance role 'ensure that there are internal control corrective actions towards social media risks' is the most significant one with a mean of 4.19, and the dual consultancy role 'provide consultations about controlling corrective actions towards social media risks' (*Mean* = 4.04). The previous finding is consistent with the recommendations of He's study.

Table 14 Descriptive statistics for social media risks

	N	*Minimum*	*Maximum*	*Mean*	*Std. deviation*
SocialMedia_A_1	75	2	5	3.92	0.801
SocialMedia_A_2	75	2	5	4.01	0.862
SocialMedia_A_3	75	1	5	4.09	0.857
SocialMedia_A_4	75	1	5	3.91	0.808
SocialMedia_A_5	75	2	5	4.11	0.831
SocialMedia_A_6	75	2	5	4.19**	0.730
SocialMedia_A_7	75	2	5	3.97	0.771
SocialMedia_A_8	75	1	5	4.01	0.862
SocialMedia_C_1	75	2	5	4.03	0.771
SocialMedia_C_2	75	2	5	3.99	0.762
SocialMedia_C_3	75	2	5	4.03	0.716
SocialMedia_C_4	75	2	5	4.04**	0.725
MEANASOCIAL	75	2	5	4.04*	0.619
MEANCSOCIAL	75	2	5	4.01*	0.660
Valid N (listwise)	75				

Notes: [a]From A_1 to A_8 are the internal auditing assurance roles in social media risks. From C_1 to C_4 are the internal auditing consultancy roles in social media risks. MEANASOCIAL, MEANCSOCIAL are the averages of the aggregations of assurance roles and consultancy roles individually. ***Higher Means*. **Average*.

Table 15 Descriptive statistics for mobile computing risks

	N	*Minimum*	*Maximum*	*Mean*	*Std. deviation*
MobileCom_A_1	75	2	5	4.23	0.798
MobileCom_A_2	75	2	5	4.32*	0.738
MobileCom_A_3	75	2	5	4.21	0.776
MobileCom_A_4	75	2	5	4.17	0.844
MobileCom_A_5	75	1	5	4.13	0.935
MobileCom_A_6	75	2	5	4.25	0.871
MobileCom_C_1	75	2	5	4.12*	0.805
MobileCom_C_2	75	2	5	4.00	0.805
MEANAMOBILE	75	2	5	4.21*	0.629
MEANCMOBILE	75	2	5	4.06*	0.695
Valid N(listwise)	75				

According to Table 15 results, all proposed assurance and consultancy internal auditing roles in mobile computing risks are significant and add value to the risk management decisions. The internal audit assurance role 'ensures to have adequate procedures for lost or stolen devices' is the most fundamental in mobile computing risks (*Mean* = 4.32).

Providing consultations on the inventory process of mobile computing devices is the most influential consultancy role in mobile computing risks (*Mean* = 4.12).

Table 16 Descriptive statistics for cloud computing and IT software

	N	*Minimum*	*Maximum*	*Mean*	*Std. deviation*
Software_A_1	75	2	5	4.28*	0.727
Software_A_2	75	2	5	4.23	0.746
Software_A_3	75	2	5	4.19	0.711
Software_A_4	75	2	5	4.15	0.783
Software_A_5	75	2	5	4.27	0.723
Software_A_6	75	2	5	4.19	0.800
Software_A_7	75	2	5	4.17	0.760
Software_A_8	75	2	5	4.28*	0.781
Software_A_9	75	1	5	4.15	0.800
Software_A_10	75	2	5	4.27	0.684
Software_C_1	75	2	5	4.21*	0.741
Software_C_2	75	2	5	4.04	0.779
Software_C_3	75	1	5	4.04	0.892
Software_C_4	75	2	5	4.13	0.759
MEANASOFT	75	2	5	4.22*	0.625
MEANCSOFT	75	2	5	4.11*	0.674
Valid N (listwise)	75				

Notes: [a]From A_1 to A_6 are the internal auditing assurance roles in mobile computing risks. From A_1 to A_10 are the internal auditing assurance roles in cloud computing and IT software risks. From C_1 to C_2 are the internal auditing consultancy roles in mobile computing risks. MEANAMOBILE, MEANCMOBILE are the averages of assurance roles and consultancy roles. ***Higher Means*. **Average*. From C_1 to C_4 are the internal auditing consultancy roles in cloud computing and software risks, MEANASOFT, MEANCSOFT are the averages of assurance roles and consultancy roles individually. ***Higher Means*. **Average*.

Table 16 results show that all potential assurance internal auditing roles in cloud computing and IT software are important with means of *more than 4*. The result reflects that internal auditors care about the part of the IT budget, which goes to IT software and programs. Moreover, the internal audit confirmation that companies have effective procedures (*contingency plans*) for cloud computing risks is the leading assurance role (*Mean* = 4.28), whereas giving consultation and training about internal control is the chief role of the suggested consultancy internal auditing roles in this category (*Mean* = 4.21).

In conclusion, results revealed that the internal auditors' sample accepted the individual potential assurance and consultancy internal auditing roles framework in each IT risk management category. As we expected, they confirmed that IT risk management's potential assurance roles provide managers with useful and valuable information related to evaluating the IT risk management process up to date. In contrast, the consultancy roles give recommendations, consultations, and training to management in order to add and strengthen the value of IT risk management decisions.

Interestingly, the descriptive analysis concluded that internal auditing assurance roles are more significant than consultancy in IT risk management. However, both roles mitigate the potential consequences of the IT risks by ensuring the IT risk management process is up to date with management and audit committee from one side and add value to the decisions related to IT risk categories from the other side.

The admission now is that the assurance and consultancy internal auditing roles in IT risk management are important. However, we have one issue, which is the final rank of importance for IT risk categories. The second stage of analysis investigates the significance of IT risk categories by comparing the mean rank of assurance internal auditing roles. In other words, the IT risk category that has a *higher mean rank* of assurance roles is very imperative. The method used is the *Friedman test* to rank the significance of IT risk categories by the weight of the assurance internal auditing roles for each category.

Table 17 presents the *Friedman test results*. *P.Value* = 0.000 for this test, which reflected the difference between IT risks groups. The higher Chi-square and small *P.Value* give an indicator that the responses between all groups are different. Also, the higher validity of this test in this case. As expected and consistent with all recent IT risks visions, cybersecurity and information security risks are the most significant IT risk category (*Mean rank* = 9.13). The second important IT risk category is the IT governance rules (*Mean rank* = 8.73). A small difference between IT software and mobile computing as third and fourth rank (*Means rank* = 8.61 and 8.08). The fifth is outsourcing risk management (*Mean rank* = 7.64). The sixth and seventh are IT investment and Social media risks (*Means rank* = 7.15 and 6.57).

As an additional analysis, this study presents a view of the interconnection between the assurance and consultancy internal audit roles as a suggested approach to sustainable business and value creation. Where this happens, this paper explores the validity and importance of integrating the assurance and consultancy internal auditing roles in IT risk management. The integration between the assurance and consultancy internal auditing roles is essential in this research. European Confederation of Institutes of Internal Auditing, GTAG, and Ernst & Young's guidelines have recommended that internal auditing change from the observer position to the consultant position, particularly in the risk management process.

Table 17 (a) Friedman test to rank the importance of IT risk categories

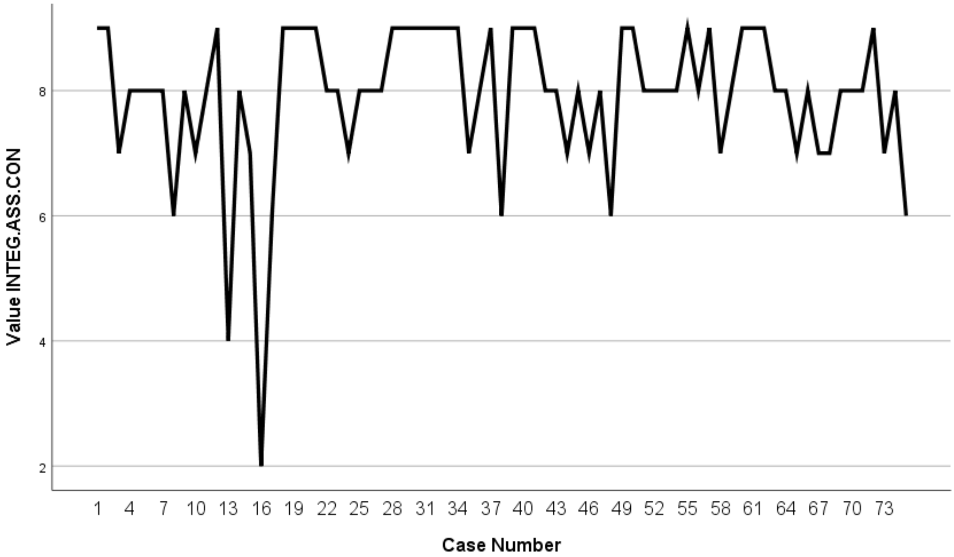
Panel A: rank	
	Mean rank
MEANCyber	9.13 (1)
MEANAITDE	7.15 (6)
MEANITGOVERN	8.73 (2)
MEANAITOUTSOUR	7.64 (5)
MEANASOCIAL	6.57 (7)
MEANAMOBILE	8.08 (4)
MEANASOFT	8.61 (3)

Table 17 (b) Friedman test to rank the importance of IT risk categories: test statistics

N	75
Chi-square	46.305
df	13
Asymp. sig.	0.000

The paper uses the assurance and consultancy internal audit roles together in IT risk management. The aim is to gain the assured function of the internal audit in the proposed framework represented in Assurance roles and gain the value-added from the consultancy roles. Figure 2 illustrates the importance of integrating the proposed assurance and consultancy internal auditing roles in IT risk management. Figure 2 shows the range of acceptance for the internal auditors' responses. The majority of the responses reflect a high degree of acceptance of what the study proposed about the usefulness of using assurance and consultancy roles in IT risk management.

Figure 2 The integrated variable distributions



In each case, this paper depends on the non-parametric tests in the next analysis. We conduct a *one-sample Wilcoxon signed-rank test (as an alternative test of T-test*), which is a non-parametric alternative to a one-sample t-test when the data cannot be assumed to be normally distributed. It uses to determine whether the median of the sample is equal to a known standard value. We create a *5 and 9 Likert scale* to the satisfaction of the internal auditors' sample about the range of the proposed IT risk categories and potential assurance and consultancy roles.

As expected and consistent with the sections' preliminary analysis, Table 18 presents the null hypothesis's rejections in all variables with *P-value* = 0.000, which means that the observed median is far higher than the hypothetical median. According to these findings, the proposed IT risks categories and the potential assurance and consultancy roles to these IT risk regions are valid and important from the sample's responses.

Table 18 Wilcoxon signed-rank test

N	*H0: refer to mean ≤ 5*	*Test*	*Sig.*	*Decision*
1	The median of ITRISKCOM[a] equals 5.	One sample Wilcoxon Signed rank test	00000*	Reject Ho
2	The median of FRAMWORKCOM[b] equals 5.		00000*	Reject Ho
3	The median of IT ASS.EVAU[c] equal 5.		00000*	Reject Ho
4	The median of IT CON.EVAU[d] equal 5.		00001*	Reject Ho
5	The median of INTEG.ASS.COM[e] equal 5.		00000*	Reject Ho

Notes: [a,b,c,d,e]Variables are ITRISKCOM for IT risk categories evaluations, FRAMWORKCOM for framework evaluations, ASS.EVAU assurance roles evaluations, ASS.EVAU consultancy roles evaluations, and INTEG.ASS.COM the integration between assurance and consultancy roles in IT risk management.

In summary, upon the previous finding, it is clear that the acceptance of the proposed internal auditing roles in IT risk management developed by this paper is highly consistent with the internal auditors' sample. Notably, the proposed IT internal audit roles cover new internal auditing mechanisms, extensions of internal audit responsibilities, and hiring qualified and experienced internal auditors in internal audit teams, consistent with the recommendations of agency theory to develop the internal audit profession.

6 Conclusions

Real-world current business activities focus on the IT facilities in most of their businesses. The evolution of IT and the implications of the information systems within companies is a double-edged sword. Accordingly, this research offered a framework of internal auditing roles in IT risk management. The proposed framework focuses on the collaboration and coordination between management, IT departments, internal auditors, and audit committee members. It is important to reduce the information gap between all these parties during the IT risk management process. Thus, suggesting internal audit roles in IT risk management is the first objective of this research.

The proposed framework of internal auditing roles in IT risk management includes seven IT risks categories. Each category involves assurance and consultancy internal auditing roles. Thus, the second objective of this research is to evaluate the proposed framework of internal auditing roles in IT risk management in the real world. The paper conducted an exploratory methodology to explore the validity of the new framework and get some feedback and remarks from the professional internal auditors in Egypt. Internal auditors from different sectors agreed that the IT risk categories are sufficient, represented faithfully, and essential. At the same time, they accepted the potential assurance and consultancy internal auditing roles in IT risk management. Consistent with my expectations, they accepted that the assurance internal auditing roles in IT risk management are more useful for the management than the consultancy internal auditing roles.

The new suggested internal audit roles provide an excellent opportunity for companies to coordinate between the IT department, the audit committee, and the internal audit. This collaboration between management, audit committee, and the internal audit in the IT risk management process increases the adequate assurance in the companies' IT risk management, governance, and IT internal control processes. Consulting roles improve IT systems and processes. However, there are some concerns about internal auditors independently because of the direct interactions with management, making this paper uses as a base to conduct further research (*questionnaire or interviews*) related to the impact of the consultancy roles on internal auditors' independence. Also, the disclosure of the assurance and consultancy IT internal audit roles in the management internal control assessment report might be a new contribution for further research in the future.

Acknowledgements

I would like to thank my dissertation supervision members Prof. Mohamed Shehata, Professor of Accounting and Auditing, Accounting Area, DeGroote Business School, McMaster University-Canada and Prof. Samir Helal, Professor of Accounting and Auditing, Accounting Department, Faculty of Commerce, Tanta University, for their mentorship. I thank Prof. Joshua Onome Imoniana, Editor of the *International Journal of Auditing Technology*, and referees for helpful comments and suggestions. All remaining errors are my own.

References

Ashurst, C., Doherty, N. and Peppard, J. (2008) 'Improving the impact of IT development projects: the benefits realization capability model', *European Journal of Information Systems*, Vol. 17, No. 3, pp.352–370.

Bailey, C., Denton, C. and Abbott, L. (2017) 'The impact of enterprise risk management on the audit process: evidence from audit fees and audit delay', *Auditing: A Journal of Practice & Theory*, Vol. 37, No. 3, pp.25–46.

Borgman, B., Mubarak, S. and Choo, K. (2015)' Cybersecurity readiness in the South Australian Government', *Computer Standards & Interfaces*, Vol. 37, pp.1–8, ISSN No. 0920-5489.

Brandas, C. (2010) 'Risks and audit objectives for IT outsourcing', *Informatics Economical*, Vol. 14, No. 1, pp.113–119.

Breger, D., Edmonds, M. and Ortegren, M. (2020) 'Internal audit standard compliance, potentially competing duties and external auditors' reliance decision', *The Journal of Corporate Accounting and Finance*, Vol. 31, No. 1, pp.112–124.

Burton, R.N. (2000) Discussions of information technology – related activities of internal auditors', *Journal of Information Systems*, Vol. 14, No. S1, pp.57–60.

Chen, Z. and Yoon, J. (2010)' IT auditing to assure a secure cloud computing', *IEEE 6th World Congress on Services*.

Conklin, A. and White, G.B. (2006) 'E-government and cyber security: the role of cyber security exercises', *39th Hawaii International Conference on System Sciences*.

Debreceny, R.S. (2013) 'Research on IT governance, risk and value: challenges and opportunities', *Journal of Information Systems*, Vol. 27, No. 1, pp.129–135.

Dhillon, G., Syedb, R. and de Sá-Soaresc, F. (2017) 'Information security concerns in IT outsourcing: identifying (in) congruence between clients and vendors', *Information & Management*, Vol. 54, No. 4, pp.452–464.

EIOD (2016) *The Code of Corporate Governance for the Public Sector Enterprise Sector in the Arab Republic of Egypt* [online] https://www.ecgi.org/codes/documents/codecgEgypt13feb2011ar.pdf (accessed 22 January 2022).

French, A.M., Shim, J.P., Otondo, R.F. and Templeton, G.T. (2018) 'An empirical study evaluating social networking continuance and success', *Journal of Computer Information Systems*, Vol. 58, No. 4, pp.353–362.

Global Technology Audit Guide (GTAG) (2012) *Auditing Application Controls* [online] https://na.theiia.org/Pages/IIAHome.aspx (accessed 22 January 2022).

González, R., Gascó, J. and Llopis, J. (2016) 'Information systems outsourcing reasons and risks: review and evolution', *Journal of Global Information Technology Management*, Vol. 19, No. 4, pp.223–249.

Gyun No, W. and Vasarhelyi, M.A. (2017) 'Cybersecurity and continuous assurance', *Journal of Emerging Technologies in Accounting*, Vol. 14, No. 1, pp.1–12.

Harb, A.S.M. (2020) 'The effect of internal audit on accounting information technology in the public joint stock pharmaceutical industries in Jordan', *Academy of Accounting and Financial Studies Journal*, Vol. 24, No. 1, pp.1–8.

He, W. (2012) 'A review of social media security risks and mitigation techniques', *Journal of Systems and Information Technology*, Vol. 14, No. 2, pp.171–180.

He, W. (2013) 'A survey of security risks of mobile social media through blog mining and an extensive literature search', *Information Management & Computer Security*, Vol. 21, No. 5, pp.381–400.

Hermanson, D., Hill, M.C. and Ivancevich, D.M. (2000) 'Information technology-related activities of internal auditors', *Journal of Information Systems*, Vol. 14, No. 1, pp.1–39.

Héroux, S. and Fortin, A. (2013) 'The internal audit function in information technology governance: a holistic perspective', *Journal of Information Systems*, Vol. 27, No. 1, pp.189–217.

Hoos, F., Messier, W.F., Smith, J.L. and Tandy, P.R. (2017) ' An experimental investigation of the interaction effect of management training ground and reporting lines on internal auditors' objectivity', *International Journal of Auditing*, Vol. 22, No. 2, pp.150–163.

Institute of Internal Auditors (IIA) (1999) *A Vision for the Future: Professional Practices Framework for Internal Auditing*, The Institute of Internal Auditors Research Foundation, Altamonte Springs, FL.

Institute of Internal Auditors (IIA) (2004) *The Professional Practices Framework*, The Institute of Internal Auditors' Research Foundation, Altamonte, Spring, FL.

Institute of Internal Auditors (IIA) (2018) *The Future of Cybersecurity in Internal Audit*, A joint research report by the Internal Audit Foundation and crowe horwath [online] https//:bookstore.theiia.org/the-future-of-cybersecurity-in-internal-audit (accessed 15 June 2018).

Islam, M.S., Farah, N. and Stafford, T.S. (2018) 'Factors associated with security/cybersecurity audit by internal audit function: an international study', *Managerial Auditing Journal*, Vol. 33, No. 4, pp.377–409.

Jiang, L., Messier, W.F. and Wood, D.A. (2019) 'The association between internal audit consulting services and firm performance', *Auditing: A Journal of Practice & Theory*, Vol. 39, pp.101–124.

Kahyaoglu, S.B. and Caliyurt, K. (2018) 'Cybersecurity assurance process from the internal audit perspective', *Managerial Auditing Journal*, Vol. 33, No. 4, pp.360–376.

KPMG (2017) 'Key risks for internal audit' [online] https://home.kpmg/cn/en/home/insights/2017/03/kpmg-internal-audit-top-10-considerations-for-2017.html.

Lacity, M.C., Khan, S.A. and Willcocks, L.P. (2009) 'A review of the IT outsourcing literature: insights for practice', *Journal of Strategic Information Systems*, Vol. 18, No. 3, pp.130–146.

Lankton, N., Price, J.B. and Karim, M. (2021) 'Cybersecurity breaches and information technology governance roles in audit committee charters', *Journal of Information Systems*, Vol. 35, No. 1, pp.101–119.

Lois, P., Drogalas, G., Karagiorgos, A. and Tsikalakis, K. (2020) 'Internal audits in the digital era: opportunities risks and challenges', *EuroMed Journal of Business*, Vol. 15, No. 2, pp.205–217.

Marshall, D.W. (2020) 'The role of internal audit in the risk management process a developing economy perspective', *The Journal of Corporate Accounting and Finance*, Vol. 31, No. 4, pp.154–165.

Rosati, P., Gogolin, F. and Lynn, T. (2020) 'Cyber-security incidents and audit quality', *European Accounting Review*, DOI: 10.1080/09638180.2020.1856162.

Roussy, M. and Perron, A. (2018) 'New perspectives in internal audit research: a structured literature review', *Accounting Perspectives*, Vol. 17, No. 3, pp.345–385.

Samantra, C., Datta, S. and Mahapatra, S. (2014) 'Risk assessment in IT outsourcing using fuzzy decision-making approach: an Indian perspective', *Expert Systems with Applications*, Vol. 41, No. 8, pp.4010–4022.

Steinbart, P., Raschke, R., Gal, G. and Dilla, W. (2012) 'The relationship between internal audit and information security: an exploratory investigation', *International Journal of Accounting Information Systems*, Vol. 13, No. 3, pp.228–243.

Steinbart, P., Raschke, R., Gal, G. and Dilla, W. (2013) 'Information security professionals' perceptions about the relationship between the information security and internal audit functions', *Journal of Information Systems*, Vol. 27, No. 2, pp.65–86.

Steinbart, P., Raschke, R., Graham, G. and Dilla, W. (2014a) 'Internal audit's contribution to the effectiveness of information security (part 1): perceptions of information security professionals', *ISACA Journal*, Vol. 2, pp.42–47.

Steinbart, P., Raschke, R., Graham, G. and Dilla, W. (2014b) 'Internal audit's contribution to the effectiveness of information security (part 2): perceptions of internal auditors', *ISACA Journal*, Vol. 3, pp.51–55.

Stoel, D., Havelka, D. and 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.

Wilkin, C.L. and Chenhall, R.H. (2020) 'Information technology governance: reflections on the past and future directions', *Journal of Information Systems*, Vol. 34, No. 2, pp.257–292.