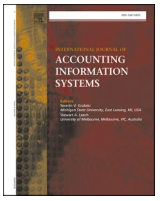
International Journal of Accounting Information Systems 52 (2024) 100663

Contents lists available at ScienceDirect

International Journal of Accounting Information Systems

journal homepage: www.elsevier.com/locate/accinf



IT governance and IT controls: Analysis from an internal auditing perspective

Tung-Hsien Wu [a], Shaio Yan Huang [b], An-An Chiu [c], David C. Yen [d,*]

[a] Department of Accounting, Feng Chia University, No. 100 Wenhwa Rd., Seatwen, Taichung 40724, Taiwan, ROC
[b] Department of Accounting and Information Technology, National Chung Cheng University, 168 University Road, Minhsiung Township, Chiayi County 62102, Taiwan, ROC
[c] Department of International Trade, Feng Chia University, No. 100 Wenhwa Rd., Seatwen, Taichung 40724, Taiwan, ROC
[d] Jesse H. Jones School of Business, Texas Southern University, 3100 Cleburne Street, Houston, TX 77004, Taiwan, ROC

ARTICLE INFO

Keywords:
Information technology (IT) governance
IT controls
IT audit

ABSTRACT

Inadequate information technology (IT) management can lead to system ineffectiveness and operational stagnation within enterprises. While the application of IT governance provides a means for companies to validate IT functionality, oversee IT operations, and mitigate IT-associated risks, there is a paucity of research examining its implications of IT governance on IT controls, particularly within the context of a firm's Internal Audit Function (IAF). Addressing this gap in the literature, this research delves into the relationship between the characteristics of the IAF and IT governance within the IAF. It further probes the linkage between IT governance associated with the IAF and IT control activities. We analyze survey data from 414 internal auditors across various Taiwanese companies using partial least squares regression. The findings suggest that IT knowledge and internal auditing roles have a significantly positive relationship with the quality of the IAF-IT relationship and IT governance processes. Similarly, IT audit competencies exhibit a significantly positive relationship with IT governance processes. Furthermore, properly structured IT governance processes and a high-quality IAF-IT relationship demonstrate a positive association with the effectiveness of general controls. This research amalgamates and extends prior investigations into IT governance and internal auditing, underlining their critical role in successfully implementing superior IT controls.

1. Introduction

Post the Enron scandal in 2000, the enactment of the Sarbanes-Oxley Act in the U.S. necessitated companies to take measures that ensure the efficacy of their internal controls over financial reporting (section 404). As information technology (IT) plays a pivotal role in ensuring the precision of a company's financial reports, IT controls have thus become an integral component of Sarbanes-Oxley compliance initiatives. To facilitate IT governance, which pertains to formalizing strategic IT decisions and essential IT oversight processes, the Information Systems Audit and Control Association (ISACA) introduced the Control Objectives for Information and Related Technology (COBIT) in 2019. However, despite these measures, public companies still report material weaknesses in IT controls. A 2021 analysis of business processes and material weaknesses among public companies registered with the U.S. Securities

* Corresponding author.
E-mail addresses: thwu@mail.fcu.edu.tw (T.-H. Wu), David.Yen@TSU.edu (D.C. Yen).

https://doi.org/10.1016/j.accinf.2023.100663
Received 13 February 2021; Received in revised form 24 July 2023; Accepted 4 December 2023
Available online 11 December 2023
1467-0895/© 2023 Elsevier Inc. All rights reserved.

and Exchange Commission by the accounting firm KPMG found that IT control material weaknesses accounted for 35 % of all material weaknesses in 2020 (KPMG, 2021a).

Given their critical role in corporate and financial security, material weaknesses in IT controls pose a significant threat to the legitimacy of companies (Haislip et al., 2016). Furthermore, such weaknesses can negatively impact the quality of the information in systems, potentially misleading management and resulting in improper decisions (Li et al., 2012). Stoel and Muhanna (2011) observe that companies with material weaknesses in IT internal controls underperformed those without such issues. In an era characterized by big data and sophisticated digital technologies, material weaknesses in IT internal controls can lead to substantial losses, thus emphasizing the need for effective IT controls.

The literature highlights the centrality of IT governance for effective IT controls (IIA, 2018). While numerous studies have probed into IT governance, a noticeable research gap persists concerning the interconnectedness among Internal Audit Functions (IAFs), IT governance, and IT controls. Some academic discourses have initiated explorations into this triadic relationship. For instance, Héroux and Fortin (2013) delve into the participation of IAFs in IT governance, shedding light on the role of internal audits within IT governance and the interplay between characteristic elements of IAF and its involvement in IT governance. Their finding spotlights two IAF characteristic elements that enhance the engagement of IAFs in IT governance: (1) the extent of resources and IT audit experience and (2) the number of IT personnel coupled with IT training or certification.

Merhout and Havelka (2008) demonstrate that internal audit departments effectively identify and augment control mechanisms to bolster information security when they conduct IT audits. A comprehensive IT audit program can recognize and document effective control mechanisms within the information system. Despite these findings, the literature primarily focuses on the impacts of IT audits and does not examine the relationship between the engagement of IAFs in IT governance and IT controls. Our research therefore scrutinizes the characteristics of IAF pertinent to its involvement in IT governance and the relationship between the participation of IAFs in IT governance and IT controls. We pose the following two questions: What are the defining characteristics of IAF that foster successful involvement in IT governance? How does this involvement correlate with IT controls?

This study explores the characteristics of internal audit departments engaged in IT governance and ascertains if such participation bolsters IT controls. This inquiry can empower businesses to optimize their internal audit department resources effectively for the execution of IT governance activities. Various business models are anchored on digital technologies. These technologies are electronic instruments, systems, platforms, and resources that engender, store, or process data, including but not limited to social media, mobile devices, big data, process mining, and the Internet of Things (Abubaker and El-Badri, 2022; Allataifeh and Moghavvemi, 2022). However, these firms encounter formidable security risks in implementing such technologies. Their principal challenge is identifying and rectifying their digital vulnerabilities. Contemporary IT audits primarily concentrate on cybersecurity risks, general IT controls, and data governance (KPMG, 2021b). KPMG (2021b) discloses that 67 % of firms fast-tracked their digital transformation strategy after COVID-19.

Digital transformation encapsulates the utilization of digital technology to enhance processes, augment efficiency, cultivate new business opportunities, and boost competitiveness by deploying new digital tools and processes (Paiva et al., 2021; Teffo et al., 2022; Yu et al., 2022). For instance, firms might use cloud technology for document storage and sharing or leverage artificial intelligence and machine learning technologies to ameliorate productivity and forecast demand. Effective IT governance is a cornerstone for these digital transformation endeavors, offering a structured framework for decisions concerning technology investments and for aligning technology with business objectives.

IT governance also assists in identifying and managing risks via processes like security and data protection policies (Spremic, 2017; Mulyana et al., 2021; De Haes et al., 2020; DeLone et al., 2018). More than 19 % of internal audit departments participate in the initial design phase of this digital transformation (KPMG, 2021b). Internal auditors should indeed be incorporated into the early stages of digital transformation to manage risks and enhance value efficiently. Their involvement plays a pivotal role in actualizing the strategic objectives of digital transformation initiatives.

This research conducts a survey to analyze the relationships between internal audit characteristics, the engagement of IAFs in IT governance, and IT controls. The defining characteristics of IAFs include IT knowledge, internal audit roles, and IT audit competencies. The engagement of IAFs in IT governance is bifurcated into two categories: IAF-IT relationship quality and IAF-IT governance processes. General controls are employed to measure IT controls, and the Partial Least Squares (PLS) method is applied to analyze the survey outcomes.

The questionnaire was distributed among internal auditors from publicly-traded Taiwanese companies, yielding an adequate sample size of 414. The results reveal that IT knowledge and internal auditing roles significantly positively correlate with the IAF-IT relationship quality. IT knowledge, internal audit roles, and IT audit competencies have positive relationships with IAF-IT governance processes. Hence, the distinct attributes of an internal audit department can enhance the engagement of IAFs in IT governance. This engagement is able to amplify the effectiveness of IT controls.

The scholarly contributions of this research manifest in elucidating the role of IAFs in IT governance and delineating the benefits derived from IAFs' involvement in IT controls. While research primarily focuses on the mechanisms of IT governance concerning internal audits (Héroux and Fortin, 2013), no study has yet to explore the relationship between the engagement of IAFs in IT governance and IT controls. An internal audit's fundamental function includes ensuring the effectiveness and efficiency of business operations, including IT controls. Our study broadens the scope of engagement of IAFs in IT governance by linking it to IT controls, hence providing an understanding of how IAFs can bolster IT controls. The results derived from this research can aid companies in devising strategies to enhance those IAF characteristics correlated with IT governance, thereby facilitating practical assessments of IT controls.

The study's findings can also help firms optimize resource allocation within IAFs. These functions should allocate a portion of

resources to analyze risks related to IT strategies and to improve IT controls. Our results further illuminate factors pertaining to the engagement of IAFs in IT governance. To achieve improved IT governance, organizations should consider IAF specialties related to IT auditing when implementing an IT governance strategy. Consequently, the outcomes of this study help guide corporations and regulators alike, enabling them to fortify the engagement of IAFs in IT governance to achieve their IT governance objectives.

The rest of this paper is as follows. Section 2 presents a comprehensive review of pertinent literature and introduces the research hypotheses formulated herein. Section 3 delineates the proposed research model and elucidates the methodology employed. Section 4 gives the empirical results derived from the execution of the research methodology. Section 5 concludes, wherein we summarize our findings, discuss the implications of the outcomes, and offer suggestions for future research directions within this field.

2. Background

2.1. Internal audit characteristics and the involvement of IAFs in IT governance

2.1.1. Involvement of IAFs in IT governance

IT governance primarily aims to align an IT strategy with a company strategy, optimizing the value of IT investments. Studies have mainly focused on the link between IT governance and IT effectiveness (Lunardi et al., 2016; Ali and Green, 2012; Nfuka and Rusu, 2011; Bradley et al., 2012) or organizational performance (Wu et al., 2015). Pang (2014) proposes that IT governance moderates the relationship between IT expenditure and IT cost efficiency.

Internal audits are pivotal in ensuring the effectiveness of IT governance. As stated in Standard 2110 of the Institute of Internal Auditors (IIA) (IIA, 2012), "the internal audit activity must assess and make appropriate recommendations for improving the governance process in its accomplishment of the following objectives: promoting appropriate ethics and values within the organization; ensuring effective organizational performance management and accountability; communicating risk and control information to appropriate areas of the organization; and coordinating the activities of and communicating information among the board, external and internal auditors, and management." Furthermore, IIA Standard 2110.A2 (IIA, 2012) emphasizes that "the internal audit activity must assess whether the IT governance of the organization supports the organization's strategies and objectives." Lastly, according to IIA (2018), an internal audit evaluates whether an organization's IT governance capability suffices to realize the organization's objectives and offers suggestions to enhance the efficiency and effectiveness of IT projects.

This study addresses IT governance regarding the IAF-IT relationship quality and IAF-IT governance processes. The IAF-IT relationship quality denotes the level of interaction between IT and IAFs. De Haes et al. (2013) suggest that a collaborative relationship between IAFs and IT relates to IT governance's relational mechanisms. In other words, the quality of the IAF-IT relationship can bolster IT governance capabilities. For instance, integrating IT and IAFs can facilitate identifying, monitoring, and mitigating IT-related risks. Moreover, the reciprocal consultation between IT and IAF managers contributes to developing effective IT policies and procedures (Héroux and Fortin, 2013).

IT governance processes involve implementing strategic IT decisions and monitoring procedures to create systems and specifications that conform to daily operational processes and policies. These monitoring systems offer feedback to decision-makers. In the realm of IAF-IT governance processes, companies evaluate the IT strategic planning process, compliance with IT-related external regulations, the effectiveness of IT controls, IT security, and management and protection of IT assets (Héroux and Fortin, 2013).

2.1.2. Internal audit characteristics

Research in the field of internal audits has examined the characteristics of Internal Audit IAFs. Ege (2015) finds that high internal audit quality, measured in factors such as IAF experience, licensing, training, and independence, reduces improper management. Similarly, Abbott et al. (2016) explore the relationship between internal audit quality and earnings quality, defining internal audit quality in terms of IAF independence and internal audit competence, based on the hourly cost of the internal audit. They report that high internal audit quality improves earnings.

Other studies such as Prawitt et al. (2009) look at the association between internal audit quality and earnings management, measuring internal audit quality based on factors like the licenses, training, and objectivity of internal auditors, the time spent auditing financial statements, and the size of the IAF (in terms of budget). They note that high internal audit quality influences earnings management behavior. Pizzini et al. (2015) find that high internal audit quality reduces audit delays. They measure internal audit quality in terms of competence, objectivity, and scale of the IAF. Competence attributes include experience, educational background, certification, and training. The scale of the IAF is the ratio of its operating costs to the company's total assets. Héroux and Fortin (2013) examine the relationship between IAF characteristics and the involvement of IAFs in IT governance by conducting a survey among IAF managers, chief financial officers, and others. They find that IAF characteristics such as IT resources, IT audit experience, IT personnel, IT training or certification, IAF senior executives' experience, auditing training, and interactions between the IAF and the board of directors significantly relate to the involvement of IAFs in IT governance.

Our study extends this line of research by considering additional factors, including IT knowledge, the role of internal auditing, and IT audit competencies, from an internal auditing perspective to gain a deeper understanding of this subject area. Merhout and Havelka (2008) suggest that measurements of IT audit quality should include assessments of the ability of internal auditors to audit IT and the characteristics of IAFs. Merhout and Havelka (2008) argue that the IT-related competencies of internal auditors might influence the procedures of IT audits. Given that the main task of internal auditors is to audit IT controls, these auditors must have sufficient IT knowledge to assess the effectiveness and adequacy of IT controls and to manage potential IT risks in accordance with corporate objectives (IIA, 2012; ITGI, 2013). Internal auditors with adequate IT auditing experience, knowledge, skills, and training can better

understand the operation of information systems and the weaknesses of internal controls and thus contribute more to the planning and implementation of IT audits than those without such knowledge. Wu et al. (2017) demonstrate that if internal auditors have sufficient IT knowledge, they can enhance IT audits and indirectly improve internal audit performance.

IAFs within businesses have two conflicting roles. They oversee and provide information that helps companies improve their operations (Stewart and Subramaniam, 2010). Thus, internal auditors should fulfill both assurance and consulting roles when performing an IT control audit (IIA, 2018). Havelka and Merhout (2013) recommend that IAFs should consider the corporate vision and mission, which might affect the procedures of a related IT audit. Steinbart et al. (2018) report that if internal auditors see themselves as consultants, their relationship with the auditee can significantly improve. In summary, modern internal auditors acknowledge that they must play both assurance and consulting roles to improve the audit process and their relationship with IT personnel.

The IT audit competencies of the IAF relate to the audit's scope and depth (Héroux and Fortin, 2013). Suppose the IT audit professionals in the IAF have enough experience and an IT background. In that case, they can facilitate communication between the IAF and the IT department, thereby enhancing coordination between the two as well as the implementation of IT audits (Havelka and Merhout, 2013). Our study explores the relationships between the characteristics of the IAF and the involvement of IAFs in IT governance. The IAF's characteristics include IT knowledge, recognition of the internal auditing role, and IT audit competencies. Therefore, we propose the following hypotheses.

H1: The IAF's IT knowledge is positively associated with the involvement of IAFs in IT governance.
H1a: The IAF's IT knowledge is positively associated with the IAF-IT relationship quality.
H1b: The IAF's IT knowledge is positively associated with IAF-IT governance processes.
H2: The internal auditing role is positively associated with the involvement of IAFs in IT governance.
H2a: The internal auditing role is positively associated with the IAF-IT relationship quality.
H2b: The internal auditing role is positively associated with IAF-IT governance processes.
H3: IT audit competencies are positively associated with the involvement of IAFs in IT governance.
H3a: IT audit competencies are positively associated with the IAF-IT relationship quality.
H3b: IT audit competencies are positively associated with IAF-IT governance processes.

2.2. Involvement of IAFs in IT governance and IT controls

2.2.1. The IAF-IT relationship and IT controls

The relationship between the Internal Audit Function (IAF) and the IT department is crucial for effective IT audits. Havelka and Merhout (2013) point out that strong interdepartmental connections aid auditors in obtaining necessary documents and improving communication, which is essential for an effective audit process. This is echoed by Steinbart et al. (2018), who argue that strong relationships between IAFs and information security departments enable better knowledge transfer and adoption of suggested improvements for security controls. From a business process perspective, IAFs can review information security effectively, thereby assisting information security managers in managing administrator permissions more efficiently (Steinbart et al., 2012). Thus, the connection between IAFs and audited departments contributes to better communication, more effective knowledge transfer, and improved internal controls.

In terms of managing IT control tasks, internal auditors must thoroughly understand the related strategies, risks, processes, and control points of IT. Moreover, developing a high-quality relationship with IT personnel based on mutual trust is necessary to obtain relevant information (Donathan, 2012). Wallace et al. (2011) emphasize that a close relationship with information security professionals may be needed to ensure that internal controls comply with legislative requirements such as the Sarbanes-Oxley Act. Furthermore, Steinbart et al. (2012) note that establishing a favorable relationship with information security personnel could assist auditors in identifying potential security risks. Steinbart et al. (2013) also recognize the significant positive impact of the relationship quality between internal auditors and information security personnel on information security. Considering these findings, the following hypothesis is proposed.

H4: The IAF-IT relationship quality is positively associated with IT controls activities.

2.2.2. IAF-IT governance processes and IT controls

IT governance processes are key in ensuring operational consistency and providing valuable feedback to decision-makers. These processes require the establishment of IT policies and standards that define, monitor, and update IT strategies as well as implement IT process and budget controls. Independent validation of these activities is crucial (De Haes et al., 2013; De Haes & Van Grembergen, 2009). De Haes and Van Grembergen (2009) identify 33 related mechanisms classified as IT governance structures, processes, or relational mechanisms using the Delphi method with senior IT professionals. They view internal auditing of IT controls as part of IT governance assurance, an independent assurance activity associated with the governance and control of IT. For businesses, developing an IT strategy is essential for smooth operation. The IAFs should be part of the discussion on IT implementation to ensure alignment between business and IT strategies. Post-implementation, IAFs must fully understand IT activities and evaluate their risks and performance. This governance process integrates strategy, activity, risk, control, and audit procedures to ensure the alignment of IT operations with enterprise policies.

Coderre (2005) advocates for continuous control assessment, involving the analysis of transactions with predesigned control tests to verify the effectiveness of internal control. This approach allows the Chief Audit Executive (CAE) to alert management to control

violations at an early stage for prompt correction. It involves three main steps: identifying control objectives, identifying key controls, and defining appropriate control test analytics. Identifying control objectives enables IAFs to assist each department in determining primary activities, sub-processes, and related control targets. Defining appropriate control test analytics involves determining an appropriate evaluation method for each control objective and critical control point (Coderre, 2005).

The role of the IAF in IT governance goes beyond continuous control assessment, including risk assessment and aligning IT and business strategies. An internal audit manager may participate in interdepartmental meetings to discuss IT strategy, uncertainties, and potential risks. This proactive involvement in IT audit planning can encompass risk assessment techniques, evaluate IT activities and relevant controls, and determine the completeness of the information regarding implemented IT controls (Héroux & Fortin, 2013). Hermanson et al. (2000) explore the impact of internal audit objectives and characteristics on IT assessments, finding a significant correlation between evaluating IT controls and IT assessments. The literature suggests that IAF-IT governance processes positively impact improved IT control activities. Hence, the following hypothesis is proposed.

H5: IAF-IT governance processes are positively associated with IT control activities.

3. Research methodology

This section delineates the structure of the research model, outlines the research methodology, and presents an analysis of the reliability and validity measures. Further, it expounds on the content included in the utilized questionnaire.

3.1. Research model

The proposed research model examines the relationships of IAF characteristics with the IAF-IT relationship quality and IAF-IT governance processes, as well as the relationship between the IAF-IT relationship quality and IAF-IT governance processes with IT controls. We use general controls to measure IT controls. General controls are closer to the computer environment, including organizational and operational controls, system development and file control, hardware and system software control, access control, and data and process control (Boritz et al., 2013; Hall, 2015). IAF characteristics comprise IT knowledge, internal audit roles, and IT competencies (Havelka and Merhout, 2013; Steinbart et al., 2013). Fig. 1 displays the proposed research model.

3.2. Dimension measurement

The constructs of this study are measured utilizing the dimensions delineated in the subsequent sections. Unless specified otherwise, all items utilize a 7-point Likert scale, with 1 representing “strongly disagree” and 7 representing “strongly agree”. Table 1 summarizes the conceptualization and operationalization of the five research constructs. The items of the questionnaire appear in Appendix A.

3.2.1. IT knowledge

IT knowledge reflects the extent of IT-related professional knowledge the IAFs possess, which encompasses an understanding of information security management, information systems, databases, and risk management (Steinbart et al., 2013). Respondents were asked to self-evaluate the scope of the IAF’s IT knowledge concerning the four factors above (i.e., the extent to which the internal audit

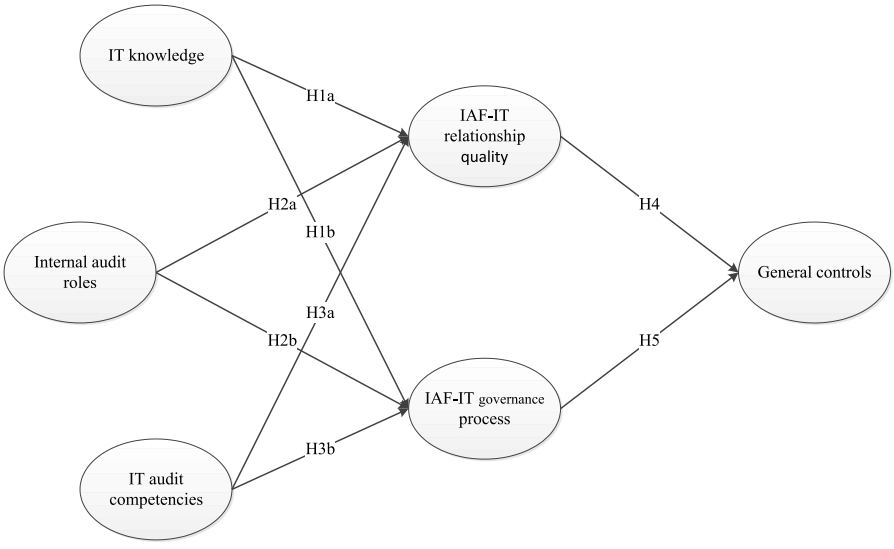


Fig. 1. Research model.

Table 1
Conceptualization and operationalization of the research constructs.

Construct	Conceptualization	Operationalization	Source
IT knowledge	The extent of IT-related professional knowledge within the IAF	The level of four types of IT knowledge is evaluated using a seven-point Likert scale.	Steinbart et al. (2013)
Internal audit roles	The roles recognized by IAF managers or employees	The roles recognized by IAF employees are evaluated using a seven-point Likert scale.	Steinbart et al. (2013)
IT audit competencies	The IT audit capabilities exhibited by the IAF	IT audit competencies are measured through four items: the number of IT audit personnel, the number of staff with a CISA certificate, the number of staff with an ISO27001 lead auditor certificate, and the number of staff with a degree in computer science.	Héroux & Fortin (2013), Nicoletti (2013), Abdolmohammadi, & Boss (2010)
IAF-IT relationship quality	The quality of the relationship between the IAF and the IT department	The relationship quality across three different contexts is evaluated using a seven-point Likert scale.	Steinbart et al. (2013)
IAF-IT governance process	The IT governance process as it relates to the IAF	The level of six items pertaining to the IT governance process is evaluated using a seven-point Likert scale.	Héroux & Fortin (2013)
General controls	General control activities associated with the information system	The level of six items related to general control activities is evaluated using a seven-point Likert scale.	Huang et al. (2011), ITGI (2007)

department is knowledgeable about information security).

3.2.2. Internal audit roles

Internal audit roles are the responsibilities acknowledged by IAF managers or employees. The measurement of the IAF's roles incorporates three items: the internal audit department's role is to identify and report deficiencies, enforce policies, and facilitate interdepartmental consultation for efficiency and effectiveness (Steinbart et al., 2013).

3.2.3. IT audit competencies

IT audit competencies refer to the IT audit capabilities of the IAFs. We measure IT audit competencies using four different items: the number of full-time IT audit employees (Héroux and Fortin, 2013), the number of IAF employees with Certified Information Systems Auditors (CISA) certificates (Héroux & Fortin, 2013), the presence of IAF employees with ISO27001 Lead Auditor certifications (Nicoletti, 2013), and the number of employees with a degree in information science or computer science. The rationale for selecting the fourth criterion is derived from the findings of Abdolmohammadi and Boss (2010), who discover that having a Chief Audit Executive (CAE) with a major in information systems or computer science positively correlates with the proportion of IAF time devoted to IT audits. Given their comprehensive understanding of IT operations, IAF employees with degrees in information systems or computer science may benefit from IT audit competency.

3.2.4. IAF-IT relationship quality

Steinbart et al. (2013) demonstrate that information security professionals' perception of the relationship quality between IAFs and information security is significantly positive. Specifically, the relationship quality between the IAF and IT professionals pertains to the efficacy of the collaboration between the internal audit and information security departments. Consequently, IT auditors are tasked with establishing meaningful relationships with IT personnel in the current study, and so we adopt items to measure the IAF-IT relationship quality, as proposed by Steinbart et al. (2013). To tailor these items to our context, we replace "information security" with "IT personnel" in the statements used to gauge the aforementioned relationship quality. These items are as follows: (1) "In my organization, there is little friction between internal audit and information technology." (2) "In my organization, the relationship between internal audit and the information technology staff is close and personal." (3) "In my organization, internal audit and information technology have a good working relationship.".

3.2.5. IAF-IT governance process

We employ the items developed by Héroux and Fortin (2013) to assess the IAF-IT governance process. (1) "A senior executive from the internal audit department attends meetings that address risk and strategy across the organization, including those related to IT." (2) "The executive (or senior management) provides input for IT internal audit planning." (3) "Risk assessment is conducted for planning overall IT internal audits." (4) "The internal audit department evaluates the IT strategic planning process." (5) "The internal audit department is responsible for assessing all relevant IT activities and IT controls." (6) "The internal audit department is responsible for assessing data integrity related to IT internal controls.".

3.2.6. General controls

General controls encompass elements such as enabling IT operations and usage, installing and accreditation of solutions and changes, managing changes, assurance of system security, data management, and end-user computing (Huang et al., 2011, ITGI, 2007). For instance, the item about enabling IT operations and usage is phrased as follows: "This process requires the production of documentation and manuals for users and IT and provides training to ensure the appropriate use and operation of applications and infrastructure.".

3.3. Respondents and PLS analysis

The Taiwan government mandates that publicly listed companies institute internal control systems for their information technologies and establish Internal Audit Functions (IAFs) to conduct audits across various company operations, including IT internal control. This study selects internal auditors of publicly listed companies in Taiwan as the target demographic for research to delve into the impact of IAF involvement in IT governance on IT controls. Paper-based questionnaires as well as self-addressed and stamped return envelopes were disseminated to selected companies in Taiwan. The collection of these questionnaires spanned from March to September 2015.

Data analysis was conducted using Smart PLS 2.0 software and employing Partial Least Squares (PLS) to probe the causal relationships between the variables within the proposed models (Ringle et al., 2005). Structural equation modeling and the PLS method are commonly applied tools for exploring causality. A key advantage of PLS lies in its ability to mitigate multicollinearity issues in scenarios characterized by smaller sample sizes or data that must adhere to normal distributions (Westlund et al., 2008). Consequently,

the PLS method was chosen as this study's primary statistical analysis tool.[1]

4. Empirical results

4.1. Demographics

Of the 1556 distributed surveys, we received 450 in return. After screening, we determined 414 of these to be complete and useful for analysis, while the remaining 36 were deemed invalid due to incomplete information. Thus, the valid response rate is 21.47 %. As per Table 2, 60.1 % of the participating respondents identified as female, 62.1 % held bachelor's degrees, and 29 % held master's degrees. A significant portion of respondents covered 36–50-year-old people (61.3 %), with 51.7 % holding positions as internal audit managers. When examining company size, a plurality of respondents (33.1 %) was employed in companies with a workforce ranging from 100 to 300, while 21 % worked in organizations with over 1000 employees.

We employed the chi-square test to assess the potential for non-response bias in the study (Hikmet and Chen, 2003). The analysis found no significant discrepancies between early ($n = 321$, collected from March to April) and late responses ($n = 93$, collected from May to September) across gender, age, job title, and company size. Further examination using the T-test on the average of items revealed only a single item with a significant difference (IAR 1, $p < 0.1$) between early and late responses (Table 3). Hence, non-response bias does not pose a significant issue in this study.

4.2. Research analyses and results

4.2.1. Reliability and validity testing

The content of this questionnaire underwent revisions based on feedback received during a pre-test conducted with a panel of three experts. Among these, two were university professors specializing in accounting information systems, while the third expert served as an audit manager for a publicly listed company in Taiwan. The questionnaire was refined semantically and grammatically to eliminate ambiguity, thus establishing an acceptable level of content validity.

We evaluate factor loadings, composite reliability, and the average variance extracted (AVE) to ascertain convergent validity. Table 4 showcases the factor analysis results, revealing that all dimension factor loadings exceed the threshold of 0.5 (Fornell and Larcker, 1981). As Table 5 shows, the composite reliability for the dimensions ranges between 0.815 and 0.924, which surpasses the recommended benchmark of 0.6 (Bagozzi and Yi, 1988). Cronbach's alpha for these dimensions falls between 0.747 and 0.902, exceeding the suggested cutoff of 0.7 (Fornell and Larcker, 1981). The AVE of the dimensions ranges from 0.600 to 0.714, again surpassing the recommended cutoff of 0.5 (Fornell and Larcker, 1981). Table 6 presents, for each dimension, that the square root of AVE exceeds all correlation coefficients (Fornell and Larcker, 1981). Furthermore, Table 4 shows that the factor loading for each construct surpasses all cross-loadings. These results affirm that the selected dimensions possess adequate reliability, convergent validity, and discriminant validity (Fornell and Larcker, 1981).

4.2.2. Hypothesis validation

As delineated in Fig. 2, hypotheses H1-H3 outline the relationships between the internal audit characteristics and the involvement of IAFs in IT governance. IT knowledge exhibits significantly positive associations with both the IAF-IT relationship quality ($\beta = 0.304$, $p < 0.001$) and the IAF-IT governance process ($\beta = 0.259$, $p < 0.001$), thereby supporting H1. The internal auditing role has significantly positive relationships with IAF-IT relationship quality ($\beta = 0.259$, $p < 0.001$) and the IAF-IT governance process ($\beta = 0.458$, $p < 0.001$), providing support for H2. IT audit competencies, however, do not exhibit a significant association with IAF-IT relationship quality, but demonstrate a significantly positive relationship with the IAF-IT governance process ($\beta = 0.109$, $p < 0.001$). As a result, H4b is supported, while H4a is not. The IAF-IT relationship quality shows significantly positive associations with general controls ($\beta = 0.153$, $p < 0.01$), thus supporting H5. The IAF-IT governance process also shows significantly positive relationships with general controls ($\beta = 0.450$, $p < 0.001$), supporting H6.

4.3. Further analysis

4.3.1. Self-serving bias

Our investigation centers around IAFs. Therefore, there is potential for self-serving bias where respondents might attribute key success factors to themselves. We can examine potential biases by studying individual thought processes and behaviors to address this issue. Implementing an experimental approach to assess respondents' interpretations of their success and failure could provide insights into a self-serving bias (Peterson et al., 2002). The literature has broached the subject of self-serving bias concerning age and gender (Mezulis et al., 2004; Sedikides et al., 1998). This study employs the T-test to analyze variance across questionnaire items differentiated by age and gender, aiming to look for potential self-serving bias. We do not include tables and figures related to this bias analysis

[1] The questionnaire adopted in this study was distributed in 2015. In Taiwan, the Chinese version of COBIT 5 was released in 2014. Consequently, the internal auditing managers of listed companies might be unfamiliar with the content of COBIT 5. COBIT 4.1 has been used for many years; thus, internal audit managers are more familiar with the COBIT4.1 standard than with COBIT 5. Compared to COBIT 5 items, COBIT 4.1 items are more feasible and accessible and provide deeper insights.

Table 2
Demographic information of the respondents ($n = 414$).

	All responses		Early responses (n = 321)		Late responses (n = 93)		Chi-squared test	
Items	Frequency	%	Frequency	%	Frequency	%	X^2	P value
Sex								
Male	165	39.9	131	40.8	34	36.6	0.544	0.461
Female	249	60.1	190	59.2	59	63.4		
Education								
High school	5	1.2	4	1.2	1	1.1	1.824	0.768
College	32	7.7	24	7.5	8	8.6		
University (bachelors)	257	62.1	195	60.7	62	66.7		
University (masters)	116	29.0	95	29.6	21	22.6		
University (doctorate)	4	1	3	0.9	1	1.1		
Age								
Below 25 years	1	0.2	1	0.3	0	0	3.5	0.623
26—–30 years	25	6.0	19	5.9	6	6.5		
31—–35 years	71	17.1	57	17.8	14	15.1		
36—–40 years	98	23.7	71	22.1	27	29		
41—–50 years	157	37.9	127	39.6	30	32.3		
over 50 years	62	15.0	46	14.3	16	17.2		
Position								
Staff	89	21.5	68	21.2	21	22.6	0.844	0.839
Senior auditor	50	12.1	38	11.8	12	12.9		
Manager	214	51.7	165	51.4	49	52.7		
Chief auditor	61	14.7	50	15.6	11	11.8		
Company size								
1–100	69	16.7	52	16.2	17	18.3	1.5	0.827
100–300	137	33.1	106	33.0	31	33.3		
300–500	51	12.3	39	12.1	12	12.9		
500–1000	70	16.9	58	18.1	12	12.9		
1000+	87	21.0	66	20.6	21	22.6		

Table 3
Factor loadings and non-response bias test for items.

Construct	Items	Mean	S.D.	Factor loading	Mean (Early responses) (n = 321)	Mean (Late responses) (n = 93)	Mean difference (Early-late)
IT knowledge (ITK)	ITK 1	4.809	0.9987	0.904	4.847	4.677	0.170
	ITK 2	4.585	1.0351	0.869	4.620	4.462	0.158
	ITK 3	5.005	1.0803	0.792	5.012	4.978	0.034
	ITK 4	5.130	0.9655	0.811	5.143	5.086	0.057
Internal audit roles (IAR)	IAR 1	5.210	1.0189	0.744	5.159	5.387	-0.228*
	IAR 2	5.099	1.0120	0.869	5.062	5.226	-0.164
	IAR 3	5.200	1.0535	0.818	5.218	5.140	0.078
IT audit competencies (ITAC)	ITAC1	0.483	0.8571	0.879	0.480	0.495	−0.015
	ITAC2	0.060	0.2931	0.591	0.059	0.065	−0.005
	ITAC3	0.075	0.4078	0.657	0.078	0.065	0.013
	ITAC4	0.244	0.5994	0.749	0.240	0.258	−0.018
IAF-IT relationship quality (IAFITRQ)	IAFITRQ 1	4.826	1.3507	0.564	4.819	4.849	−0.030
	IAFITRQ 2	5.036	1.0741	0.926	5.040	5.022	0.019
	IAFITRQ 3	5.205	1.0932	0.951	5.218	5.161	0.057
IAF-IT governance process (IAFITGP)	IAFITGP 1	4.855	1.0477	0.737	4.875	4.785	0.090
	IAFITGP 2	4.440	1.1871	0.792	4.467	4.344	0.123
	IAFITGP 3	4.626	1.1188	0.811	4.654	4.527	0.127
	IAFITGP 4	4.995	1.0758	0.742	5.006	4.957	0.049
	IAFITGP 5	5.014	1.0914	0.795	5.037	4.935	0.102
	IAFITGP 6	4.713	1.0879	0.770	4.726	4.667	0.059
General controls (GC)	GC1	5.085	1.1264	0.771	5.125	4.946	0.178
	GC2	4.829	1.0284	0.813	4.838	4.796	0.042
	GC3	4.865	1.0536	0.854	4.879	4.817	0.061
	GC4	5.019	1.0343	0.832	5.059	4.882	0.177
	GC5	5.266	0.9997	0.795	5.262	5.280	−0.018
	GC6	5.179	1.0021	0.847	5.190	5.140	0.050

ITK = information technology knowledge, IAR = internal audit role, ITAC = IT audit competencies, IAFITRQ = IAF-IT relationship quality, IAFITGP = IAF-IT governance processes, GC = general controls. Note: * = significant at $p < 0.1$, ** = significant at $p < 0.05$, and *** = significant at $p < 0.01$.

Table 4
Results of factor analysis.

	TK	IAR	ITAC	IAFITRQ	IAFITGP	GC
ITK 1	**0.904**	0.317	0.225	0.340	0.478	0.331
ITK 2	**0.869**	0.298	0.222	0.335	0.456	0.342
ITK 4	**0.811**	0.417	0.190	0.359	0.445	0.406
ITK 3	**0.792**	0.323	0.098	0.309	0.371	0.392
IAR 2	0.308	**0.869**	0.015	0.292	0.449	0.386
IAR 3	0.369	**0.818**	0.028	0.325	0.600	0.422
IAR 1	0.284	**0.744**	0.067	0.302	0.328	0.379
ITAC 1	0.203	0.053	**0.879**	0.044	0.211	0.174
ITAC 4	0.185	0.026	**0.749**	0.047	0.123	0.083
ITAC 3	0.065	−0.009	**0.657**	0.002	0.040	0.054
ITAC 2	0.067	−0.041	**0.591**	−0.040	0.030	0.036
IAFITRQ 3	0.437	0.366	0.059	**0.951**	0.400	0.322
IAFITRQ 2	0.367	0.364	0.059	**0.926**	0.367	0.297
IAFITRQ 1	0.090	0.171	−0.044	**0.564**	0.072	0.149
IAFITGP 3	0.439	0.445	0.154	0.267	**0.811**	0.378
IAFITGP 5	0.430	0.526	0.185	0.315	**0.795**	0.408
IAFITGP 2	0.401	0.401	0.167	0.289	**0.792**	0.376
IAFITGP 6	0.415	0.456	0.190	0.307	**0.770**	0.438
IAFITGP 4	0.354	0.392	0.064	0.302	**0.742**	0.393
IAFITGP 1	0.376	0.497	0.145	0.264	**0.737**	0.362
GC3	0.345	0.323	0.146	0.211	0.448	**0.854**
GC6	0.372	0.442	0.123	0.270	0.430	**0.847**
GC4	0.395	0.393	0.132	0.265	0.442	**0.832**
GC2	0.300	0.373	0.139	0.242	0.395	**0.813**
GC5	0.375	0.465	0.116	0.346	0.413	**0.795**
GC1	0.334	0.409	0.121	0.247	0.363	**0.771**

ITK = information technology knowledge, IAR = internal audit role, ITAC = IT audit competencies, IAFITRQ = IAF-IT relationship quality, IAFITGP = IAF- IT governance processes, GC = general controls.

Table 5
Reliability and validity of the selected dimensions.

	AVE	Composite Reliability	Cronbach's Alpha
ITK	0.714	0.909	0.866
IAR	0.659	0.853	0.747
ITAC	0.529	0.815	0.780
IAFITRQ	0.693	0.866	0.770
IAFITGP	0.600	0.900	0.867
GC	0.671	0.924	0.902

ITK = information technology knowledge, IAR = internal audit role, ITAC = IT audit competencies, IAFITRQ = IAF-IT relationship quality, IAFITGP = IAF-IT governance process, GC = general controls.

Table 6
Square root of AVEs and correlation coefficients.

	SRAVE	ITK	IAR	ITAC	IAFITRQ	IAFITGP	ITC
ITK	0.845	1					
IAR	0.812	0.401	1				
ITAC	0.727	0.221	0.042	1			
IAFITRQ	0.833	0.398	0.379	0.046	1		
IAFITGP	0.775	0.520	0.588	0.196	0.376	1	
ITC	0.819	0.433	0.489	0.158	0.323	0.508	1

SRAVE = square root of the average variance extracted, ITK = information technology knowledge, IAR = internal audit role, ITAC = IT audit competencies, IAFITRQ = IAF-IT relationship quality, IAFITGP = IAF-IT governance processes, GC = general controls.

in the manuscript, because of page constraints.

Mezulis et al. (2004) note that self-serving bias exhibits significant variance among those aged over 55 and 8 to 11. To compare these groups, we conduct a T-test for respondents over 50 and those under 50. Our findings indicate that the mean score of the 17 questionnaire items from respondents over 50 is significantly higher than those from respondents under 50. This outcome aligns with previous research, demonstrating a notable variance of the self-serving bias in respondents over 50.

To perform PLS analysis, we divide the sample into two groups: respondents over 50 and those under 50. The results for the group under 50 are congruent with the primary findings. However, the outcomes for the group over 50 vary from the main results.

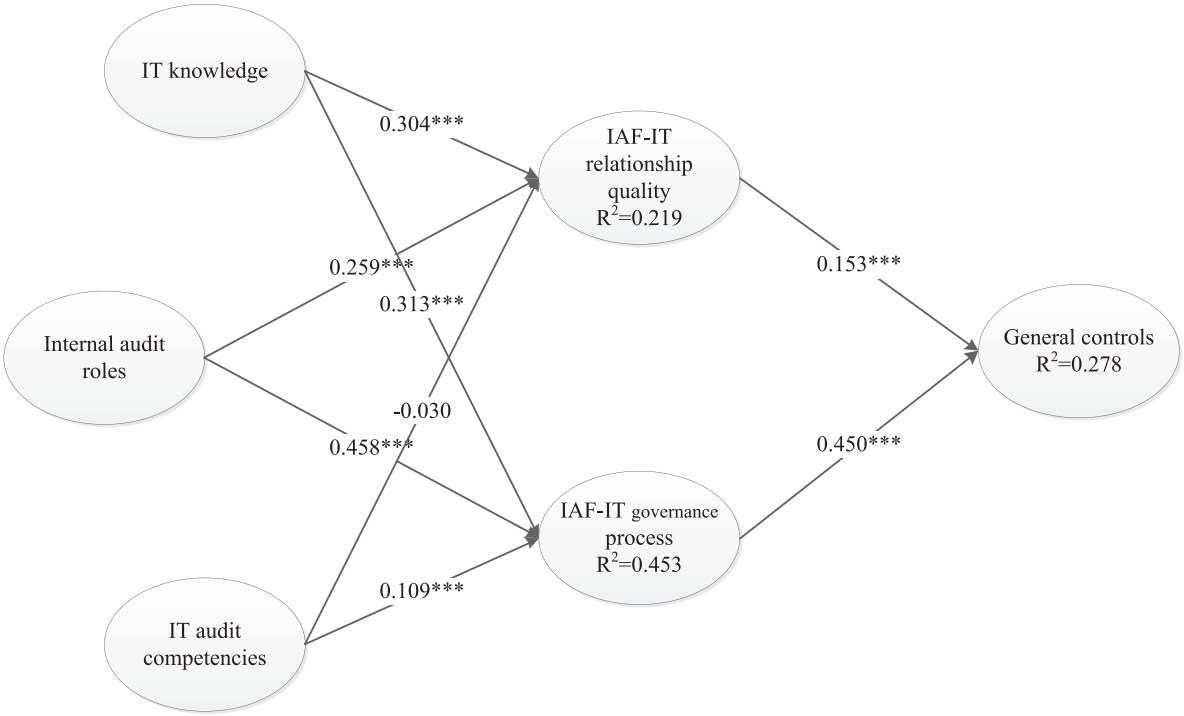


Fig. 2. Results of PLS analysis. Note: * = significant at $p < 0.05$, ** = significant at $p < 0.01$, and *** = significant at $p < 0.001$.

Specifically, IT knowledge does not exhibit a significantly positive relationship with IAF-IT relationship quality (β = 0.161). Similarly, IT audit competencies do not significantly correlate with the IAF-IT governance process (β = 0.056). Moreover, the IAF-IT governance process does not show a significantly positive relationship with general controls (β = -0.047). These PLS analysis outcomes suggest that while our primary results include respondents over 50, the self-serving bias observed in this older sample does not significantly influence the overall findings of our study.

Sedikides et al. (1998) also postulate that self-serving bias is more prevalent among males than females. The T-test conducted for our study shows that only the averages of 6 out of the total questionnaire items are significantly higher for male respondents than for females. This finding suggests that, contrary to their assertion, no substantial self-serving bias issues appear between genders in our study.

4.3.2. Common method bias

Given the simultaneous collection of our data on dependent and independent variables, common method bias possibly permeates our dataset (Podsakoff et al., 2012). As no ideal approach exists for gauging common method bias (Podsakoff et al., 2012; Richardson, Simmering, & Sturman, 2009), this study utilizes three distinct methods for such an assessment: Harman's single factor test, the unmeasured latent method construct (ULMC), and the confirmatory factor analysis (CFA) marker technique.

First, we implement Harman's single-factor test. In this method if the exploratory factor analysis (EFA) of all variables in the study yields an eigenvalue suggesting that the initial factor explains more than 50 % of the variance among variables, it signifies the presence of common method bias. All variables are inputted into an exploratory factor analysis deploying an unrotated principal component factor analysis, and we force the outcome to extract a single factor. The resultant aggregated factors explain less than 50 % of the

Table 7
ULMC: Chi-Square, Goodness-of-Fit Values, and Model Comparison Test.

Model	χ2	df	CFI
1. trait-only	1101.014	284	0.862
2. method-only	3268.107	299	0.498
3. trait/method	663.62	258	0.931
4. trait/method-R	683.424	273	0.931
Chi-Square Model Comparison Test			
△Models	Δχ2	Δdf	Chi-Square Critical Value; 0.05
1. trait-only vs. method-only	2167.093***	15	25
2. trait-only vs. trait/method	437.394***	26	38.89
3. trait/method vs. trait/method-R	19.804	15	25

variance, or more specifically 30 %. This preliminary analysis indicates no significant common method bias, which is in accordance with the criteria set forth by Podsakoff et al. (2003).

Second, we conduct ULMC analysis using confirmatory factor analysis (CFA) models for all questionnaire items. The procedure follows the steps outlined by Richardson et al. (2009), where we fit four different models. These models include trait-only, method-only, trait/method, and trait/method-R models. As delineated in Table 7, the method-only model is significantly inferior compared to the trait-only model ($\Delta\chi2(15) = 2167.093$, $p < 0.001$). This implies that "observed variance in the independent and dependent constructs is not because of method alone" (Richardson et al., 2009, p. 780). Conversely, the trait/method model exhibits significant improvement over the trait-only model (M1, $\Delta\chi2(26) = 437.394$, $p < 0.001$), suggesting the presence of congeneric common method bias. However, the trait/method-R model fit is not significantly worse than the trait/method model ($\Delta\chi2(15) = 19.804$, $p = 0.180$). This implies that although common method bias is present, it does not significantly bias the correlations between factors.

In addition to the preceding measures, we perform a CFA marker technique that tends to yield more reliable results when an optimal marker variable is utilized (Richardson et al., 2009; Williams, Hartman, & Cavazotte, 2010). For our study, we opt for 'compatibility' as the marker variable. We conjecture that this marker does not have a direct relationship with most of our hypothesis variables and exhibits minimal correlations with other indicators, ranging from 0.125 to 0.399 (refer to Table 8). The marker could indicate respondents' receptiveness toward the compatibility of Computer Assisted Audit Tools and Techniques (CAATTs) (Premkumar & Potter, 1995). This measure could be used to estimate the compatibility of CAATTs with hardware/software as well as the compatibility of the methodology used for CAATTs when respondents answered our queries. Following the procedure and terminology recommended by Williams et al. (2010), we fit five CFA models: initial, baseline, Method-C, Method-U, and Method-R. Table 9 presents the model fit analysis results, including the chi-square, degrees of freedom, and Comparative Fit Index (CFI) values.

Phase I: Model Comparisons. The fit of each model is presented in Table 9, which includes the chi-square, degrees of freedom, and CFI values. We note that the CFI values are somewhat lower than the commonly suggested values of 0.90 or 0.95. This may be partly due to the relatively large number of indicators (26) for the substantive variables and the consequent number of constrained parameters in the factor loading matrix. We compare the Baseline Model and Method-C Model to test the null hypothesis that the method factor loadings (assumed to be equal) associated with the marker variable do not relate to each of the 26 substantive indicators. The chi-square difference test between these two models supports rejecting the restriction to 0 of the 26 method factor loadings in the Baseline Model ($\Delta\chi2(1) = 5.153$, $p = 0.023$).

We next juxtapose the Method-U and Method-C Models to ascertain if the effect of the method marker variable remains consistent for all 26 items loading on the substantive indicators. This comparison aims to test the null hypothesis postulating the equality of the method factor loadings. The chi-square difference test supports rejecting the constraints inherent in the Method-C Model ($\Delta\chi2(25) = 115.733$, $p < 0.001$). This infers that the Method-U Model is the most suitable one to account for the marker variance on substantive indicators.

The comparison between the Method-U and Method-R Models offers a statistical examination to discern whether the variable marker method effects significantly influence the three correlations. The chi-square difference test reveals no significant difference ($\Delta\chi2(15) = 0.003$, $p = 1.000$). Prior assessments suggest that marker variable effects are significant and constitute substantial effects within the Method-U model. However, the comparison between the Method-U and Method-R Models demonstrates that the influences of the marker variable do not substantially bias the estimations of factor correlations. This outcome aligns with the conclusions drawn from Harman's single-factor test and the ULMC technique.

5. Conclusion and suggestions

5.1. Analyses and discussion

The potential for significant financial losses due to inadequate IT controls necessitates substantial attention to IT controls by businesses (Association of Certified Fraud Examiners, 2016; Stoel & Muhanna, 2011). The findings of this research illustrate a positive correlation between the involvement of Internal Audit Functions (IAFs) in IT governance and improvements in IT controls, thus offering contributions to scholarly discourse on IT governance. Our study broadens the conversation regarding the relationships among IAF quality, information security, and information security controls by integrating the dimension of IAF-IT relationship quality (Steinbart et al., 2013, 2018). Additionally, the results augment the research landscape on the interplay between IAF characteristics, their involvement in IT governance, and IT controls (Merhout and Havelka, 2008).

The IAF-IT relationship quality is significantly influenced by IT knowledge and internal audit roles. This aligns with the findings of Steinbart et al. (2013), who assert that a comprehensive understanding of information security can bolster the relationship quality between IAFs and information security. However, Steinbart et al. (2013) find no significant impact of the internal audit role on the relationship quality between IAFs and information security, which is a discrepancy with our findings. Our study further illustrates that

Table 8
Correlation coefficients for compatibility.

	GC	IAFITGP	IAFITRQ	IAR	ITAC	ITK
Compatibility	0.27	0.236	0.261	0.147	0.125	0.399

ITK = information technology knowledge, IAR = internal audit role, ITAC = IT audit competencies, IAFITRQ = IAF-IT relationship quality, IAFITGP = IAF-IT governance processes, GC = general controls.

Table 9
Marker Variable: Chi-Square and Model Comparison Test.

Model	$\chi 2$	df	CFI
1. CFA	1246.88	356	0.862
2. Baseline	2434.001	367	0.713
3. Method-C	2428.848	366	0.714
4. Method-U	2313.115	341	0.726
5. Method-R	2313.119	356	0.729
Chi-Square Model Comparison Test			
△Models	$\Delta\chi 2$	Δdf	Chi-Square Critical Value; 0.05
1. Baseline vs. Method-C	5.153*	1	3.84
2. Method-U vs. Method-C	115.733***	25	37.65
3. Method-U vs. Method-R	0.003	15	25

IT knowledge, internal audit roles, and IT audit competencies significantly affect the IAF-IT governance process. This finding is in accordance with Merhout and Havelka (2008), who establish that the involvement of IAFs in IT governance is significantly associated with IT personnel and IT training or certification.

Our study also indicates that the IAF-IT relationship quality significantly influences general controls, which aligns with Steinbart et al.'s (2013) findings. They present that the strength of the relationship between IAFs and information security directly impacts information security. Additionally, we observe that superior IAF-IT relationship quality can enhance knowledge transfer between the two departments. A robust working relationship can assist IAFs in comprehending the IT department's strategy, process, operations, and internal control when conducting an IT audit. As a result, the IT department is more likely to welcome suggestions of the IAF, leading to a more comprehensive implementation of IT controls.

Our findings demonstrate that an enhanced IAF-IT governance process can improve general controls. This confirms the utility of IT governance audits carried out by IAFs, which evaluate the interplay of IT strategy, processes, risks, and control mechanisms. With an in-depth understanding of the IT risks that stem from a given IT strategy and its related processes, IAFs can suggest suitable IT controls. This insight ensures that risk is managed effectively and that organizational IT goals align with the overall business strategy, further validating the importance of IAF involvement in IT governance.

5.2. Managerial implications

5.2.1. Internal audit characteristics and the involvement of IAFs in IT governance

This study enhances the literature by illuminating the ways in which IT audit competencies can bolster the participation of IAFs in IT governance. The prevalent use of COBIT for IT governance implementation in most organizations tends to focus on stakeholders such as board members, top-level management, and IT departments, often sidelining IAFs. However, it is crucial for IAFs to have a comprehensive understanding of the IT strategy, system processes, and associated risks. The lack of sufficient IT knowledge or IT audit competencies within the IAF may lead to potential risks. This research hence underlines the need for organizations to recognize the critical role of IAFs in IT governance implementation, ensuring their effective participation.

Our findings also reinforce those of previous studies by demonstrating that IT governance can be leveraged to enhance the implementation of IT controls. According to a survey by Information Systems Audit and Control Association & Protiviti (2016), most companies have fewer than six full-time internal auditors. Moreover, 44 % of Asian and 63 % of North American companies are reluctant to recruit additional audit staff. The same survey finds that IAFs generally lack the requisite knowledge for IT audits, leading them to rely on external resources for IT audit skills or task execution. Our research posits that IAF's IT knowledge and audit competencies can augment IT governance. Therefore, organizations should bolster the IT knowledge and audit competencies of IAFs by offering appropriate IT training. It may be beneficial to recruit new employees with advanced IT knowledge, IT audit certifications, capabilities, and associated skills. This can improve IT governance by leveraging employees' IT backgrounds, experiences, and expertise.

Internal auditors must recognize that their roles could be influenced by the company's decision-making style and processes. It is crucial that the board of directors and management comprehend not only the regulatory compliance needs of the IAFs, but also its critical role in enhancing operational efficiency through effective internal control assessments. These key personnel should aim to diversify the tasks assigned to the IAFs, fostering a continual expansion of internal auditors' understanding of their roles, scope of work, and job requirements. As such, future research could explore the potential relationship between the tasks assigned to the IAF by the board or management, and how it influences the auditors' perception of their role and the execution of IT governance. This line of inquiry could provide valuable insights into how to most effectively position the IAF within an organization's IT governance structure.

5.2.2. The involvement of IAFs in IT governance and IT controls

This study contributes to the literature by elucidating the association between the enhancement of IAFs' involvement in IT governance and improved IT controls. The survey conducted by Information Systems Audit and Control Association & Protiviti (2016) reveals in 68 % of all companies that the IT audit function has a significant or moderate correlation with technology-oriented projects. Additionally, around 65 % of the companies surveyed face some challenges post-implementation in their projects. In the past three years, 51 % of IT auditors completed post-implementation project reviews, and 48 % were involved in project evaluations. In most

companies, IT auditors are tasked with conducting general control audits. Given our findings that the IAF-IT relationship quality and the IAF-IT governance process can boost IT controls, organizations must prioritize the integration of IT auditors in the execution of IT governance. Currently, most companies tend to involve IT auditors in IT governance during the post-implementation stage of projects. However, to achieve optimal results, organizations should engage IT auditors during all project phases - planning, design, testing, and implementation. As such, internal auditors must possess a comprehensive understanding of the operations and processes of information systems, along with the requisite competency to audit these systems. In essence, internal auditors should be equipped to propose suitable control points, thereby enabling more effective IT controls. This approach not only broadens the scope of IT governance but also potentially enhances the success of technology-oriented projects within organizations.

The emphasis on IT governance is crucial for corporations to ensure the effective implementation of internal controls within operational systems, supporting robust corporate governance. This study provides evidence of the nexus between IAF-IT relationship quality and IT controls. Hence, senior management and boards of directors aiming to enhance their IT governance should seriously consider the quality of the IAF-IT relationship. Boosting the quality of this relationship can aid the IAF in gaining deeper insights into the operation of information systems. This is clearly a priority when dealing with systems that require customization. The complete recording of processes and associated data for such systems in a vendor's standard documentation is often an uphill task. By enhancing the IAF-IT relationship quality, businesses can foster better information exchange, facilitating more effective IT governance and leading to more reliable internal controls.

The most critical organizational vulnerability often lies in the absence of robust internal controls. This study establishes a significant correlation between the processes of IAF-IT governance and IT controls. IAFs should dedicate more effort to conducting audits of information systems. This effort can aid companies in identifying potential risks and weak points related to IT, thus enabling the development of practical solutions for circumventing and rectifying these threats or issues. For instance, IAFs can participate in cross-departmental meetings to discuss IT strategies and operational policies, risk assessments, IT audit planning, IT compliance, and the effectiveness of implemented IT controls. By doing so, IAFs can play a proactive role in enhancing IT governance and internal control mechanisms, ultimately fortifying the organization's resilience against potential IT risks.

5.3. Future research

This study investigates the influence of IT governance on IT internal controls by examining a sample of Taiwanese firms. Given Taiwan's status as an emerging market, the findings may have relevance across various geographical regions and countries. Nevertheless, the findings may not be entirely transferable to Western contexts, and further research could explore the dynamics in those regions. Despite geographical considerations, Information Systems Audit and Control Association & Protiviti (2016) find negligible variation in IT audit processes across different organizations, with 80 % of Asian companies and 86 % of North American companies performing IT audit risk assessments. Both regions prioritize IT general controls and process audits. However, according to the Association of Certified Fraud Examiners (Association of Certified Fraud Examiners, 2016) fraud and audit control survey, there is a marked difference in reliance on internal audits for fraud control – 94.7 % in Asia versus 61.4 % in the U.S. This disparity could be due to U.S. companies having the option to voluntarily implement internal audit mechanisms or outsource auditing to a third-party vendor. Taiwan regulations, on the other hand, require publicly listed companies to maintain IAFs with an adequate number of internal auditors adhering to standardized job specifications. Therefore, an analysis of the Taiwan context provides valuable insights that could be pertinent to firms in Europe and the U.S. For instance, the experience of Taiwanese companies in maintaining a certain number of in-house staff for efficient IT internal controls could provide meaningful lessons for other countries. In conclusion, enhancing the involvement of IAFs in IT governance can bolster the effectiveness of internal IT controls. Future research could delve deeper into the impact of various IT governance domains - such as IT strategic alignment, IT value delivery, IT risk management, IT resource management, and IT performance management - on IAF involvement and IT governance effectiveness. Such studies should contribute further to understanding the pivotal role of IAFs.

Data availability

Data will be made available on request.

Appendix A. Modified items recommended by a panel of experts

Dimension	Items
IT knowledge	1. The internal audit department is knowledgeable about information security.
	2. The internal audit department is knowledgeable about databases.
	3. The internal audit department is knowledgeable about information systems.
	4. The internal audit department is knowledgeable about risk management.
Internal audit role	1. The internal audit department's role is to identify and report deficiencies.
	2. The internal audit department's role is to enforce policies.
	3. The internal audit department's role is to consult with various departments for efficiency and effectiveness.
IAF-IT relationship quality	1. In my organization, there is little friction between internal audits and information technology.
	2. In my organization, the relationship between internal audits and information technology staff is close and personal.

(*continued on next page*)

(*continued*)

Dimension	Items
	3. In my organization, internal audits and information technology have a good working relationship.
IAF-IT governance process	1. The senior executive or officer of the internal audit department attends meetings that address risk and strategy across the organization, including those related to IT.
	2. The executive (or senior management) provides input for IT internal audit planning.
	3. Risk assessment is conducted for planning overall IT internal audits.
	4. The internal audit department evaluates the IT strategic planning process.
	5. The internal audit department is responsible for assessing all relevant IT activities and IT controls.
	6. The audit department is responsible for assessing data integrity related to IT controls.
IT controls	1. Specific, measurable, actionable, realistic, results-oriented, and timely (SMART) process goals and objectives are defined and communicated to execute each IT process effectively. These goals are linked to the business goals and are supported by suitable metrics.
	2. An owner with clearly defined roles and responsibilities is assigned for each IT process. For example, these processes may include responsibility for process design, interaction with other processes, accountability for the results, measurement of process performance, and identifying improvement opportunities.
	3. Each key IT process is designed and established such that it is repeatable. A logical but flexible and scalable sequence of activities that leads to the desired results and is sufficiently flexible for handling exceptions and emergencies is provided. Consistent processes are used whenever possible, and processes are tailored only when unavoidable.
	4. The key activities and end-deliverables of processes are defined. Unambiguous roles and responsibilities for the effective and efficient execution of these key activities are assigned, communicated, and documented to ensure accountability for the process end-deliverables.
	5. Methods of documenting, reviewing, maintaining, approving, storing, communicating, and training with all policies, plans, and procedures that drive an IT process are defined and communicated. Responsibilities for each of these activities are assigned and reviewed appropriately. These policies, plans, and procedures are accessible, correct, understood, and up to date.
	6. A set of metrics that provide insight into the outcomes and performance of the process is identified. Targets that reflect the process goals and performance indicators and enable the achievement of process goals are established. Methods of obtaining data are defined. Actual measurements are compared with targets, and action is taken in response to deviations, if necessary. Metrics, targets, and methods are aligned with the overall performance monitoring approach for IT.
Compatibility(Marker variable)	1. Computer-assisted audit tools and techniques (CAATTs) would be compatible with our existing software platform
	2. Computer-assisted audit tools and techniques (CAATTs) would be compatible with our existing hardware platform
	3. Computer-assisted audit tools and techniques (CAATTs) would be compatible with our existing applications development methodology

References

Abbott, L.J., Daugherty, B., Parker, S., Peters, G.F., 2016. Internal audit quality and financial reporting quality: The joint importance of independence and competence. J. Account. Res. 54 (1), 3–40.

Abdolmohammadi, M.J., Boss, S.R., 2010. Factors associated with IT audits by the internal audit function. Int. J. Account. Inf. Syst. 11 (3), 140–151.

Abubaker, F., El-Badri, H.A., 2022. Using Digital Storytelling as a Tool for Reflection in the Libyan EFL Literature Classroom. In English as a Foreign Language in a New-Found Post-Pandemic World. IGI Global, pp. 182–205.

Ali, S., Green, P., 2012. Effective information technology (IT) governance mechanisms: An IT outsourcing perspective. Inf. Syst. Front. 14 (2), 179–193.

Allataifeh, H.A., Moghavvemi, S., 2022. Digitally-Enabled Innovation Processes: The Emergence of a New Management Logic. In Emerging Technologies for Innovation Management in the Software Industry. IGI Global, pp. 44–59.

Association of Certified Fraud Examiners (2016). Report to the Nation: Occupational Fraud and Abuse. Retrieved from https://www.acfe.com/-/media/files/acfe/pdfs/2016-report-to-the-nations.ashx.

Bagozzi, R.P., Yi, Y., 1988. On the evaluation of structural equation models. J. Acad. Mark. Sci. 16 (1), 74–94.

Boritz, J.E., Hayes, L., Lim, J.H., 2013. A content analysis of auditors' reports on IT internal control weaknesses: The comparative advantages of an automated approach to control weakness identification. Int. J. Account. Inf. Syst. 14 (2), 138–163.

De Haes, S., Caluwe, L., Huygh, T., & Joshi, A. (2020). Governance Objectives to Lead Digital Transformation. In *Governing Digital Transformation* (pp. 47-61). Springer, Cham.

Bradley, R.V., Byrd, T.A., Pridmore, J.L., Thrasher, E., Pratt, R.M., Mbarika, V.W., 2012. An empirical examination of antecedents and consequences of IT governance in US hospitals. J. Inf. Technol. 27, 156–177.

Coderre, D., 2005. Continuous Auditing: Implications for Assurance, Monitoring and Risk Assessment. GTAG# 3-Global. In: Technology Audit Guide. The Institute of Internal Auditors, NJ.

De Haes, S., Van Grembergen, W., 2009. An exploratory study into IT governance implementations and its impact on business/IT alignment. Inf. Syst. Manag. 26 (2), 123–137.

De Haes, S., Van Grembergen, W., Debreceny, R.S., 2013. COBIT 5 and enterprise governance of information technology: building blocks and research opportunities. J. Inf. Syst. 27 (1), 307–324.

DeLone, W., Migliorati, D., Vaia, G., 2018. Digital IT governance. In: CIOs and the Digital Transformation. Springer, Cham, pp. 205–230.

Donathan, C., 2012. So, you want to be an IT auditor: practitioners need a combination of technical and people skills to forge a career in auditing Technology. Intern. Audit. 69 (5), 25–27.

Ege, M.S., 2015. Does internal audit function quality deter management misconduct? Account. Rev. 90 (2), 495–527.

Fornell, C., Larcker, D.F., 1981. Structural equation models with unobservable variables and measurement error: Algebra and statistics. J. Mark. Res. 382–388.

Haislip, J.Z., Masli, A., Richardson, V.J., Sanchez, J.M., 2016. Repairing organizational legitimacy following information technology (IT) material weaknesses: Executive turnover, IT expertise, and IT system upgrades. J. Inf. Syst. 30 (1), 41–70.

Hall, J.A., 2015. Information Technology Auditing. Cengage Learning.

Havelka, D., Merhout, J.W., 2013. Internal information technology audit process quality: Theory development using structured group processes. Int. J. Account. Inf. Syst. 14 (3), 165–192.

Hermanson, D.R., Hill, M.C., Ivancevich, D.M., 2000. Information technology-related activities of internal auditors. J. Inf. Syst. 14 (s-1), 39–53.

Héroux, S., Fortin, A., 2013. The internal audit function in information technology governance: A holistic perspective. J. Inf. Syst. 27 (1), 189–217.

Hikmet, N., Chen, S.K., 2003. An investigation into low mail survey response rates of information technology users in health care organizations. Int. J. Med. Inf. 72 (1–3), 29–34.
Huang, S.M., Hung, W.H., Yen, D.C., Chang, I.C., Jiang, D., 2011. Building the evaluation model of the IT general control for CPAs under enterprise risk management. Decis. Support Syst. 50 (4), 692–701.
Information Systems Audit and Control Association & Protiviti (2016). A Global Look at IT Audit Best Practices: Assessing the International Leaders in an ISACA/ Protiviti Survey. Retrieved from https://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/a-global-look-at-it-audit-best-practices.aspx.
Institute of Internal Auditors (IIA), 2012. International Standards for the Professional Practice of Internal Auditing. The Institute of Internal Auditors, Altamonte Springs, FL.
Institute of Internal Auditors (IIA), 2018. Global Technology Audit Guide (GTAG): Auditing IT Governance. The Institute of Internal Auditors, Lake Mary, FL.
IT Governance Institute (ITGI), 2007. COBIT 4.1: Framework, Control Objectives. Management Guidelines, Maturity Models. IT Governance Institute, Rolling Meadows, IL.
IT Governance Institute (ITGI), 2013. COBIT 5 for Assurance. IT Governance Institute, Rolling Meadows, IL.
KPMG (2021a) Trends in material weaknesses Retrieved from https://assets.kpmg/content/dam/kpmg/bm/pdf/2022/02/materials-weakness-non-ipo.pdf.
KPMG (2021b). Agile, resilient & transformative Retrieved from https://assets.kpmg/content/dam/kpmg/xx/pdf/2021/08/agile-resilient-and-transformative-report.pdf.
Li, C., Peters, G.F., Richardson, V.J., Watson, M.W., 2012. The consequences of information technology control weaknesses on management information systems: The case of Sarbanes-Oxley internal control reports. MIS Q 179–203.
Lunardi, G.L., Maçada, A.C.G., Becker, J.L., Van Grembergen, W., 2016. Antecedents of IT governance effectiveness: an empirical examination in Brazilian firms. J. Inf. Syst. 31 (1), 41–57.
Merhout, J.W., Havelka, D., 2008. Information technology auditing: A value-added ITG partnership between IT management and audit. C*Ommun. Assoc. Inf. Syst.* 23 (1), 26.
Mezulis, A.H., Abramson, L.Y., Hyde, J.S., Hankin, B.L., 2004. Is there a universal positivity bias in attributions? A meta-analytic review of individual, developmental, and cultural differences in the self-serving attributional bias. Psychol. Bull. 130 (5), 711–747.
Mulyana, R., Rusu, L., & Perjons, E. (2021). IT Governance Mechanisms Influence on Digital Transformation: A Systematic Literature Review. In *Twenty-Seventh Americas' Conference on Information Systems (AMCIS), Digital Innovation and Entrepreneurship, Virtual Conference, August 9-13, 2021.* (pp. 1-10).
Nfuka, E.N., Rusu, L., 2011. The effect of critical success factors on ITG performance. Ind. Manag. Data Syst. 111 (9), 1418–1448.
Nicoletti, B., 2013. Governance of Cloud Computing. In Cloud Computing in Financial Services. Palgrave Macmillan, London, pp. 87–117.
Paiva, I.E., Maravilhas, S., Marinho, F.S., Sampaio, R.R., 2021. Digital transformation, public policies, and the triple helix: a case study of the city of Salvador. In: Handbook of Research on Digital Transformation and Challenges to Data Security and Privacy. IGI Global, pp. 289–310.
Pang, M.S., 2014. IT governance and business value in the public sector organizations—The role of elected representatives in IT governance and its impact on IT value in US state governments. Decis. Support Syst. 59, 274–285.
Peterson, D.K., Kim, C., Kim, J.H., Tamura, T., 2002. The perceptions of information systems designers from the United States, Japan, and Korea on success and failure factors. Int. J. Inf. Manag. 22 (6), 421–439.
Pizzini, M., Lin, S., Ziegenfuss, D.E., 2015. The impact of internal audit function quality and contribution on audit delay. Audit. J. Pract. Theory 34 (1), 25–58.
Podsakoff, P.M., MacKenzie, S.B., Lee, J.Y., Podsakoff, N.P., 2003. Common method biases in behavioral research: a critical review of the literature and recommended remedies. J. Appl. Psychol. 88 (5), 879.
Podsakoff, P.M., MacKenzie, S.B., Podsakoff, N.P., 2012. Sources of method bias in social science research and recommendations on how to control it. Annu. Rev. Psychol. 63 (1), 539–569.
Prawitt, D.F., Smith, J.L., Wood, D.A., 2009. Internal audit quality and earnings management. Account. Rev. 84 (4), 1255–1280.
Premkumar, G., Potter, M., 1995. Adoption of computer aided software engineering (CASE) technology: an innovation adoption perspective. ACM SIGMIS Database: the DATABASE for Advances in Information Systems 26 (2–3), 105–124.
Richardson, H.A., Simmering, M.J., Sturman, M.C., 2009. A tale of three perspectives: examining post hoc statistical techniques for detection and correction of common method variance. Organ. Res. Methods 12 (4), 762–800.
Ringle, C. M., Wende, S., and Will, A. 2005. "SmartPLS 2.0," University of Hamburg, Hamburg, Germany (http://www.smartpls.de).
Sedikides, C., Campbell, W.K., Reeder, G.D., Elliot, A.J., 1998. The self-serving bias in relational context. J. Pers. Soc. Psychol. 74 (2), 378–386.
Spremic, M., 2017. Governing digital technology–how mature IT governance can help in digital transformation? Int. J. Econ. Manage. Syst. 2, 214–223.
Steinbart, P.J., Raschke, R.L., Gal, G., Dilla, W.N., 2012. The relationship between internal audit and information security: An exploratory investigation. Int. J. Account. Inf. Syst. 13 (3), 228–243.
Steinbart, P.J., Raschke, R.L., Gal, G., Dilla, W.N., 2013. Information security professionals' perceptions about the relationship between the information security and internal audit functions. J. Inf. Syst. 27 (2), 65–86.
Steinbart, P.J., Raschke, R.L., Gal, G., Dilla, W.N., 2018. The influence of a good relationship between the internal audit and information security functions on information security outcomes. Acc. Organ. Soc. 71, 15–29.
Stewart, J., Subramaniam, N., 2010. Internal audit independence and objectivity: emerging research opportunities. Manag. Audit. J. 25 (4), 328–360.
Stoel, M.D., Muhanna, W.A., 2011. IT internal control weaknesses and firm performance: An organizational liability lens. Int. J. Account. Inf. Syst. 12 (4), 280–304.
Teffo, M.C., Motjolopane, I., Masenya, T.M., 2022. Academic library innovation through a business model canvas lens: a case of South African Higher Education Institutions. In: Innovative Technologies for Enhancing Knowledge Access in Academic Libraries. IGI Global, pp. 22–39.
Wallace, L., Lin, H., Cefaratti, M.A., 2011. Information security and Sarbanes-Oxley compliance: An exploratory study. J. Inf. Syst. 25 (1), 185–211.
Westlund, A.H., Källström, M., Parmler, J., 2008. SEM-based customer satisfaction measurement: On multicollinearity and robust PLS estimation. Total Qual. Manag. 19 (7–8), 855–869.
Williams, L.J., Hartman, N., Cavazotte, F., 2010. Method variance and marker variables: A review and comprehensive CFA marker technique. Organ. Res. Methods 13 (3), 477–514.
Wu, T.H., Huang, S.M., Huang, S.Y., Yen, D.C., 2017. The effect of competencies, team problem-solving ability, and computer audit activity on internal audit performance. Inf. Syst. Front. 19 (5), 1133–1148.
Wu, S.P.J., Straub, D.W., Liang, T.P., 2015. How information technology governance mechanisms and strategic alignment influence organizational performance: Insights from a matched survey of business and IT managers. MIS Q. 39 (2), 497–518.
Yu, P., Chen, D., Ahuja, A., 2022. Smart and sustainable economy: how COVID-19 has acted as a catalyst for china's digital transformation. In AI-Enabled Agile Internet of Things for Sustainable FinTech Ecosystems. IGI Global, pp. 106–146.