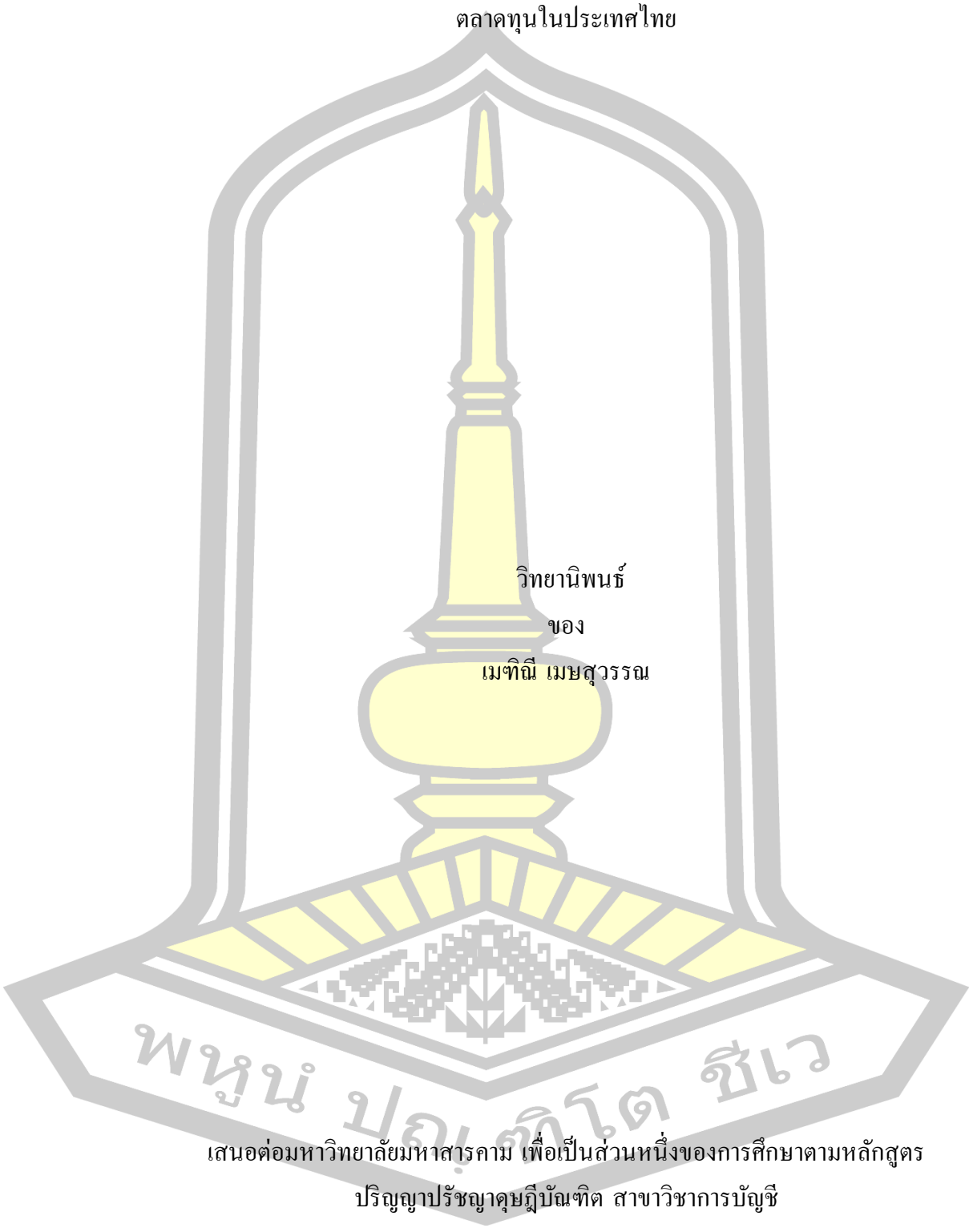
The effect of information technology audit on audit quality of auditors in the capital market in Thailand

Metinee Messuwan

A Thesis Submitted in Partial Fulfillment of Requirements for
degree of Doctor of Philosophy in Accounting
January 2025

Copyright of Mahasarakham University

ผลกระทบของการตรวจสอบเทคโนโลยีสารสนเทศที่มีต่อคุณภาพการตรวจสอบของผู้สอบบัญชี
ตลาดทุนในประเทศไทย



วิทยานิพนธ์

ของ

เมฑิณี เมษสุวรรณ

เสนอต่อมหาวิทยาลัยมหาสารคาม เพื่อเป็นส่วนหนึ่งของการศึกษาตามหลักสูตร
ปริญญาปรัชญาดุษฎีบัณฑิต สาขาวิชาการบัญชี
มกราคม 2568
ลิขสิทธิ์เป็นของมหาวิทยาลัยมหาสารคาม

The effect of information technology audit on audit quality of auditors in the capital market in Thailand

Metinee Messuwan

A Thesis Submitted in Partial Fulfillment of Requirements

for Doctor of Philosophy (Accounting)

January 2025

Copyright of Mahasarakham University

The examining committee has unanimously approved this Thesis, submitted by Miss Metinee Messuwan , as a partial fulfillment of the requirements for the Doctor of Philosophy Accounting at Mahasarakham University

Examining Committee

..... Chairman
(Asst. Prof. Sumintorn Baotham , Ph.D.)

..... Advisor
(Assoc. Prof. Nuttavong Poonpool , Ph.D.)

..... Co-advisor
(Asst. Prof. Salakjit Ninlaphay , Ph.D.)

..... Committee
(Asst. Prof. Utis Bhongchirawattana , Ph.D.)

..... External Committee
(Asst. Prof. Dararat Phoprachak , Ph.D.)

Mahasarakham University has granted approval to accept this Thesis as a partial fulfillment of the requirements for the Doctor of Philosophy Accounting

....
(Assoc. Prof. Charuay Savithi , Ph.D.) (Assoc. Prof. Krit Chaimoon , Ph.D.)
Dean of Mahasarakham Business School Dean of Graduate School

พหูน ปณฺ ฑิโต ชีเว

TITLE The effect of information technology audit on audit quality of auditors in the capital market in Thailand

AUTHOR Metinee Messuwan

ADVISORS Associate Professor Nuttavong Poonpool , Ph.D.
Assistant Professor Salakjit Ninlaphay , Ph.D.

DEGREE Doctor of Philosophy **MAJOR** Accounting

UNIVERSITY Mahasarakham University **YEAR** 2025

ABSTRACT

The key objective of this research is to examine the effect of information technology audits on the audit quality of auditors in the capital market in Thailand. An information technology audit can be categorized into four domains, namely, financial statement audit, operational audit, compliance audit, and information technology control.Additionally, audit outcomes are comprised of reducing audit risk, data security, and audit quality. On the other hand, its antecedents are technological change awareness, business environment, and regulatory. For this paper, 365 auditors operating in Thailand's capital market were chosen as a research sample. The data was gathered by a questionnaire and analyzed by using inferential statistics, specifically multiple regression analyses.

The results conclude that the approach of information technology audit has a positive impact on the outcome of reducing audit risk, and reducing audit risk has a positive impact on audit quality. Furthermore, information technology audit has a positive impact on certain aspects of data security, such as financial statement audit, operational audit, and information technology control, and data security has a positive impact on audit quality.

Regarding the influence of antecedents on each dimension of information technology audit, the study finds that technological change awareness, business environment, and regulatory factors have a positive influence on information technology control. Furthermore, technological change awareness and regulatory factors positively impact compliance audits. However, the business environment positively influences operational audit. These findings have been thoroughly discussed in this research, which includes both theoretical and practical recommendations. The study also emphasizes suggestions for future research.

Keyword : Information technology audit, Reducing audit risk, Data security, Audit Quality

ACKNOWLEDGEMENTS

The completion of this dissertation would not have been possible without the generous support of the following people:

Firstly, I am deeply grateful to my family for their endless support physically, with mental feelings, and with love to encourage me to complete a Ph.D. Their good wishes and blessings have made me successful as a graduate student.

Secondly, I am very grateful to my advisors, Associate Professor Dr. Suwan Wangcharoendate and Associate Professor Dr. Nattawong Phunphun, who provided me with ideas, inspiration, and direction. Their continuous guidance was instrumental to the completion of this research. Furthermore, I highly appreciate my co-advisor, Assistant Professor Dr. Salakjit Ninlaphay, who has been my mentor all along the way.

Additionally, I would like to thank all the members of the thesis committee for their valuable feedback on this research.

Thank you so much.

Metinee Messuwan

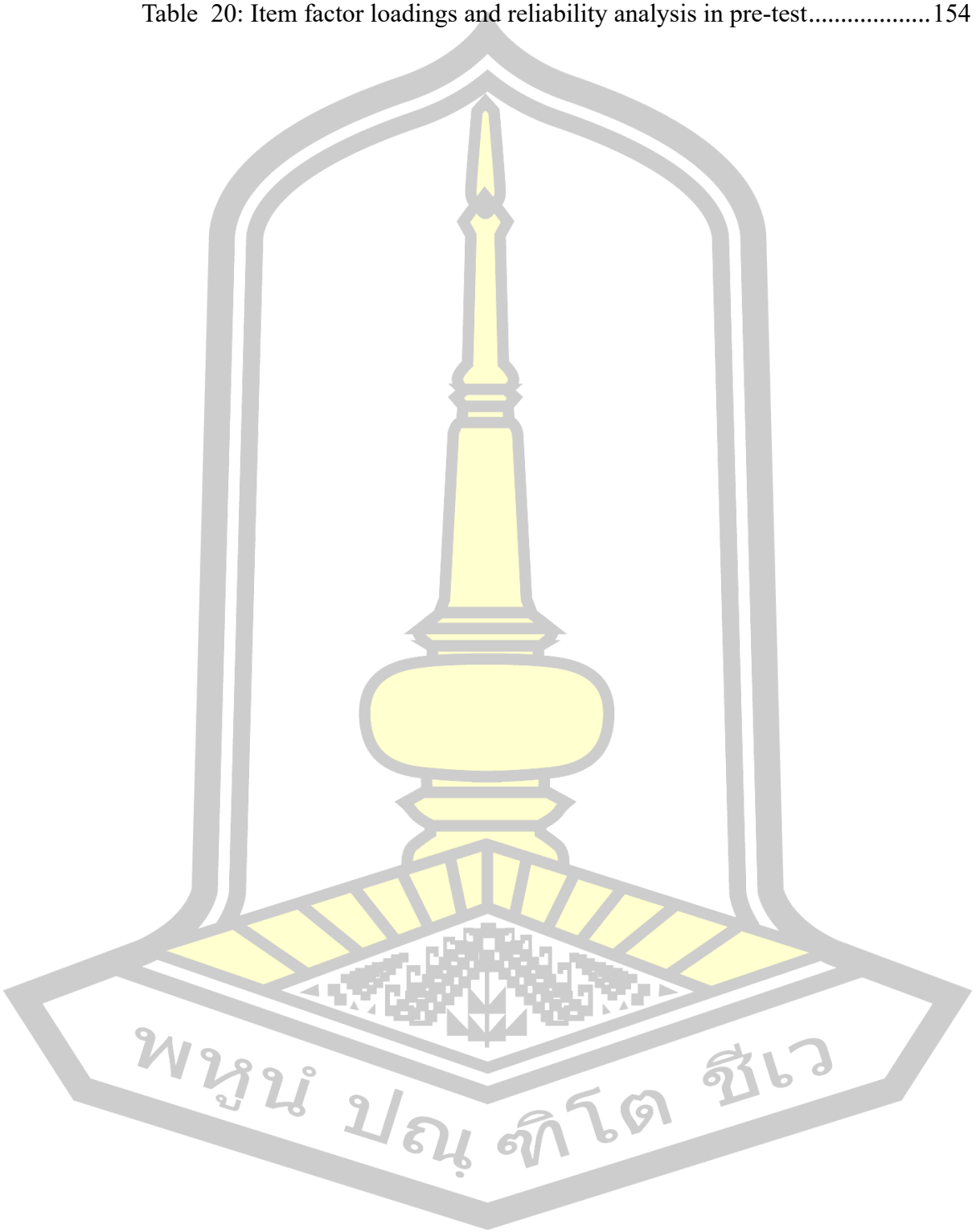
TABLE OF CONTENTS

Page

พหุน ปณ ฑิโต ชีเว

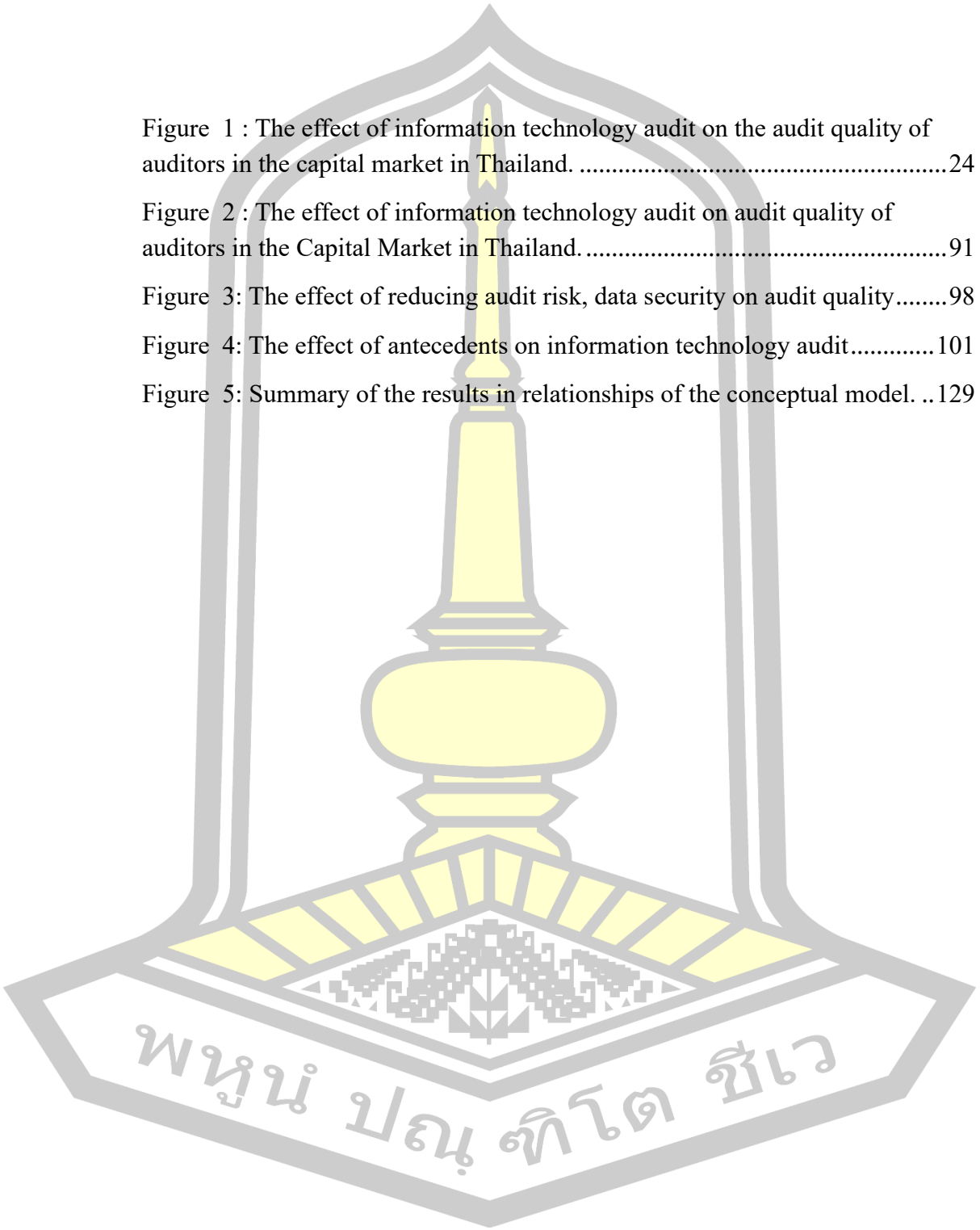
LIST OF TABLE

Page



LIST OF FIGURES

Page



CHAPTER I

INTRODUCTION

Overview

Digital disruption is a rapid, technology-induced, and difficult-to-anticipate market change process that overwhelms leading companies to adapt to the new environment (Ivanov et al., 2018). Over the past decade, digital technologies have led to far-reaching changes in business environments of companies. They lead to changes in customer requirements, the way business is conducted, competition and interaction between businesses (Osmundsen et al., 2018). Moreover, digital technologies foster new ways of collaborating, organizing resources, designing products, and developing new standards and solutions that enhance organizational efficiency and competitiveness. (Markus & Loebbecke, 2013). Some companies have leveraged the evolution of digital technologies to secure a prominent position in the market and gain a competitive advantage in today's rapidly changing environment (Klos & Spieth, 2020). Driven by efficiency and growth ambitions, we expect firms' focus on digital technologies to continue increasing (Schneider & Kokshagina, 2021). The digital transformation's central paradigm has emerged owing to the variety of digital technologies over the years.

The continuous growth of digital technology has led to the evolution of increasingly complex threats in information technology security. In 2013, threats included cyberattacks, data breaches, software vulnerabilities, hardware failures, human error, and natural disasters. These threats arise from the increased reliance on information technology and inadequate information technology governance, which can impact data accuracy, information security, and investor confidence. Consequently, there has been a growing awareness of information technology security (Hall, 2011). In Thailand, there is an emphasis on the development and utilization of technology to drive and promote the advancement and development of the country. To transform service delivery by leveraging digital data and creating new service systems through technology. As

a result, in 2019, the National Cyber Security Agency was designated as the provider of services related to the prevention, monitoring, surveillance, risk reduction, maintenance, and recovery from threats posed by cyber threats (Standards and Guidelines for Promoting the Development of Cyber Security Service Systems, 2023). During the COVID-19 pandemic, there was a response to the increasing cyber risks associated with the growth of digital work. This has led organizations worldwide to adjust their cybersecurity strategies. According to a survey conducted by a leading accounting firm in the United States, the rate of unauthorized data access is on the rise. In 2020, the increased use of virtual private networks (VPNs) due to remote work led cybercriminals to target organizations. This includes the company Colonial Pipeline, which reported that cybercriminals from the Darkside group disrupted the operations of oil pipeline businesses in the United States by stealing passwords, resulting in operational disruptions (Gaurav, 2020). Therefore, to ensure the appropriateness and security of information technology usage, and to support users in conducting activities effectively (The Securities and Exchange Commission, Thailand, 2019). The role of information technology auditing has progressively become increasingly important over time.

Information technology audit is the oversight and management of the effectiveness of information systems, including auditing, security controls, and risk management of information technology (Information Systems Audit and Control Association, 2020). Information technology auditing has become a critical issue in mitigating vulnerabilities and threats arising from the increasing risks associated with technology. This will enhance the efficiency of business operations, data processing, and reporting, as well as increase the reliability of the information. Auditors will evaluate the efficiency and effectiveness of the information technology controls within the system and related operations. This includes the adequacy of information technology controls to reduce the risk of losses arising from errors, fraud, and other misconduct, as well as disasters or incidents that disrupt system functionality. The increase in technology-related threats has broadened the scope of operations and created opportunities for auditors to respond to changes in the environment. (Agoes, 2012). For this

reason, KPMG (2009) believes that information technology auditing is a crucial component of overall audit activities. This is based on a synthesis of research that emphasizes the growing importance of information technology auditing as a key element of modern auditing approaches. Integration of information technology auditing into financial statement audit, operational audit, compliance audit, and information technology control (Devale & Kulkarni, 2012). will facilitate a more comprehensive assessment of organizational processes and controls. This approach is necessary as technology has increasingly played a profound role in most business processes, impacting financial accuracy, compliance with regulations, and operational efficiency. Therefore, this research needs to study information technology auditing impact on reducing audit risk and data security as mediating variable.

Reducing audit risk involves minimizing errors that arise from significant events that need assessment. The audit risk that occurs may stem from errors or fraud present in the client's financial statements. Auditors can reduce audit risk by increasing the number of audit procedures. Maintaining an appropriate level of audit risk is a critical component of auditing. Additionally, strengthening effective controls can help reduce the risk of misstatements due to errors or fraud (Lorentzon, 2023). This includes ensuring appropriate segregation of duties, regularly reviewing financial records, and continuously monitoring high-risk areas. These actions can reduce the risk of control and detection, which are components of overall audit risk that contribute to improved audit effectiveness (Lessambo, 2018).

Data security refers to the practices and measures taken to protect data from unauthorized access, use, modification, or destruction. In today's environment, it is crucial to implement a secure data storage plan to safeguard data from potential breaches by third parties (Wang et al., 2020). Since data integrity and security are essential for proper and reliable assessments, organizations must prioritize these measures to maintain trust and reliability in their data management practices. This approach not only protects sensitive information but also enhances the overall resilience of the organization against data-related risks. The mediating variable consists of reducing audit risk and

data security able to relate with audit quality. In accordance with the research of Hurtt, R. K. (2011), which states that audit risk has a positive relationship with the effectiveness of the audit process, particularly in terms of the sufficiency and appropriateness of audit evidence. Considering reliable and appropriate information enables auditors to express opinions and exercise professional judgment in observing and questioning experts effectively. This helps reduce the risk of overlooking suspicious circumstances or incorrect assumptions during evidence gathering and audit evaluation (Riyadi et al., 2021). And reducing audit risk ultimately impacts the accuracy, reliability, and effectiveness of the audit. Furthermore, if the data is safe, stringent data security measures can aid in the detection and prevention of fraudulent actions, boosting the audit's credibility (Petter Lovaas, 2012).

Audit quality is the opinion of an auditor about evaluation of how well information complies with pertinent facts. The auditor may find and disclose fraud or mistakes in the client's accounting system. However, comments on the auditor's financial reports must be supported by adequate relevant data. Therefore, the information is appropriately reliable accuracy will help quality audit work. (Federation of Accounting Professions, 2014). If the information received is incomplete. There is an error that may obstruct the audit of the auditor a result of inaccurate information in the reporting. Currently, businesses have increasingly applied technology in their operations to facilitate the management of a large volume of data and enhance operational efficiency. Which impacts the information used in the accounting examination of accountants. If there is effective governance and control of information technology, accurate and secure information will foster confidence and reduce errors resulting from inappropriate decision-making which contributes to the enhancement of the Audit quality (The Securities and Exchange Commission, Thailand, 2022). However, information technology auditing needs to get influence from technology change awareness, business environment, and regulatory as antecedent variable.

Technology change awareness has increased in the present day, as the adoption of technology can lead to greater efficiency, quick access to information, and cost-effectiveness (Badavar Nahandy, 2011). And it helps enhance various capabilities in operations, reduce working time, increase the ability to test large volumes of data, reduce audit risk, and provide flexible analytical information with more comprehensive data. These factors contribute to an improved audit process. (Liana Elefterie, 2016). With the increasing technological changes, organizations have become more reliant on technology, leading to adjustments in the business environment and changes in the working conditions. When information technology innovations are successfully implemented, information technology now plays a significant role in business processes by creating new demands, developing new products, and managing new procedures (Attaran, 2003). Additionally, the increase in regulations regarding cybersecurity is a result of the continuous growth of information technology, which has led to an increase in information technology related threats. This has led to operational disruptions and errors, adding complexity to businesses across all industries (Azizi et al., 2024). Therefore, these factors have created a need to ensure confidence in the use of information technology. The role of information technology audits has become increasingly vital in ensuring organizations effectively navigate the complexities of digital transformation while mitigating associated risks (Isaca, 2019). Moreover, the relationship and effectiveness among variables can be explained with defense-in-depth (DiD) theory and contingency theory.

The discussion has employed two theories to explain the research relationships, namely the defense-in-depth (DiD) theory of Smith C.L., (2003) The advancements in information technology have been described, including the emerging threats in information technology. Detecting intruders has become imperative for various organizations, and they should adopt appropriate methods to select and implement technologies as the security of information and information technology can contribute to the accuracy and credibility of information. The effective best practice of information technology audit. The d e f e n s e -i n -d e p t h t h e o r y serves as a fundamental approach in auditing

information technology, aiding in the reduction of anomalies and ensuring data security. Acknowledged by data security experts, the defense-in-depth theory is considered a safeguard for data security, providing assurance and guiding the implementation of policies to address potential future incidents.

Therefore, the influence of various factors impacts behavioral changes such as, rapidly evolving information technology, which can be effectively applied in operational practices to achieve success additionally, the pressure from environmental factors and evolving regulations necessitates behavioral changes to achieve the expected outcomes and meet the desired goals, there is an increasing utilization of information technology to enhance the efficiency of management, including compliance with the increasing regulations and guidelines, accountants must adapt to the changing environment. However, the growing threats in information technology necessitate the implementation of intrusion detection and the preservation of information and information technology security (Yeboah, 2013). The escalating threats in information technology have resulted in an expansion of the scope of responsibilities for auditors. The Thai standard on auditing now mandates that auditors must comprehend information technology to effectively plan, control, and assess information technology. This ensures confidence in the appropriate and secure use of information technology in accordance with the established standards.

Based on the discussion, the conclusion can be drawn that, according to defense-in-depth theory, the relationship between factors influencing the auditing process of accountants can be explained as follows: The environmental context plays a crucial role and has a significant impact on the auditing process. This includes the rapid development of technology and the continual updates and revisions of regulations and guidelines. These factors act as pressures that drive changes in the operational practices of accountants in response to the evolving environment. The escalating threats in information technology have led to the necessity of implementing intrusion detection and preserving the security of information and information technology. Consequently, this has resulted in an expansion of the scope of responsibilities for accountants, particularly in response to technology-related risks. This is done to ensure

confidence in the appropriate and secure utilization of information technology in accordance with established standards.

Another theory is contingency theory of Fiedler (1972) contingency theory explains the relationship between reducing audit risk and data security impact on the audit quality. Contingency theory is a compilation of various ideas that highlight the appropriateness of aligning strategies and behaviors of accountants in making decisions to achieve individual success in business operations (Chandler, 1962). The most appropriate approach should be a method that aligns with the environment. Each type and method of audit will yield different results depending on the unique circumstances of the environment. The selection of the most suitable approach depends on the specific situation, as each method has both advantages and limitations in terms of its effectiveness in conducting an audit such as for instance, inaccurate or insufficient information that was made accessible for an audit. The audit of the auditor might be hampered by a mistake. Due to the presence of inappropriate information for reporting, the importance of auditing information technology becomes paramount in assessing and controlling the security of information technology. This ensures the generation of reliable and appropriate information in accordance with established standards.

Based on the discussion, the conclusion can be drawn that, according to contingency Theory explaining the relationship between reducing audit risk and data security impact on the quality of accounting examinations, selecting appropriate approaches will lead to successful outcomes in business operations. such as an increasing reliance on information technology can be a contributing factor to the emergence of technology-related threats that reduce the security of information. This poses a challenging situation for the auditing profession, as ensuring the security of information becomes more complex and demanding. Contingency theory explains the relationship between reducing audit risk and data security impact on audit quality (Brown-Liburd, Issa, et al., 2015). based on earlier studies Mariana Carroll et at., (2007) Stating that the increased use of information technology over the past two to three decades has had an impact on the expansion of the scope of auditing work. This impact has led to the need for

regulating and controlling information technology to ensure efficient operations and the production of appropriate information. This, in turn, contributes to the presentation of opinions by auditors.

Nevertheless, during the period of technological advancement, the risk aspect of information technology becomes crucial and has implications for business decision-making. Therefore, the increasing demand for research related to information technology audit, with a focus on the significance of these services, becomes necessary to comprehend potential issues that may arise during the process of information technology audit (Weidenmier & Ramamoorti, 2006). consistent with the research of Filipek (2007) stated that there is a necessity to enhance understanding related to information technology audit. Due to the advancements in information technology and the increased utilization of information technology expenses, as well as the emergence of new laws and professional requirements related to information technology audit in order to enhance confidence in the use of information technology, the practice of auditing information technology is widely employed to assess operations, effectiveness, controls, security maintenance of information systems, and to identify opportunities for improvement in weak areas of the information system, resulting in obtaining reliable information (Omoteso, 2013). Furthermore, researchers also believe that the current practice of information technology audit has a significant impact on the audit quality. This is because information technology audit focuses on the characteristics of the organizational information systems that utilize information technology, aiming to ensure the security and efficient functioning of information technology, as well as obtaining complete and secure information.

The information technology audit is an examination that contributes to obtaining accurate and reliable information. This will enable accountants to perform their auditing tasks more effectively. As considering reliable and appropriate information is sufficient, appropriate information aids auditors in expressing opinions and using reasoning to observe and raise relevant suspicions concerning professionals adequately. This helps to mitigate the risk of overlooking questionable situations or erroneous assumptions during

evidence gathering and audit evaluation. (Federation of Accounting Professions, 2010). based on earlier stated that information technology audit involves assessing the risks arising from the utilization of information technology and controlling its usage to mitigate potential risks. Additionally, there are other issues that have not been examined in past research. (Aditya et al., 2018). The increasing interest in the field of information technology audit has influenced the demand for guidance in the practice of information technology audit. As a result, the topic of information technology audit has become one of the intriguing subjects. Consequently, the researchers are interested in examining the effect of information technology audit on audit quality of auditors in the capital market in Thailand. To achieve the desired outcomes for this study, the following research questions are proposed:

Research questions

The study on the mediating effect of reducing audit risk and data security between information technology audit and audit quality of auditors in the capital market in Thailand questions are as follows:

The study on the effect of information technology audit on audit quality of auditors in the capital market in Thailand questions are as follows:

1. How the relationship between information technology audit has a positive impact on reducing audit risk?

2. How the relationship between information technology audit has a positive impact on data security?

3. How the relationship between reducing audit risk have a positive impact on audit quality?

4. How the relationship between data security has a positive impact on audit quality?

5. How the relationship between technological change awareness, business environment, regulatory have a positive impact on information technology audit?

Purposes of the research

The main research objective is to examine the mediating effect of reducing audit risk and data security between information technology audit and audit quality. In addition, the detailly research objectives are as follows:

1. To study information technology audit has a positive impact on reducing audit risk

2. To study information technology audit has a positive impact on data security

3. To study reducing audit risk has a positive impact on audit quality

4. To study data security has a positive impact on audit quality

5. To study technological change awareness, business environment, and regulatory have a positive impact on information technology audit

Scope of the research

The objective of this study is to examine the effect of information technology audit on audit quality of auditors in the capital market in Thailand. The study employs a quantitative research approach and utilizes data collected from a sample of 365 securities auditors in the capital market. (The Securities and Exchange Commission, Thailand, 2023). Data as of April 23, 2023.

Definition

Information technology audit The process of gathering and evaluating evidence plays a pivotal role in assessing the security control procedures of information systems. This involves the identification and reporting of information congruence, ensuring the production of secure, comprehensive, and accurate information. Moreover, it encompasses the supervision of information technology and the management of technological risks. This comprehensive

	approach aims to optimize the utilization of resources and achieve objectives with utmost efficiency.
Financial statement audit	The examination of accounting data and financial reports is conducted to assess the completeness and reliability of the information.
Operational audit	The auditing process involves examining and evaluating operational procedures and methods to ensure confidence in the efficiency
Compliance audit	The inspection of work practices in accordance with regulations is carried out to ensure that operations are conducted in compliance with the law and regulations.
Information technology control	The supervision and oversight of both internal and external information systems that utilize computers.

พหุน ปณ ฑิโต ชีเว

Audit quality	The expression of opinions by certified accountants that are consistent with relevant facts and comply with accounting standards, based on accurate, reliable, complete, and up-to-date information.
Reducing audit risk	Reducing errors arising from critical events that require assessment can be achieved through careful consideration of both internal and external factors impacting the organization.
Data security	Protecting and overseeing the security of data is crucial to mitigate risks and prevent unauthorized actions by users, such as cyber-attacks or breaches.
Technological change awareness	The acceptance of information technology, including the recognition of its advantages in application, contributes to enhancing efficiency.
Business environment	Various forces and factors can impact business operations positively or negatively, leading to changes in the way businesses operate.
Regulatory	Guidelines for standardizing practices or operating procedures are essential to ensure efficiency and mitigate risks.
Auditing skill	The abilities and expertise in evaluating evidence or conducting financial data verification, as well as providing advice on financial risks of companies.

CHAPTER II

LITERATURE REVIEW AND CONCEPTUAL FRAMEWORK

The previous section provided an overview of the important aspects of information technology audit and identified the research objectives, research questions, and scope of the study. This section focuses on understanding the theoretical foundations and the evolution of information technology development. It emphasizes the significance of information technology audit and presents the definition of information technology audit. Additionally, it reviews relevant literature related to research assumptions and conceptual framework. Therefore, this section is divided into three main parts. The first part presents the foundational theories, defense-in-depth theory in depth and the contingency theory. The second part discusses the relevant literature to explain the background, the meaning of information technology audit, the objectives of information technology audit, and the conceptual framework. Furthermore, this part elaborates on the audit quality, explaining its background, the meaning of audit quality, and the significant components related to audit quality. Finally, the third part presents empirical evidence concerning the information technology audit and audit quality. Additionally, this section reveals the relationship between the research assumptions regarding information technology audit and audit quality, including prior events.

Theoretical foundation

Legitimacy theory

The legitimacy theory by Suchman (1995) explains that corporate actions and activities occur due to social expectations. This is because the company receives rights and powers from society to use natural resources and human resources under the condition that the management of the company must operate their business according to social expectations, this is like a corporate commitment to society (Gray, Kouhy & Lavers, 1995). The companies that consider themselves as a portion of society will look to serve social expectations

with the belief that if the company cannot meet social expectations, they will be reject by society which led the companies cannot succeed (Suttipun, 2021). Therefore, for the company to succeed, the management must focus on the social expectations checking whether the business is still responding to the social expectations or not.

Hence, the legitimacy theory uses to explain information technology audits, which arise from the reliance on digital technology. Some companies take advantage of the evolution of digital technology to maintain their dominant position in the market and gain a competitive edge in today's rapidly changing environment (Klos and Spieth, 2020). The continuous growth of digital technology has led to the evolution of more complex threats in information technology security. These threats stem from increased dependence on information technology and inadequate information technology governance, which may impact data integrity, security, and investor confidence. This has led to increased awareness of information technology security (Hall, 2011). COSO ERM, COBIT, and the ISO 27001 standard prescribe audits based on this concept, particularly for information technology audits.

Information technology audit must adhere to specific standards or guidelines that need to be considered to ensure the success of technology audits and instill confidence in the efficient utilization of information technology resources (Yeboah, 2013). Currently, auditing information technology has adopted international frameworks as guidelines for practice. These frameworks include COSO ERM, COBIT, and the ISO 27001 standards, which are utilized as guidelines to prevent risks arising from information technology and to maintain the security of information technology. These standards, guidelines, and frameworks are applied in the management and governance of information technology.

The Committee of Sponsoring Organizations of the Treadway Commission - Enterprise risk management (COSO-ERM)

COSO ERM is an organizational framework established by the Committee of Sponsoring Organizations of the Treadway Commission. The COSO framework was designed to provide a methodology for assessing and developing to achieve the business objectives outlined in three categories: namely, operating with effectiveness and efficiency, which focuses on using resources efficiently and achieving predetermined goals. The second reliability of financial reporting aims to establish trustworthy financial reports since accurate financial reporting serves as crucial information for both internal and external decision-making. and the final compliance with laws and regulations involves adhering to laws, regulations, rules, and requirements to prevent adverse consequences resulting from non-compliance with legal requirements.

Control Objectives for Information and related Technology (COBIT standard)

The COBIT standard refers to the objectives of control for information and information technology related to the framework of controls and standards disseminated by the information technology audit and control association (ISACA). COBIT aims to govern and manage information technology by providing guidelines for information technology governance. Experts argue that one of the primary reasons many organizations worldwide adopt COBIT is its comprehensive coverage of all aspects of information technology. There are four goals of the COBIT audit process, namely, the auditor must gain an understanding of the organization's business requirements and associated risks and understand relevant controls. The second process contains the evaluation of the appropriate controls as well as the documented controls. The auditor must also assess the compliance of all controls to ensure that established controls are working as indicated. And the final goal of the COBIT audit process is to compute the inherent and future risk if certain controls are not met, or if certain controls should be recommended to reduce the future risk score.

Information technology - Security techniques - Code of practice for information security controls based on ISO/IEC 27001 (ISO/IEC 27001)

ISO/IEC 27001 is a data security standard published jointly by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) under the title "Information technology - Security techniques - Code of practice for information security management." ISO guidelines are considered the best international standards for good practices in data security and provide the minimum foundation for controls that all data security programs should specify in one way or another, depending on the size and complexity of the organization. The objective of ISO 27001 auditing is to assess compliance with the following criteria: (Yeboah, 2013). namely, Information Security Policy, Access Controls, and Physical and Environmental Security

These frameworks serve as guidelines to mitigate risks arising from information technology and to maintain Information technology security. They are used for the management and governance of information technology. Currently, Information technology audits adopt international frameworks as best practices to ensure successful Information technology audits and to build confidence in the efficient use of Information technology resources (Yeboah, 2013).

Defense-in-Depth theory

Defense-in-depth (DiD) theory of Smith C.L., (2003) Mention the advancement of technology has led to various technological threats and risks in the realm of information technology. Thus, it has become essential to implement measures to detect intruders, as ensuring the security of information and information technology aids in maintaining accuracy and reliability of data. The best practice for this purpose is to conduct information technology audits, with a focus on deep prevention, as it forms the foundation of the audits. Deep prevention helps mitigate abnormalities and enhance data security.

The defense-in-depth theory is widely acknowledged among data security experts as an effective approach to safeguarding data. It involves a multi-layered

security strategy that includes data security assurance and policy implementation to address potential incidents that may arise in the future (Caballero, 2013).

Defense-in-depth theory is a viable strategy to achieve data assurance in high-network environments. Currently, information systems are one of the most critical components of organizations. Therefore, appropriate audits should be conducted to ensure a high level of security. The primary objective of technology audits is to review and provide recommendations, certifications, and guidance to organizations regarding data security measures. In line with this, the National Security Agency (NSA) has published the Defense-in-depth framework, which summarizes the best practices for data assurance. The defense-in-depth theory approach involves comprehensive measures that encompass reviewing and enhancing data security policies and practices. By implementing defense-in-depth theory, organizations can better protect their information assets in today's interconnected environment. (Yeboah, 2013).

Therefore, various factors influence behavioral changes, such as the rapid development of information technology, which can be applied to work practices for successful outcomes. Additionally, pressure from the changing environment and regulations necessitate behavioral changes to achieve the desired results. Consequently, there is an increasing use of information technology in management to enhance efficiency and comply with the growing regulatory requirements, leading to changes in the behavior of accountants. Moreover, the escalating threats in information technology require the detection of intruders and the maintenance of information and technology security (Yeboah, 2013). As a result, the scope of accountants' work has expanded after the emergence of technology-related threats. The accounting examination standards now require accountants to understand information technology to plan, control, monitor, and evaluate it. This ensures that the use of information technology is appropriate and secure, following standardized protocols.

In summary, the defense-in-depth theory explains the relationship between factors that impact the examination of auditors. The environment is a crucial factor that influences the examination process, whether it is the rapid

development of technology or the changing regulations, both of which create pressure for changes in work practices among auditors. However, the increasing threats in information technology necessitate the detection of intruders and the maintenance of information and technology security. Consequently, the scope of auditors work has expanded due to technology-related threats, ensuring the appropriate and secure use of information technology in accordance with standardized protocols.

Contingency theory

Contingency theory of Fiedler (1972) mentions the management that depends on the situation means that the external environment has an impact on the operations. The situation acts as a determinant for decision-making and appropriate management approaches. For example, changes in the economic, social, and technological systems in the present have altered traditional business and service processes. These changes are made to adapt to the evolving environment and meet the expectations of customers (Betti & Sarens, 2020). Indeed, the increasing influence of information technology has significantly impacted the field of accounting examinations. The emergence of technology-related threats has necessitated the inclusion of Information technology audit. This presents opportunities for auditors to respond and adapt to the changes in the evolving environment. With the growing importance of safeguarding information and technology systems, audits now have the chance to demonstrate their ability to address technological challenges and ensure the security and efficiency of information processes. As a result, auditors must remain vigilant in staying up to date with technological advancements and incorporating information technology audit practices in their examination processes to meet the demands of the changing environment (Solomon, 2003). The research conducted by Mariana Carroll et al., in 2007 found that the increasing reliance on information technology over the past two to three decades has led to changes in the auditing processes. Auditing now focuses on examining and ensuring that information technology is adequately controlled, secure, and functioning effectively. Technology auditing incorporates the application of standards as a

framework to govern and oversee information technology. For example, the ISO 27001 standard is used to manage and maintain information security. Additionally, the adoption of COBIT standards aids in controlling and safeguarding information technology to foster confidence and trust in its use by implementing these standards. The overall security of information systems is strengthened, reducing risks and protecting data from unauthorized access. This, in turn, enhances the credibility of processed and stored data within information systems (Riad, 2015). Reliable and secure information empowers auditors to perform their tasks efficiently and with confidence, promoting overall effectiveness in their work.

In summary, the Contingency theory aligns with the findings of this study, which indicate that information technology audit has a significant role in business due to the rapid development of information technology. Organizations increasingly rely on information technology, but they also face risks, particularly from cybersecurity threats and data security breaches. Technology auditing helps assess and control the use of information technology to enhance security and reduce risks from technological threats. Consequently, the scope of accountants' work expands as they must ensure that technology applications do not introduce unacceptable risks to the business. Therefore, evaluating the use of information technology is crucial (Petter Lovaas, 2012). to ensure the appropriateness and compatibility of information, without becoming an impediment to the accountants' ability to express opinions and perform their duties effectively.

The defense-in-depth theory explains the relationship between factors that the effect of information technology audit. Factors such as rapid technological advancements and evolving regulations create pressure for changes in the auditing processes of accountants to adapt to the changing environment. The increased cybersecurity threats from the growing use of information technology also necessitate the detection of intruders and safeguarding information and technology. This leads to an expanded scope of work for auditors to ensure the appropriateness and security of technology usage in accordance with standards. Moreover, the contingency theory explains the

correlation between Information technology auditing and audit quality. As information technology rapidly develops, organizations increasingly rely on it. However, there are risks of technological threats that can compromise information efficiency and security. Information technology auditing plays a crucial role in evaluating and controlling the use of technology to enhance security and ensure the generation of reliable and appropriate information. This importance of technology auditing ensures the audit quality (Lombardi et al., 2015; Byrnes et al., 2018).

Relevant literature review and hypotheses development

The digital disruption is a situation which occurs in nowadays business very often. With the development of digital technologies, the classical system of doing business has been disrupted and many companies have to react to digitalization (Genzorova et al., 2019). Digital transformation has brought significant changes to the business environment of various companies, resulting in shifts in customer demands, business operations, competition, and interactions between businesses (Osmundsen et al., 2018). Moreover, digital technologies foster new ways of collaborating, organizing resources, designing products, and developing new standards and solutions that enhance organizational efficiency and competitiveness. (Markus & Loebbecke, 2013). Some companies have leveraged the evolution of digital technologies to secure a prominent position in the market and gain a competitive advantage in today's rapidly changing environment (Klos & Spieth, 2020). Driven by efficiency and growth ambitions, we expect firms' focus on digital technologies to continue increasing (Schneider & Kokshagina, 2021). The digital transformation's central paradigm has emerged owing to the variety of digital technologies over the years.

The continued growth of digital technologies has led to the evolution of threats. included cyberattacks, data breaches, software vulnerabilities, hardware failures, human error, and natural disasters. These threats arise from the increased reliance on information technology and inadequate information

technology governance, which can impact data accuracy, information security, and investor confidence.

Damage caused by using information technology

The progress in information technology has led to significant roles for these technologies in driving business activities within the Thai capital market. Simultaneously, the complexity and expansion of these information technology aspects have amplified multidimensional risks. These include risks originating from information technology, which refers to potential hazards arising from the utilization of information technology in business operations, as well as risks stemming from cyber threats. Originally, the risks related to information technology were considered part of operational risks. However, presently, technology-related risks have gained paramount importance due to the increasing reliance on information technology. Consequently, technological or cyber threats have emerged, impacting business operations, reputation, and confidence in various services and products within the market. Additionally, there are consequences resulting from technological risks, as outlined below (The Securities and Exchange Commission, Thailand, 2019).

1. Information technology reliability and improper processing
2. Information access that is not allowed Data modifications or corruption might happen from this. unsuitable information reflecting unauthorized or unrealized transactions among other things. When the database is used, such vulnerabilities could appear.
3. Possibility for employees in information technology to have access to information outside their responsibilities. and breaking the regulations for the separation of tasks.
4. Information alteration without authorization
5. Unapproved modifications to computer systems
6. Improper manual assistance
7. The potential for data loss or unavailability when necessary

The cybersecurity threats arise from the increasing reliance on information technology, coupled with inadequate control and supervision over information technology operations. The lack of sufficient and appropriate governance and oversight in managing information technology has led to cybersecurity risks that adversely impact accuracy, data integrity, and investor confidence. Consequently, numerous organizations have become more cognizant of information technology security (Hall, 2011) and have begun adopting internationally recognized security standards as a framework for governing and overseeing information technology. Such standards include information technology assurance with COBIT standards, information technology assurance framework, risk information technology framework, iso, and The Thai Standard on Auditing to possess a comprehensive understanding of information technology in order to plan, control, assess risks, and examine practices carried out in a manner that is appropriate and compliant with standards, auditors must expand the scope of their work in assessing information technology. This ensures confidence that the use of information technology is suitable and secure according to established standards and supports users in carrying out activities efficiently. (The Securities and Exchange Commission, Thailand, 2019). Generally, information technology is beneficial for various operational activities. The control of information technology is relevant to Financial Statement Audit, Operational Audit, Compliance Audit and Information technology Control requirements to ensure the accuracy and integrity of data used by auditors in designing and implementing audit procedures. The role of information technology audit, therefore, becomes increasingly significant over time.

Information technology audit has become an unavoidable factor (Drljača & Latinović, 2017). Organizations that utilize information technology must undergo information technology audit, especially large-sized companies that are ready to implement information technology in their operations (Tawakkal, Kurniati, & Wisudiawan, 2016). The increasing reliance on information technology has led to a growing demand for information technology audit practices, and companies are becoming more aware of the importance of

information technology audits in ensuring the integrity of information technology implementation within the organization (Petter Lovaas, 2012). Furthermore, in the current auditing landscape, information technology audits have become more intriguing and the need to enhance the efficiency and effectiveness of information technology audit professionals is evident (Cascarino, 2012).

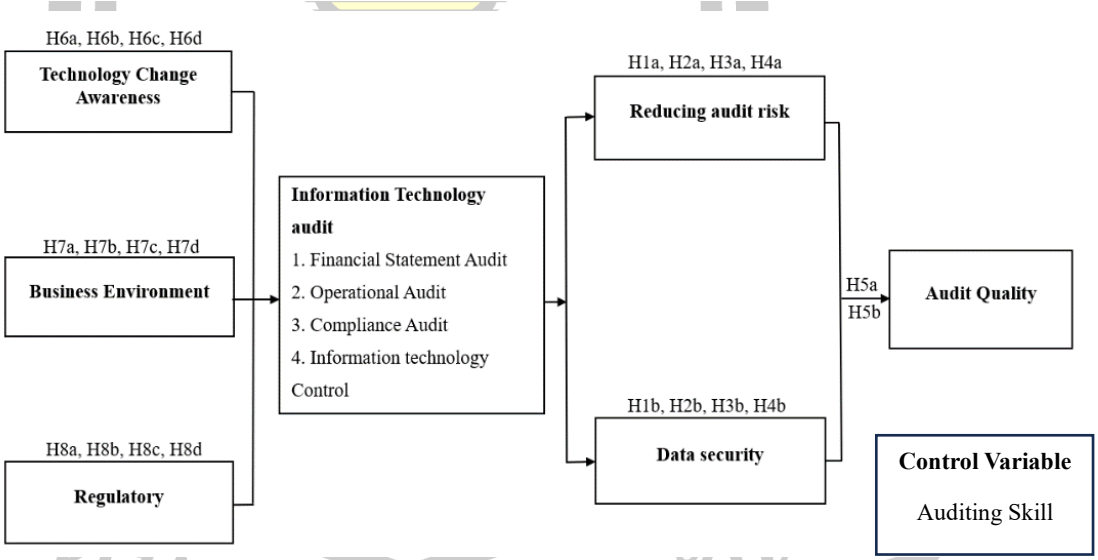
The impact of information technology (IT) and innovation development has influenced the complexity of information technology audit practices due to emerging challenges and opportunities (Rosário, 2013). In such conditions, information technology audits must be able to link various aspects of the organization, information technology audits strategies, information technology with the company's business to create business alternatives (Tingliao L. &., 2015). Additionally, auditors must be prepared to adapt to the new business environment, thus information technology auditors require extensive knowledge and capabilities to assess the risks arising from technological changes (Juiz, 2015). Moreover, experiences in auditing, including information technology audit, financial statement audit, and operational audit, are essential for auditors.

Therefore, information technology auditing should be an integral part of overall auditing practices. In other words, information technology audits can be conducted alongside financial statement audit, and operational audit, and other types of audits to support auditing activities and enhance independence and impartiality (Tingliao L., 2016). However, the use of information technology audits in practice is relatively low due to the lack of guidelines for information technology audit and comprehensive approaches covering all aspects of information security control related to data security. Thus, there is a need for a study on current information technology audit practices, especially after an increase in threats. This study examines whether accountants have utilized information technology audit practices to improve efficiency and effectiveness in accounting practices. Additionally, it points out the gaps in academic research regarding information technology audit practices and the lack of exploration of the role of information technology audit, technology governance, and other related aspects. This approach provides a theoretical perspective and examines

whether the mentioned information technology audit practices will impact the efficiency and quality of auditing activities (Chou, 2015). In other words, the academic research on information technology audit and its influencing factors on the quality of information technology audit practices has not been thoroughly explained and examined in empirical literature (Merhout, 2008). This has led researchers to study the research topic of the effect of information technology audit on audit quality of auditors in the Capital Market in Thailand. To conduct this study, a conceptual framework needs to be setting about the effect of information technology audit on the audit quality of auditors in the capital market in Thailand which has been established as follows:

Conceptual framework

Figure 1 : The effect of information technology audit on the audit quality of auditors in the capital market in Thailand.



Information technology audit

Information technology audit involves supervision, efficiency assessment, and management of information systems, including auditing, security control, and risk management of information technology (ISACA, 2013). This has emerged due to the increasing prominence of information technology and the consequent technological or cyber threats that impact business operations, reputation, and confidence in services (The Securities and Exchange Commission, Thailand, 2019).

In the year 2000, the transition to e-business brought about changes in operational processes to align with evolving scope, expanding the audit process to encompass technology-related audits. This involved examining information system development, assessing technological environment effectiveness, and evaluating the timeliness, completeness, reliability, and alignment of information system outputs with goals and objectives. Consequently, the audit framework required adaptation (Mahzan & Veerankutty, 2011).

In Thailand, there is a growing emphasis on utilizing technology as a tool for driving development and transforming service provision through digital data and the creation of new service systems via technology. This is intended to enhance efficient governance and management (Ministry of Information and Communication Technology, 2016). Simultaneously, the utilization of information technology comes with inherent risks that need to be considered. Insufficient management and security maintenance of information technology can adversely affect operations, necessitating the development of risk management guidelines for information technology. Auditing information technology is often conducted based on standards, such as ISO 27001, which serves as a framework for managing information security. Moreover, the COBIT standard, widely accept internationally, is applied for controlling and ensuring the security of information technology (The Securities and Exchange Commission, Thailand, 2019). The meaning of information technology audit is outlined as follows:

Table 1: Summary of the definition of information technology audit.

Author(s)	Definition
Weber (1999)	The IT equipment auditing service encompasses the examination of office equipment, software, network systems, and computer hardware. IT audits aid in swiftly identifying and resolving issues and deficiencies.
Mark Petterson. (2005)	Information technology audit involves controlling the security and functionality of technology to ensure efficiency.
Singleton et al., (2007)	Information technology audits serve as a tool for assessing whether information systems have the capability to safeguard assets and maintain data integrity within an organization.
Merhout et al., (2008)	Information technology audit serves as a tool to instill confidence in the efficient utilization of information technology.
Mahzan and Veerankutty (2011)	The process of information technology audit involves gathering and evaluating evidence to assess whether information systems protect technological assets. information technology audit ensures data integrity, optimizes resource utilization, and achieves organizational objectives efficiently.
Dale Stoel , Douglas Havelka, Jeffrey W. Merhout (2012)	Information technology audit involves evaluating the effectiveness or cost of information systems.

Table 1: Summary of the definition of information technology audit (continue)

Author(s)	Definition
Aditya et al. (2018)	Information technology audit refers to a systematic, independent, and objective process that is conducted periodically and adheres to standards to ensure rational assurance and continuous improvement of utilizing information technology, leading to successful outcomes.
Munoko et al., (2020)	Information technology auditing serves as risk assurance and control, enhancing operational efficiency.

Based on the above definition, it can be summarized that an information technology audit is a process of collecting and evaluating evidence to assess the information security control procedures. This includes identifying and reporting on the conformity of information to ensure the generation of secure, comprehensive, and accurate information. also involves supervising information technology and managing technological risks to efficiently utilize resources and achieve objectives effectively.

Therefore, information technology auditing plays a crucial role in reducing vulnerabilities and cybersecurity threats that have been on the rise in information technology. This helps businesses, data processing, and reporting to become more efficient and enhances the trustworthiness of the data. During information technology auditing, auditors evaluate the effectiveness and outcomes of technology controls in data systems and related operations, as well as the adequacy of information technology controls to mitigate the risk of losses due to errors, fraud, or other events, including disasters or incidents that may render information systems inoperable. With the increasing complexity of technology-related threats, there is an expanding scope of information technology auditing practices and opportunities for accountants to respond to the changes in such an environment. (Hall, 2011). To examine and ensure that information technology is properly controlled, secure, and functions adequately.

Table 2 : Summary of key literature reviews on information technology audit

Author(s)	Key Issue Examine	Finding
Bagranoff & Vendrzyk, (2000)	The evolving role of is audit: a field study comparing the perceptions of is and financial auditors.	During the past decade, information technology audits have changed from being a small support piece of financial audits to being a driving force in the overall public audit**.**
Bagchi, (2006)	The intersection of information technology and auditing, examining how advances in it affect the audit process.	Integrating information technology audits with operational audits helps organizations identify areas for improvement in both information technology processes and operational efficiencies. This approach enhances overall organizational performance and effectiveness.
Merhout & Havelka, 2008	Factors influence the information technology audit process and develop a model that can be used to improve process quality.	Information technology audits are special projects that require proper quality audit processes and project management principles to help improve business decisions by providing high-quality, timely data.
Majdalawieh & Zaghloul, (2009)	Factors within the various elements of the IS audit.	Information technology audits should be an integral part of overall audit practice. In other words, the information technology audit can be conducted simultaneously with a financial audit, operational audit and other types of audits.

Author(s)	Key Issue Examine	Finding
Hall, (2011)	Information technology auditing and assurance.	Integrating information technology and financial audits, organizations can better identify and mitigate risks associated with financial reporting. Effective information technology controls enhance the reliability of financial data, reducing the likelihood of material misstatements.
Nugi Nkwe, (2011)	The adoption rate of it and challenges and successes of it auditing and how it has changed auditing in Botswana.	Information technology audit is an essential component of overall audit activity. Information technology audit should be delivered as part of an audit.
Devale & Kulkarni, (2012)	The advent of leading edge auditing techniques which allow auditors to identify risks and evaluate the adequacy of controls over critical information systems in their organizations	Information technology audit, financial audit and operational audit are essential for a modern Information technology audit.

Author(s)	Key Issue Examine	Finding
Gantz & Philpott, (2013)	The basics of it audit.	Effective management of information technology related risks through thorough information technology audits not only strengthens the control environment but also enhances the overall quality and reliability of financial audits, ultimately contributing to better organizational performance and trust in financial reporting.
Lawati & Ali, (2015)	Issues involved in conducting information technology (IT) auditing in the banking sector of Oman, how these issues can be handled in accordance with IT audit standards.	An information technology audit can be carried out concurrently with operational, financial, and other kinds of audits.
Kramer, (2016)	Examines the crucial role of IT audits in ensuring compliance with the Sarbanes-Oxley Act (SOX), which was enacted to protect investors from fraudulent financial reporting by corporations.	Developing a unified audit plan that incorporates both information technology and financial audit objectives allows for a more efficient allocation of resources and minimizes redundancy in audit procedures

Author(s)	Key Issue Examine	Finding
Salihu and Hoti (2019)	Implementing it audit recommendations on organizations regarding the security incidents.	Information technology auditing is an assessment of a business's information systems environment, which affects economic data. In addition, the efficiency, effectiveness and productivity of information technology systems are derived from information technology auditing. New auditing approaches will help improve financial audit results, compliance and audit efficiency.
Eulerich et al. (2022)	This study examines how the use of technology-based audit techniques (TBATs) influences audit efficiency, effectiveness, and costs.	Information technology audits focused on assessing compliance with regulatory requirements and internal controls.

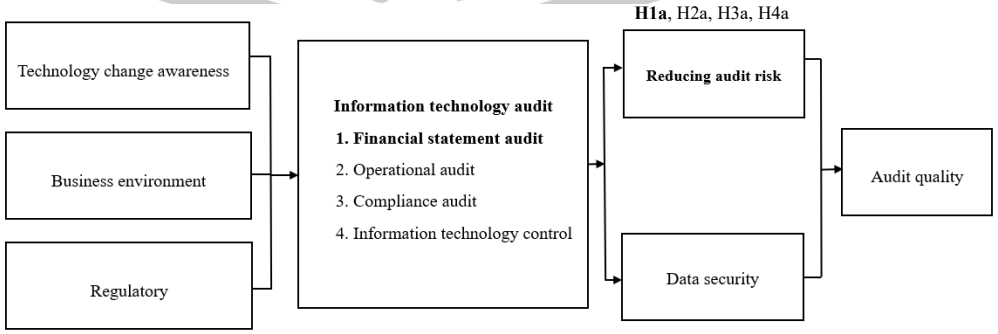
The aforementioned shows that the process of information technology audit involves gathering and assessing evidence related to information to identify and report on the adequacy of information, as well as controlling information technology to ensure secure, complete, and accurate information. Content-based audits alone cannot guarantee the appropriateness and sufficiency of information. Generally, audits provide assurance services, including financial statement audits, operational audits, and compliance audit, to increase confidence for stakeholders. However, in the current environment, the information system's conditions impact data processing and the presentation of meaningful information, potentially conflicting with reality. Therefore, Information technology control is essential for auditors to have reasonable confidence in achieving objectives. The objectives of controls related to financial statement audit, operational audits, and compliance audit are efficient information technology control and ensuring correct and secure information data processing. This encompasses general Information technology Control and application control. Auditors must consider Information technology Control to gain reasonable assurance and enhance information security. From the synthesis of previous research, it is evident that over the past decade, information technology audits have evolved from merely supporting financial audits to becoming a driving force in overall public auditing. This aligns with the research by Majdalawieh & Zaghloul (2009), which states that information technology auditing should be an integral part of overall audit practices. In other words, information technology audits can be conducted concurrently with financial audits, operational audits, and other types of audits. Therefore, information technology audits consist of the following components:

Financial Statement Audit is the process of examining financial accounting data and financial reporting to assess their completeness, reliability, and compliance with established criteria. This is achieved by adhering to fundamental principles, including the professional ethics of accounting practitioners, generally accept auditing standards, and the exercise of professional judgment in observation and suspicion of professional misconduct. The fundamental principles of financial statement audit in conducting a

financial statement audit to ensure the reliability of the work of the auditor for the benefit of stakeholders. (Federation of Accounting Professions, 2010).

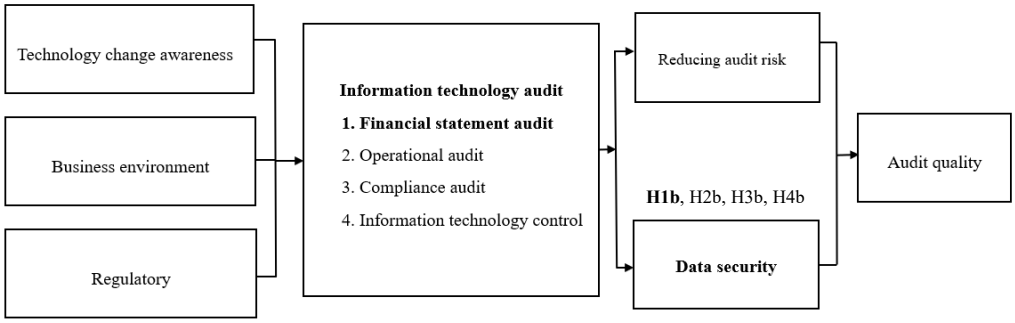
Therefore, the information technology audit has been applied with the use of standards as a framework for governing and managing information technology security. Additionally, it helps strengthen the data security system, reduce risks, and protect data from being compromised (Riad, 2015). This ensures confidence and reliability in using information technology and enhances the trustworthiness of data processed and stored within the information system. Information that is reliable and secure enables auditors to perform their duties efficiently, leading to accurate and precise auditing and certification of financial statements, thereby reducing errors in expressing opinions on financial statements (Salameh, 2011). Auditors must gather comprehensive, accurate, and adequate information to minimize the risk of conducting audits or expressing inappropriate opinions on financial statements that misrepresent significant information to an acceptable level (Federation of Accounting Professions, 2014). The research of Albrecht et al. (2015) stated that auditors may not be able to identify fraud if the environment is at high risk. This gap in the ability to detect fraud can lead to higher audit risk. However, the research of Watts and Zimmerman (1986) highlights that audits contribute to reducing information asymmetry between managers and stakeholders by ensuring that reported figures are reliable. This is consistent with the research of Asare et al. (1994) who stated that auditors can assess the probability of errors in specific areas of financial statements. These techniques reduce audit risk by identifying areas that require closer examination. Thus, the hypotheses are proposed as follows:

H1a: Financial statement audit have a positive effect on reducing audit risk.



Additionally, the review of financial reports ensures the completeness and reliability of information, which contributes to the accuracy of the auditor's risk assessment. This is crucial for preparing an audit report that allows the auditor to draw reasonable conclusions to support their opinions. Therefore, the review of financial reports ensures the accuracy and reliability of information and reduces audit risks (Riyadi et al., 2021). This is consistent with the research by Rosati et al. (2020), which states that if auditors increase their efforts in auditing and testing materiality adequately, information security incidents will not negatively impact audit quality. This means that if auditors thoroughly examine accounting data and materiality, it will ensure data security and maintain audit quality. Based on the above statement, the following hypothesis can be established:

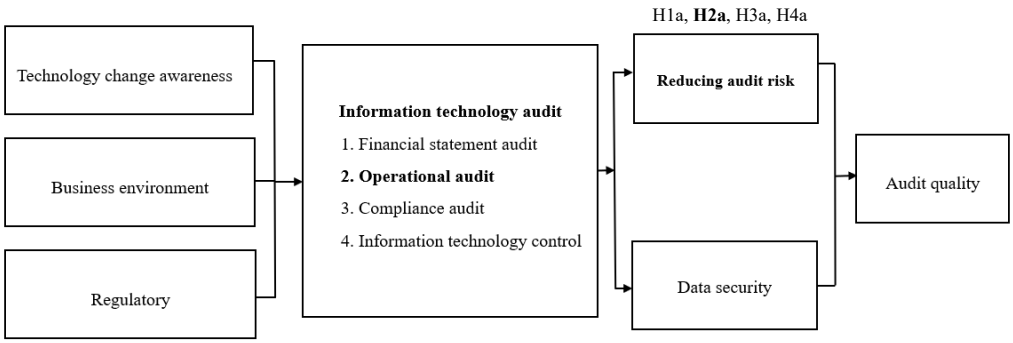
H1b: Financial statement audit have a positive effect on data security.



An operational audit is an examination of processes, methods of operation, and various responsibilities within an organization to ensure that the workflow and responsibilities within each unit are carried out efficiently according to the defined processes. This results in the effective use of resources (Efficiency) and the achievement of set goals. This should consider the sufficiency and efficiency of risk management activities (Federation of Accounting Professions, 2010).

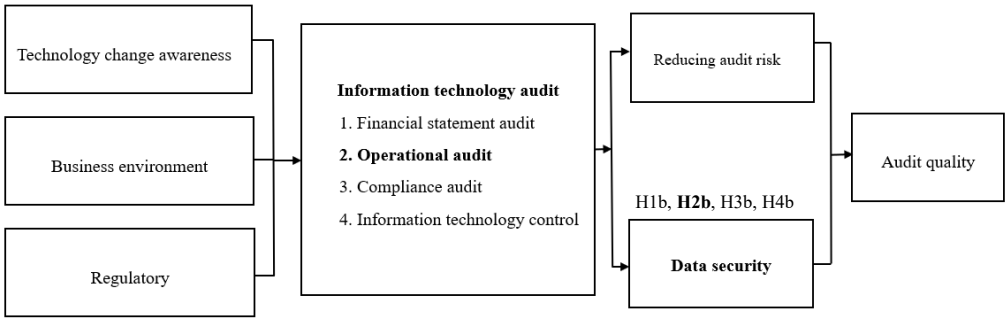
Operating procedures and methods of operation contribute to confidence that these procedures are carried out effectively and help reduce the auditor's audit risk, including the risk of inappropriate expression of opinions on the financial report (Robson et al., 2007; Curtis and Turley, 2007; Peecher et al., 2007). Power (1997) argues that operational audits are more concerned with operational efficiency than with controls over financial reporting, which limits their influence on reducing audit risk. However, Gupta's (2020) study found that operational audits not only highlight areas where efficiencies can be gained but also encourage better adherence to procedures. This reduces the likelihood of misstatements and thus impacts audit risk positively. Research indicates that operational audits help in identifying weaknesses in internal controls (Sawyer et al., 2014). Consistent with research by Arens et al. (2019) and Kinney & Shepardson (2011), effective operational audits reduce the chance of errors or fraud in financial reporting, thereby lowering the overall audit risk. evaluating and recommending improvements to these controls, operational audits mitigate control risk, a major component of audit risk. Thus, the hypotheses are proposed as follows:

H2a: Operational audit have a positive effect on reducing audit risk.



Therefore, evaluating the effectiveness of operations will help manage the approach and set an appropriate scope for the audit (Bagchi, 2006). The audits will help reduce information risks and improve data efficiency. Good data will reduce audit risks and enhance audit effectiveness (Hall, 2011). The audit process helps eliminate or minimize losses by identifying vulnerabilities and risks, determining whether appropriate security controls are in place, and ensuring that security measures and audits are accurate (Bosworth & Kabay, 2002). Based on the above discussion, the following hypothesis can be established:

H2b: Operational audit have a positive effect on data security.

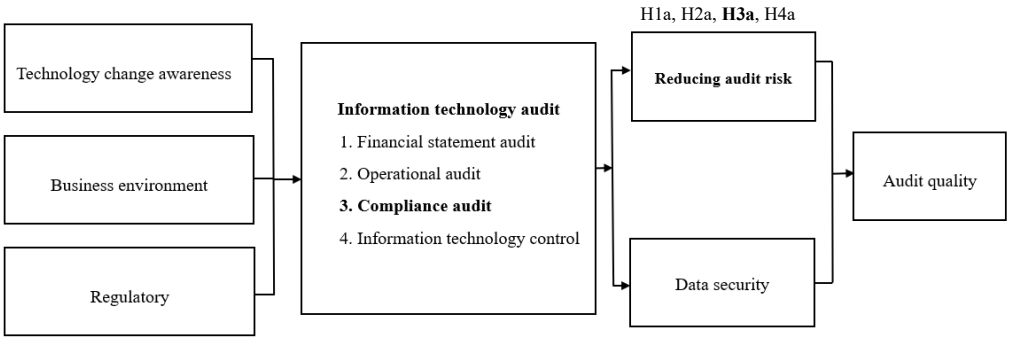


Compliance audit is an examination conducted to ensure that operations are following laws, regulations, governing agency directives, and organizational policies. Neglecting the importance of legal and regulatory compliance can lead to risks arising from non-compliance with laws, standards, regulations, relevant practices, and ethical standards in conducting operations. Such negligence could result in reputational damage or interventions from authorities. When conducting a compliance audit.

Compliance audits are crucial to following regulations; their impact on reducing audit risk may be limited. Key limitations include their focus on regulatory requirements rather than financial accuracy, minimal fraud detection, and limited scope for assessing internal control effectiveness. As a result, compliance audits may not substantially reduce audit risk, as they are not designed to address all factors that contribute to material misstatements in financial statements. Kinney & Shepardson (2011) note that because compliance

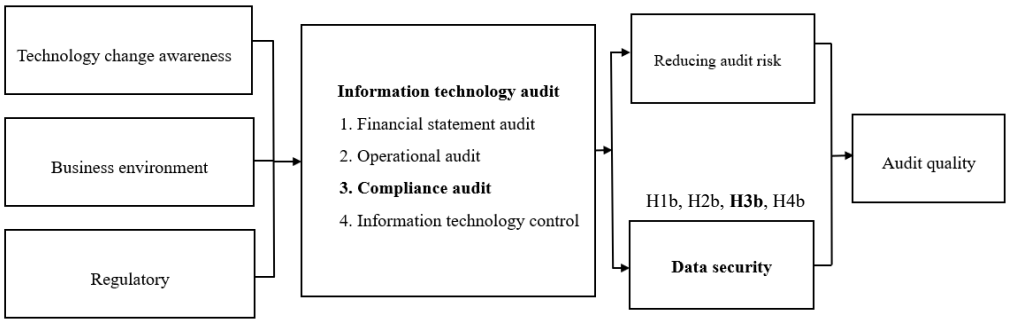
audits do not target financial accuracy, they may not capture complex financial misstatements, limiting their ability to impact audit risk. and Bazerman et al. (1997) suggest that compliance audits may be influenced by organizational pressure to meet regulatory requirements in the shortest time possible, which can lead to a surface-level approach that doesn't meaningfully reduce audit risk. Chen et al. (2015) show that organizations with effective compliance audits tend to exhibit better regulatory adherence, which directly supports more reliable financial reporting, lowering the likelihood of material misstatements. This is consistent with the research of Gantz (2014), who stated that Compliance with laws, regulations, and standards helps reduce audit risks and increase information security. As information technology threats continue to rise, it is crucial to mitigate the risk of losses due to errors, fraud, and other incidents, as well as disasters or events that disrupt system functionality. The COSO ERM, COBIT, and ISO 27001 standards mandate the need for information technology audits. This expanded scope of practice presents opportunities for auditors to respond to the changes in the environment during the audit process, ensuring compliance with laws, regulations, and rules to reduce audit risk and enhance data security (Gantz, 2014). Based on the above, the following hypothesis can be formulated:

H3a: Compliance audit have a positive effect on reducing audit risk.



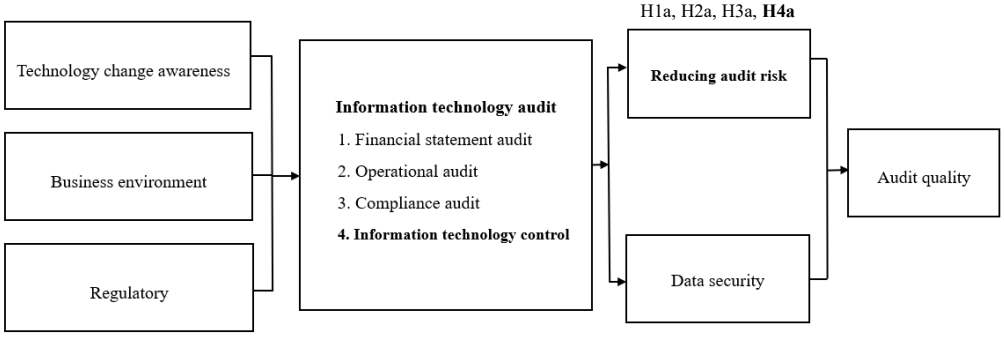
Compliance audits ensure that an organization is following legal and regulatory standards, while information security protects sensitive data from breaches and unauthorized access. This literature review compiles key findings from various studies on the intersection between compliance audits and information security. According to Cohen et al. (2010), compliance audits involve assessing potential risks to information security. By identifying vulnerabilities and areas of non-compliance, auditors can recommend corrective actions that complement information protection measures. However, on the other hand, compliance audits do not always imply that the organization has robust information security. Sometimes, compliance may be considered more fundamental than a comprehensive security strategy. An organization may be compliant with regulations but still be vulnerable to emerging threats if its security measures are outdated or incomplete (Duncan & Whittington, 2014). Therefore, although compliance audits are an essential component of an information security strategy, they are not the sole factor in ensuring data protection. Messier et al. (2016) argue that such ongoing audits compel organizations to stay current with evolving standards and technologies, enhancing their data security. Compliance audits are often periodic, requiring regular review and updating of security measures. This continuity fosters a culture of continuous improvement, which allows organizations to adapt to new threats and incorporate updated security practices. Beekman et al. (2017) emphasize that effective data security requires an ongoing risk management approach, which compliance audits alone may not provide, as they often lack depth in areas such as advanced threat detection and response. Based on the above, the following hypothesis can be formulated:

H3b: Compliance audit has a positive effect on data security.



Information technology control is an activity of controlling information technology, comprising two types Arens et al. (2017), who stated that auditing standards address two types of controls for auditing: 1) general controls, which apply to all IT functions, including IT management, system development alternatives, physical and online security related to access to hardware, software, and data, backup planning and contingency for unforeseen emergencies, and hardware controls; and 2) application controls, which are procedures and methods within application systems to ensure that all transactions are approved, recorded, and processed completely, accurately, and timely, thereby enhancing the reliability of data or information. Effective information helps auditors accurately assess risks, which is crucial for preparing audit reports that enable auditors to reach reasonable conclusions. Reliable and adequate information helps auditors' express opinions and exercise professional judgment appropriately, which reduces the risk of overlooking suspicious situations or incorrect assumptions in evidence collection and audit evaluation. (Petter Lovaas, 2012). According to Bhattacharjee et al. (2017), when auditors assess that an organization has implemented effective IT controls in line with regulatory standards, they can adjust audit procedures and reduce detection risk, thus enhancing audit efficiency. Hall & Singleton (2018), the sheer complexity of modern IT systems can introduce new risks, as auditors may struggle to fully understand and assess the effectiveness of all controls in place. This complexity could contribute to higher audit risk, particularly if auditors lack specialized technical expertise. Based on the above, the following hypothesis can be formulated:

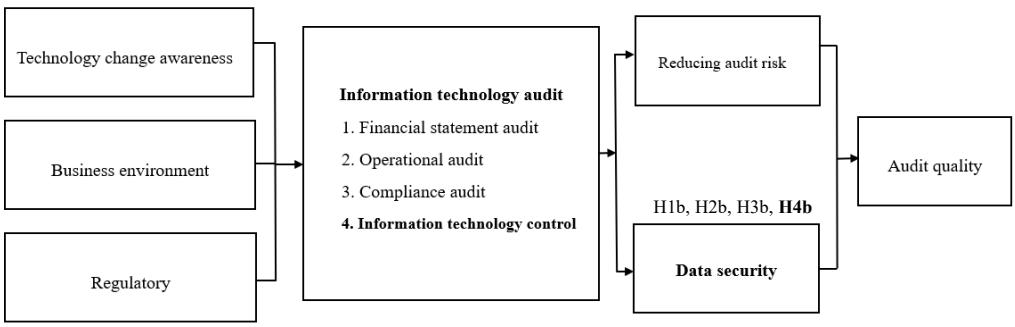
H4a: Information technology control has a positive effect on reducing audit risk.



These risk control activities encompass the inspection and control of data processing, ensuring data completeness, security, privacy, safeguarding technology assets, auditing and controlling system maintenance and program changes, continuous data processing inspection and control, system application inspection and control, and system development inspection and control. Additionally, research by Shahabuddin et al. (2011) further emphasizes that to achieve the objectives of information technology system auditing, it is essential to have clear policy directions and established best practices. Evaluating deficiencies is essential to identify effective information technology security measures and reduce risks during the audit process. By identifying critical deficiencies in the current information technology audit framework, is possible to address and manage information technology risks more effectively (Yeboah, 2013)

These activities align with the research of arens et al. (2017), which states that accounting standards include two types of controls for auditing: 1) General controls that apply to all information technology activities, including managing information technology, developing alternative systems, physical and online security related to accessing hardware, software, and data, planning emergency backups, and controlling hardware. 2) Application controls that specifically operate at the business process. ensuring the security of the information obtained. Based on the above, the following hypothesis can be formulated:

H4b: Information technology control has a positive effect on data security.



Examination practice guidelines auditors involve conducting financial statement audits in accordance with the generally accepted accounting standards set by the professional accounting body. These standards on auditing encompass fundamental principles, important audit procedures, and various related practices. The financial statement audit by accountants involves examining accounting data and financial reports, such as balance sheets, income statements, cash flow statements, and notes to financial statements. The purpose is to assess whether the information presented is complete, reliable, and compliant with the established criteria. Auditors are responsible for financial statements auditing to express their opinion on the accuracy of the financial statements, adhering to the fundamental principles. (Federation of Accounting Professions, 2014).

Deficiencies in the auditing process, or audit risks, are risks of not detecting errors or misrepresentations of important financial information during the audit process. Audit risks are inherent in the structure of financial reporting and are related to complex calculations and transactions. (Saeidi, 2019). The risk of internal control refers to the risk of misrepresenting important and relevant information that internal controls fail to prevent, leading to the presentation of inaccurate or erroneous information in the reports. (Al-Shaer, 2020). Furthermore, the audit risk may also impact the effectiveness of financial reporting. The significance of audit risk lies in its influence on the accuracy and reliability of financial reports. High audit risk can lead to increased issues with the financial statements. (Riyadi et al., 2021). The research of Defond and Zhang (2014). Audit quality involves the examination of errors in financial statements and reporting errors, as well as building confidence in financial reporting for stakeholders, which arises from performing duties in accordance with accounting audit standards. Furthermore, Hermanson et al. (2000) emphasized the necessity of information technology auditing as it fosters data and information confidence by safeguarding information and reducing risks associated with technology usage. Strengthening effective controls can help reduce the risk of misstatements due to errors or fraud (Lorentzon, 2023).

Reducing audit risk

Reducing audit risk involves minimizing errors arising from events that need evaluation, which can be significant factors stemming from both internal and external aspects of an organization. Information technology auditing aids in mitigating risks during audits by ensuring data and technology security, along with guaranteeing the accuracy of financial reports to prevent distortion that might arise from information errors. This aligns with Karagiorgos et al. (2010) research, stating that reliable, comprehensive, and efficient data use instills confidence in making economic decisions. This, in turn, results in clear financial statements and plays a crucial role in financial report auditing. Efficient information assists the accountant auditors in accurately assessing risks, an essential aspect of creating accurate and supportive audit reports (Federation of Accounting Professions, 2014).

This perspective also aligns with Hurtt, R. K., (2011) research, indicating that the risk in accounting audits positively relates to the efficiency of the accounting audit process, specifically the sufficiency and appropriateness of audit evidence. Relying on observation and suspicion helps mitigate risks by avoiding overlooking suspicious situations or incorrect assumptions in evidence collection and assessment. Accountant auditors must emphasize observation and suspicion to reduce risks and support the preparation of quality accounting information beneficial to financial statement users (Al-Shaer, 2020). Moreover, audit risk can impact the efficiency of financial reporting. Lowering audit risk affects the accuracy and credibility of financial reports, ultimately influencing the effectiveness of accounting audits (Riyadi et al., 2021).

พหุน ปณ ฑิโต ชีเว

The audit will help reduce risk of data and enhance the efficiency of information. High-quality information will reduce audit risk in the accounting audit and contribute to the effectiveness of the audit process. (Hall, 2011). To enhance the information security and obtain high-quality information, it is essential to address the control of information input into the information system, the control of data processing, and the control of information output from the information system. These controls contribute to improving information security and increasing the efficiency of operations. By mitigating the risk of unauthorized access to the information system or information, these controls prevent data loss, damage, and misrepresentation. This study is based on the research conducted Hermanson et al. (2000) The activities of information technology control by information system auditors are essential for evaluating the risks associated with information technology. This helps instill confidence that an organization's data and information are protected and reduces the risks that may arise from the internal use of technology within the organization.

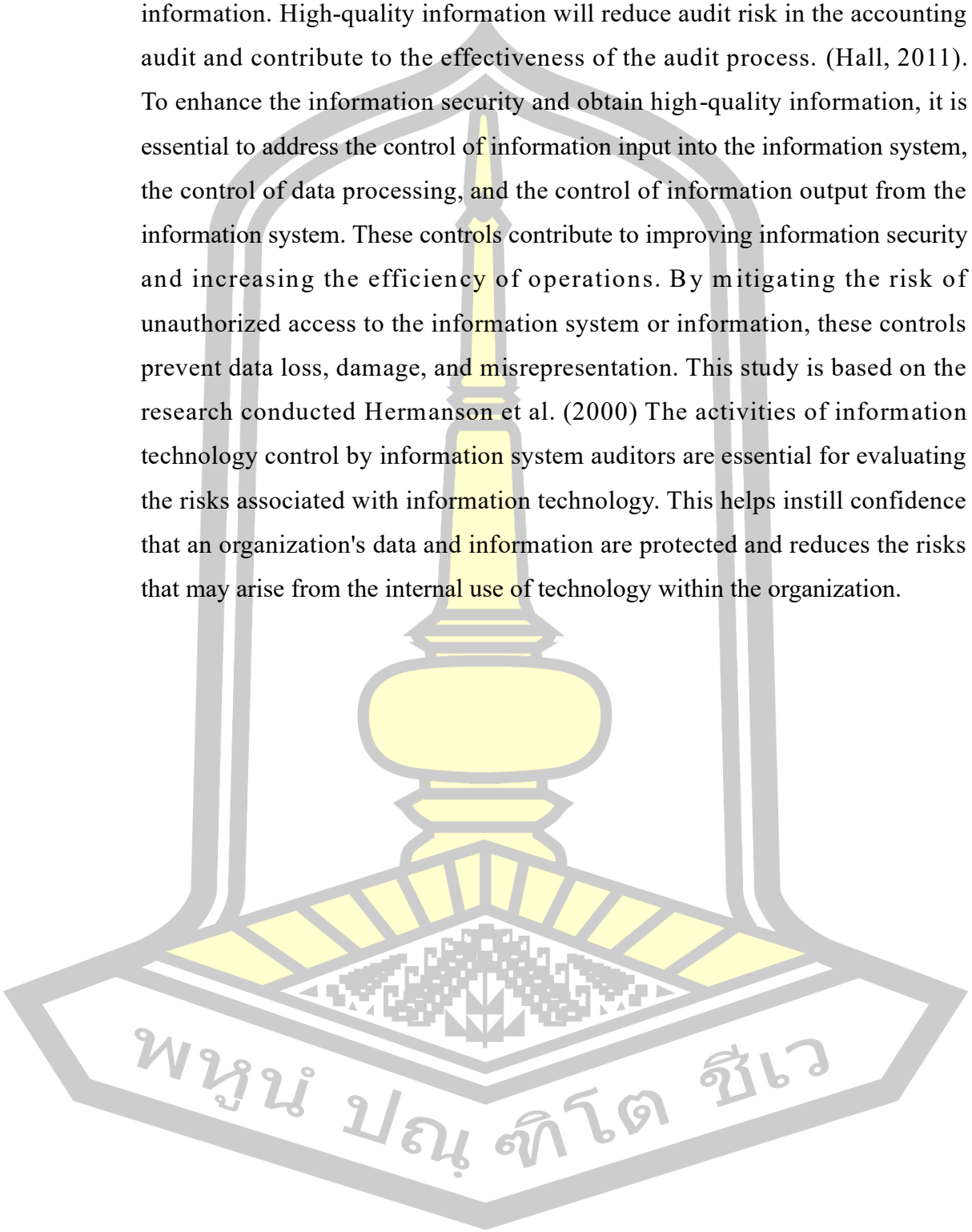


Table 3: Summary of key literature reviews on relationship between reducing audit risk and audit quality

Author(s)	Key Issue Examine	Finding
Nelson, (2009)	A Model and Literature Review of Professional Skepticism in Auditing.	Applying professional skepticism and thorough testing, auditors can lower detection risk, thus reducing overall audit risk and enhancing the credibility and quality of the audit report
Hurtt, R. K. (2010)	Examine the relationship between audit risk and audit quality, with a specific focus on the sufficiency and appropriateness of audit evidence.	Found a positive correlation between audit risk and audit quality concerning the sufficiency and appropriateness of audit evidence.
Francis, (2011)	A Framework for Understanding and Researching Audit Quality.	High audit risk increases the likelihood of undetected material misstatements, which can compromise audit quality. Conversely, reducing audit risk by thoroughly assessing and addressing these components results in more reliable and higher-quality audits.

Author(s)	Key Issue Examine	Finding
Arens, Elder, & Beasley, (2012)	Presentation of the auditing process, starting from understanding the client's business and industry to the final stages of audit completion and reporting. It covers each phase of the audit process in detail, including planning, evidence collection, and audit risk assessment.	Reducing audit risk can enhance the accuracy and reliability of the audit.
Knechel, (2013)	Examines whether adherence to established auditing standards contributes to better audit outcomes and whether these standards are effective in safeguarding the interests of stakeholders.	Analytical procedures and data analytics can help auditors identify unusual transactions and trends, reducing detection risk and enhancing audit quality.
Bell et al., (2015)	Relationship between audit firm tenure, the provision of non-audit services (NAS), and internal assessments of audit quality.	Effective audit planning, which includes a detailed risk assessment, is crucial in reducing audit risk. Auditors who invest time in planning and understanding client risks are better positioned to provide high-quality audits

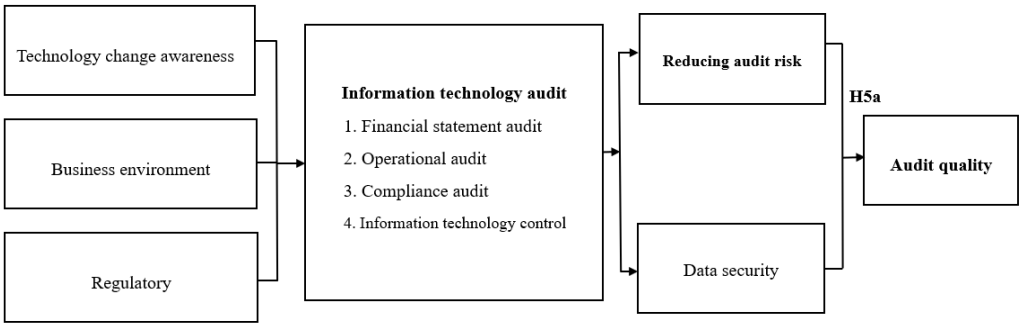
Author(s)	Key Issue Examine	Finding
Knechel et al., (2016)	Review of academic research on audit quality, synthesizing key insights and perspectives from various studies over time.	Studies have shown that reducing audit risk often requires increased audit effort, such as additional testing and review. This additional effort generally leads to more accurate and high-quality audit outcomes
Beridze, (2017)	Evolving digital transformation will automatically affect the role of IT audit. In the era of digital transformation, IT audit will become increasingly involved to ensure that IT implementation does not create unacceptable risks to the business.	Reducing audit risks helps ensure that the audit report is free from distortions caused by errors.
Al-Shaer, (2020)	Investigates the association between sustainability reporting quality and post-audit financial reporting quality.	Audit risk can impact the effectiveness of financial reporting.
Riyadi et al., (2021)	Determine the direct and indirect effect of the variable competence of human resources, job relevant information and financial planning on the quality of financial reports as well as through information technology.	Reducing audit risk can enhance the accuracy and reliability of financial reporting, resulting in more effective auditing.

From the above synthesis, it was found that reducing audit risk can positively affect audit quality. When audit risks are minimized, the likelihood of detecting material misstatements increases, leading to more accurate, reliable, and comprehensive audit outcomes. This, in turn, enhances the overall quality of the audit.

Clearly, information technology auditing continues to play a crucial role in maintaining data security, data integrity, and fraud prevention within information systems. Additionally, information technology auditing provides appropriate recommendations for risk prevention (Beridze, 2017). This means that information technology auditing helps reduce audit risks from the use of information technology and ensures the security of data and information technology. Furthermore, it ensures that audit reports are free from distortion caused by errors due to auditors receiving adequate information, thereby reducing audit risk. This allows auditors to draw reasonable conclusions to support their opinions (Federation of Accounting Professions, 2014).

This is consistent with the research by Hurtt, R. K. (2011), which found a positive correlation between audit risk and audit quality concerning the sufficiency and appropriateness of audit evidence. The use of professional judgment and skepticism by auditors helps reduce the risk of overlooking suspicious situations or using erroneous assumptions in evidence collection and assessment. Auditors must emphasize the importance of observation and suspicion regarding professionals to be a tool for producing quality accounting information beneficial to financial statement users (AlShaer, 2020). Furthermore, audit risk can impact the effectiveness of financial reporting. Reducing audit risk can, in turn, affect the accuracy and reliability of financial reporting, leading to more efficient audits (Riyadi et al., 2021). This leads to the formulation of the following hypotheses.

H5a: Reducing audit risk has a positive effect on audit quality.



Data security

Data security involves overseeing and ensuring the safety of data to prevent risks or unauthorized actions by users, such as threats or cyberattacks. These risks jeopardize the security, accuracy, and reliability of information. Significant changes in information technology, environmental changes in internal controls, and auditing result in an unavoidable information technology revolution. These changes stimulate the need for timely, relevant, valuable, aligned, and accurate information, enhancing information technology reliance (Kayrak, 2012).

In recent years, the growing demand for examining and maintaining information security has escalated. Trustworthy and sufficiently appropriate information consideration supports accountant auditors in forming opinions and using judgment to observe and suspiciously consider professionals' actions, thus reducing the risk of overlooking doubtful situations or incorrect assumptions during evidence collection and audit assessment (Petter Lovaas, 2012).

Therefore, auditing information technology is an essential process that ensures accurate and credible information. This, in turn, empowers accountant auditors to perform their auditing tasks more effectively.

Table 4: Summary of key literature reviews on relationship between data security and audit quality

Author(s)	Key Issue Examine	Finding
Bagchi, (2006)	The intersection of information technology and auditing, examining how advances in it affect the audit process.	Regular security audits mitigate the risk of data breaches and improve the quality of financial reporting and auditing outcomes.
Majdalawieh & Zaghloul, (2009)	Explore the role of IT auditing in enhancing corporate governance and organizational performance.	Assessing Data Security: The literature highlights that auditors must assess an organization's data security practices as part of their audit planning process. This assessment can influence the auditor's evaluation of the overall risk of material misstatement.
Hall, (2011)	Information technology auditing and assurance.	Adequate data security controls reduce the risk of unauthorized access, data tampering, and fraud. This ensures the integrity of the financial data being audited, leading to higher audit quality.
Gantz, (2014)	The basics of it audit.	Data security controls reduce the risk. This ensures the integrity of the financial data being audited, leading to higher audit quality.

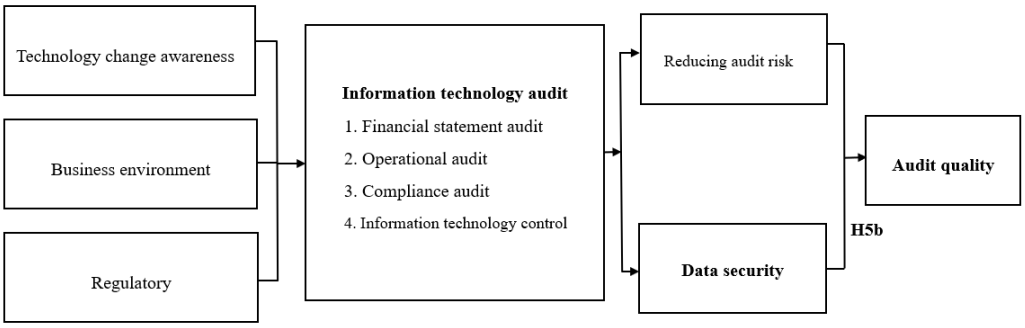
Author(s)	Key Issue Examine	Finding
Krahel & Vasarhelyi, (2014)	Discuss the current state and future of auditing. Expert consensus is used as a basis to examine the current state of auditing and generate modifications both needed and likely to occur in the audit profession.	Robust data security measures enhance the reliability of financial data used in audits. When data is secure, auditors can have greater confidence in the integrity of the information being audited, leading to higher audit quality.
Beridze., (2017)	Evolving digital transformation will automatically affect the role of IT audit. In the era of digital transformation, IT audit will become increasingly involved to ensure that IT implementation does not create unacceptable risks to the business.	The new auditing strategy identifies information security, data integrity, and fraud risks in information systems and offers the appropriate prevention suggestions, as well as enhancing the scope of the audit using this innovative audit strategy

Author(s)	Key Issue Examine	Finding
Rosati et al., (2020)	Determine the direct and indirect effect of the variable competence of human resources, job relevant information and financial planning on the quality of financial reports as well as through information technology.	Data security measures help auditors reduce inherent and control risks. By ensuring data integrity, auditors can focus more on substantive testing and analysis, which improves the audit's thoroughness and accuracy
Schroeder et al., (2021)	Discuss how effective data security practices play a critical role in minimizing risks related to data breaches and fraud, both of which can lead to material misstatements in financial reporting.	Effective data security practices help minimize risks associated with data breaches and fraud, which can lead to material misstatements. A secure environment allows auditors to focus on substantive testing rather than spending time investigating potential data compromises

The literature highlights a significant relationship between data security and audit quality, emphasizing that robust data security measures enhance the reliability of financial data and minimize risks of material misstatements. Effective IT controls play a crucial role in this relationship, contributing to overall audit quality. As organizations face evolving cybersecurity threats, the integration of data security practices into the audit process will be vital for ensuring high-quality audits.

Therefore, examination ensures accurate and reliable information. This helps auditors perform their audit tasks more efficiently since considering credible and appropriate information enables them to express opinions and use professional judgment in observing and suspecting professionals suitably. This, in turn, reduces the risk of overlooking suspicious situations or erroneous assumptions in evidence collection and audit assessments (Petter Lovaas, 2012). Some studies suggest that heavy reliance on automated data security controls can give a false sense of security, leading auditors to overlook other essential audit procedures (Rashid et al., 2018). For example, overly automated data security processes may lead auditors to trust the system's accuracy and reliability without sufficient verification, which could compromise audit quality if issues go undetected (Zhou & Kapoor, 2011). Nonetheless, Chen et al. (2018) found that strict information security practices positively promote audit quality by protecting data integrity and reducing the risk of data breach or alteration. Information security measures enable auditors to work with reliable and unaltered data, resulting in more accurate audit results and reliable conclusions. Additionally, Rose et al. (2017) suggest that enhanced data security facilitates a smoother audit process by reducing disruptions associated with data inconsistencies or security incidents. Based on the above discussion, the following hypotheses can be formulated:

H5b: Data security has a positive effect on audit quality.



Audit quality

Audit quality is of paramount importance in the audit process, as high-quality audits lead to improved decision-making for stakeholders, as stated by DeAngelo (1981). The quality of accounting audits encompasses various dimensions such as reliability, responsiveness, assurance, diligence, and detectability. If auditors can incorporate these dimensions into their practice, the likelihood of achieving better audit quality increases. Additionally, Arens and colleagues (2015) define audit quality as the probability that auditors detect and report on violations in clients' accounting systems in accordance with professional ethics (New York State Society of Certified Public Accountants, 2013). Principles to be followed in achieving audit quality include honesty, fairness, professional care, competence, confidentiality, and independence.

Discussion and audit quality depends on the perspectives of various stakeholders, such as users, auditors, regulatory agencies, and society. All parties involved in the financial reporting process may have different views on the indicators of audit quality. Financial report users may believe that audit quality involves presenting information that is not materially misstated, while auditors may define audit quality as adhering to all procedures set forth in the satisfactory audit methodology of their office. Regulatory agencies may consider audit quality as compliance with professional standards and the ability to detect and report errors or irregularities in clients' accounting systems. Therefore, ensuring audit quality requires competent and independent

individuals (Tandiontong, 2016). Following international standards on quality control (ISQC), firms and their personnel must ensure compliance with professional standards and laws to instill confidence in the auditing process.

In the following section of the article, we will examine the components in the content that determine audit quality. According to DeAngelo (1981), the concept of audit quality refers to "the joint probability assessed by the market that the auditor will (a) discover a breach in the client's accounting system and (b) report the breach." In this definition, audit quality depends on the skills of the auditor in detecting misstatements in the accounting records and the independence of the auditor.

From the literature review and related research, it is evident that audit quality is an assessment of the auditor's ability to detect existing inaccuracies and appropriately address the identified issues. Therefore, in this study, we have reviewed and interpreted the previous documents and research works accordingly.

Definition of audit quality

Based on the literature review and previous research, the term "Audit quality" is defined as the evaluation and verification of the accuracy and appropriateness of accounting data and financial reporting during an audit. This definition encompasses the ability to detect accounting errors and instill confidence in the accounting data and financial reports presented to relevant stakeholders (Arens et al., 2015). In addition, there are research studies that provide further insights into the meaning of "Audit quality," as follows:

พหุน ปณ ฑิโต ชีเว

Table 5: Summary the definition of audit quality.

Source(s)	Definition
DeAngelo (1981)	Provided a comprehensive perspective on audit quality by defining it as the joint probability that auditors will (a) discover violations in the client's accounting system and (b) report those violations. This definition highlights the importance of auditors' skills in detecting misrepresentations in accounting data and their independence in performing their duties effectively.
Palmrose (1988)	Audit quality refers to the level of assurance that provides confidence in financial statements.
Bradshaw et al., (2001)	Error detection includes identifying significant errors and continuous process improvement issues.
Francis (2011)	The alignment of the audit data and processes with the actual financial reporting.
Knechel et al., (2013)	Audit quality can be assessed through four categories: input data, processes, outcomes, and context.
Okolie (2014)	Financial statements are free from any material misstatements and presented accurately and completely to provide useful information to the users. Therefore, if a professional performs substandard work, fails to apply their knowledge and skills fully, or overlooks detected errors, Audit quality can lead to financial reports with errors and negatively impact the reliability of the professional's work.
Taylor (2015)	Audit quality refers to the adherence to accounting standards, accurate audit reporting, and the reporting of material misstatements in financial statements.

Table 5: Summary the definition of audit quality (continue).

Source(s)	Definition
Denise et al., (2018)	Audit quality refers to the quality of the audit process, which can be achieved through various methods of obtaining evidence to report by auditors. The reporting must not contradict the truth, be comprehensive, and comply with legal requirements.
Manita et al. (2020)	Audit quality also entails identifying differences in financial statements and disclosing them to the stakeholders by the auditors.

Based on the meaning, the expression of opinions by certified accountants that are consistent with relevant facts and comply with accounting standards, based on accurate, reliable, complete, and up-to-date information on financial reports are the responsibilities of auditors. Performing these tasks in an environment conducive to financial reporting will enhance the quality of the auditing process.

To promote audit quality, various components have been identified, which can be summarized as follows: (International Federation of Accountants, 2014).

1. Input factors: the audit team must be aware of conducting their work in accordance with professional ethics and the skills required for the auditing process. These factors including independence, professional competence, and appropriate supervision contribute to a comprehensive and effective audit process. Effective oversight that creates an appropriate.

2. Process: the auditing of financial statements must adhere to accounting standards, relevant regulations, and controls for quality. These factors include compliance with accounting standards, laws, and related regulations, and the quality control procedures of the audit firm. They appropriately utilize information technology.

3. Output: stakeholders receive different information from the audit. Auditors provide confidence in financial statements to users, reports to those responsible for governance, and communications to external oversight bodies.

These factors include reports on audited financial statements to users, reports to those in charge of oversight, reports to management, and reports to financial and legal authorities. From the entity: Audited financial statements, reports from those responsible for governance, including audit committee.

4. Contextual factors: various environmental factors influence audit quality, such as business and relevant legal practices, relationships, and characteristics of different parties involved, including auditors, management, oversight personnel, and oversight bodies during the audit process. The impact of financial reporting frameworks and business governance on the quality of financial reporting is also considered during the audit

Auditors who adhere to professional standards and relevant legal requirements, including issuing reports that are appropriate for the circumstances, contribute to the audit quality. This, in turn, instills confidence in financial report users and stakeholders, making the accounting profession widely accept and helping to mitigate the risk of errors arising from the audit process. Such errors could potentially harm the capital markets and the overall economy.

The technological environment, with its potential threats to accuracy, data security, and stakeholders' trust, poses risks that need to be addressed. The role of information technology auditing is crucial in reducing vulnerabilities and technological threats. By doing so, it ensures the delivery of accurate information and enhances the credibility of information (Riad, 2015).

The role of information technology auditing is crucial in reducing vulnerabilities and technological threats. If there is effective governance and control of information technology, accurate and secure information will foster confidence and reduce errors resulting from inappropriate decision-making, which contributes to the enhancement of the audit quality (The Securities and Exchange Commission, Thailand, 2022). However, information technology auditing needs to get influence from technology change awareness, business environment, and regulatory as antecedent variables.

Table 6: Summary of key literature reviews on the relationship between technology change awareness, business environment, regulatory and information technology audit

Author(s)	Key Issue Examine	Finding
Fargher & Jiang, (2008)	Discuss the challenges posed by dynamic business contexts on audit quality.	Auditing firms must consider the increasingly complex and dynamic business environments, influenced by globalization, market volatility, and technological disruption. This affects audit quality by increasing the complexity of transactions and the scope of risks that auditors need to manage
Francis (2011)	A framework for understanding and researching audit quality.	Discussed how the dynamic nature of modern business environments demands an increased focus on risk assessment to maintain audit quality.
Knechel et al., (2012)	Challenges faced by auditors in different industries particularly highlight the impact of technological advancements on audit practices.	The business environment varies across industries, and technological changes bring sector-specific risks. For example, auditing in the tech sector involves more complex IT systems, requiring auditors to have a higher level of technological proficiency.

Author(s)	Key Issue Examine	Finding
Kuenkaikaew & Vasarhelyi, (2013)	Emphasize the importance of continuous learning and education for auditors in the context of rapidly evolving technologies and business environments shaped by digital transformation.	Continuous education on emerging technologies improves auditors' effectiveness, ensuring they can address complex business environments shaped by digital transformation.
DeFond and Zhang (2014)	Explore how client characteristics significantly influence audit procedures, particularly in the context of businesses experiencing rapid technological changes or operating within highly regulated environments.	Reviewed regulatory frameworks, noting that stricter regulation tends to enhance audit quality but may also increase costs.

Author(s)	Key Issue Examine	Finding
Issa, Sun, & Vasarhelyi, (2016)	Highlight the critical importance of technological awareness for auditors in the context of the growing integration of automation tools in financial statement audits.	Awareness of emerging technologies is critical. However, without proper training and adaptation, the benefits of technology may not be fully realized, leading to risks like over-reliance on automated systems
Appelbaum et al. (2017)	Underscores several key benefits associated with the use of data analytics in financial statement audits.	Discussed how big data analytics enhances the efficiency of audits by allowing for better risk assessment and fraud detection.
Dai & Vasarhelyi, (2017)	Integration of artificial intelligence (AI) and robotic process automation (RPA) in audit procedures.	This technological change improves the efficiency of audits, but auditors must remain aware of the associated risks and regulatory concerns, such as ensuring algorithm transparency and compliance with automated decision-making regulations.

Author(s)	Key Issue Examine	Finding
Rozario & Thomas, (2019)	Examine the challenges IT auditors face considering rapid technological advancements, particularly focusing on emerging technologies	Technological advancements often precede regulatory frameworks, meaning IT auditors must be proactive in understanding how emerging technologies will be regulated. For example, blockchain technology, though not yet comprehensively regulated, poses challenges for auditors who must ensure the integrity of blockchain-based transactions while anticipating future regulations
Eilifsen et al., (2020)	Discuss the challenges auditors face due to frequent regulatory changes, particularly those related to technology.	Frequent regulatory changes, particularly those regarding technology (e.g., data privacy regulations like GDPR), present challenges for auditors, as they must stay current with evolving rules. This directly impacts audit quality, as a lack of compliance could lead to penalties or failed audits
Lopez & Peters, (2021)	Explore the complexities of the business environment in highly competitive industries, particularly regarding the role of IT audits.	In highly competitive industries with extensive IT infrastructures, IT audits focus not only on compliance but also on risk management. IT auditors must ensure that companies' systems are not only regulatory-compliant but also secure from the growing number of cyber threats.

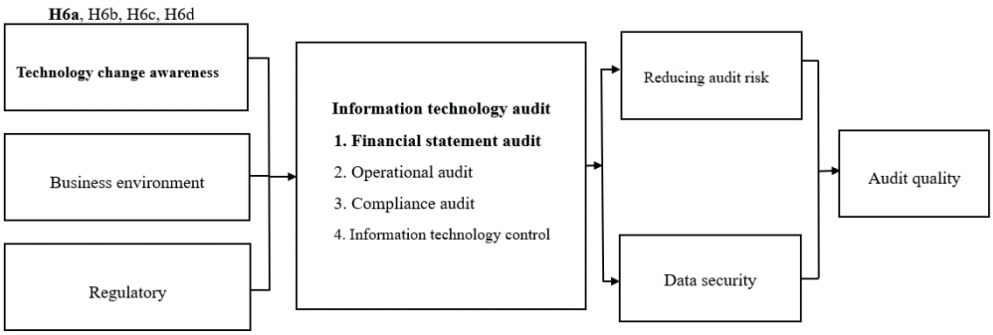
Based on the above synthesis, the factors that impact information technology audit include technology change awareness, business environment, and regulatory.

Technology change awareness

Technology change awareness refers to accept information technology and recognizing its advantages in efficiently applying technology. The constant technological changes and expansion of information technology necessitate swift and cost-effective access to detailed and beneficial data. The trend of incorporating new technology is crucial within organizations, adapting it to various conditions, necessities, and requirements. The significance of information technology and its advancements are vital factors for progress and development in today's world (Badavar Nahandy, 2011).

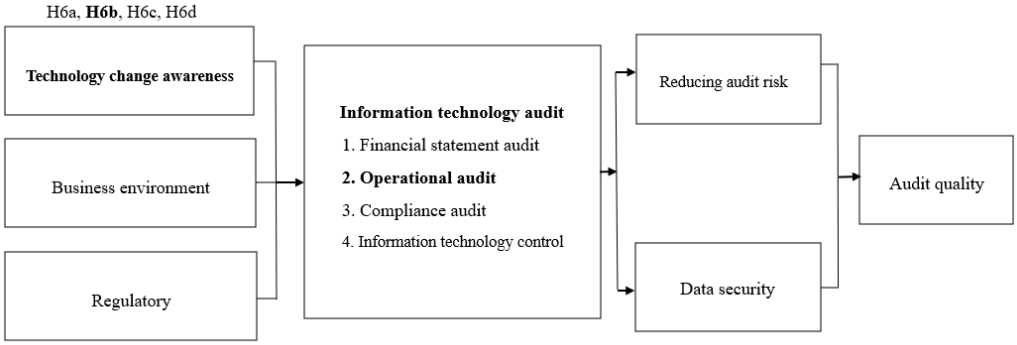
Information technology leads to transformations and diverse capabilities in the work environment, enabling high-speed data processing, real-time access, and contemporary electronic data exchange. Furthermore, it provides high-quality data at a low cost. These characteristics contribute to the growing significance of information technology, as it reduces work time, enhances the ability to test large amounts of data, mitigates audit risks, and yields flexible analytical information, along with more comprehensive data. These factors result in the improvement of audit processes (Liana Elefterie, 2016). Based on the above discussion, the following hypotheses can be formulated:

H6a: Technological change awareness have a positive effect on financial statement audit.



The increased use of information technology necessitates auditing resources or auditing technological risks to prevent errors or deficiencies that could lead to inaccurate data presentation. This requires accountant auditors to understand the information system to plan, command, control, monitor, and verify operations (Singleton J. A., 2005). From the text, the following assumptions can be made:

H6b: Technological change awareness have a positive effect on operational audit.

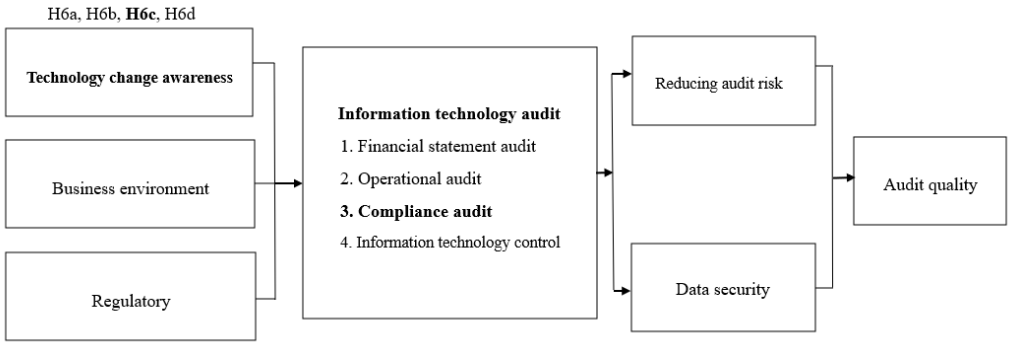


Information technology brings numerous benefits, but it also entails associated risks. For instance, computer assets may be lost or stolen, and the likelihood of fraud increases. Incorrect usage of technology can lead to losses in competitive advantage. Data can be lost or stolen, privacy may be violated, and businesses may experience interruptions due to the risks. Consequently, it is essential to control the security of technology and protect sensitive data (Okereafor, 2008).

Therefore, continuous monitoring to respond to preventive measures is necessary to address the risks and benefits related to information technology, such as (1) cybercrimes targeting individuals or groups seeking financial gain from the system, (2) cyber-attacks often interconnected to political motives for data gathering, and (3) cyber-terrorism aiming to cause harm to electronic systems. Implementing and managing information technology projects, supervising information technology, and security management systems are

necessary to ensure compliance with laws and regulations (Santy Setiawan, 2020). Based on the above text, the following assumptions can be made:

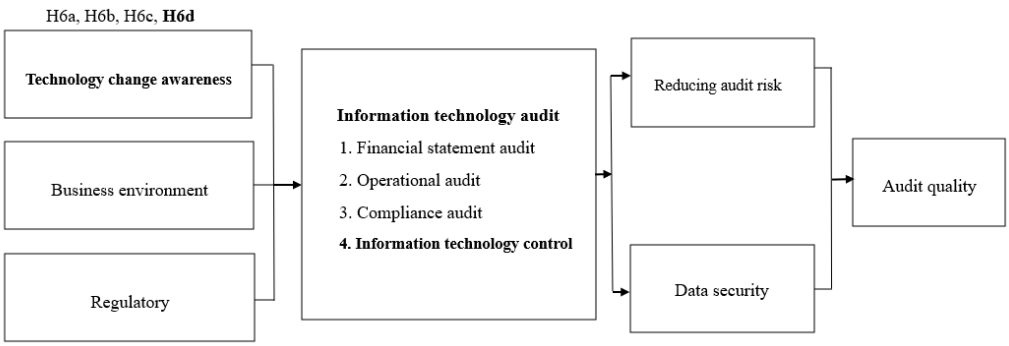
H6C: Technological change awareness have a positive effect on compliance audit.



Therefore, the audit of information technology focuses on the information system of the technology. This type of audit is related to evaluating usage, operations, and controlling the sources of information to safeguard the integrity of data (Singleton J. A., 2005).

The standards on auditing regarding the audit of information technology encompass two types of controls for examination: 1) General controls, which apply to all aspects of information technology, including information technology management, alternative system development, physical and online security related to hardware, software, and data access, contingency and emergency backup planning, and hardware controls; and 2) Application controls, which specifically address business process-level operations and their use in business transactions, such as control between sales processes (Federation of Accounting Professions, 2014).

H6d: Technological change awareness have a positive effect on information technology control.



Business environment

Business environment refers to various forces that impact business operations positively or negatively. It results in operational changes, similar to the growth of information technology which demands modifications in the work environment. Information technology reduces work time, increases the ability to test a large volume of data, examines larger data samples in more detail, and consequently enables auditors to better understand and test various issues within data. It also reduces audit risks and provides more flexible and comprehensive analytical information (Liana Elefterie, 2016). With the increasing use of technology, risks should not escalate to a point where companies can't handle them. The information technology of each organization needs assessment and management due to current technological risks (Devale, 2012). Relying on technology's increased presence stems from a changing environment.

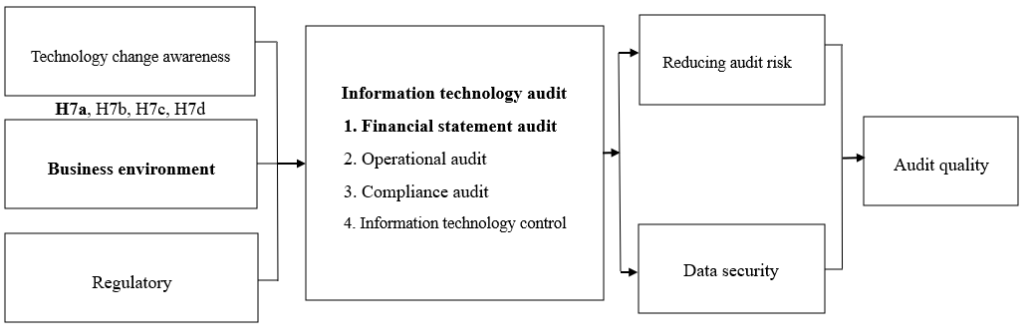
Research by Eilfsen et al. (2020) suggests that environmental pressures play a crucial role in the use of information technology across various companies. This has turned information technology into a tool for modern business. The continuous growth of information technology triggers the development of information technology-related threats, leading to operational disruptions and errors. Thus, auditing information technology becomes significant to mitigate vulnerabilities and the increasing threats. This helps ensure compliance with regulations, efficient data processing, reporting, and enhances data reliability.

According to Betti and Sarens (2020), when the environment changes, customer expectations also change, resulting in changes to business methods and operations. These changes must consider the increasing importance of technology and information, which are essential for individuals, industries, and governments (Mark Muro, 2017).

The audit has evolved and adapted to the changing business environment and auditing processes. It is understood that the use of tools and technology significantly impacts financial reporting. Additionally, the accounting profession has been influenced by changes in audit methods, examination processes, and professional development, which are considered necessary characteristics of the

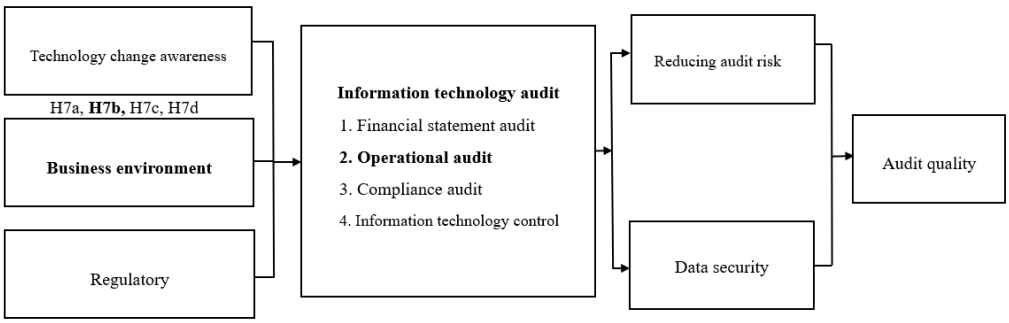
profession (Federation of Accounting Professions, 2014). Based on the above information, the following assumptions can be made:

H7a: Business environment have a positive effect on financial statement audit.



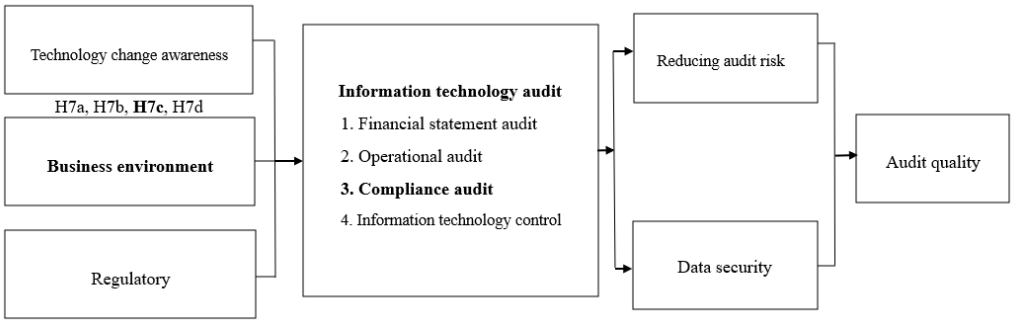
The business environment plays a critical role in how companies manage risks, which is a central focus of operational audits. Auditors must assess whether a company's risk management strategies align with the external environment and can address potential threats. As businesses adopt new technologies, the processes and risks evolve. Auditors must ensure that their scope includes a thorough examination of technology-related risks, such as system failures or data breaches, while also evaluating how technology enhances operational efficiency (Gepp et al., 2018). Based on the above information, the following assumptions can be made:

H7b: Business environment have a positive effect on operational audit.



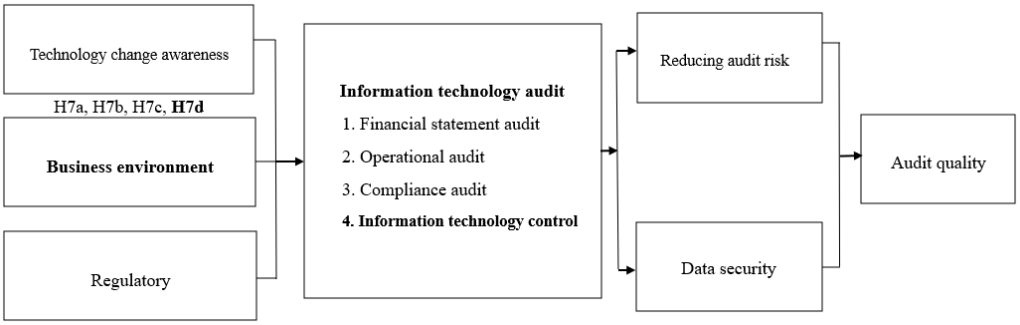
Increasing risks to the point where they become unmanageable. The information technology of each organization must be assessed and managed since there are currently risks arising from technological threats (Devale, 2012). Therefore, Operational audits must account for the ability of a company's operations to adapt to rapid changes in the business environment. Auditors need to evaluate whether internal processes are flexible and scalable to meet the demands of a changing market (Krahel & Vasarhelyi, 2014). Based on the above information, the following assumptions can be made:

H7C: Business environment have a positive effect on compliance audit.



The reliance on advanced information technology is influenced by the changing environment. Research by Eilfsen et al. (2020) states that environmental pressures play a crucial role in the adoption of information technology by various companies, turning information technology into a tool for modern business. The continuous growth of information technology leads to the emergence of evolving technological threats, which cause operational disruptions and errors. Therefore, the audit of information technology becomes essential to mitigate vulnerabilities and threats related to the increasing information technology risks. This will help ensure compliance with regulations and guidelines, efficient data processing, reporting, and enhance data credibility. Based on the above information, the following assumptions can be made:

H7d: Business environment have a positive effect on information technology control.



Regulatory

Regulatory refers to guidelines or operational approaches that establish uniform standards to ensure efficiency and mitigate risks. Increased regulations focus on privacy, cybersecurity, flexibility, and essential technology platforms, adding complexity to businesses across all industries. The digital transformation mentioned earlier helps companies adapt to the requirements of new customers (Hilali et al., 2020).

In Thailand, there's an increasing emphasis on developing and utilizing technology to drive national progress and reshape service delivery. This involves using digital data and technology-driven service systems to enforce effective governance and control. However, using technology also entails risks that need to be managed. To address this, there's a need for comprehensive management and security measures. Technology audits are conducted with applied standards as a framework for overseeing technology, such as ISO 27001, which is used to manage information security. Additionally, COBIT is used as a framework for managing technology risks and ensuring the security of information technology. These standards enhance data security, reduce risks, and protect data from being compromised (The Securities and Exchange Commission, Thailand, 2019).

Thus, a control framework that fits the present scenario is required. Technology audits encompass financial audits, operational audits, compliance audits, and Information technology control audits. Technology audits involve the application of standards as a framework for overseeing technology, such as

ISO 27001, used to manage information security. Furthermore, COBIT, a widely accept framework for managing technology risks, is applied to control and maintain information technology security. This promotes confidence and trust in using information technology, enhances the credibility of processed and stored data, and aids efficient accounting work (Riad, 2015). Reliable and secure information contributes to the effectiveness of accountants' work.

Factors driving the need for Information technology audit services include the adoption of new regulations and professional requirements and the use of Information technology in relevant organizational operations. This is due to concerns related to the Information technology audit, such as confidentiality, security, integrity, availability, and credibility of data in computers and other processing systems. Therefore, accounting professionals must provide additional guidance for Information technology audits, as well as financial audits to prevent non-compliance with laws and regulations. Though audits are planned and executed with appropriate procedures, the outcome of non-compliance with laws and regulations may lead to the presentation of conflicting essential facts. Therefore, auditors should understand laws and regulations that can be applied in planning and executing the work framework (Federation of Accounting Professions, 2010).

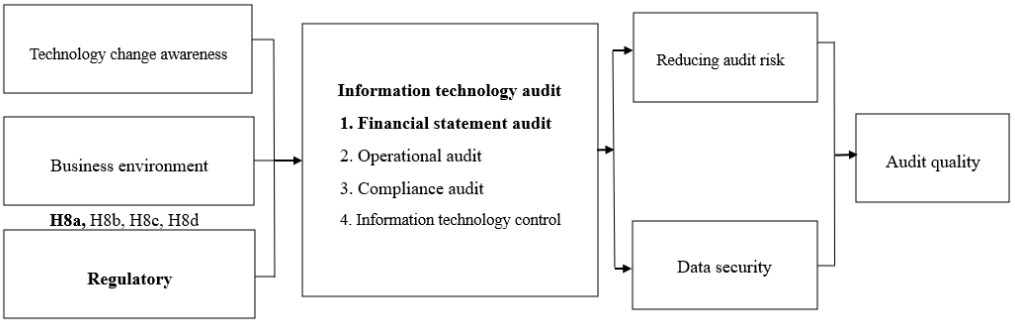
The increased regulations aim to emphasize privacy, cybersecurity, flexibility, and necessary technological platforms, which add complexity to businesses across industries. The mentioned digital transformations enable companies to meet evolving customer demands (Hilali et al., 2020).

Havelka and Merhout (2012) refer to two main factors that drive the increased demand for information technology audit services. The first factor is new regulations and professional requirements, and the second factor is the use of information technology in the operations of information technology audited organizations. Due to concerns related to information technology auditing, such as confidentiality, security, integrity, availability, and reliability of computer and other processing systems, it is essential for information technology audit professionals to provide additional guidance for information technology audit in this environment (Guan, 2004).

Reputable organizations such as the American Institute of Certified Public Accountants (AICPA) and the International Federation of Accountants (IFAC) have published guidance for accountants in this area. The importance of providing efficient audit services is highlighted due to the increasing demand for information technology audit and new regulations. International standards such as information technology Assurance with COBIT, information technology Assurance Framework, Risk information technology Framework, or ISO, as well as accounting standards, require auditors to understand information technology to plan, control, assess risks, and information technology audit related work appropriately to meet standards, ensuring that the use of information technology is appropriate and secure according to the established criteria (Federation of Accounting Professions, 2019).

Financial audits help to curb non-compliance with laws and regulations. Even though audits are planned and performed properly, the risk of non-compliance cannot be eliminated. Non-compliance with laws and regulations can lead to the presentation of material misstatements, just as operational audits can. Therefore, auditors should understand the laws and regulations that can be used to plan the operational audit framework (Federation of Accounting Professions, 2010). Based on the above information, the following assumptions can be made:

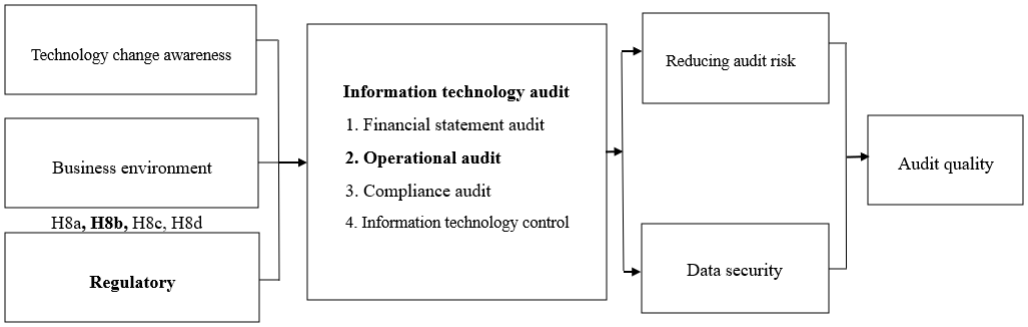
H8a: Regulatory have a positive effect on financial statement audit.



As the regulatory landscape continues to evolve, auditors must stay informed about emerging trends and challenges to ensure their audits remain relevant and effective. The integration of compliance and operational audits,

along with a focus on risk management, will be key in addressing the complexities of regulatory compliance and operational efficiency. Changes in regulations can significantly influence operational auditing processes. Auditors must continuously adapt their methodologies to align with evolving regulatory requirements, ensuring that the audit process remains relevant and effective (Wang & Huang, 2020). Based on the above information, the following assumptions can be made:

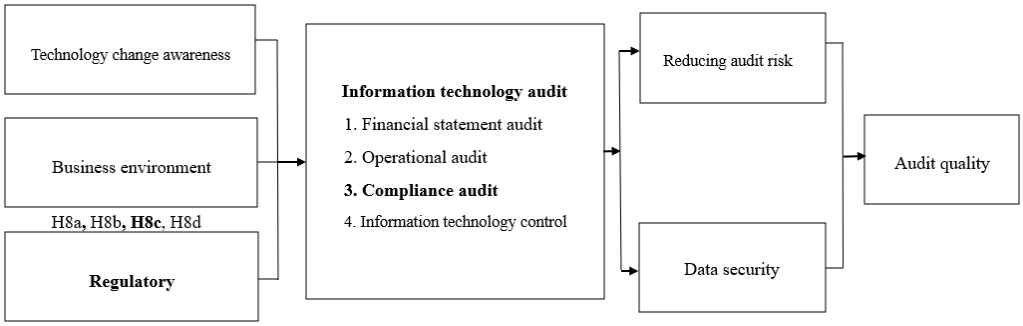
H8b: Regulatory have a positive effect on operational audit.



According to Tarantino (2009), the main perspective of technology auditing is to provide assurance and governance oversight and risk management. However, it is essential to understand that the role of information technology audit management goes beyond this. ISO 27001 states that applying standards for information security management helps strengthen the security systems, reduce risks, and protect data from unauthorized access. Similarly, COBIT standards are used to control and maintain the security of information technology, instilling confidence and trust in the use of information technology and enhancing the trustworthiness of data processed and stored within the information system (Riad, 2015).

The role of information technology auditing is crucial for the success of an organization. Currently, providing guidance on technology control issues related to business processes helps promote work and development policies necessary to ensure data assurance. It also helps to reduce vulnerabilities in information technology. Based on the above information, the following assumptions can be made:

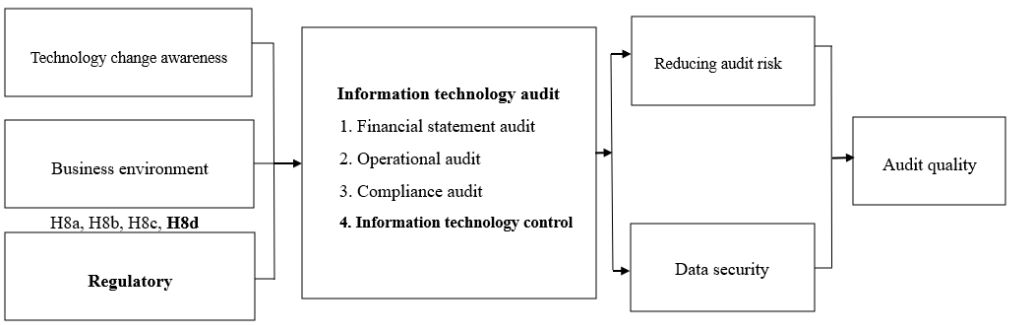
H8C: Regulatory have a positive effect on compliance audit.



The increased regulations aim to emphasize privacy, cybersecurity, flexibility, and necessary technological platforms, which add complexity to businesses across industries. The mentioned digital transformations enable companies to meet evolving customer demands (Hilali et al., 2020).

Havelka and Merhout (2012) refer to two main factors that drive the increased demand for information technology audit services. The first factor is new regulations and professional requirements, and the second factor is the use of information technology in the operations of information technology audited organizations. Due to concerns related to information technology auditing, such as confidentiality, security, integrity, availability, and reliability of computer and other processing systems, it is essential for information technology audit professionals to provide additional guidance for information technology audit in this environment (Guan, 2004). Based on the above information, the following assumptions can be made:

H8d: Regulatory have a positive effect on information technology control.



Auditing skill

The auditor is responsible for providing an independent opinion on the accuracy of financial reports based on their expertise. According to research by Bonner & Pennington (1991) and Libby & Luft (1993), experienced auditors are better able to assess relevant information and disregard irrelevant information. Nowadays, the development of information technology has a significant impact on information, and various processes are integrated with information technology due to increasing reliance on it. In this changing environment, information technology auditing has become essential for reducing vulnerabilities and increasing information technology threats. This helps ensure compliance with regulations and standards, enhances information processing and reporting efficiency, and increases the reliability of information. Therefore, it is necessary for the auditing profession to provide additional guidance on information technology auditing (Guan, 2004). Reputable organizations such as the American Institute of Certified Public Accountants (AICPA) and the International Federation of Accountants (IFAC) have emphasized the importance of effective auditing services in response to the growing demand for information technology audits and new regulations. International security standards are being adopted as a framework for information technology governance, and auditors are required to understand information technology to plan, supervise, assess risks, and review their work for appropriateness and compliance with standards. This has led to an expanded scope of work for auditors in evaluating information technology to ensure its appropriate and secure use according to established standards (The Federation of Accounting Professions under the Royal Patronage, 2019). International Standards on Auditing (ISA) emphasize that the objective of auditors should ensure financial reports are free from material misstatements caused by errors or fraud (misrepresentation). The effectiveness of auditing relies on individuals with relevant qualifications and independence, who can correctly and efficiently understand and execute auditing procedures. Currently, extensive research indicates that finding suitable personnel with the required skills remains a significant challenge. Observational research on the audit quality performed by

auditors and the technology of auditing has shown a positive correlation between the skills and expertise of the auditors and the quality and reliability of the audits (Carcello and Nagy, 2004; Gul et al., 2013; Sari, 2018) and research by Muhamad (2017) indicated that auditing skills significantly influence technology audits with a supporting influence of 54.7%. This highlights the importance of professional accounting skills for technology auditing, ensuring accurate and precise results.

Currently, auditors must use their expertise and knowledge in various areas of auditing to ensure the accuracy of financial reports (Bita Mashayekhi, 2018). The International Standards on Auditing (ISA) emphasize that the auditor's objective is to ensure that financial reports are free from material misstatements, whether due to error or fraud. This must be done independently to maintain high-quality audits. Numerous studies show that having the right personnel with the appropriate skills for the job remains a significant challenge. Extensive empirical research on audit quality reveals that the skills and expertise of auditors are crucial for audit quality and reliability, with a positive correlation (Carcello and Nagy, 2004; Gul et al., 2013; Sari, 2018). Additionally, Muhamad's (2017) research indicates that auditing skills significantly influence information technology auditing, supporting it by 54.7%. This suggests that professional auditing skills are necessary for effective, accurate, and precise information technology audits. In the present day, the application of information technology in managing large volumes of data enhances operational efficiency and impacts the information used in auditing. Appropriate, reliable, and accurate information contributes to the quality of audits. Conversely, incomplete or erroneous information can hinder the audit process (The Federation of Accounting Professions under the Royal Patronage, 2014). Good governance and control of information technology ensure accuracy, security, and trust in information, reduce errors, and improve decision-making, all of which enhance audit quality (The Securities and Exchange Commission, 2022).

Therefore, auditors need to have auditing skills to ensure the quality of their audits. Highly capable auditors gain their abilities through work experience, which enables them to conduct audits thoroughly, accurately, and

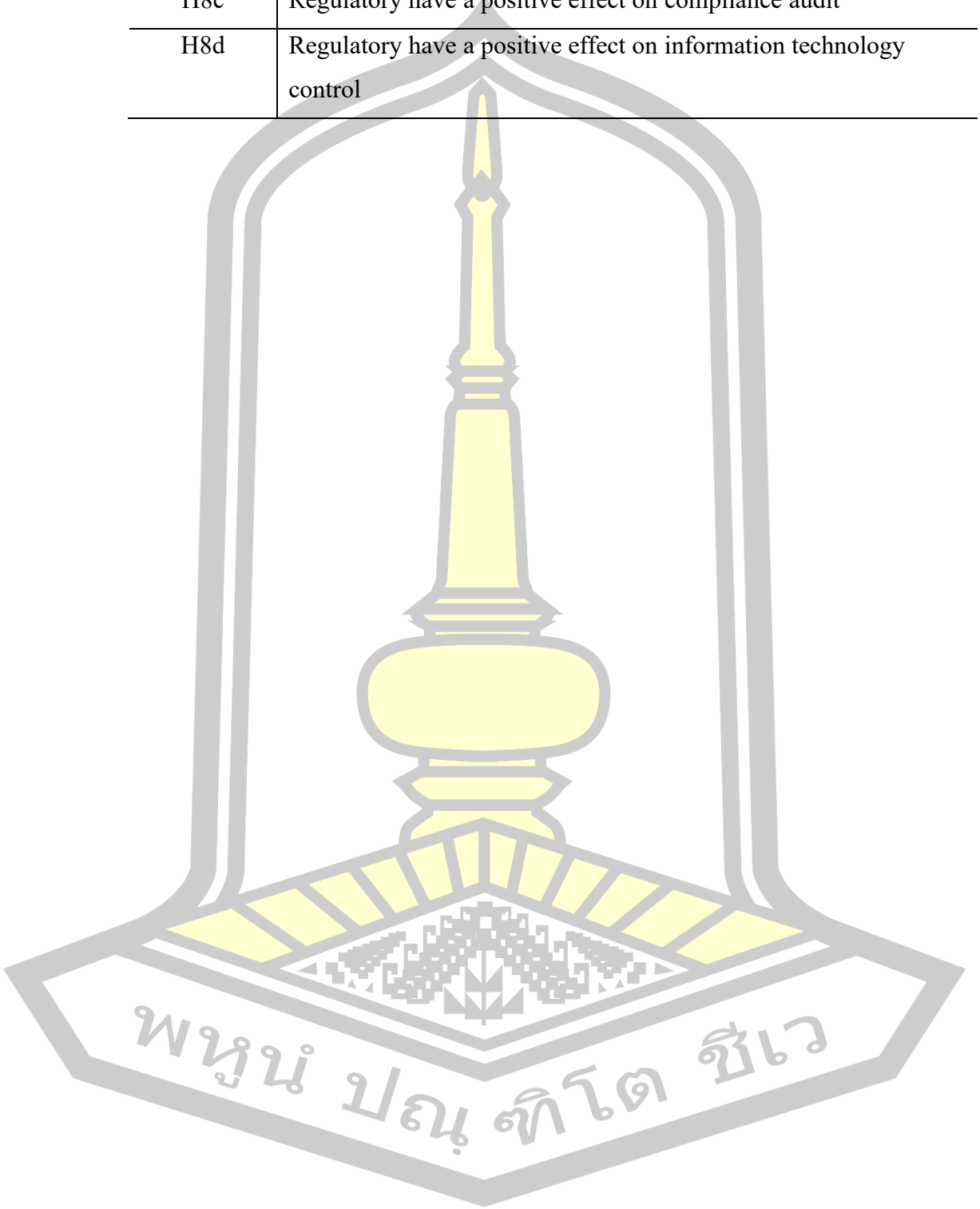
impartially (Carolita & Rahardjo, 2012). Hoffman's (1998) research suggests that experience helps auditors develop superior skills and make correct decisions, allowing them to work effectively even in unusual situations. This aligns with Rezazadeh's (2017) research, which states that work experience enhances auditing capabilities, influences the time and volume of work auditors handle, and improves their expertise in conducting audits. Professional abilities, such as the quality of work performance, general knowledge, and specialized skills, also increase with experience. Singgih and Bawono (2010) mention that work experience is a learning process that enhances the potential to develop positive behaviors through formal and informal education, as well as a process for improving higher-level skills. Purnamasari (as cited in Samsi, Riduwan, and Suryono, 2013) notes that employees with extensive work experience have an advantage in detecting, understanding, and identifying the causes of errors that may occur during an audit (Carolita & Rahardjo, 2012).

The research by Gunasti Hudiwinarsih (2010) states that auditors with less than 5 years of experience (90%) tend to have insufficient experience as auditors, which may lead to a lack of expertise in the role. This is consistent with the research by Sumardi and Hardiningsih (2002), which indicates that auditors with little or no experience may have different technical skills and methods of drawing conclusions. It can be concluded that the longer an auditor has professional experience, the higher their professional attitude will be. Such experience significantly influences decision-making at the time of audit assignment and the complexity auditors face. Similarly, Hudiwinarsih (2005) noted that experienced auditors are better at detecting errors. The longer an auditor’s experience, the better they are at providing detailed recommendations on issues and solutions.

Table 7: Summary of hypothesized relationships

Hypotheses	Description of Hypothesized Relationships
H1a	Financial statement audit have a positive effect on reducing audit risk
H1b	Financial statement audit have a positive effect on data security
H2a	Operational audit have a positive effect on reducing audit risk.
H2b	Operational audit have a positive effect on data security
H3a	Compliance audit have a positive effect on reducing audit risk
H3b	Compliance audit have a positive effect on data security
H4a	Information technology control have a positive effect on reducing audit risk
H4b	Information technology control have a positive effect on data security
H5a	Reducing audit risk have a positive effect on audit quality
H5b	Data security have a positive effect on audit quality.
H6a	Technological change awareness have a positive effect on financial statement audit
H6b	Technological change awareness have a positive effect on operational audit
H6c	Technological change awareness have a positive effect on compliance audit
H6d	Technological change awareness have a positive effect on information technology control
H7a	Business environment have a positive effect on financial statement audit
H7b	Business environment have a positive effect on operational audit
H7c	Business environment have a positive effect on compliance audit
H7d	Business environment have a positive effect on information technology control
H8a	Regulatory have a positive effect on financial statement audit
H8b	Regulatory have a positive effect on operational audit

Hypotheses	Description of Hypothesized Relationships
H8c	Regulatory have a positive effect on compliance audit
H8d	Regulatory have a positive effect on information technology control



CHAPTER III

RESEARCH METHODS

This section explains the research methodology, which is divided into four main components: sample selection and data collection, research instruments, research methods, and statistical analysis used for data analysis. The first component provides details about the sample and data collection process, including the sample selection procedures. The second component discusses the research instruments used in the study. The third component elaborates on the research methods, focusing on the accuracy and reliability of the methods employed. The fourth component covers the statistical analysis techniques utilized in data analysis, describing the types of statistics used for testing research hypotheses and analytical equations. Finally, a summary table of definitions and variable operations will be presented.

The sample selection and data collection

This study utilizes a quantitative research approach from primary data obtained to examine the effect of information technology audit on the audit quality of auditors in the capital market in Thailand. The study employs a quantitative research approach and utilizes data collected from a sample of 365 securities auditors in the capital market. (The Securities and Exchange Commission, Thailand, 2023). Data as of April 23, 2023. Currently, many companies tend to adopt control mechanisms in their audit practices to manage emerging risks. Additionally, there is limited exploration research on the influence of information technology audit on audit quality. Therefore, it is essential to investigate these relationships thoroughly.

Population and Sample

The data for this research was obtained from the website of the Securities and Exchange Commission (SEC) at www.sec.or.th. The database of the SEC includes a list of auditors in the capital market as of April 23, 2023, totaling 365 individuals. The response rate acceptable for social science research to be 20% or higher for mail surveys (Aaker et al., 2001).

The data collection process involves the following steps:

1. Instrument Validation: The questionnaire was sent to 5 experts to examine the research instrument, as follows:

1.1 Assistant Professor Dr. Sumintorn baotham

1.2 Associate Professor Dr. Nuttavong Poonpool

1.3 Assistant Professor Dr. Ingorn Nachairit

1.4 Associate Professor Dr. Suwan Wangcharoendate

1.5 Assistant Professor Dr. Utis Bhongchirawattana

2. Ethics for Research Involving Human Subjects: Certificate of Approval number: 071-617/2024

3. Population Selection: After identifying the target population, the researcher prepares the questionnaires according to the population size.

4. Pre-testing and Validation: Before sending out the questionnaires, the researcher ensures that they are accurate and complete. The questionnaires are enclosed in stamped envelopes.

5. Introduction Letter: Each questionnaire is accompanied by an introduction letter explaining the research objectives and assuring the confidentiality of respondents' personal information.

6. Approval and Main Respondents: The approved respondents are identified as the primary data sources due to their crucial responsibilities in the internal audit within the organization. In quantitative research, the primary data sources play a vital role in ensuring data accuracy and leading to a genuine understanding of the business (Campbell, 1995).

7. Collaboration and Response: The researcher requests cooperation from the respondents to complete and return the questionnaires through the postal service within 15 days after receiving them.

8. Data Validation: After receiving the completed questionnaires, the researcher examines the completeness and accuracy of the answers. The data are then collected and recorded on a computer for further analysis.

The research tools used for data collection

The research tools used for data collection include questionnaires developed based on predefined research objectives and frameworks. The questionnaires are divided into six sections as follows: Section 1: General Information of auditors in the capital market. This section consists of a checklist with five items, including gender, age, educational level, work experience, and average monthly income. Section 2: Opinions on the information technology audit by auditors in the capital market this section employs a proportional estimate questionnaire with 25 items, categorized into four areas: financial statement audit items (5 items), operational audit items (5 items), compliance audit items (5 items), and information technology control items (5 items). Section 3: Opinions on the audit quality in this section, a rating scale questionnaire with five items is used to assess the audit quality. Section 4: Opinions on external factors affecting the information technology audit by auditors in the capital market this section consists of five items and uses a proportional estimate format to measure external factors' impact on the information technology audit. Section 5: Opinions on internal factors affecting the information technology audit by auditors in the capital market similarly, this section contains five items and employs a proportional estimate format to evaluate internal factors' influence on the information technology audit. Section 6: Opinions and suggestions regarding the information technology audit by auditors in the capital market this section includes open-ended questions where respondents can provide their opinions and suggestions related to the information technology audit. These questionnaires will be sent to a total of 365

individuals for data collection, and once complete questionnaires are received, the researcher will validate their accuracy and completeness before recording and analyzing the data using a computer.

Research methodology

This research methodology consists of two main parts. The first part involves validating the instruments related to the validity and reliability of the questionnaire. The second part is concerned with statistical hypothesis testing and hypothesis testing. Hypothesis testing relies on the fundamental assumptions of regression analysis, which are related to testing the linearity of the measurable phenomena, variance, normal distribution, and the relationships between variables.

Validity and reliability

Validity reflects the accuracy of the measurement that evinces the concept of consideration (Hair et al., 2010). To verify the research instrument accuracy and validity, two types of validity, comprising content validity and construct validity, are tested.

Content validity.

Content validity involves "the systematic examination of the test content to determine whether it covers a representative sample of the behavior domain to be measured" (Anastasi, 1997). It refers to the degree to which the essence of the scale represents the construct of being measured content validity requires two or more experts in academic research to review and suggest better solutions to ensure that all questions are sufficient to cover the domain of the variable content. Regarding the relevant theory and literature review, each of the items in a questionnaire will be subjectively assessed by a specialist and related academic expert.

Construct validity refers to a set of measured items that reflects the theoretical latent construct that those items are designed to measure (Hair et al., 20010). If the scale really reflects and indicates its designated construct, then convergent validity and discriminant validities should be established.

Convergent validity demonstrates items that are indicators of a specific construct convergence or share a high proportion of variances in common (Hair et al., 2010). It is the accuracy of a scale correlating with other scales that are designed to measure the same construct. Discriminate validity is the extent to which a construction is truly distinct from other constructs (Hair et al., 2010). It is the accuracy of a scale in distinguishing itself from other scales to measure a different construct. In addition, factorial validity is also used to examine construct validity. Factorial validity tests by using factor analysis, it is applied to identify important factors and reduce low correlated items. Moreover, to ensure the construct validity, the size of the factor loading must be greater than the 0.40 cut-off and be statistically significant (Nunnally and Berstein, 1994)

Table 8: Results of Validity Testing

Variables	Factor Loadings
Financial Statement audit (FAS)	0.607-0.775
Operational audit (OAU)	0.650-0.798
Compliance audit (CAU)	0.778-0.891
Information technology control (ITC)	0.675-0.758
Reducing audit risk (RAR)	0.780-0.804
Data security (DSR)	0.651-0.788
Audit quality (AUQ)	0.656-0.873
Technology change awareness (TCA)	0.769-0.876
Business environment (BEM)	0.722-0.830
Regulatory (RGR)	0.743-0.924

พหุน ปณ ฑิโต ชีเว

Reliability

Reliability is the degree to which the measurement is trusted and error-free (Hair et al., 2010). In this research, Cronbach's alpha coefficient will be used to test the internal consistency of each construct. Internal consistency is an approach to evaluate the consistency or reliability within a collection of multiple items that represent the scale (Thoumrungroje, 2013). Coefficient alpha or Cronbach's alpha will be employed to estimate the reliability. Accordingly, Cronbach's alpha should be greater than 0.70 to ensure internal consistency (Nunnally and Bernstein, 1994; Hair et al., 2006). Moreover, the minimum thresholds for item reliability are arbitrary, and the scale of item total correlation should exceed 0.3 to indicate acceptance of item reliability (Thoumrungroje,2013). As shown on Table 9, the result of all reliability in both Cronbach's alpha coefficients and item total correlation are demonstrated. Cronbach's alpha is a range between 0.710 and 0.920, which exceeds 0.70, to indicate high reliability. Moreover, the item total correlations were scaled from 0.489 to 0.945 in that all scales exceed 0.3; this research shows that item reliability is acceptable.

Table 9: Results of Reliability Testing

Variables	Item total correlation	Cronbach Alpha
Financial Statement audit (FAS)	0.401-0.567	0.710
Operational audit (OAU)	0.453-0.605	0.748
Compliance audit (CAU)	0.640-0.779	0.867
Information technology control (ITC)	0.491-0.579	0.746
Reducing audit risk (RAR)	0.535-0.687	0.767
Data security (DSR)	0.456-0.611	0.744
Audit quality (AUQ)	0.557-0.782	0.804
Technology change awareness (TCA)	0.605-0.755	0.849
Business environment (BEM)	0.571-0.696	0.823
Regulatory (RGR)	0.636-0.867	0.920

Statistical techniques

Before conducting the hypothesis testing, all data will be thoroughly examined and recorded in the data file. Subsequently, the basic assumptions of regression analysis, such as normality, will be tested. Such as outlier, missing data, normality, linearity, and multicollinearity.

Qualitative analysis

Qualitative analysis involves examining the fundamental data obtained from the respondents' profiles in general to verify the accuracy within the range. Frequency and percentage will be tested to facilitate ease of analysis. Additionally, the analysis of standard deviation also measures the dispersion of scores from the mean. (Trainor, 2014).

Variance inflation factor (VIF)

To address the issue of multicollinearity, this research will utilize the Variance Inflation Factor (VIF) as an indicator to detect high levels of multicollinearity among independent variables. If the VIF is less than the threshold of 10 then multicollinearity does not occur. (Hair et al., 2010). As shown in table 10, 12 and 14 and according to chapter 4, the VIF value of all constructs demonstrates the value is less than ten.

Correlation Analysis

Correlation analysis will be conducted to test the relationships among all variables, and a correlation matrix will be prepared to display the relationships among all variables for initial analysis. If variables exhibit a high correlation, with a correlation coefficient greater than 0.8 and significant p-values, multicollinearity may occur (Hair et al., 2010). Therefore, factor analysis will be utilized to group variables with high correlations together, and factor scores of all variables will be prepared to mitigate the issue of multicollinearity. In this research, factor analysis will be employed to group variables with high correlations together and prepare factor scores of all variables to avoid multicollinearity issues.

Multiple regression analysis

Ordinary Least Squares (OLS) In this research, Ordinary Least Squares (OLS) regression is used as an appropriate method to test all proposed hypotheses. Multiple regression analysis is employed to examine whether there is a partial relationship between the independent and dependent variables. If the significance level (sig) is greater than 0.05, it indicates that the null hypothesis is accept, while if sig is less than 0.05, the null hypothesis is reject. The regression is performed to explore the relationship between the composite measurements of information technology audit quality and the dimensions of technology adoption. The aim is to reduce the risk in the audit process and enhance data security. Additionally, the regression is carried out to investigate the relationship between the motivational factors of accountants and the dimensions of information technology adoption based on the conceptual model. Numerous equations are formulated to examine all relationships relevant to the hypotheses in each sub-model in Chapter Two. All equations are statistically analyzed using regression analysis. Furthermore, the statistical equations are presented below for reference:

The investigation of the relationships between four dimensions composed of Information Technology audit and Reducing audit risk is presented in equation 1 as shown:

Equation 1: $$RAR_i = \alpha_1 + \beta_1 FSA_i + \beta_2 OAU_i + \beta_3 CAU_i + \beta_4 ITC_i + \beta_5 AUS1_i + \beta_6 AUS2_i + \beta_7 AUS3_i + \beta_8 AUS4_i + \varepsilon_1$$

The investigation of the relationships between four dimensions composed of Information Technology audit and Data security is presented in equation 2 as shown:

Equation 2: $$DSR_i = \alpha_2 + \beta_9 FSA_i + \beta_{10} OAU_i + \beta_{11} CAU_i + \beta_{12} ITC_i + \beta_{13} AUS1_i + \beta_{14} AUS2_i + \beta_{15} AUS3_i + \beta_{16} AUS4_i + \varepsilon_2$$

The investigation of the relationships between Reducing audit risk, Data security and Audit Quality is presented in equation 3 as shown:

Equation 3: $AUQ_i = \alpha_3 + \beta_{17}RAR_i + \beta_{18}DSR_i + \beta_{19}AUS1_i + \beta_{20}AUS2_i + \beta_{21}AUS3_i + \beta_{22}AUS4_i + \varepsilon_3$

The investigation of the relationships between 3 antecedents and Financial Statement Audit is presented in equation 4 as shown:

Equation 4: $FSA_i = \alpha_4 + \beta_{23}TCA_i + \beta_{24}BEM_i + \beta_{25}RGR_i + \beta_{26}AUS1_i + \beta_{27}AUS2_i + \beta_{28}AUS3_i + \beta_{29}AUS4_i + \varepsilon_4$

The investigation of the relationships between 3 antecedents and Operational Audit is presented in equation 5 as shown:

Equation 5: $OAU_i = \alpha_5 + \beta_{30}TCA_i + \beta_{31}BEM_i + \beta_{32}RGR_i + \beta_{33}AUS1_i + \beta_{34}AUS2_i + \beta_{35}AUS3_i + \beta_{36}AUS4_i + \varepsilon_5$

The investigation of the relationships between 3 antecedents and Compliance Audit is presented in equation 6 as shown:

Equation 6: $CAU_i = \alpha_6 + \beta_{37}TCA_i + \beta_{38}BEM_i + \beta_{39}RGR_i + \beta_{40}AUS1_i + \beta_{41}AUS2_i + \beta_{42}AUS3_i + \beta_{43}AUS4_i + \varepsilon_6$

The investigation of the relationships between 3 antecedents and Information technology Control is presented in equation 7 as shown:

Equation 7: $ITC_i = \alpha_7 + \beta_{44}TCA_i + \beta_{45}BEM_i + \beta_{46}RGR_i + \beta_{47}AUS1_i + \beta_{48}AUS2_i + \beta_{49}AUS3_i + \beta_{50}AUS4_i + \varepsilon_7$

Whereas:

ITA_i = Information technology audit as a whole

FAS_i = Financial statement audit

OAU_i = Operational audit

CAU_i = Compliance audit

ITC_i = Information technology Control

RAR_i = Reducing audit risk

DSR_i = Data security

AUQ_i = Audit quality

AUS1 = Experience in auditing in the stock market not more than 5 years

AUS2 = Experience in auditing in the stock market 6-10 years

AUS3 = Experience in auditing in the stock market 11-15 years

AUS4 = Experience in auditing in the stock market more than 15 years

TCA_i = Technology change awareness

BEM_i = Business environment

RGR_i = Regulatory

α = Constant

β = Regression coefficient

ε = Error term

พหุน ปณ ฑิโต ชีเว

CHAPTER IV

RESULTS AND DISCUSSION

The previous chapter describes research methods that provide to recognize the methods used in data collection, analysis, and hypothesis testing. This chapter describes the results of hypothesis testing which are organized as follows. Firstly, the descriptive statistics are expressed for increased understanding of sample characteristics. Secondly, the results of correlation analysis and hypotheses testing result with regression analysis techniques are detailed. Finally, the summary of hypotheses testing is also provided.

Respondent characteristics and descriptive statistics

Respondent Characteristics

In this research, the respondents are auditors in the Capital Market in Thailand, which has a significant direct influence on the auditing process, as explained by the demographic characteristics of auditors in the capital market, including gender, age, status, education level, experience auditing on the stock exchange, and average monthly income.

The results presented demographic characteristics of 93 key participants, about 62.37 percent are female and 37.63 percent are male. The rank of age is not more than 30 years old of those who most participated in the questionnaire (45.16 percent). Most of the respondents are single (75.27 percent). For the education level, most of the respondents earned a bachelor's degree (74.19 percent). Additionally, most respondents have experience Auditing in The Stock Exchange of Thailand, ranking not more than 5 years (52.69 percent) and Most of them received an average monthly income not more than 100,000 baht (44.09 percent). See Appendix A for more details.

Results of descriptive statistics

Table 10 reveals the descriptive statistics, including the means and standard deviation of all variables of the 93 usable respondents. In this research, all the variables are gathered from the survey and measured by a five-point Likert scale. The results show that the mean scores for all constructs are ranked 4.53 to 4.89. The mean scores for the measure of Information Technology audit, namely, Compliance Audit is 4.82, Information technology control is 4.77, Financial Statement audit is 4.63 and Operation audit is 4.53 ordered from highest to lowest, respectively. The standard deviation value of each dimension of Information Technology audit above is 0.39, 0.33, 0.31 and 0.29 respectively. These results also show that Auditors in the Capital Market recognize the significance of information technology audit in four dimensions. Besides, the mean scores for the consequences of Information Technol information technology audit consist of audit quality 4.89, reducing audit risk 4.87 and data security 4.75. The standard deviation value of each consequence above is 0.30, 0.25 and 0.23 respectively. These results also show that auditors in the Capital Market are conscious of the significance of results of auditing which can be provided.

Furthermore, the results also show that the mean score of antecedent variables consists of regulatory is 4.83, technology change awareness is 4.79 and business environment 4.57. The standard deviation value of each variable above are 0.37, 0.33 and 0.32 respectively. These results indicate that Auditors in the Capital Market are aware of the vital factors that motivate their audit behaviors.

พหุน ปณ ฑิโต ชีเว

Table 10: Descriptive statistics and correlation matrix

Variables	FAS	OAU	CAU	ITC	RAR	DSR	AUQ	TCA	BEM	RGR
Mean	4.63	4.53	4.82	4.77	4.87	4.75	4.89	4.79	4.57	4.83
S.D.	0.29	0.39	0.33	0.31	0.25	0.30	0.23	0.33	0.37	0.32
OAU	.149									
CAU	.171	.170								
ITC	.065	-.118	.092							
RAR	-.113	.226*	.256*	.254*						
DSR	.234*	.289**	.216*	.241*	.074					
AUQ	.157	.237*	.757**	.212*	.420**	.251*				
TCA	.193	.324**	.461**	-.150	.135	.536**	.465**			
BEM	.078	.258*	.163	-.169	-.079	-.043	-.024	.035		
RGR	.156	.303**	.832**	.129	.391**	.417**	.808**	.660**	.125	

Note: ** p < 0.01, * p < 0.05

Results of correlation analysis

Table 10 shows the Pearson correlation coefficient of all variables. Results demonstrate that all dimensions of information technology audit have a significant, positive relationship with reducing audit risk ($r = -.113 – .256$, $p < 0.05$), data security ($r = .074 – .289$, $p < 0.05$) and audit quality ($r = .157 – .757$, $p < 0.01$). are significantly, positively related to all dimensions of Information Technology audit.

For correlation analysis, the empirical evidence suggests that there are positive relationships among the antecedents including technological change awareness ($r = -.150 – .536$, $p < 0.01$), business environment ($r = -.169 – .258$, $p < 0.05$) and regulatory ($r = .125 – .832$, $p < 0.01$). The evidence shows that each variable is not highly correlated with each other, which is a sign that multicollinearity problems may not occur. Moreover, generally accept levels of multicollinearity are analyzed using variance inflation factors (VIFs) (Hair et al., 2010).

Hypotheses testing and results

To verify the hypotheses, this research selects the full sample for multiple linear regression analysis. In addition, all hypotheses in this research are transformed into seven equations. There is a control variable for auditing skill, which are included in equations for testing as follows.

Figure 2 : The effect of information technology audit on audit quality of auditors in the Capital Market in Thailand.

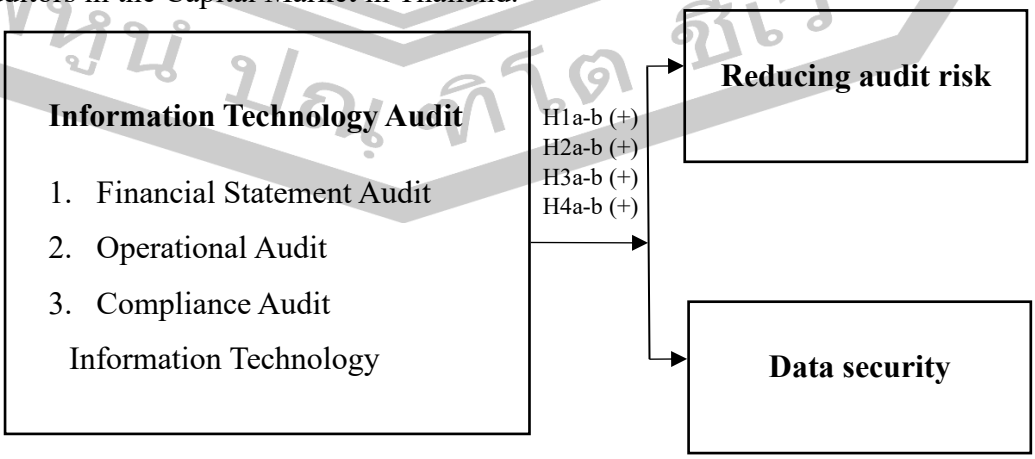


Figure 2 illustrates relationships among each dimension of Information Technology audit and consequence variables based on Hypotheses 1a-1b, 2a-2b, 3a-3b and 4a-4b. This research proposes that each dimension of Information Technology audit; namely, financial statement audit, Operational audit, Compliance audit and Information technology control are positively associated with the overall consequences, which are reducing audit risk and data security. These hypotheses are analyzed by multiple regression in equations 1 and 2 according to chapter 3.

Table 11: Descriptive statistics and correlation matrix of information technology audit, reducing audit risk and data security.

Variables	**FAS**	**OAU**	**CAU**	**ITC**	**RAR**	**DSR**
Mean	4.63	4.53	4.82	4.77	4.87	4.75
S.D.	0.29	0.39	0.33	0.31	0.25	0.30
OAU	.149					
CAU	.171	.170				
ITC	.065	-.118	.092			
RAR	-.113	.226*	.256*	.254*		
DSR	.234*	.289**	.216*	.241*	.074	

Note: ** $p < 0.01$, * $p < 0.05$

Table 11 reveals the Pearson correlation coefficient, mean, and standard deviation of all variables. The results indicate that the mean scores for all constructions are ranked between 4.87 and 4.75 respectively. In addition, the standard deviation value for all constructs is ranked between 0.25 and 0.30 respectively.

Besides, the correlations among each dimension of Information Technology audit, namely, financial statement audit (FAS), Operational audit (OAU), Compliance audit (CAU) and Information technology control (ITC) are positively correlated with all consequence variables. Firstly, the results show the positive correlation between each dimension of information technology audit and reducing audit risk ($r = -.113, .226, .256, .254$; $p < 0.05$, respectively). Secondly, each dimension of information technology audit has a significant positive correlation to data security ($r = .234, .289, .216, .241$; $p < 0.01$, serially). These results show that each dimension of information technology audit has a certain significance for reducing audit risk, data security and audit quality. When the level of information technology audit that Auditors in the Capital Market is high, the high level of the overall consequence variable is obtained.

As shown in Table 12, variance inflation factors (VIFs) are used to test multicollinearity problems in each part of the regression analysis. Table 10 reveals that the results in equations 1 and 2 indicate that the maximum VIF value of four dimensions of financial statement audit is 1.281, which is not exceeding 10 in the scale (Hair et al., 2010). Therefore, both VIF and correlations certify that multicollinearity problems do not occur.

Additionally, in Table 12, the regression results are presented for the impact of each dimension of information technology audit on outcomes consisting of audit risk reduction and information security.

Table 12: The results of regression analysis for the relationship between each dimension of information technology audit and its consequences.

Independent Variables	**Dependent Variables**	
	RAR **Eq.1**	**DSR** **Eq.2**
Financial statement Audit (FAS)	0.180* (0.085)	0.238* (0.105)
Operation audit (OAU)	0.175* (0.068)	0.199* (0.080)
Compliance audit (CAU)	0.178* (0.079)	0.058 (0.093)
Information technology control (ITC)	0.240** (0.081)	0.285** (0.095)
Control Variables: Experience in auditing in the stock market 6-10 years (AUS2)	0.054 (0.061)	0.079 (0.072)
Experience in auditing in the stock market 11-15 years (AUS3)	0.039 (0.105)	0.139 (0.124)
Experience in auditing in the stock market more than 15 years (AUS4)	0.056 (0.074)	0.198* (0.088)
Adjusted R^2	0.163	0.192
Maximum VIF	1.281	1.281
Bata coefficients with standard errors in parenthesis, ** P < 0.01, * P < 0.05		

First, the result shows that financial statement audit has significant effect on reducing audit risk ($\beta_1 = 0.180$, $p < 0.05$) and data security ($\beta_9 = 0.238$, $p < 0.05$) after controlling the relevant variables. This result indicates that auditing accounting information and financial reports will help ensure the completeness and reliability of the information because the auditing process requires caution and careful planning (Alktani, 2014). Therefore, reliable information will help auditors work effectively, make the audit and certification of financial

statements accurate and precise, and reduce errors in expressing opinions in financial statements (Salameh, 2011). The auditor must collect complete, correct, appropriate, and sufficient information when auditing the accounts to reduce the risk of expressing inappropriate opinions on financial statements that contain material misstatements to an acceptable level. (Federation of Accounting Professions, 2014). Auditing financial reports will help ensure the completeness and reliability of the information, which will assist in making the auditor's risk assessment accurate. This is important for preparing an audit report that enables the auditor to reach a reasonable conclusion to support their opinion. Therefore, auditing financial reports helps ensure the accuracy and reliability of the information and reduces audit risk (Riyadi et al., 2021). This is consistent with the research of Rosati et al. (2020), who stated that if auditors increase their efforts in auditing and sufficiently test materiality, information security incidents will not result in a decrease in audit quality. This means that if auditors have thoroughly checked accounting information and materiality, it will help ensure the information is secure and maintain audit quality. ***Thus, hypotheses 1a and 1b are supported.***

Second, the result shows that operational audit has a significant, positive effect on reducing audit risk (β_2= 0.175, $p < 0.05$) and data security (β_{10}= 0.199, $p < 0.05$). This result implies that Auditing work procedures helps ensure that the sequence of work tasks and duties in each unit is carried out efficiently and appropriately according to specified procedures, resulting in the work achieving its specified goals. (Federation of Accounting Professions, 2014). Therefore, reviewing the operating procedures and methods of operation contributes to confidence that these procedures are carried out effectively and helps reduce the auditor's audit risk, including the risk of inappropriate expression of opinions on the financial report (Robson et al.,2007; Curtis and Turley, 2007;Peecher et al., 2007). The assessment of the effectiveness of the work will evaluate the results, provide recommendations, and prepare the audit report. In terms of substantive audit procedures, the dimensions of materiality and audit risk are used to manage the approach and determine the appropriate scope of the audit. (Bagchi,

2006). The above-mentioned audits will help reduce information risk and improve information efficiency. Good information will reduce audit risk and improve audit efficiency (Hall, 2011). The audit process will help eliminate or minimize losses by identifying vulnerabilities and risks, determining if appropriate security controls are in place, and ensuring that security measures and audits are valid (Bosworth & Kabay, 2002). ***Thus, hypotheses 2a and 2b are supported.***

Third, the result shows that compliance audit has a significant, positive effect on reducing audit risk ($\beta_3 = 0.178$, $p < 0.05$) These results indicate that monitoring the organization's compliance with rules and regulations to achieve its set goals will increase confidence in its adherence to rules, regulations, and policies. (Federation of Accounting Professions, 2014). Auditing has become an important part of reducing vulnerabilities, which helps ensure that business operations, data processing, and reporting are efficient and increases the reliability of audit data. It also ensures that operations comply with rules and regulations, thereby helping to reduce audit risks (Gantz, 2014). This is consistent with the research of Judijanto et al. (2023) who stated that regulatory compliance is an important issue. Organizations that comply with regulatory requirements tend to have more effective audits, which can reduce inaccuracies in financial reporting. ***Thus, hypotheses 3a are supported.***

Compliance audit has no significant effect on data security ($\beta_{11} = 0.058$, $p > 0.05$) Based on the results, it can be said that compliance audits are conducted to ensure that the organization adheres to various standards and regulations. These audits can identify gaps and weaknesses and help the organization address these issues. However, on the other hand, compliance audits do not always imply that the organization has robust information security. Sometimes, compliance may be considered more fundamental than a comprehensive security strategy. An organization may be compliant with regulations but still be vulnerable to emerging threats if its security measures are outdated or incomplete (Duncan & Whittington, 2014). Therefore, although compliance audits are an essential component of an information security strategy, they are

not the sole factor in ensuring data protection. Regularly updating security practices, investing in advanced technologies, and fostering a culture of security awareness are also crucial. ***Thus, hypotheses 3b are not supported.***

Fourth, the result shows that information technology control has a significant, positive effect on reducing audit risk ($\beta_4 = 0.240$, $p < 0.01$) and data security ($\beta_{12} = 0.285$, $p < 0.01$) after controlling the relevant variables. The empirical results verify the establishment of the study hypotheses. This result indicates that information technology control involves assessing information technology related risks, which helps ensure that an organization's data or information is protected and reduces the risks associated with the use of technology within the organization. These risk control activities include auditing and controlling the processing of information technology data, auditing and controlling data completeness, auditing and controlling security and privacy systems, safeguarding information technology assets, auditing and controlling system maintenance and program modifications, continuous monitoring and controlling of data processing, auditing and controlling system applications, and auditing and controlling system development. This is consistent with Arens et al. (2017), who stated that auditing standards address two types of controls for auditing: 1) General controls, which apply to all IT functions, including IT management, system development alternatives, physical and online security related to access to hardware, software, and data, backup planning and contingency for unforeseen emergencies, and hardware controls; and 2) Application controls, which are procedures and methods within application systems to ensure that all transactions are approved, recorded, and processed completely, accurately, and timely, thereby enhancing the reliability of data or information. Effective information helps auditors accurately assess risks, which is crucial for preparing audit reports that enable auditors to reach reasonable conclusions. Reliable and adequate information helps auditors' express opinions and exercise professional judgment appropriately, which reduces the risk of overlooking suspicious situations or incorrect assumptions in evidence

collection and audit evaluation. (Petter Lovaas, 2012). ***Thus, hypotheses 4a and 4b are supported.***

Figure 3: The effect of reducing audit risk, data security on audit quality

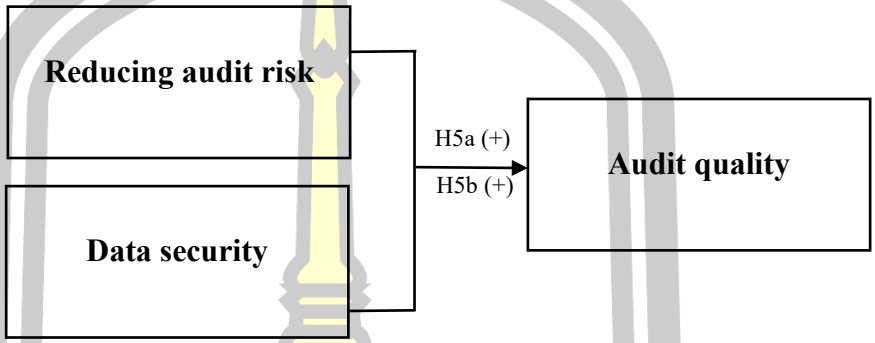


Figure 3 illustrates relationships among reducing audit risk, data security on audit quality based on Hypotheses 5a-5b. These hypotheses are analyzed by multiple regression in equations 3 according to chapter 3.

Table 13: Descriptive statistics and correlation matrix of reducing audit risk, Data security on audit quality.

Variables	RAR	DSR	AUQ
Mean	4.87	4.75	4.89
S.D.	0.25	0.30	0.23
DSR	.074		
AUQ	.420**	.251*	

Note: ** $p < 0.01$, * $p < 0.05$

Table 13 reveals the Pearson correlation coefficient, mean, and standard deviation of all variables. The results indicate that the mean scores for all constructs are ranked between 4.75 and 4.87 respectively. In addition, the standard deviation value for all constructs is ranked between 0.25 and 0.30 respectively.

Besides, the correlations between reducing audit risk, data security are positively correlated with audit quality. The results show the positive correlation between reducing audit risk, data security and audit quality ($r = .420, .251$; $p < 0.01$, respectively). These results show that each dimension of Reducing Audit Risk, Data Security has a certain significance for audit quality.

Table 14: The results of regression analysis for the relationship between reducing audit risk, data security on audit quality.

Independent Variables	**Dependent Variables**
	AUQ
	Eq.3
Reducing Audit Risk (RAR)	0.362**
	(0.084)
Data Security (DSR)	0.142*
	(0.071)
Control Variables: Experience in auditing in the stock market 6-10 years (AUS2)	0.071
	(0.050)
Experience in auditing in the stock market 11-15 years (AUS3)	0.213*
	(0.085)
Experience in auditing in the stock market more than 15 years (AUS4)	0.026
	(0.061)
Adjusted R^2	0.268
Maximum VIF	1.156
Bata coefficients with standard errors in parenthesis, ** P < 0.01, * P < 0.05	

As shown in Table 14, it can be seen from the regression results, as to the impacts reducing audit risk, data security on audit quality.

Also, variance inflation factors (VIFs) are used to test multicollinearity problems in each part of the regression analysis. Table 14 reveals that the results in equations 3 indicate that the maximum VIF is 1.156 Thus, the VIF value is well below the cut-off value of 10 (Hair et al., 2010). Subsequently, there are no significant multicollinearity problems existing in this research.

First, the result shows that reducing audit risk has significant effect on audit quality (β_{17}= 0.362, $p < 0.01$) The result demonstrates that reducing errors from events that require assessment ensures that the auditor's report is free from distortions that may arise from mistakes. This is because auditors need to obtain sufficient and appropriate information to mitigate audit risk, which helps auditors reach reasonable conclusions to support their opinions. (Federation of Accounting Professions, 2014). Consistent with the research by Hurtt, R. K. (2011), audit risk is positively related to the performance of audits in terms of the sufficiency and appropriateness of audit evidence. The use of professional judgment, including observation and skepticism, helps reduce the risk of overlooking suspicious situations or using incorrect assumptions in evidence collection and audit evaluation. Auditors must prioritize professional judgment and skepticism as tools to ensure the quality of accounting information and provide benefits to financial statement users. (AlShaer, 2020). Additionally, audit risk can impact the effectiveness of financial reporting. Reducing audit risk affects the accuracy and reliability of financial reports, which in turn influences the overall effectiveness of the audit (Riyadi et al., 2021). ***Thus, hypotheses 5a are supported.***

Second, the study results show that data security significantly affects audit quality (β_{18}= 0.142, $p < 0.05$). Westland's (2021) research indicates that cybersecurity incidents can reduce data integrity, preventing auditors from relying on the accuracy of the data, which affects audit quality. Therefore, auditors should consider and assess the impact of such risks on the audit (Vendrzyk, 2003). Because auditing ensures that data is accurate and reliable, it improves the auditor's audit efficiency. Considering sufficient reliable and

appropriate data allows auditors to express opinions and exercise professional judgment in observing and questioning effectively, which reduces the risk of overlooking suspicious situations or making false assumptions during evidence collection and audit assessment (Petter Lovaas, 2012). Therefore, strict data security can help detect and prevent fraudulent activities if data is secure. It will increase the credibility of the audit. ***Thus, hypotheses 5b are supported***.

Figure 4: The effect of antecedents on information technology audit

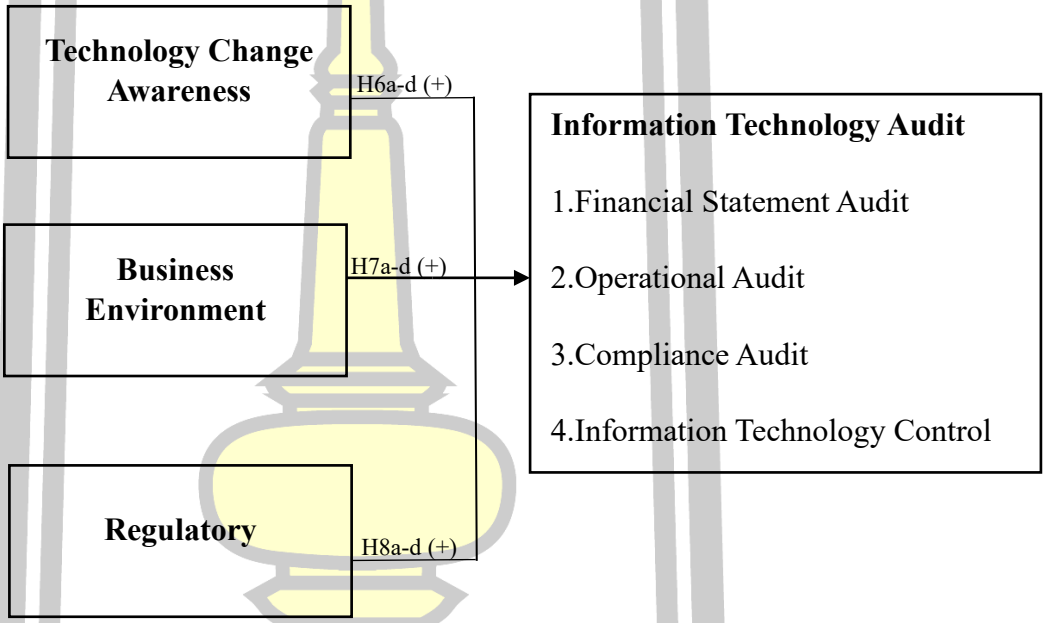


Figure 4 illustrates relationships among each antecedent on dimension of information technology audit variables based on Hypotheses 6a-6d, 7a-7d and 8a-8d. This research proposes that antecedents; namely, technology change awareness, business environment and regulatory are positively associated with dimension of information technology audit. These hypotheses are analyzed by multiple regression in equations 4,5,6 and 7 according to chapter 3.

Table 15: Descriptive statistics and correlation matrix of antecedents on dimension of information technology audit.

Variables	FAS	OAU	CAU	ITC	TCA	BEM	RGR
Mean	4.63	4.53	4.82	4.77	4.79	4.57	4.83
S.D.	0.29	0.39	0.33	0.31	0.33	0.37	0.32
OAU	.149						
CAU	.171	.170					
ITC	.065	-.118	.092				
TCA	.193	.324**	.461**	-.150			
BEM	.078	.258*	.163	-.169	-.079		
RGR	.156	.303**	.832**	.129	.391**	.417**	

Note: ** $p < 0.01$, * $p < 0.05$

Table 15 reveals the Pearson correlation coefficient, mean, and standard deviation of all variables. The results indicate that the mean scores for all constructions are ranked between 4.82, 4.77, 4.63, and 4.53 respectively. In addition, the standard deviation value for all constructions is ranked between 0.39, 0.33, 0.31, and 0.29 respectively.

Besides, the correlations among antecedent's variables and each dimension of information technology audit, namely, technology change awareness (TCA), business environment (BEM) and regulatory (RGR) are positively correlated with financial statement audit, operational audit, compliance audit and information technology control. Firstly, the results show that technology change awareness is significantly and positively correlation to each dimension of financial statement audit, operation audit, compliance audit and information technology control ($r = .193, .324, .461, -.150$; $p < 0.01$, successively). Secondly, the result shows that the business environment is significantly and positively correlated to each dimension of information technology audit ($r = .078, .258, .163, -.169$; $p < 0.05$, successively). Finally, the results demonstrate that regulatory is significantly and positively correlated to financial statement audit, operational audit, compliance audit and information technology control ($r = .156, .303, .832, .129$; $p < 0.01$, respectively).

พหุน ปณ ฑิโต ชีเว

Table 16: The results of the relationships between 3 antecedents on dimensions of information technology audit.

Independent Variables	Dependent Variables			
	FAS **Eq.4**	**OAU** **Eq.5**	**CAU** **Eq.6**	**ITC** **Eq.7**
Technology change awareness (TCA)	0.158 (0.117)	0.312* (0.149)	0.162* (0.078)	0.393** (0.121)
Business Environment (BEM)	0.032 (0.080)	0.203* (0.101)	0.042 (0.053)	0.199** (0.082)
Regulatory (RGR)	0.043 (0.127)	0.017 (0.161)	0.955** (0.084)	0.421** (0.131)
Control Variables: Experience in auditing in the stock market 6-10 years (AUS2)	0.052 (0.071)	0.134 (0.090)	0.068 (0.047)	0.008 (0.074)
Experience in auditing in the stock market 11-15 years (AUS3)	0.237 (0.122)	0.298 (0.155)	0.057 (0.081)	0.212 (0.126)
Experience in auditing in the stock market more than 15 years (AUS4)	0.206* (0.085)	0.118 (0.108)	0.020 (0.056)	0.158 (0.088)
Adjusted R^2	0.070	0.187	0.697	0.156
Maximum VIF	1.967	1.967	1.967	1.967

Bata coefficients with standard errors in parenthesis, ** $P < 0.01$, * $P < 0.05$

Also, variance inflation factors (VIFs) are used to test multicollinearity problems in each part of the regression analysis. Table 16 reveals the maximum VIF is 1.967. Thus, the VIF value is well below the cut-off value of 10 (Hair et al., 2010). Subsequently, there are no significant multicollinearity problems existing in this research.

First, the result shows that technology change awareness has no significant effect on financial statement audit ($\beta_{23} = 0.158$, $p > 0.05$). Information technology leads to changes in the traditional organizational structure, resulting in profound changes in the organization's mission and

objectives. The most important features of technology are high-speed data processing, real-time access, and modern electronic data exchange. It also provides high-quality information at a low cost. Auditing must also adopt new methods or approaches to deliver services and perform duties. Particularly, the accounting and auditing profession may encounter various conveniences and possibilities in the new environment. This creates new opportunities for recording and reporting data, leading to increased efficiency and effectiveness in the profession (Mohammadi, 2012). Although information technology advancements may make the audit environment more complex, there are new methods and tools available for auditors to manage audits in complex environments. Therefore, the use of information technology auditing methods is increasingly necessary in such complex environments. (Arab Mazar Yazdy, 2001) The increased use of information technology has led to the necessity for auditing resources or assessing Information technology related risks (Singleton J. A., 2005). To avoid errors or deficiencies that could result in the presentation of inaccurate information, auditors must understand the information systems to plan, direct, supervise, and review operations. Kranacher Riley (2019) states that the auditing profession places significant emphasis on the auditing process using professional auditing standards and sometimes focuses on measuring the outcomes of audits, which present the auditor's reports and opinions on financial statements. The concept of auditing is defined as adherence to professional auditing standards, the profession's ethics and morals, auditing guidelines, as well as the rules and procedures set by professional organizations to regulate the auditing profession and to maintain the independence and integrity of auditors. Therefore, the research of Nurjannah (2019) believes that audit quality involves conducting the audit process efficiently and effectively according to auditing standards, by identifying errors and irregularities and taking action to meet the needs and requirements of financial statement users. Therefore, awareness of technology change may not impact the financial statement audit, as auditing continues to adhere to standard criteria in the audit process. ***Thus, hypotheses 6a are not supported.***

Second, the result shows that technology change awareness has significant effect on operational audit ($\beta_{30} = 0.312$, $p < 0.05$). Based on the results, technology change awareness lead to more effective oversight in managing and utilizing technology, which in turn enhances organizational efficiency and performance. (Kroll et al., 2008; Sundaramurthy & Lewis, 2003) Currently, organizations are increasing their investments in information technology because they recognize the tremendous benefits that Information technology can provide to their operations and service delivery. (Brynjolfsson & Hitt, 2011; Chen & Zhu, 2004; Devaraj & Kohli, 2003; Kohli & Grover, 2008) However, the research by Dehning & Stratopoulos (2002) indicates that Information technology skills and knowledge are positively associated with a company's performance. Yayla & Hu (2014) provide evidence that a high level of Information technology awareness leads to improved company performance. Nonetheless, the rapid technological changes and increasing complexity make it difficult for organizations to develop a consistent approach between their business strategies and the digital platforms created to support these strategies. (Bradley et al., 2011; Schmidt & Buxmann, 2011) Therefore, operational audit is conducted to ensure that operations or procedures within various departments of an organization are efficient, resources are used effectively, and the organization's objectives and goals are achieved. The focus is on efficiency, effectiveness, and economy of the activities. If there are obstacles or issues, they can be addressed. This type of audit evaluates current performance to focus on future outcomes and is sometimes referred to an operational audit. The purpose of an operational audit is to assess whether the organization’s resources are being used efficiently and economically and to review operations or plans to ensure that the results align with the established objectives and goals and that activities are carried out according to the planned schedule, which indicates effectiveness. Thus, awareness of technology changes plays a pivotal role in transforming operational audits, with significant implications for audit effectiveness and the evolution of auditing as a practice in a technology-driven environment. ***Thus, hypotheses 6b are supported.***

Third, the result shows that technology change awareness has significant effect on compliance audit ($\beta_{37} = 0.162$, $p < 0.05$). From the results, it can be said that information technology offers numerous benefits but also involves associated risks. For example, computer assets may be lost or stolen, the likelihood of fraud may increase, improper use of technology could lead to a competitive disadvantage, data may be lost or stolen, privacy could be breached, and business operations might be disrupted by these risks. This necessitates the implementation of technology security controls and the protection of confidential information."(Okereafor, 2008). Therefore, continuous monitoring to respond to preventive measures is essential for managing the risks and benefits associated with information technology, such as: (1) Cybercrime involving individuals or groups seeking financial gain from exploiting systems; (2) Cyberattacks often linked to political motivations for data collection; and (3) Cyberterrorism aimed at causing damage to electronic systems. It is necessary to have systems for auditing and managing information technology projects, overseeing information technology, and implementing security management systems to ensure compliance with laws and regulations. (Santy Setiawan, 2020). ***Thus, hypotheses 6c are supported***.

Fourth, the result shows that technology change awareness has significant effect on information technology control ($\beta_{44} = 0.393$, $p < 0.01$). Based on the above results, Currently, organizations invest significant amounts of money in Information technology because they recognize the tremendous benefits that Information technology can provide to their operations and service delivery (Brynjolfsson & Hitt, 2011; Chen & Zhu, 2004; Devaraj & Kohli, 2003; Kohli & Grover, 2008). However, information technology often comes with risks, such as data breaches, security issues, and software errors, which can undermine stakeholder confidence and negatively impact performance. These risks are not only technical issues related to information technology but also represent internal control problems for management (Cereola & Cereola, 2011; Zhang et al., 2015). Management develops appropriate internal control processes to prevent these risks and protect both the company's physical and informational

assets (Cereola & Cereola, 2011; Shih, 2010). This ensures that the company's information systems are reliable, secure, and not vulnerable to computer attacks (Frost & Choo, 2017). Therefore, information technology controls by information systems auditors are essential for assessing information technology related risks. This helps ensure that an organization's data or information is protected and that risks associated with the use of technology within the organization are minimized. This risk control activity includes the auditing and control of information technology data processing, the verification and control of data completeness and accuracy, the auditing and control of security and privacy systems, the protection of Information technology assets, the auditing and control of system maintenance and program modifications, the continuous auditing and control of data processing, the auditing and control of system applications, and the auditing and control of system development. In line with Arens et al. (2017) research, auditing standards address two types of controls for audits: 1) General controls, which apply to all Information technology related work, including Information technology management, system development alternatives, physical and online security related to access to hardware, software, and data, backup and contingency planning for unpredictable emergencies, and hardware controls; and 2) Application controls, which involve implementing procedures and methods within systems to reasonably ensure that all transactions are authorized, recorded, processed completely, accurately, and in a timely manner. Consequently, awareness of technological changes helps organizations enhance their operational efficiency and leads to effective Information technology controls, thus improving the efficiency of Information technology usage. ***Thus, hypotheses 6d are supported.***

Fifth, the result shows that business environment has no significant effect on financial statement audit ($\beta_{24} = 0.032$, $p > 0.05$). As mentioned above, it is evident that the changing environment will impact the transformation of traditional organizational structures. Auditing will also need to adopt new methods or approaches to deliver services and perform duties. In particular, the accounting and auditing profession may encounter various conveniences and

possibilities in the new environment. This creates new opportunities for recording and reporting information, resulting in increased efficiency and effectiveness in auditing (Mohammadi, 2012). According to Betti and Sarens (2020) as business operations evolve, the increasing importance of technology and information must be considered. Auditing must also develop and adapt to the business environment, understanding that the use of tools and technology impacts the auditing process. However, financial statement audits must continue to adhere to auditing standards, professional ethics and morals, auditing guidelines, as well as the rules and procedures established by professional organizations to regulate the auditing profession and maintain the independence and integrity of auditors. (Menezes Brás, 2018). ***Thus, hypotheses 7a are not supported.***

Sixth, the result shows that business environment has significant effect on operational audit ($\beta_{31} = 0.203$, $p < 0.05$). Auditing has continuously evolved and adapted to the changing business environment, understanding that the use of tools and technology significantly impacts financial reporting. Additionally, the profession has been affected by changes in auditing methods, review processes, and professional development, which are considered essential characteristics of the profession (Federation of Accounting Professions, 2014). According to Betti and Sarens (2020). As business operations evolve, the increasing importance of technology and information must be considered, and auditing must also develop and adapt to the business environment. ***Thus, hypotheses 7b are supported.***

Seventh, the result shows that business environment has no significant effect on compliance audit ($\beta_{38} = 0.042$, $p > 0.05$). The research by Eilfsen et al. (2020) states that environmental pressures play a significant role in the adoption of information technology by companies, making Information technology a crucial tool for modern businesses. The continuous growth of information technology has led to the evolution of Information technology threats, causing operational disruptions and errors. The increased use of technology should not escalate risks to a point where companies cannot manage them. Therefore, each organization's Information technology must be assessed and managed due to the

current risks posed by technological hazards (Devale, 2012). Such environmental changes are constantly evolving, but their impact on compliance audits is not always direct or significant. ISACA has stated that frequent changes in technology, demands, competition, and regulatory developments force businesses to adapt quickly. However, the research indicates that these changes do not always alter the fundamental principles or effectiveness of compliance audits. The role of auditing remains to ensure the effectiveness of controls and compliance, rather than responding to every change in the business environment (Alexiou, 2019). This is consistent with a research study that explores the concept of expectation in auditing, which states that changes in the business environment may not align with adjustments in auditing approaches. This misalignment could lead to a situation where compliance audits are unaffected by certain changes if they fall outside the scope of current auditing guidelines (Paul Olojede, 2020). ***Thus, hypotheses 7c are not supported.***

Eight, the result shows that business environment has significant effect on information technology control ($\beta_{45} = 0.199$, $p < 0.01$). The increased reliance on information technology arises from a changing environment, which enhances the efficiency of business operations, data processing, and reporting. The continuous growth of information technology has led to an evolution of information technology related threats. In audits, information technology auditors assess the effectiveness and efficiency of information technology controls within data systems and related operations, including the adequacy of these controls, to mitigate the risk of loss due to errors, fraud, and other actions, as well as disasters or events that render systems inoperative." (Riad, 2015) These threats arise from increased reliance on information technology and a lack of control. Consequently, many organizations have begun to recognize the importance of information technology security (Hall, 2011). The research by Zhong and Chen (2023) confirm that the business environment has a significant impact on information technology controls, particularly through its influence on technology innovation and organizational governance. The research highlights that a well-adapted business environment fosters high-quality economic

development by promoting innovation, which in turn requires more stringent information technology controls to manage the associated risks. Consistent with the research by Rubino et al. (2017), information technology controls help organizations better assess and manage risks, which is particularly crucial in a constantly changing business environment. The research indicates that the business environment significantly impacts information technology control systems. External and internal pressures from the business environment, such as market demands and technological advancements, drive organizations to adjust their information technology controls accordingly. These adjustments are essential for maintaining operational efficiency, ensuring data integrity, and reducing risks such as fraud or data breaches. Therefore, information technology controls are relevant to business adaptation in a constantly evolving business context, where technology or market conditions are perpetually changing. Organizations must continuously update and enhance their information technology controls to ensure that they remain effective and aligned with business objectives. (Saukkonen & Kirjavainen, 2019). This research highlights the importance of robust information technology controls that respond to the changing business environment, ensuring that organizations can manage their operations and protect their assets effectively. ***Thus, hypotheses 7d are supported.***

Ninth, the result shows that regulatory has no significant effect on financial statement audit ($\beta_{25} = 0.043$, $p > 0.05$). Changing regulatory impact, the operations and financial reporting of companies, including shifts in business, the economy, laws, and regulations, making it necessary to have appropriate responses and disclosures in financial statements. Additionally, this affects the auditing process, as auditors need to expand their work to address the increased risk of significant misstatements in financial statements. However, auditors are responsible for providing an opinion on whether they have obtained reasonable assurance that the financial statements are free from material misstatement, whether due to fraud or error, and must present accurate information in accordance with relevant accounting standards (Judijanto et al., 2023).

Therefore, while changing regulations may impact on company operations, the audit of financial statements still relies on adhering to relevant accounting standards. ***Thus, hypotheses 8a are not supported.***

Tenth, the result shows that regulatory has no significant effect on operational audit ($\beta_{32} = 0.017$, $p > 0.05$). The research by Hilali et al. (2020) states that increased regulations focusing on privacy and cybersecurity have added complexity to businesses. This has led to an emphasis on information technology audits to control and secure information technology. Therefore, the growing regulatory requirements necessitate changes in business processes and create a need to evaluate and review practices to ensure they are appropriate and comply with standards operational audit is the examination of operational systems, methods, and processes with the objective of improving performance. This type of audit focuses on reviewing each step of the operational process, including measuring actual performance against the organization's established standards. It emphasizes comparing the performance with resource usage, evaluating whether the output/input ratio is cost-effective (Fadhilah, 2022). Thus, regulations affect business operations, but operational auditing is a process where auditors examine an organization's practices to improve performance. Some studies suggest that in certain situations, regulatory changes may have little or no impact on operational audits, particularly when the changes do not alter the core processes or risk factors being audited. This is especially the case if the operational audit focuses more on internal efficiency rather than regulatory compliance (KPMG, 2020). ***Thus, hypotheses 8b are not supported.***

Eleventh, the result shows that regulatory has significant effect on compliance audit ($\beta_{39} = 0.955$, $p < 0.01$). From these results, it can be concluded that auditing serves as a form of assurance. However, it is important to note that the role of audit management extends beyond this. ISO 27001 states that applying the standard for managing information security helps to strengthen data security systems, reduce risks, and protect data from theft. COBIT is applied to control and maintain information technology security, ensuring

confidence and reliability in the use of information technology, and increasing the reliability of the data processed and stored within information systems. (Riad, 2015). The role of information technology auditing is crucial to the success of an organization. Currently, providing guidance on information technology control issues related to business processes helps promote the development and implementation of necessary policies to ensure data assurance and reduce vulnerabilities in information technology. ***Thus, hypotheses 8c are supported.***

Finally, the result shows that regulatory has significant effect on information technology control ($\beta_{46} = 0.421$, $p < 0.01$). Based on the above results, financial reporting is governed by accounting norms and standards that support the measurement, disclosure, presentation, and recognition of financial information. These reports must be prepared for stakeholders, creditors, investors, and regulatory organizations. Financial reporting is used for making informed lending and investment decisions by providing complete information (De Villiers & Sharma, 2020). Financial reports play a crucial role in investment decisions. Traditional methods of financial reporting often led to errors and inefficiencies. Modernizing financial processes with advanced information technology helps improve the accuracy, transparency, and reliability of the reports. (Ashraf et al., 2020). This enhances the accuracy, efficiency, and quality of the financial reporting process. However, the use of information technology depends on other factors, such as usability and the purpose of technology. Therefore, the use of information technology must be controlled in accordance with regulations and standards to ensure the information is accurate and reliable. Regulations impact information technology controls because technology is increasingly used in audits to improve audit efficiency. Still, information technology use must be regulated to ensure compliance with regulations and standards, ensuring that operations are effective and trustworthy. As stated in Riyadi et al. (2021) research, auditors must perform audits according to generally accept auditing standards set by the Accounting Professional Council. Auditing standards comprise fundamental principles and key auditing

procedures, as well as related practices, which help prevent deficiencies in audit work. ***Thus, hypotheses 8d are supported.***

Summary

Table 17: The summary of hypothesized relationships

Hypothesis	Description of Hypothesized Relationships	Results
H1a	Financial statement audit have a positive effect on reducing audit risk	**Accept**
H1b	Financial statement audit have a positive effect on data security	**Accept**
H2a	Operational audit have a positive effect on reducing audit risk.	**Accept**
H2b	Operational audit have a positive effect on data security	**Accept**
H3a	Compliance audit have a positive effect on reducing audit risk	**Accept**
H3b	Compliance audit have a positive effect on data security	**Reject**
H4a	Information technology control have a positive effect on reducing audit risk	**Accept**
H4b	Information technology control have a positive effect on data security	**Accept**
H5a	Reducing audit risk have a positive effect on audit quality	**Accept**
H5b	Data security have a positive effect on audit quality.	**Accept**
H6a	Technological change awareness have a positive effect on financial statement audit	**Reject**

Table 17: The summary of hypothesized relationships (continued)

Hypothesis	Description of Hypothesized Relationships	Results
H6b	Technological change awareness have a positive effect on operational audit	**Accept**
H6c	Technological change awareness have a positive effect on compliance audit	**Accept**
H6d	Technological change awareness have a positive effect on information technology control	**Accept**
H7a	Business environment have a positive effect on financial statement audit	**Reject**
H7b	Business environment have a positive effect on operational audit	**Accept**
H7c	Business environment have a positive effect on compliance audit	**Reject**
H7d	Business environment have a positive effect on information technology control	**Accept**
H8a	Regulatory have a positive effect on financial statement audit	**Reject**
H8b	Regulatory have a positive effect on operational audit	**Reject**
H8c	Regulatory have a positive effect on compliance audit	**Accept**
H8d	Regulatory have a positive effect on information technology control	**Accept**

พหุน ปณ ฑิโต ชีเว

CHAPTER V

CONCLUSION

This research focuses on inspecting the Impact of information technology auditing (financial Statement audit, operational audit, compliance audit and information technology control) and audit outcomes (reducing audit risk, data security and audit quality) of Auditors in the Capital Market in Thailand. Additionally, Impact of antecedent's variables on each dimension of Information Technology Audit. This research proposes that Antecedents is (technology change awareness, business environment and regulatory).

Summary

This research investigates the relationships among each dimension of information technology audit, reducing audit risk, data security and audit quality of auditors in the Capital Market in Thailand. The newly proposed dimensions of information technology audit are comprised of financial statement audit, operational audit, compliance audit, and information technology control. In addition, technological change awareness, business environment, and regulatory are designed as the antecedents of information technology audit. In terms of auditing skill are proposed to be control variables that are included in each equation of regression analysis.

Thus, the main question of this study is: (1) To test the relationship between information technology audit has a positive impact on reducing audit risk? (2) To test the relationship between information technology audit has a positive impact on data security? (3) To test the relationship between reducing audit risk has a positive impact on audit quality? (4) To test the relationship between data security has a positive impact on audit quality? (5) To test the relationship between technological change awareness, business environment, regulatory have a positive impact on information technology audit?

The purpose of this study is: (1) To study information technology audit have a positive impact on reducing audit risk (2) To study information

technology audit has a positive impact on data security (3) To study reducing audit risk has a positive impact on audit quality (4) To study data security has a positive impact on audit quality (5) To study technological change awareness, business environment, regulatory have a positive impact on information technology audit

The population of this research consists of Auditors in the Capital Market in Thailand. Auditors in the Capital Market are certified public accountants who have been approved by the Office of the Securities and Exchange Commission (SEC). A suitable sample of 365 Auditors in the Capital Market was sent questionnaires via mail, and 93 questionnaires were returned, accounting for 25.48%.

A review of the literature on information technology auditing indicates that most previous research has focused on the importance of information technology audit services in relation to the implementation of information technology (Weidenmier & Ramamoorti, 2006). The growing interest in information technology auditing has led to an increased demand for guidelines on information technology audit practices, making information technology auditing a compelling topic. Additionally, there are other issues that previous research has yet to explore (Aditya et al., 2018). The use of information technology by companies has made information technology a vital tool in modern business. It serves as a driving force for national development, transforming service delivery through digital data and the creation of new service systems via technology. The continuous growth of information technology has led to the evolution of information technology threats. Consequently, information technology auditing has become crucial in mitigating the increasing vulnerabilities and threats in information technology. information technology auditing involves overseeing the efficiency and management of information systems, including the examination of security controls and information technology risk management. (ISACA, 2013). This ensures the accuracy and reliability of information, thereby enhancing the effectiveness of auditors in their audit practices. Considering information that is reliable and adequately sufficient enables auditors to express opinions and exercise

professional skepticism, which helps reduce the risk of overlooking suspicious situations or erroneous assumptions during evidence gathering and audit evaluation. There is limited empirical research that explores the dimensions of information technology auditing and its impact on audit quality outcomes. Therefore, this research aims to fill these gaps. Two theories are utilized to explain the phenomena: defense-in-depth theory and contingency theory. defense-in-depth theory This explains the relationship between the factors affecting auditors' work, highlighting that the environment is a crucial factor influencing the audit process. Rapid technological advancements, environmental changes, and regulations exert pressure on auditors to adapt their practices. As the environment evolves and information technology threats increase, there is a growing need for intrusion detection, information security, and information technology security measures. Consequently, the scope of auditors' work has expanded in response to information technology threats, ensuring that the use of information technology is appropriate and secure according to standards. Meanwhile, Contingency Theory explains the relationship reducing audit risk and data security impact on the audit quality, suggesting that choosing an appropriate approach leads to successful performance outcomes. For example, the increasing reliance on information technology has led to information technology threats that compromise information security. Incomplete or erroneous information can hinder auditors' work, making information technology auditing crucial for evaluating, overseeing, and controlling information technology operations effectively. This ensures that the information produced is appropriate and can be used for professional judgment and skepticism by auditors.

According to the first research question, the results found that financial statement audit has a positive influence on reducing audit risk. operational audit has a positive influence on reducing audit risk. Compliance audit has a positive influence on reducing audit risk. Moreover, information technology control has a positive influence on reducing audit risk.

In the second research question, the results found that financial statement audit has a positive influence on data security, operational audit has a positive

influence on data security, and Information technology control has a positive influence on data security.

The finding in the third research question showed that reducing audit risk has a positive influence on audit quality.

The finding, according to the fourth research question found that data security has a positive influence on audit quality.

The discovery in the fifth research question found that technological change awareness has a positive effect on compliance audit, and Information technology control. Next, business environment has a positive effect on operational audit, and Information technology control. In addition, regulatory has a significantly positive effect on compliance audit, and Information technology control. In summary, the results are concluded and provided in Table 18

Discussion

First, according to hypotheses 1a and 1b, the findings were that financial statement audit has significant effect on reducing audit risk and data security. This is consistent with the research of Alktani and Ghareeb (2014), This result indicates that auditing accounting information and financial reports will help ensure the completeness and reliability of the information because the auditing process requires caution and careful planning. Therefore, reliable information will help auditors work effectively, make the audit and certification of financial statements accurate and precise, and reduce errors in expressing opinions in financial statements (Salameh, 2011). And this is consistent with the research of Riyadi et al. (2020), who stated that if auditors increase their efforts in auditing and sufficiently test materiality, information security incidents will not result in a decrease in audit quality. This means that if auditors have thoroughly checked accounting information and materiality, it will help ensure the information is secure and maintain audit quality.

Second, according to hypotheses 2a and 2b, the findings were that operational audit has significant effect on reducing audit risk and data security. This is consistent with the research of Peecher et al. (2006), operational audit procedures and methods of operation contributes to confidence that these procedures are carried out effectively and helps reduce the auditor's audit risk, including the risk of inappropriate expression of opinions on the financial report. Bagchi (2006) stated that the audits help reduce data risk and improve data efficiency. Quality data can lower audit risk and enhance audit effectiveness (Hall, 2011). The audit process helps eliminate or minimize losses.

Third, according to hypotheses 3a, the findings were that compliance audit has significant effect on reducing audit risk. This is consistent with the research of Gantz (2014) stated that Auditing has become a crucial part of risk reduction, ensuring that business operations, data processing, and reporting are efficient and enhancing the reliability of audit information. It also helps ensure compliance with laws and regulations, thereby reducing audit risk. This is consistent with the research of Judijanto et al. (2023), which states that compliance audits are a key factor. Organizations that adhere to regulatory requirements tend to conduct more effective audits, which can reduce inaccuracies in financial reporting.

Fourth, according to hypotheses 3b, the findings were that compliance audit has no significant effect on data security. This is consistent with the research of Duncan & Whittington (2014). which states that compliance audits are conducted to ensure that the organization adheres to various standards and regulations. These audits can identify gaps and weaknesses and help the organization address these issues. However, on the other hand, compliance audits do not always imply that the organization has robust information security. Sometimes, compliance may be considered more fundamental than a comprehensive security strategy. An organization may be compliant with regulations but still be vulnerable to emerging threats if its security measures are outdated or incomplete.

Fifth, according to hypotheses 4a and 4b, the findings were that information technology control has significant effect on reducing audit risk. The empirical results verify the establishment of the study hypotheses. This result indicates that Information Technology Control involves assessing Information Technology related risks, which helps ensure that an organization's data or information is protected and reduces the risks associated with the use of technology within the organization. These risk control activities include auditing and controlling the processing of Information Technology data, auditing and controlling data completeness, auditing and controlling security and privacy systems, safeguarding Information Technology assets, auditing and controlling system maintenance and program modifications, continuous monitoring and controlling of data processing, auditing and controlling system applications, and auditing and controlling system development. This is consistent with Arens et al. (2017), who stated that auditing standards address two types of controls for auditing: 1) General controls, which apply to all IT functions, including IT management, system development alternatives, physical and online security related to access to hardware, software, and data, backup planning and contingency for unforeseen emergencies, and hardware controls; and 2) Application controls, which are procedures and methods within application systems to ensure that all transactions are approved, recorded, and processed completely, accurately, and timely, thereby enhancing the reliability of data or information. Effective information helps auditors accurately assess risks, which is crucial for preparing audit reports that enable auditors to reach reasonable conclusions. Reliable and adequate information helps auditors' express opinions and exercise professional judgment appropriately, which reduces the risk of overlooking suspicious situations or incorrect assumptions in evidence collection and audit evaluation. (Petter Lovaas, 2012).

Sixth, according to hypotheses 5a and 5b, the findings were that reducing audit risk and data security has significant effect on audit quality. Consistent with the research by Hurtt, R. K. (2011), audit risk is positively related to the performance of audits in terms of the sufficiency and appropriateness of audit evidence. The use of professional judgment, including observation and

skepticism, helps reduce the risk of overlooking suspicious situations or using incorrect assumptions in evidence collection and audit evaluation. Auditors must prioritize professional judgment and skepticism as tools to ensure the quality of accounting information and provide benefits to financial statement users. (AlShaer, 2020). Additionally, audit risk can impact the effectiveness of financial reporting. Reducing audit risk affects the accuracy and reliability of financial reports, which in turn influences the overall effectiveness of the audit. And research of Westland's (2021) research indicates that cybersecurity incidents can reduce data integrity, preventing auditors from relying on the accuracy of the data, which affects audit quality. Therefore, auditors should consider and assess the impact of such risks on the audit.

Seventh, according to hypotheses 6a, the findings were that technology change awareness has no significant effect on financial statement audit. Consistent with the research by Mohammadi (2012) Information technology leads to changes in the traditional organizational structure, resulting in profound changes in the organization's mission and objectives. The most important features of technology are high-speed data processing, real-time access, and modern electronic data exchange. It also provides high-quality information at a low cost. Auditing must also adopt new methods or approaches to deliver services and perform duties. Particularly, the accounting and auditing profession may encounter various conveniences and possibilities in the new environment. This creates new opportunities for recording and reporting data, leading to increased efficiency and effectiveness in the profession. Therefore, the research of Nurjannah (2019) believes that audit quality involves conducting the audit process efficiently and effectively according to auditing standards, by identifying errors and irregularities and taking action to meet the needs and requirements of financial statement users. Therefore, awareness of technology change may not impact the financial statement audit, as auditing continues to adhere to standard criteria in the audit process.

Eight, according to hypotheses 6b, the findings were that technology change awareness has significant effect on operational audit. Currently, organizations are increasing their investments in information technology because they recognize the tremendous benefits that Information technology can provide to their operations and service delivery. (Brynjolfsson & Hitt, 2011; Chen & Zhu, 2004; Devaraj & Kohli, 2003; Kohli & Grover, 2008) However, the research by Yayla & Hu (2014) provides evidence that a high level of information technology awareness leads to improved company performance. Nonetheless, the rapid technological changes and increasing complexity make it difficult for organizations to develop a consistent approach between their business strategies and the digital platforms created to support these strategies. (Bradley et al., 2011; Schmidt & Buxmann, 2011) Therefore, operational audit is conducted to ensure that operations or procedures within various departments of an organization are efficient, resources are used effectively, and the organization's objectives and goals are achieved. The focus is on efficiency, effectiveness, and the economy of the activities. Thus, awareness of technology changes plays a pivotal role in transforming operational audits, with significant implications for audit effectiveness and the evolution of auditing as a practice in a technology-driven environment.

Ninth, according to hypotheses 6c and 6d, the findings were that technology change awareness has significant effect on Compliance audit and Information technology control. Consistent with the research by Okereafor, A. A. (2008) from the results, it can be said that information technology offers numerous benefits but also involves associated risks. For example, computer assets may be lost or stolen, the likelihood of fraud may increase, improper use of technology could lead to a competitive disadvantage, data may be lost or stolen, privacy could be breached, and business operations might be disrupted by these risks. This necessitates the implementation of technology security controls and the protection of confidential information. Therefore, continuous monitoring to respond to preventive measures is essential for managing the risks and benefits associated with information technology, such as: (1) Cybercrime involving individuals or groups seeking financial gain from exploiting systems;

(2) Cyberattacks often linked to political motivations for data collection; and (3) Cyberterrorism aimed at causing damage to electronic systems. It is necessary to have systems for auditing and managing information technology projects, overseeing information technology, and implementing security management systems to ensure compliance with laws and regulations. (Santy Setiawan, 2020). And Zhang et al., (2015). Information technology often comes with risks, such as data breaches, security issues, and software errors, which can undermine stakeholder confidence and negatively impact performance. These risks are not only technical issues related to Information technology but also represent internal control problems for management. Therefore, Information technology controls by information systems auditors are essential for assessing Information technology related risks. This helps ensure that an organization's data or information is protected and that risks associated with the use of technology within the organization are minimized. This risk control activity includes the auditing and control of Information technology data processing, the verification and control of data completeness and accuracy, the auditing and control of security and privacy systems, the protection of Information technology assets, the auditing and control of system maintenance and program modifications, the continuous auditing and control of data processing, the auditing and control of system applications, and the auditing and control of system development.

Tenth, according to hypotheses 7a, the findings were that business environment has no significant effect on financial statement audit. Consistent with the research by Mohammadi (2012) changing environment will impact the transformation of traditional organizational structures. Auditing will also need to adopt new methods or approaches to deliver services and perform duties. In particular, the accounting and auditing profession may encounter various conveniences and possibilities in the new environment. This creates new opportunities for recording and reporting information, resulting in increased efficiency and effectiveness in auditing. According to Betti and Sarens (2020) as business operations evolve, the increasing importance of technology and information must be considered. Auditing must also develop and adapt to the business environment, understanding that the use of tools and technology

impacts the auditing process. However, financial statement audits must continue to adhere to auditing standards, professional ethics and morals, auditing guidelines, as well as the rules and procedures established by professional organizations to regulate the auditing profession and maintain the independence and integrity of auditors. (Menezes Brás, 2018).

Eleventh, hypotheses 7b, the findings were that business environment has significant effect on operational audit. Auditing has continuously evolved and adapted to the changing business environment, understanding that the use of tools and technology significantly impacts financial reporting. Additionally, the profession has been affected by changes in auditing methods, review processes, and professional development, which are considered essential characteristics of the profession (Federation of Accounting Professions, 2014). According to Betti and Sarens (2020). as business operations evolve, the increasing importance of technology and information must be considered, and auditing must also develop and adapt to the business environment.

Twelfth, hypotheses 7c, the findings were that the business environment has no significant effect on compliance audit. The research by Eilfsen et al. (2020) states that environmental pressures play a significant role in the adoption of information technology by companies, making Information technology a crucial tool for modern businesses. The continuous growth of information technology has led to the evolution of Information technology threats, causing operational disruptions and errors. The increased use of technology should not escalate risks to a point where companies cannot manage them. Therefore, each organization's Information technology must be assessed and managed due to the current risks posed by technological hazards (Devale, 2012). ISACA has stated that frequent changes in technology, demands, competition, and regulatory developments force businesses to adapt quickly. However, the research indicates that these changes do not always alter the fundamental principles or effectiveness of compliance audits. The role of auditing remains to ensure the effectiveness of controls and compliance, rather than responding to every change in the business environment (Alexiou, 2019).

Thirteenth, hypotheses 7d, the findings were that business environment has significant effect on information technology control. The research by Zhong and Chen (2023) confirm that the business environment has a significant impact on information technology controls, particularly through its influence on technology innovation and organizational governance. The research highlights that a well-adapted business environment fosters high-quality economic development by promoting innovation, which in turn requires more stringent information technology controls to manage the associated risks. Consistent with the research by Rubino et al. (2017), information technology controls help organizations better assess and manage risks, which is particularly crucial in a constantly changing business environment. The research indicates that the business environment significantly impacts information technology control systems. External and internal pressures from the business environment, such as market demands and technological advancements, drive organizations to adjust their information technology controls accordingly. These adjustments are essential for maintaining operational efficiency, ensuring data integrity, and reducing risks such as fraud or data breaches. Therefore, information technology controls are relevant to business adaptation in a constantly evolving business context, where technology or market conditions are perpetually changing. Organizations must continuously update and enhance their information technology controls to ensure that they remain effective and aligned with business objectives. (Saukkonen & Kirjavainen, 2019).

Fourteenth, hypotheses 8a, the findings were that regulatory has no significant effect on financial statement audit. Changing regulatory impacts, the operations and financial reporting of companies, including shifts in business, the economy, laws, and regulations, making it necessary to have appropriate responses and disclosures in financial statements. Additionally, this affects the auditing process, as auditors need to expand their work to address the increased risk of significant misstatements in financial statements. However, auditors are responsible for providing an opinion on whether they have obtained reasonable assurance that the financial statements are free from material misstatement,

whether due to fraud or error, and must present accurate information in accordance with relevant accounting standards (Judijanto et al., 2023).

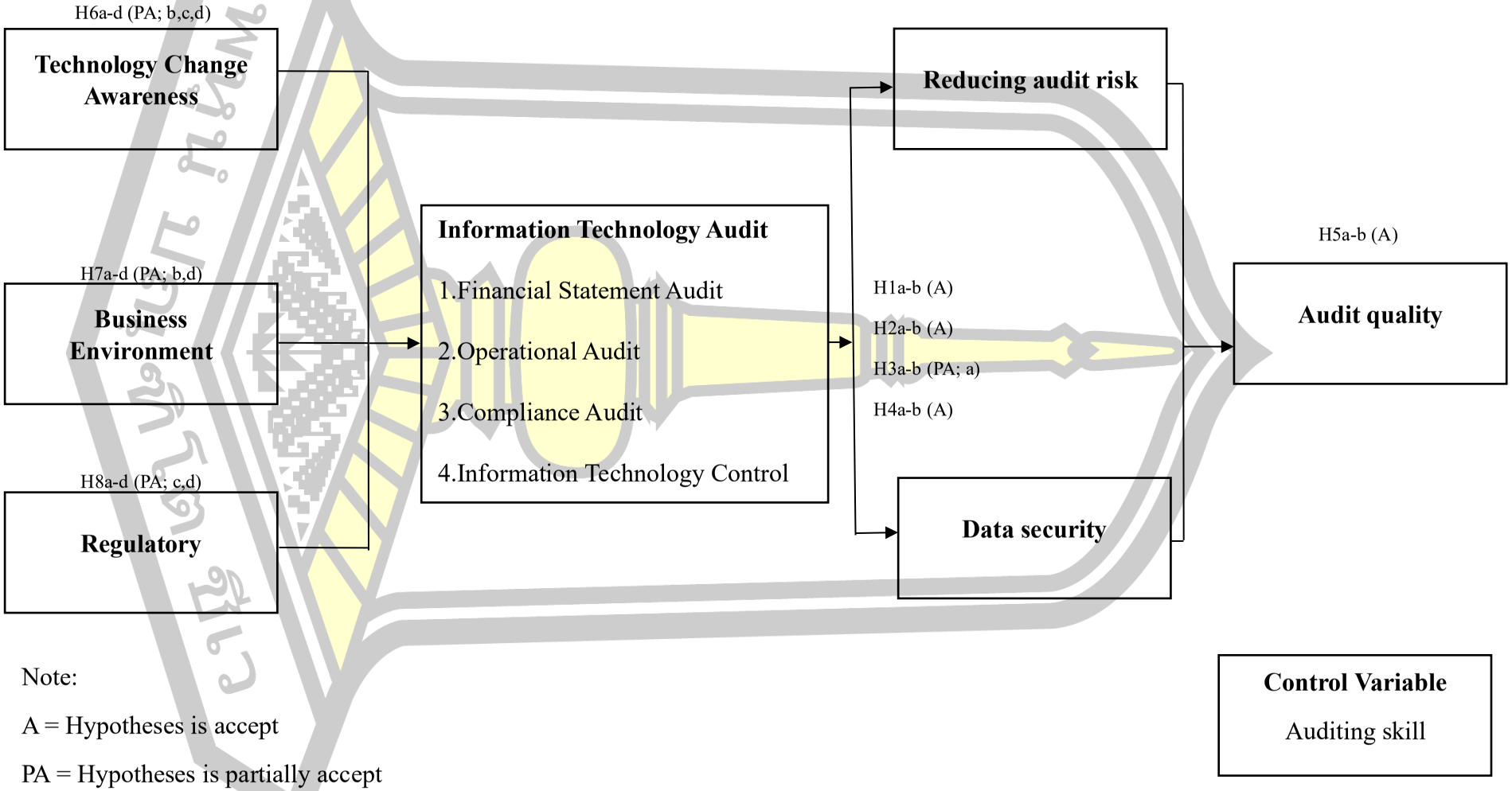
Fifteenth, hypotheses 8b, the findings were that regulatory has no significant effect on operational audit. The research by Hilali et al. (2020) states that increased regulations focusing on privacy and cybersecurity have added complexity to businesses. This has led to an emphasis on information technology audits to control and secure information technology. Therefore, the growing regulatory requirements necessitate changes in business processes and create a need to evaluate and review practices to ensure they are appropriate and comply with standards Operational Audit is the examination of operational systems, methods, and processes with the objective of improving performance. This type of audit focuses on reviewing each step of the operational process, including measuring actual performance against the organization's established standards. It emphasizes comparing the performance with resource usage, evaluating whether the output/input ratio is cost-effective (Fadhilah, 2022). Thus, regulations affect business operations, but operational auditing is a process where auditors examine an organization's practices to improve performance. Some studies suggest that in certain situations, regulatory changes may have little or no impact on operational audits, particularly when the changes do not alter the core processes or risk factors being audited. This is especially the case if the operational audit focuses more on internal efficiency rather than regulatory compliance (KPMG, 2020).

Sixteenth, hypotheses 8c, the findings were that regulatory has significant effect on Compliance audit. the role of audit management extends beyond this. ISO 27001 states that applying the standard for managing information security helps to strengthen data security systems, reduce risks, and protect data from theft. COBIT is applied to control and maintain information technology security, ensuring confidence and reliability in the use of information technology, and increasing the reliability of the data processed and stored within information

systems. (Riad, 2015). The role of information technology auditing is crucial to the success of an organization. Currently, providing guidance on information technology control issues related to business processes helps promote the development and implementation of necessary policies to ensure data assurance and reduce vulnerabilities in information technology.

Finally, hypotheses 8d, the findings were that regulatory has significant effect on information technology control. Financial reporting is used for making informed lending and investment decisions by providing complete information (De Villiers & Sharma, 2020). Financial reports play a crucial role in investment decisions. Traditional methods of financial reporting often led to errors and inefficiencies. Modernizing financial processes with advanced information technology helps improve the accuracy, transparency, and reliability of the reports. (Ashraf et al., 2020). This enhances the accuracy, efficiency, and quality of the financial reporting process. However, the use of information technology depends on other factors, such as usability and the purpose of the technology. Therefore, the use of information technology must be controlled in accordance with regulations and standards to ensure the information is accurate and reliable. Regulations impact information technology controls because technology is increasingly used in audits to improve audit efficiency. Still, information technology use must be regulated to ensure compliance with regulations and standards, ensuring that operations are effective and trustworthy. As stated in Riyadi et al. (2021) research, auditors must perform audits according to generally accept auditing standards set by the Accounting Professional Council. Auditing standards comprise fundamental principles and key auditing procedures, as well as related practices, which help prevent deficiencies in audit work.

Figure 5: Summary of the results in relationships of the conceptual model.



Note:

A = Hypotheses is accept

PA = Hypotheses is partially accept

R = Hypotheses is reject

*T*able 18: Summary of results is all research questions

Research Question	Hypothesis	Results	Conclusion
1) To test the relationship between information technology audit has a positive impact on reducing audit risk?	H1a H2a H3a H4a	Financial statement audit, Operational audit, Compliance audit, and Information Technology Control has a positive influence on reducing audit risk.	Accept
2) To test the relationship between information technology audit has a positive impact on data security?	H1b H2b H3b H4b	Financial statement audit, Operational audit, and Information Technology Control has a positive influence on data security.	Partially Accept
3) To test the relationship between reducing audit risk has a positive impact on audit quality?	H5a	Reducing audit risk has a positive influence on audit quality.	Accept

Research Question	Hypothesis	Results	Conclusion
4) To test the relationship between data security has a positive impact on audit quality?	H5b	Data security has a positive influence on audit quality.	Accept
5) To test the relationship between technological change awareness, business environment, regulatory have a positive impact on information technology audit?	H6a-d H7a-d H8a-d	Technological change awareness has a positive influence on Compliance audit and Information Technology Control. Business environment has a positive influence on Operational audit and Information Technology Control. Regulatory has a positive influence on Compliance audit and Information Technology Control.	Partially Accept Partially Accept Partially Accept

Theoretical and practical contributions

The conceptual model analyzed in this research provides theoretical contributions and practical contributions as follows.

Theoretical contributions

The relationships among dimensions of information technology audit, consequences, and antecedent construct, are the purposes of this research. The discovery provides theoretical contributions as follows.

Firstly, the defense-in-depth theory was developed and recognized to ensure information security. Ensuring information security helps to address future events, such as technological advancements that may lead to technological threats. Intrusion detection has become essential, and organizations should have appropriate methods for selecting and implementing technology. Since information and information technology security ensures the accuracy and reliability of information, the best practice is to review information technology, considering defense-in-depth as a foundation. This helps reduce anomalies and enhance data security. The increasing technological threats necessitate intrusion detection and the protection of information and information technology. As a result, the scope of work for auditors has expanded following technological threats to ensure that the use of information technology is appropriate and secure according to standards.

Finally, contingency theory was applied to explain how external environments impact operations, or how situations determine decision-making and appropriate management styles. Similarly, changes in the current economic, social, and technological systems have transformed traditional business and service processes to better respond to the changing environment and meet customer expectations. Additionally, auditing has been affected by the rise of information technology following technological threats, leading to an expansion of auditors' scope to include information technology audits and creating opportunities for auditors to respond to changes in the environment.

Practical contributions

The results of this research help auditors in the Capital Market understand and identify key dimensions of professional auditing expertise, which can be applied in practices to improve the value of their audit outcomes.

The results of this research indicate that information technology auditing is a crucial component that enhances the efficiency of data processing and reporting while also increasing the reliability of information. Since auditors must exercise caution and careful planning, reliable information enables auditors to work more effectively and reduces the risk of inappropriate opinions. Therefore, information technology auditing ensures that data is protected and minimizes risks associated with an organization's use of technology. Reliable and secure information allows auditors to perform their duties more efficiently.

Limitations and future research directions

Limitation

This study is not without limitations. The sample size of this research the number of responses from the sample group is relatively small. As a result, it may affect the analysis of the power of the statistical test so that the results of the hypotheses are also impacted.

Despite these limitations, this study serves as an initial effort to contribute to the understanding of information technology auditing by auditors in the Capital Market in Thailand.

Future research direction

According to the results of this research, there are many suggestions for future research as follows.

The results of this study show that some of the research hypotheses are not statistically significant. Future research may reinvestigate the research hypotheses that are not statistically significant and need to expand the research contributions by collecting data from other populations in order to increase the level of reliable results.

REFERENCES

Aaker, D. A., Kumar, V., & George, Day, S. (2001). Marketing Research (7th. ed.). Hoboken, NJ: Wiley.

Aditya, B. R., Ferdiana, R., & Santosa, P. I. (2018). Toward Modern IT Audit-current issues and literature review. 2018 4th International Conference on Science and Technology (ICST). https://doi.org/10.1109/icstc.2018.8528627

Agoes, Sukrisno dan Jan Hoesada. (2012). Bunga Rampai Auditing. Jakarta: Salemba Empat

Albrecht, W. S., Albrecht, C., & Albrecht, C. C. (2015). Fraud Examination. Cengage Learning.

Alexiou, S. (2019). Trends, challenges and strategies for effective audit in a rapidly changing landscape. ISACA Journal, 6. Retrieved from https://www.isaca.org/resources/isaca-journal/issues/2019/volume-6/trends-challenges-and-strategies-for-effective-audit-in-a-rapidly-changing-landscape google schola

Ali, M. A., Hussin, N., Flayyih, H. H., Haddad, H., Al-Ramahi, N. M., Almubaydeen, T. H., Hussein, S. A., & Abunaila, A. S. H. (2023). A multidimensional view of intellectual capital and dynamic innovative performance. Journal of Risk and Financial Management, 16(3), 139. https://doi.org/10.3390/jrfm16030139

Alktani, S. a. (2014). Evaluation of the quality of the internal auditing position in the public sector in Saudi Arabia: An applied study. Global Review of Accounting and Finance.

Al-Shaer, H. (2020). Sustainability reporting quality and post-audit financial reporting quality: Empirical evidence from the UK. Business Strategy and the Environment, 29(6), 2355–2373. https://doi.org/10.1002/bse.2507

Anastasi, A. &. (1997). Psychological Testing . Upper Saddle River, NJ: Prentice Hall.

Appelbaum, D., Kogan, A., & Vasarhelyi, M. A. (2017). Big Data and Analytics in the Modern Audit Engagement: Research Needs. *Auditing: A Journal of Practice & Theory*, 36(4), 1-27.

Arab Mazar Yazdy, M. (2001). Impact of new information technology on internal controls. Journal of Accounting, 146.

Arens, A. A., Elder, R. J., & Beasley, M. S. (2012). Auditing and Assurance Services: An Integrated Approach

Arens, A. A., Elder, R. J., & Beasley, M. S. (2017). Auditing and Assurance Services, Global Edition (17th Edition). In Prentice Hall eBooks.

Arens, A. R. (2015). Auditing & Jasa Assurance. Erlangga: Edisi Kelimabelas.

Arias-Oliva, M., Pelegrín-Borondo, J., & Matías-Clavero, G. (2019). Variables Influencing Cryptocurrency use: A technology acceptance model in Spain. Frontiers in Psychology, 10. https://doi.org/10.3389/fpsyg.2019.00475

Asare, S., K. Hackenbrack, and W. R. Knechel. 1994. Client acceptance and continuation decisions. In Auditing Symposium XII: Proceedings of the 1994 Deloitte and Touche/University of Kansas Symposium on Auditing Problems, edited by R. P. Srivastava, 163–178 Lawrence, KS: University of Kansas.

Ashraf, M., Michas, P. N., & Russomanno, D. (2020). The impact of Audit Committee Information Technology expertise on the reliability and timeliness of financial reporting. The Accounting Review, 95(5), 23–56. https://doi.org/10.2308/accr-52622

Attaran, M. (2003). Information technology and business-process redesign. Business Process Management Journal, 9(4), 440–458. https://doi.org/10.1108/14637150310484508

Azizi, N. M., Hakimi, M., Amiri, N. F., & Shahidzay, N. a. K. (2024). The role of IT (Information Technology) Audit in Digital Transformation: Opportunities and challenges. Open Access Indonesia Journal of Social Sciences, 7(2), 1473–1482. https://doi.org/10.37275/oaijss.v7i2.230

Badavar Nahandy, J. H. (2011). IT Auditing. Conference on Emerging Trends in Computer Engineering and Information Technology. Roudsar: lslamic Azad University.

Bagchi, S.K. (2006). Commercial Bank Audit–Need for a Multidimensional

Approach with Focus on Disclosure Requirement under Basel Accord II. The Chartered Accountant, April, 1475-1480.

Bagranoff, N., Vendrzyk, V. (2000). The changing role of IS audit among the big five accounting firms, Information Systems Control Journal, 5 .33-7.

Beekman, N., Sier, D., & Thompson, J. (2017). Risk management in information security. Journal of Cybersecurity.

Bell, T. B., Causholli, M., & Knechel, W. R. (2015). Audit firm tenure, Non-Audit services, and internal assessments of audit quality. Journal of Accounting Research, 53(3), 461–509. https://doi.org/10.1111/1475-679x.12078

Beridze, T. (2017). Information Technology Audit in Georgia. European Scientific Journal, 72.

Betti, N., & Sarens, G. (2020). Understanding the internal audit function in a digitalised business environment. Journal of Accounting & Organizational Change, 17(2), 197–216. https://doi.org/10.1108/jaoc-11-2019-0114

Bhattacharjee, S., Maletta, M. J., & Moreno, K. K. (2017). SOX Compliance and IT Controls. Journal of Information Systems.

Bita Mashayekhi & Alemeh Yazdanian. (2018). A Survey on Key Components of Internal Audit . Journal of Accounting and Auditing Review, 135-158.

Bob Duncan & Mark Whittington. (2014). Compliance with standards, assurance and audit: Does this equal security.Conference: Security of Information and Networks.

Bohren, C.F., and Hoffman, D.R. (1998) Absorption and scattering of light by small particles. A Wiley-interscience Publication, New York.

Bonner, S. & Pennington, N.(1991).Cognitive Processes and Knowledge as Determinants of Auditor Expertise, Journal of Accounting Literature,1-50.

Bradley, R. V., Pratt, R. M., Byrd, T. A., & Simmons, L. L. (2011). The role of enterprise architecture in the quest for IT value. MIS Quarterly Executive, 10(2), 73-80.

Bradshaw, M. T. (2001). Do Analysts and Auditors Use Information in Accruals? Journal of Accounting Research, 45-73.

Brown-Liburd, H., Issa, H., & Lombardi, D. (2015). Behavioral implications of big data's impact on audit judgment and decision making and future research directions. Accounting Horizons, 29(2), 451–468. https://doi.org/10.2308/acch-51023

Brynjolfsson, E., and Hitt, L.M. (2000). Beyond computation: Information technology, organization transformation and business performance. Journal of Economic Perspectives, 14(4): 23-48.

Byrnes, P. E., Al-Awadhi, A., Gullvist, B., Brown-Liburd, H., Teeter, R., Warren Jr, J. D., & Vasarhelyi, M. (2018). Evolution of auditing: From the traditional approach to the future audit. Continuous auditing: Theory and application, 285-297.

Caballero, A. (2013). Information Security Essentials for IT Managers. In Elsevier eBooks (pp. 379–407). https://doi.org/10.1016/b978-0-12-394397-2.00021-0

Campbell, S. B. (1995). Behaviour problems in preschool children: A review of recent research. Journal of Child Psychology and Psychiatry, 113-149.

Cannon, D. M., & Growe, G. A. (2004). SOA compliance: Will IT sabotage your efforts? Journal of Corporate Accounting & Finance, 15(5), 31–37. https://doi.org/10.1002/jcaf.20035

Carcello, J. V., & Nagy, A. L. (2004). Client size, auditor specialization and fraudulent financial reporting. Managerial Auditing Journal, 19(5), 651–668. https://doi.org/10.1108/02686900410537775

Carolita, M. K., & Rahardjo, S. N. (2012). PENGARUH PENGALAMAN KERJA, INDEPENDENSI, OBJEKTIFITAS, INTEGRITAS, KOMPETENSI, DAN KOMITMEN ORGANISASI TERHADAP KUALITAS HASIL AUDIT. (STUDI PADA KANTOR AKUNTAN PUBLIK DI SEMARANG). DJA (Diponegoro Journal of Accounting), 1(1), 771–780.

Carroll, M. (2007). An Information Systems Auditor's Profile. University of South Africa.

Cascarino, R. E. (2012). Auditor's Guide to IT Auditing. Wiley.

Cereola, S.J., Cereola, R.J.: Breach of data at TJX: an instructional case used to study COSO and COBIT, with a focus on computer controls, data security, and privacy legislation. Issues Account. Educ. 26, 521–545 (2011)

Chandler, A. D. (1962). Strategy and Structure: Chapters in the History of the American Industrial Enterprise. http://ci.nii.ac.jp/ncid/BA77058084

Chen, L. (2018). The impact of audit quality disclosure on auditor effort: Evidence from the banking industry. Journal of Banking and Finance, 42(1), 215-239. https://doi.org/10.1016/j.jbankfin.2017.11.008

Chen, Y., and Zhu, J. (2004). Measuring information technology's indirect impact on firm performance. Information Technology and Management, 5(1): 9-22.

Chou, D. C. (2015). Cloud computing risk and audit issues. Computer Standards &Amp; Interfaces, 137–142.

Cohen, J., Krishnamoorthy, G., & Wright, A. (2010). The Role of Internal Controls in Improving Financial Reporting Quality.

Curtis, E., & Turley, S. (2007). The business risk audit – A longitudinal case study of an audit engagement. Accounting Organizations and Society, 32(4–5), 439–461. https://doi.org/10.1016/j.aos.2006.09.004

Dai, J., & Vasarhelyi, M. A. (2017). Toward blockchain-based accounting and assurance. Journal of Information Systems, 31(3), 5-21.

Dale Stoel, D. H. (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, 60-79.

Dalibor P. Drljaca, B. L. (2016). Frameworks for Audit of an Information System in Practice. Journal of Information Technology and Applications, 78-85.

De Villiers, C., & Sharma, U. (2020). A critical reflection on the future of financial, intellectual capital, sustainability and integrated reporting. Critical Perspectives on Accounting, 70, 101999. https://doi.org/10.1016/j.cpa.2017.05.003

DeAngelo, L. (1981). Auditor Size and Audit Quality. Journal of Accounting

and Economics , 183-199.

Defond, M. &. (2014). A Review of Archival Auditing Research. Journal of Accounting and Economics, 275-326.

DeFond, M. L., & Zhang, J. (2014). A review of archival auditing research. Journal of Accounting and Economics, 58(2-3), 275-326.

Dehning, B., and Stratopoulos, T. (2002). DuPont analysis of an IT-enabled competitive advantage. The International Journal of Accounting Information Systems, 3(3): 165–176.

Denise Dickins, A. J.-S. (2018). Selecting an auditor for Bradco using indicators of audit quality. Journal of Accounting Education, 32-44.

Devale, A. a. (2012). Applications of Data Mining Techniques in Life Insurance. International Journal of Data Mining & Knowledge Management Process, 31-40.

Devale , A.B., and Kulkarni ,R.V. (2012).“A review of expert system in Information System Audit”, International Journal of Computer Science and Information Technologies (IJCSIT), vol. 3, no. 5, pp.5172-5175

Devaraj, S., and Kohli, R. (2003). Performance impacts of information technology: Is actual usage the missing link? Management Science, 49(3): 273-289.

DeZoort, F. T., & Taylor, M. H. (2015). COMMENTARY—A Public Interest View of Auditor Independence: Moving Toward Auditor Reliability When Considering and Promoting Audit Quality. Accounting and the Public Interest, 53-63.

Eilifsen, A., Kinserdal, F., Messier Jr, W. F., & McKee, T. E. (2020). An exploratory study into the use of audit data analytics on audit engagements. Accounting Horizons, 34(4), 75-103. https://doi.org/10.2308/HORIZONS-19-121

Eshitemi, B. &. (2016). Effect of Audit Quality on the Financial Performance of Listed Parastatals in Nairobi Security Exchange. Social Science and Humanity Journal, 186-199.

Eulerich, M., Masli, A., Pickerd, J., & Wood, D. A. (2022). The Impact of Audit

Technology on audit task Outcomes: Evidence for Technology-Based Audit Techniques*. Contemporary Accounting Research, 40(2), 981–1012. https://doi.org/10.1111/1911-3846.12847

Fadhilah, N. H. K. (2022). Management Audit on the process of selling Non-Cash Fuel oil to the Government at PT. ABC. Advances in Economics, Business and Management Research/Advances in Economics, Business and Management Research. https://doi.org/10.2991/aebmr.k.220204.039

Fargher, N. L., & Jiang, L. (2008). Changes in the audit environment and auditors' propensity to issue Going-Concern opinions. Auditing a Journal of Practice & Theory, 27(2), 55–77. https://doi.org/10.2308/aud.2008.27.2.55

Federation of Accounting Professions. (2010). ISA 200: Overall Objectives of the Independent Auditor and the Conduct of an Audit in Accordance with Auditing Standards. Federation of Accounting Professions.

Federation of Accounting Professions. (2014). International Standard on Auditing (ISA) 315 . Federation of Accounting Professions

Federation of Accounting Professions. (2018).Regulations of the Federation of Accounting Professions on the ethics of professional accountants. Federation of Accounting Professions.

Federation of Accounting Professions. (2020). Standard for Quality Management Issue 1. Federation of Accounting Professions.

Fiedler, F. E. (1972). Predicting the effects of leadership training and experience from the contingency model. Journal of Applied Psychology, 56(2), 114–119. https://doi.org/10.1037/h0032668

Filipek, R. 2007. IT audit skills found lacking. The Internal Auditor 64 (3): 15-16.

Francis, J. R. (2011). A Framework for Understanding and Researching Audit Quality. A Journal of Practice & Theory , 125–152.

Francis, J. R. (2011). A framework for understanding and researching audit quality. Auditing: A Journal of Practice & Theory, 30(2), 125-152.

Frost, R.B., and Choo, C.W. (2017). Revisiting the information audit: a

systematic literature review and synthesis. International Journal of Information Management, 37(1): 1380–1390.

Gantz, S. D. (2014). The Basics of IT Audit. Elsevier.

Gantz, S. D., & Philpott, D. R. (2013). The Basics of IT Audit.

Gaurav, B. (2020). 5 Cybersecurity Threats to Be Aware of in 2020. IEEE. https://www.computer.org/ publications/tech-news/trends/5-cybersecurity-threats-to-be-aware-of-in-2020

Genzorova, T., Corejova, T., & Stalmasekova, N. (2019). How digital transformation can influence business model, Case study for transport industry. Transportation Research Procedia, 40, 1053–1058. https://doi.org/10.1016/j.trpro.2019.07.147

George A. Drogalas. (2010). Internal audit contribution to efficient risk management. Journal of Business Administration, University of Macedonia.

Gray, R., Kouhy, R., & Lavers, S. (1995). Corporate social and environmental reporting. Accounting, Auditing & Accountability Journal, 1(1), 72-90.

Guan, D. C. (2004). The evolution of IT auditing and internal control standards in financial statement audits The case of the United States. Managerial Auditing Journal, 544-555.

Gul, F. A., Wu, D., & Yang, Z. (2013). Do Individual Auditors Affect Audit Quality? Evidence from Archival Data. The Accounting Review, 88(6), 1993–2023. https://doi.org/10.2308/accr-50536

Gupta, K. (2020). Contemporary Auditing. Tata Mcgraw Hill Education Private Limited.

Hair, J. B. (2010). Multivariate Data Analysis. New York: Pearson.

Hall, J. A. (2004). Information Technology Auditing and assurance. http://ci.nii.ac.jp/ncid/BB08363155

Hall, J. A. (2011). Information Technology Auditing and assurance(3 ed.). South-Western Cengage Learning.

Hall, J. A., & Singleton, T. (2018). IT Auditing and Application Controls for Financial Reporting and SOX Compliance.

Hermanson, D. R., Hill, M. C., & Ivancevich, D. M. (2000). Information Technology-Related Activities of Internal Auditors. Journal of Information Systems, 14(s-1), 39–53. https://doi.org/10.2308/jis.2000.14.s-1.39

Hudiwinarsih, G. (2010). AUDITORS' EXPERIENCE, COMPETENCY, AND THEIR INDEPENDENCY AS THE INFLUENCIAL FACTORS IN PROFESSIONALISM. Journal of Economics Business and Accountancy Ventura, 13(3). https://doi.org/10.14414/jebav.v13i3.18

Hurtt, R. K. (2010). Development of a Scale to Measure Professional Skepticism. Auditing: A Journal of Practice & Theory, 29(1), 149–171.

Hurtt, R. K. (2011). Development of a scale to measure professional skepticism. Auditing a Journal of Practice & Theory, 29(1), 149–171. https://doi.org/10.2308/aud.2010.29.1.149

IAASB. (2014). A Framework for Audit Quality: Key Elements That Create an Environment for Audit Quality (Vol. 3). IFAC.

"Information Systems Audit and Control Association. (22 October 2020). ISACA Updates IT Audit Framework (ITAF). Information Systems Audit and Control Association.

International Federation of Accountants. (2014). A Framework for Audit Quality, Key Elements That Create an Environment for audit quality. Federation of Accounting Professions of Thailand.

Isaca. (2019). Audit in the era of digital transformation.ISACA Journal. 6: 1-3.

ISACA. (2020). ISACA Updates IT Audit Framework (ITAF).https://www.isaca.org/about-us/newsroom/press-releases/2020/isaca-updates-it-audit-framework-itaf

ISACA.(2013).IT Audit Framework (ITAF™): A Professional Practices Framework for IT Audit (4th Edition). Printed in the United States of America.

Issa, H., Sun, T., & Vasarhelyi, M. A. (2016). Research Ideas for Artificial Intelligence in Auditing: The Formalization of Audit and Workforce Supplementation. Journal of Emerging Technologies in Accounting, 13(2), 1-20.

Ivanov, D., Dolgui, A., & Sokolov, B. (2018). The impact of digital technology and Industry 4.0 on the ripple effect and supply chain risk analytics. International Journal of Production Research, 57(3), 829–846. https://doi.org/10.1080/00207543.2018.1488086

Jamal Mohammadi., Ali Ghaffari., Alireza Hadavi., & Kamran Mohammadi. (2013). Analysis of the Role of Internal Control in Performing the Responsibility of Managers of Public Sector. European Online Journal of Natural and Social Sciences.2(3). 2321-2330.

Judijanto, L., Nurdiani, T. W., Ningsih, T. W., & Ryketeng, M. (2023). The effect of regulatory compliance and digital audit adoption on auditor performance and financial reporting accuracy in Indonesia. The ES Accounting and Finance, 2(01), 77–86. https://doi.org/10.58812/esaf.v2i01.154

Juiz, C. &. (2015). To govern IT, or not to govern IT? Communications of the ACM, 58-64.

Karagiorgos, T. (2010). Corporate social responsibility and financial performance : an empirical analysis on Greek companies. European Research Studies Journal, 13(4), 85-108.

Kayrak, M. (2012). Information Technology Audit in the Context of Information Criteria. Journal of Turkish Court of Accounts, 143-167.

Khalid Said Al Hilali, B. M. (2020). Coaching and Mentoring. Concepts and Practices in Development of Competencies: A Theoretical Perspective. International Journal of Academic Research in Accounting, Finance and Management Sciences, 41-54.

Klos, C., & Spieth, P. (2020). READY, STEADY, DIGITAL?! How foresight activities do (NOT) affect individual technological frames for managerial SENSEMAKING. Technological Forecasting and Social Change, 163, 120428. https://doi.org/10.1016/j.techfore.2020.120428

Klos, C., & Spieth, P. (2020). READY, STEADY, DIGITAL?! How foresight activities do (NOT) affect individual technological frames for managerial SENSEMAKING. Technological Forecasting and Social Change, 163,

120428. https://doi.org/10.1016/j.techfore.2020.120428

Knechel W.R., K. G. (2013). Audit Quality: Insights from the Academic Literature, Auditing. A Journal of Practice and Theory, 385-421.

Knechel, W. R. (2013). Do Auditing Standards Matter?.Current Issues in Auditing,7(2):A1-A16.

Knechel, W. R., Krishnan, G. V., Pevzner, M., Shefchik, L. B., & Velury, U. K. (2016). Audit Quality: Insights from the Academic Literature. Auditing A Journal of Practice & Theory. 32

Knechel, W. R., Krishnan, G., V., Pevzner, M., Bhaskar, L. S., & Velury, U. (2012). Audit Quality Indicators: Insights from the Academic Literature. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.2040754

Kohli, R., and Grover, V. (2008). Business value of IT: An essay on expanding research directions to keep up with the times. Journal of the Association for Information Systems, 9(1): 23-39.

KPMG.(2020).Creating dynamic controls amid continuing regulatory change. KPMG LLP. https://assets.kpmg.com/content/dam/kpmg/cn/pdf/en/2020/12/regulatory-change-management-enhancement-and-transformation.pdf

Krahel, J. P., & Vasarhelyi, M. A. (2014). The Future of Audit. Journal of Information Systems and Technology Management, 11(1).

Kramer, J. (2016). IT Audits and the Sarbanes-Oxley Act.

Kroll, M., Walters, B.A. and Wright, P. (2008), “Board vigilance, director experience, and corporate outcomes”, Strategic Management Journal, Vol. 29 No. 4, pp. 363-382.

Lawati,A. & Ali,s. (2015). Business perception to learn the art of Operating System auditing: A case of a local bank of Oman”, Proceedings of the 8th IEEE GCC Conference and Exhibition (GCCCE).

Liana Elefterie, G. B. (2016). Effect of Audit Quality on the Financial Performance of Listed Parastatals in Nairobi Security Exchange. Social Science and Humanity Journal, 186-199.

Libby, R. & Luf, J.(1993).Determinants of Judgment Performance in

Accounting Settings: Ability, Knowledge, Motivation, and Environment, Accounting Organizations and Society.425-450.

Lombardi, D. R., Bloch, R., & Vasarhelyi, M. A. (2015). The current state and future of the audit profession. Current Issues in Auditing, 9(1), P10-P16.

Lorentzon, J. I., Fotoh, L. E., & Mugwira, T. (2023). Remote auditing and its impacts on auditors' work and work-life balance: auditors' perceptions and implications. Accounting Research Journal, 37(1), 1–18. https://doi.org/10.1108/arj-06-2023-0158

Mahzan, N., & Veerankutty, F. (2011). IT auditing activities of public sector auditors in Malaysia. AFRICAN JOURNAL OF BUSINESS MANAGEMENT, 5(5), 1551–1563. https://doi.org/10.5897/ajbm09.423

Majdalawieh, M., & Zaghloul, A. (2009). IT Auditing: A Path to Improved Governance and Performance.

Majdalawieh, M., Zaghloul, I. (2009), Paradigm shift in information systems auditing. Managerial Auditing Journal, 24(4), 352-367.

Mark Muro, S. S. (2017). Advanced Industry, Digitalization, and Innovation Policy. Information Technology and Innovation Foundation and Metropolitan Policy Program at Brookings. Washington.

Markus, M. L., & Loebbecke, C. (2013). Commoditized digital processes and business community platforms: new opportunities and challenges for digital business strategies. MIS Quarterly, 37(2), 649–654. https://dialnet.unirioja.es/servlet/articulo?codigo=4277562

Mary-Jo Kranacher & Richard Riley (2019). Forensic Accounting and Fraud Examination (2nd Edition). John Wiley & Sons, Inc.

Menezes Montenegro, T., & Brás, F. A. (2018). A review of the concept and measures of audit quality across three decades of research. International Journal of Accounting, Auditing and Performance Evaluation, 14(2-3), 183-253.

Merhout, J. W. (2008). nformation Technology Auditing: A Value-Added IT Governance Partnership between IT Management and Audit. Communications of the Association for Information Systems.

Merhout, J. W., & Havelka, D. (2008). Information Technology Auditing: A Value-Added IT Governance Partnership between IT Management and Audit. Communications of the Association for Information Systems, 23.

Messier, W. F., Glover, S. M., & Prawitt, D. F. (2016). Auditing and Assurance Services.

Ministry of Information and Communication Technology. (2016, February 8). Digital development plan for economy and society. Retrieved from Ministry of Information and Communication Technology:

Mohammadi, J. B. (2012). Current Topics in Auditing. Tehran: Sanei Press.

Muhamad Sandi Akbar, I. S. (2017). Competence and Professional Care of External Auditor on Information Technology Audit. Trikonomika, 21-27.

Munoko, I. B.-L. (2020). The Ethical Implications of Using Artificial Intelligence in Auditing. Journal of Business Ethics, 209–234.

"National Cyber Security Agency. (2023). Standards and Guidelines for Promoting the Development of Cyber Security Service Systems. https://drive.ncsa.or.th/s/rPWACibPZKsRocm"

Nelson, M. W. (2009). A Model and Literature Review of Professional Skepticism in Auditing.

New York State Society of Certified Public Accountants . (2013). Code of Professional Conduct. 3 Park A Venue New York. New York : New York .

Nkwe, N. (2011). State of Information Technology Auditing in Botswana. Asian Journal of Finance & Accounting, 3(1). https://doi.org/10.5296/ajfa.v3i1.894

Nunnally, J. a. (1994). The Assessment of Reliability. Psychometric Theory, 248-292.

Nurjannah, R. (2019). Analysis of The Effect of Corporate Governance, Leverage, And Audit Quality On Profit Management With Company Size As A Moderating Variable On The Goods Consumer Company Registered In Indonesia Stock Exchange (Idx). International Journal of Public Budgeting, Accounting and Finance, 2(1), 1-11.

Okereafor, A. A. (2008). Patterns of Brain Injury in Neonates Exposed to

Perinatal Sentinel Events. Pediatrics. Pediatrics.

Okolie, A. O. (2014). Audit Quality and Earnings Response Coefficients of Quoted Companies in Nigeria. Journal of Applied Finance & Banking, 139-161.

Olojede, P., Erin, O., Asiriuwa, O., & Usman, M. (2020). Audit expectation gap: an empirical analysis. Future Business Journal, 6(1). https://doi.org/10.1186/s43093-020-00016-x

Omoteso, K. (2013). Audit Effectiveness: Meeting the IT challenge. http://ci.nii.ac.jp/ncid/BB13066308

Osmundsen, K., Iden, J., & Bygstad, B. (2018). Digital Transformation: drivers, success factors, and implications. MCIS, 37. https://aisel.aisnet.org/mcis2018/37/

Palmrose, Z. (1988). An Analysis of Auditor Litigation and Audit Service Quality. The Accounting Review, 55-73

Peecher, M. E., Schwartz, R., & Solomon, I. (2007). It's all about audit quality: Perspectives on strategic-systems auditing. Accounting Organizations and Society, 32(4–5), 463–485. https://doi.org/10.1016/j.aos.2006.09.001

Petter L. & Suzanne C. Wagner, "IT Audit Challenges for Small and Medium Sized Financial Institutions", Annual Symposium on Information Assurance and Secure Knowledge Management, pp.16-22, 2012.

Petter Lovaas, S. C. (2012). IT Audit Challenges for Small and Medium-Sized Financial Institutions. Annual Symposium on Information Assurance and Secure Knowledge Management, 16-22.

Petterson, M. (2005). The keys to effective IT auditing. Journal of Corporate Accounting & Finance, 41-46.

Ramadhan, M. (2016). Pengaruh Independensi, Kompetensi, dan Pengalaman Kerja Terhadap Kualitas Audit. Jakarta: Skripsi.

Ramadhan, S., and Hudiwinarsih, G., (2015). The accounting students' perception towards accounting professions. The Indonesian Accounting Review, 5(2), 179 – 186.

Rashid, A., et al. (2018) Scoping the Cyber Security Body of Knowledge. IEEE

Security and Privacy, 16, 96-102.https://doi.org/10.1109/MSP.2018.2701150

Reid, L. C. (2019). Impact of auditor report changes on financial reporting quality and audit costs: Evidence from the UnitedKingdom. Contemporary Accounting Research, 1501-1539.

Rezaee, Z. &. (1988). The impact of emerging information technology on auditing. Managerial Auditing Journal, 465-471.

Riad, A. (2015). ISO/IEC 27001. linkedin.

Riadh Manita a, N. E. (2020). The digital transformation of external audit and its impact on corporate governance. Technological Forecasting and Social Change.

Riyadi, A., Khaddafi, M., F, F., F, F., & Ilham, R. N. (2021). Internal factor of systemamtic risk model with information technology as intervening variables to increasing quality of government financial reports in Indonesia: Actual case from Riau Island Province. MORFAI JOURNAL, 1(1), 22–35. https://doi.org/10.54443/morfai.v1i1.13

Robson, K., Humphrey, C., Khalifa, R., & Jones, J. (2007). Transforming audit technologies: Business risk audit methodologies and the audit field. Accounting Organizations and Society, 32(4–5), 409–438. https://doi.org/10.1016/j.aos.2006.09.002

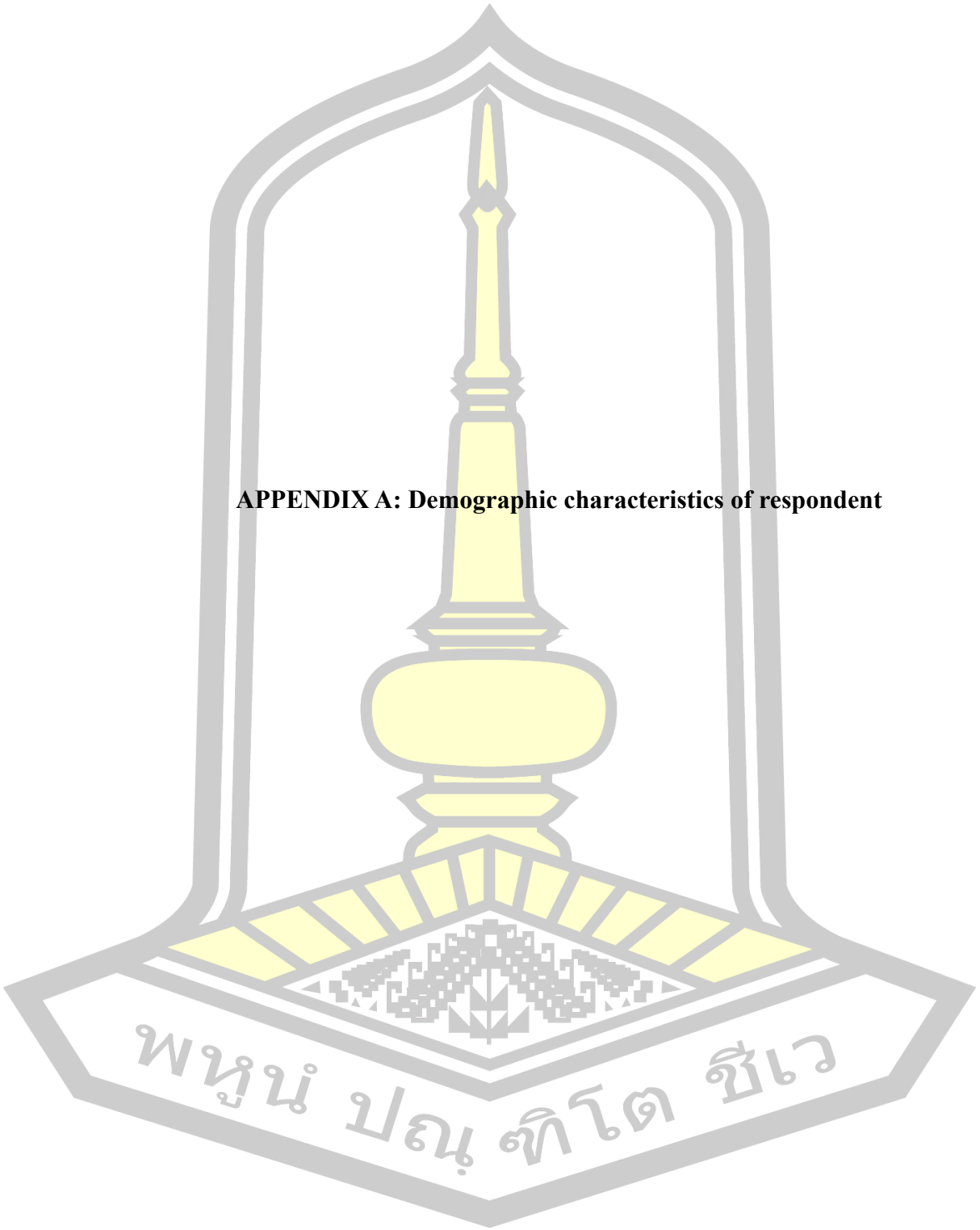
Rosário, T. P. (2013). IT Audit Management Architecture and Process Model. Business Information Systems, 187-198.

Rosati, P., Gogolin, F., & Lynn, T. (2020). Cyber-Security incidents and audit quality. European Accounting Review, 31(3), 701–728. https://doi.org/10.1080/09638180.2020.1856162

Rose, A. M., J. M. Rose, K. Sanderson, and J. C. Thibodeau. 2017. When should audit firms introduce analyses of big data into the audit process? Journal of Information Systems 31 (3): 81-99.

Rozario, A. M., & Thomas, J. (2019). Reengineering the audit with blockchain and smart contracts. Journal of Emerging Technologies in Accounting, 16(1), 21-35.

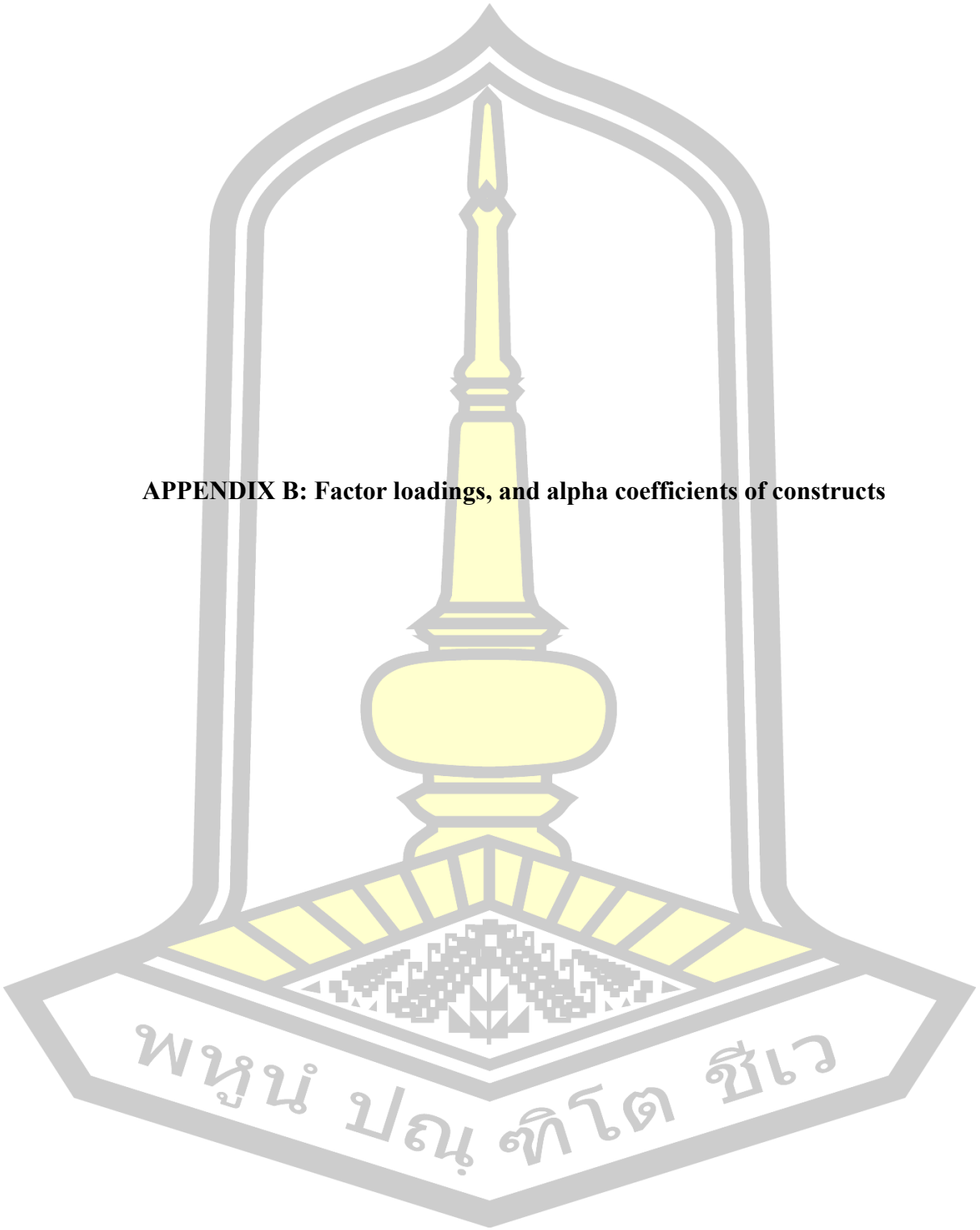
APPENDICES



APPENDIX A: Demographic characteristics of respondent

Table 19: Demographic characteristics of respondent

Description	Categories	Frequencies	Precent
1.Gender	Male	35	37.63
	Female	58	62.37
	Total	**93**	**100.00**
2.Age	Not more than30 year old	42	45.16
	31-40 year old	30	32.26
	41-50 year old	3	3.23
	More than 50 year old	18	19.35
	Total	**93**	**100.00**
3.Marital Status	Single	70	75.27
	Married	23	24.73
	Total	**93**	**100.00**
4.Education Levels	Bachelor's degree	69	74.19
	Higher than bachelor's degree	24	25.81
	Total	**93**	**100.00**
5. experience Auditing in The Stock Exchange of Thailand	Not more than 5 years	49	52.69
	6-10 years	24	25.81
	11-15 years	6	6.45
	more than 15 years	14	15.05
	Total	**93**	**100.00**
6.Average revenue per month	Not more than 100,000 Bant	41	44.09
	100,001-150,000 Bant	28	30.11
	150,001-200,000 Bant	14	15.05
	More than 200,000 Bant	10	10.75
	Total	**93**	**100.00**



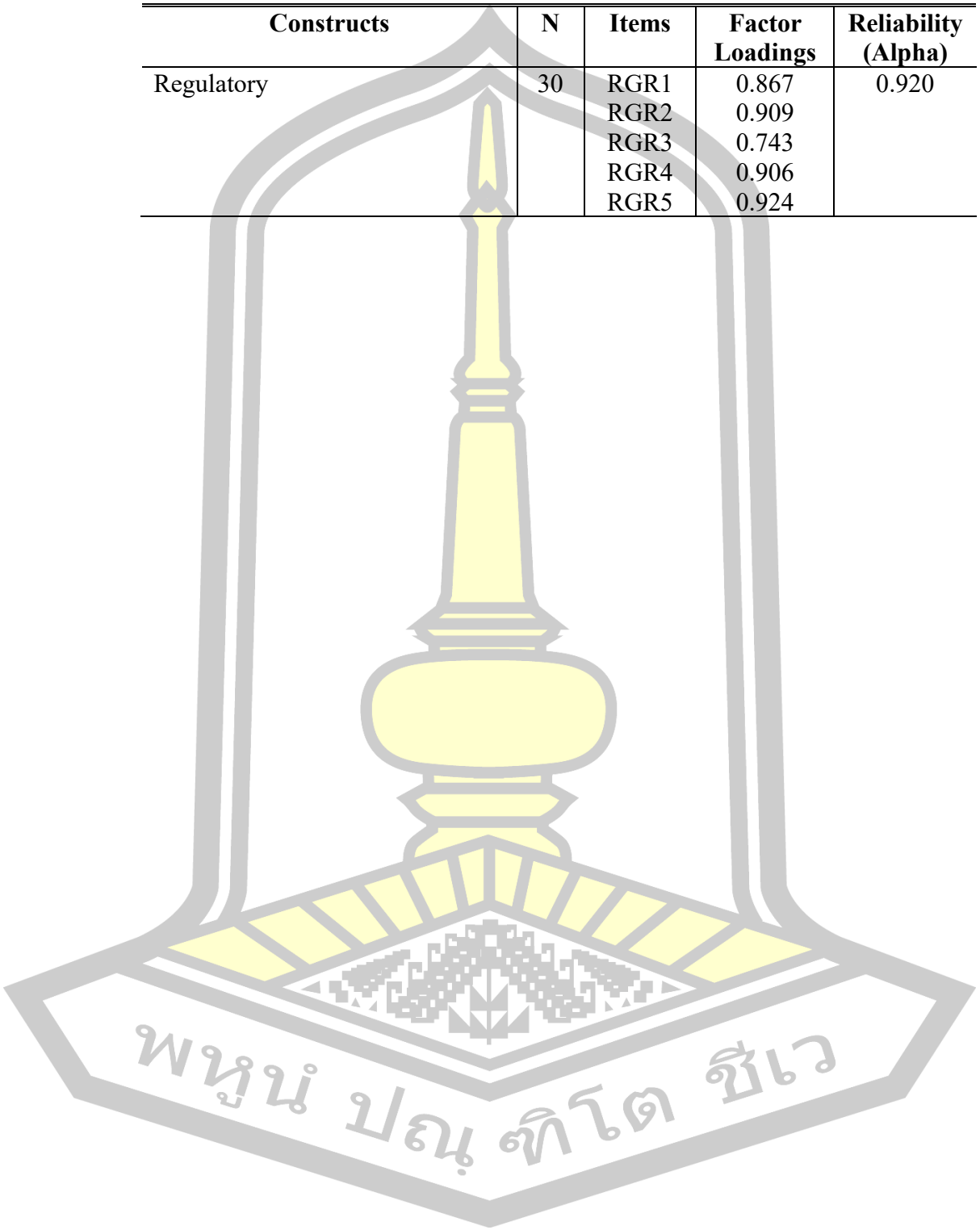
APPENDIX B: Factor loadings, and alpha coefficients of constructs

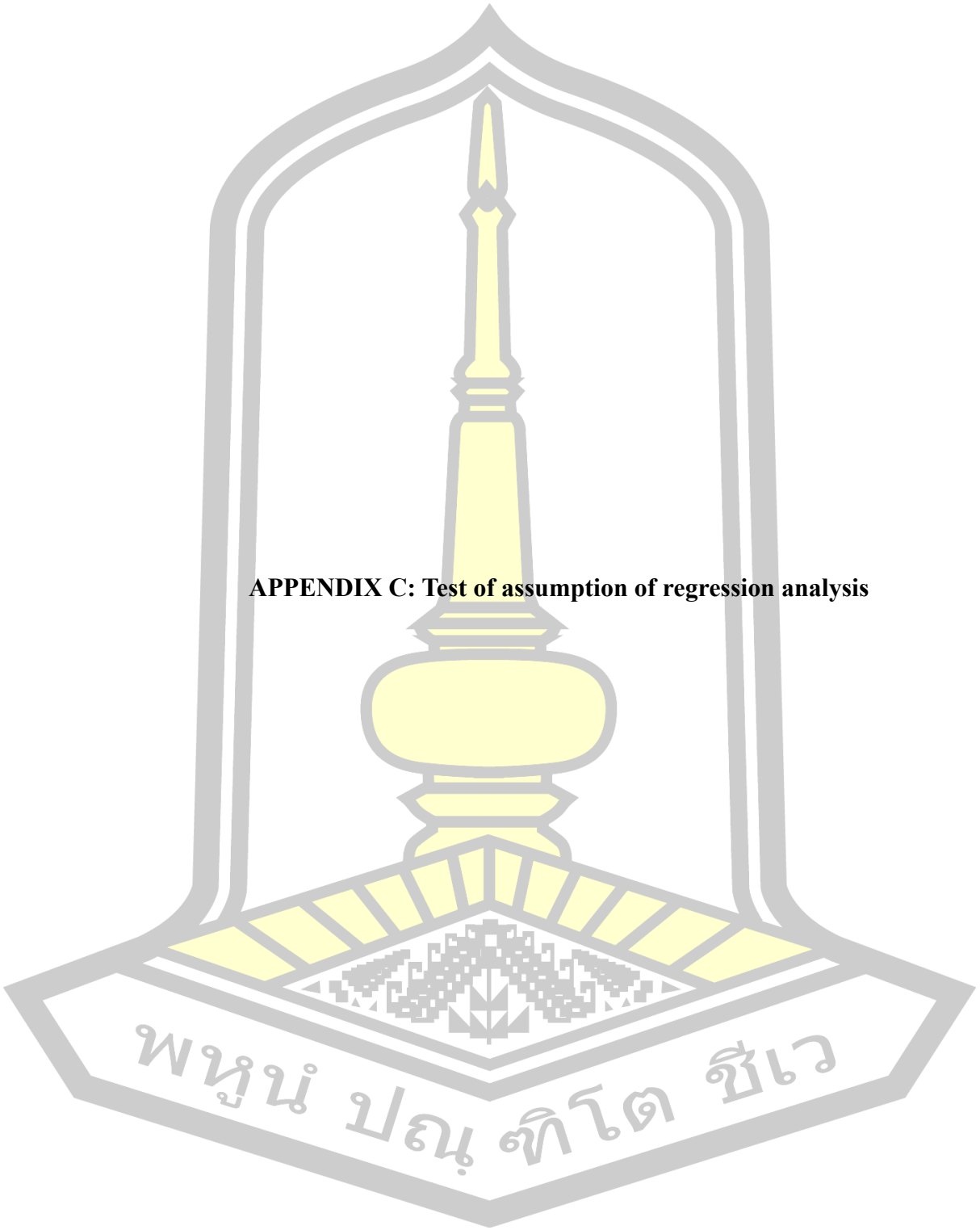
Table 20: Item factor loadings and reliability analysis in pre-test

Constructs	N	Items	Factor Loadings	Reliability (Alpha)
Financial Statement audit	30	FSA1	0.607	0.710
		FSA2	0.656	
		FSA3	0.672	
		FSA4	0.689	
		FSA5	0.775	
Operational Audit	30	OAU1	0.650	0.748
		OAU2	0.703	
		OAU3	0.754	
		OAU4	0.654	
		OAU5	0.798	
Compliance Audit	30	CAU1	0.862	0.867
		CAU2	0.891	
		CAU3	0.778	
		CAU4	0.857	
Information technology Control	30	ITC1	0.700	0.746
		ITC2	0.698	
		ITC3	0.707	
		ITC4	0.675	
		ITC5	0.758	
Reducing audit risk	30	RAR1	0.804	0.767
		RAR2	0.780	
		RAR3	0.784	
		RAR4	0.792	
Data security	30	DSR1	0.679	0.744
		DSR2	0.651	
		DSR3	0.734	
		DSR4	0.788	
		DSR5	0.665	
Audit Quality	30	AUQ1	0.777	0.804
		AUQ2	0.701	
		AUQ3	0.774	
		AUQ4	0.873	
		AUQ5	0.656	
Technology Change Awareness	30	TCA1	0.769	0.849
		TCA2	0.871	
		TCA3	0.826	
		TCA4	0.876	
Business Environment	30	BEM1	0.724	0.823
		BEM2	0.830	
		BEM3	0.731	
		BEM4	0.722	
		BEM5	0.820	

Table 20: Item factor loadings and reliability analysis in pre-test (continue)

Constructs	N	Items	Factor Loadings	Reliability (Alpha)
Regulatory	30	RGR1	0.867	0.920
		RGR2	0.909	
		RGR3	0.743	
		RGR4	0.906	
		RGR5	0.924	



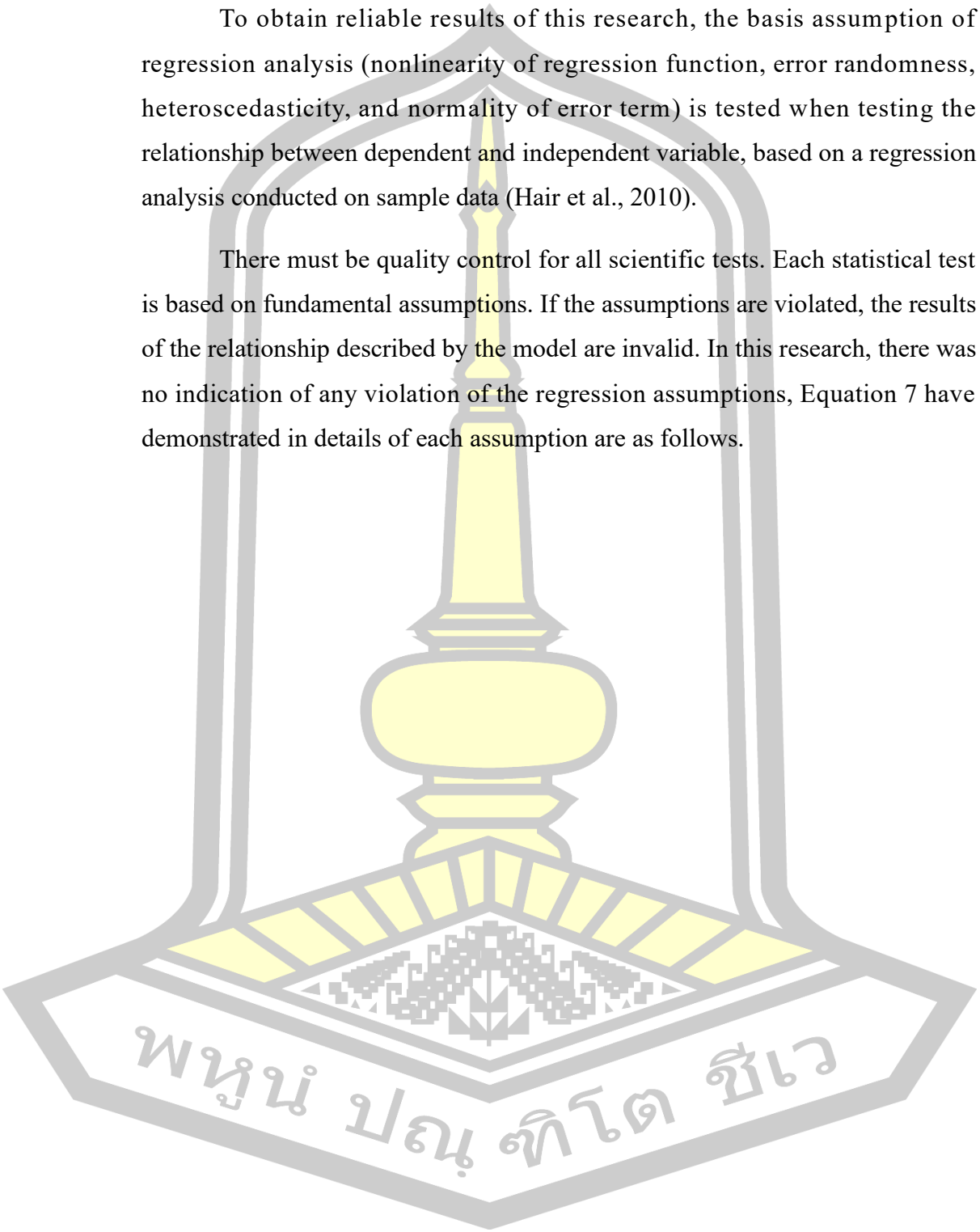


APPENDIX C: Test of assumption of regression analysis

Testing the assumptions of linear regression

To obtain reliable results of this research, the basis assumption of regression analysis (nonlinearity of regression function, error randomness, heteroscedasticity, and normality of error term) is tested when testing the relationship between dependent and independent variable, based on a regression analysis conducted on sample data (Hair et al., 2010).

There must be quality control for all scientific tests. Each statistical test is based on fundamental assumptions. If the assumptions are violated, the results of the relationship described by the model are invalid. In this research, there was no indication of any violation of the regression assumptions, Equation 7 have demonstrated in details of each assumption are as follows.



Equation 1: $RARi = \alpha_1 + \beta_1 FSA_i + \beta_2 OAU_i + \beta_3 CAU_i + \beta_4 ITC_i + \beta_5 AUS1_i + \beta_6 AUS2_i + \beta_7 AUS_{3i} + \beta_8 AUS4_i + \varepsilon_1$

Interdependence of error term

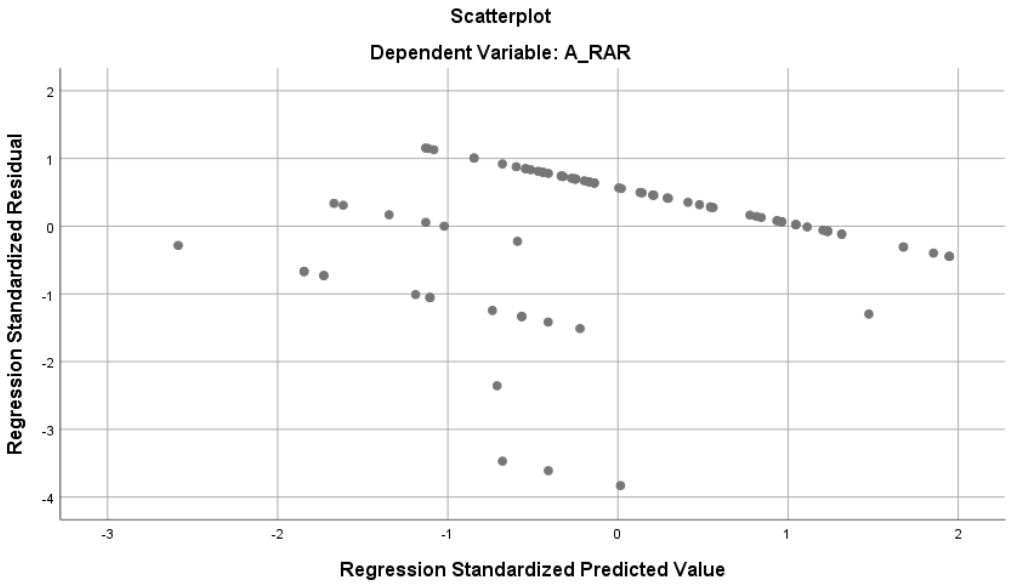
Model Summary[b]

Model	R	R square	Adjusted R Square	Std. Error of the Estimate	Durbin-Watson
1	.476[a]	.226	.163	.22779	1.894

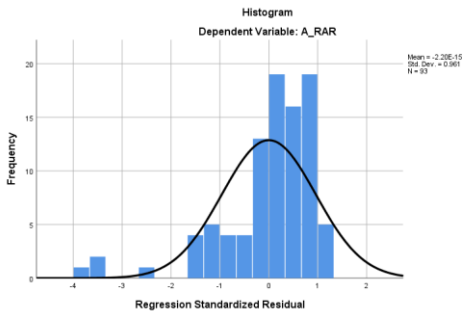
a. Predictors: (Constant), A_ITC, A_FSA, A_CAU, A_OAU, AUS

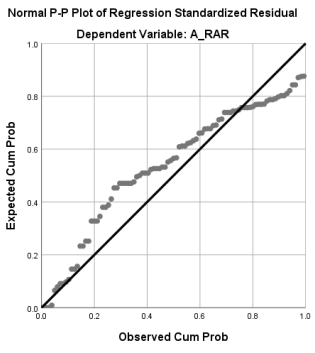
b. Dependent Variable: A_RAR

Heteroscedasticity



Normality of residual





Equation 2: DSR = $\alpha_2 + \beta_9 FSA_i + \beta_{10} OAU_i + \beta_{11} CAU_i + \beta_{12} ITC_i + \beta_{13} AUS1_i + \beta_{14} AUS2_i + \beta_{15} AUS3_i + \beta_{16} AUS4_i + \varepsilon_2$

Interdependence of error term

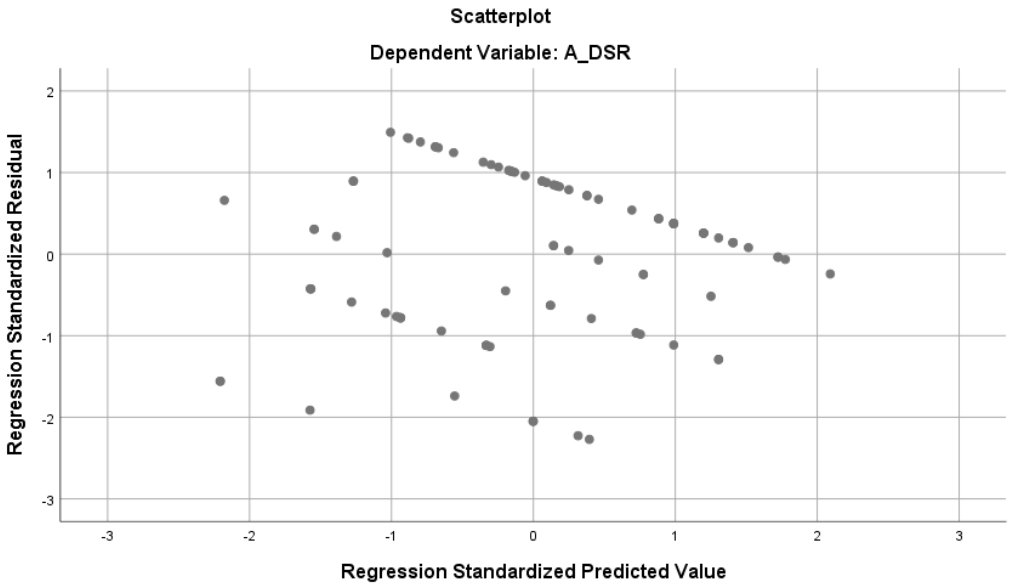
Model Summary[b]

Model	R	R square	Adjusted R Square	Std. Error of the Estimate	Durbin-Watson
1	.504[a]	.254	.192	.26855	1.643

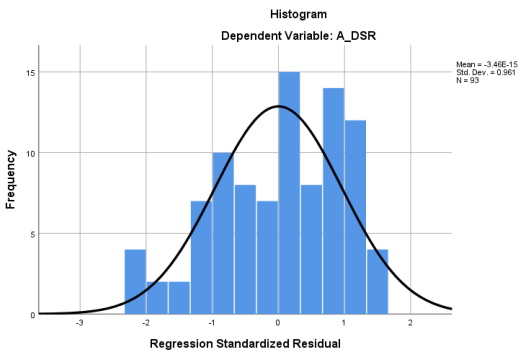
a. Dependent Variable: A_DSR

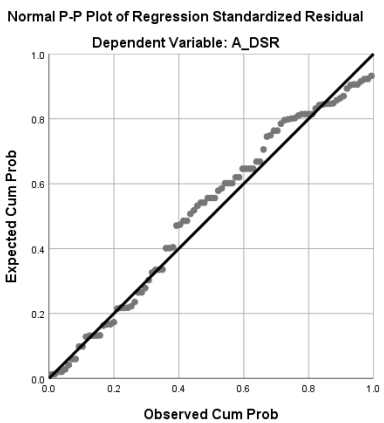
b. Predictors: (Constant), A_ITC, A_FSA, A_CAU, A_OAU, AUS

Heteroscedasticity



Normality of residual





Equation 3: AUQ = $= \alpha_3 + \beta_{17}RAR_i + \beta_{18}DSR_i + \beta_{19}AUS1_i + \beta_{20}AUS2_i + \beta_{21}AUS3_i + \beta_{22}AUS4_i + \varepsilon_3$

Interdependence of error term

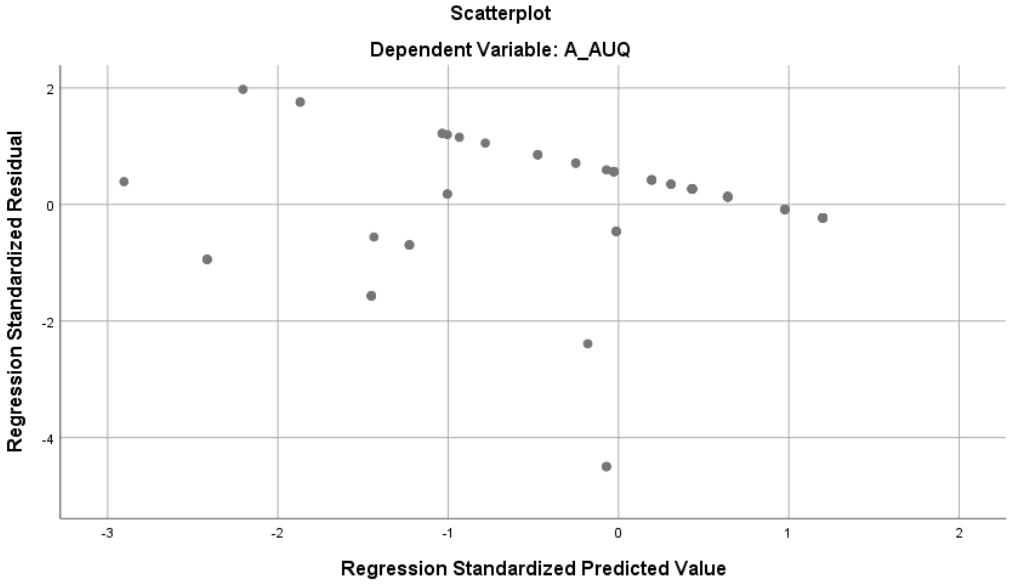
Model Summary[b]

Model	R	R square	Adjusted R Square	Std. Error of the Estimate	Durbin-Watson
1	.554[a]	.307	.268	.19640	2.033

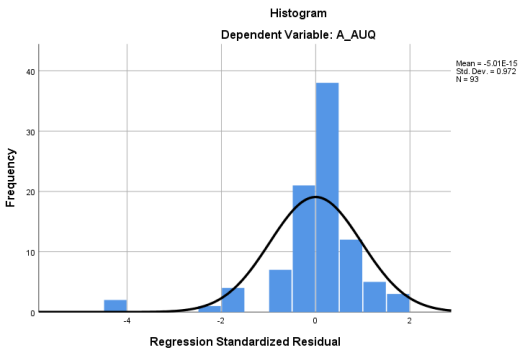
a. Predictors: (Constant), A_DSR, A_RAR, AUS

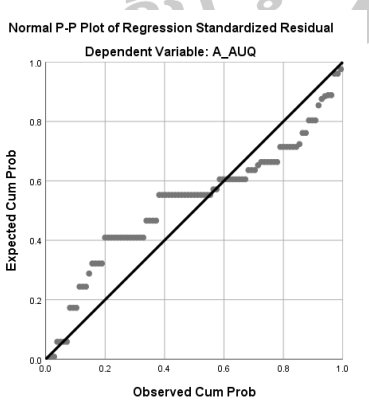
b. Dependent Variable: A_AUQ

Heteroscedasticity



Normality of residual





Equation 4: FSA = $\alpha_4 + \beta_{23}TCA_i + \beta_{24}BEM_i + \beta_{25}RGR_i + \beta_{26}AUS1_i + \beta_{27}AUS2_i + \beta_{28}AUS3_i + \beta_{29}AUS4_i + \varepsilon_4$

Interdependence of error term

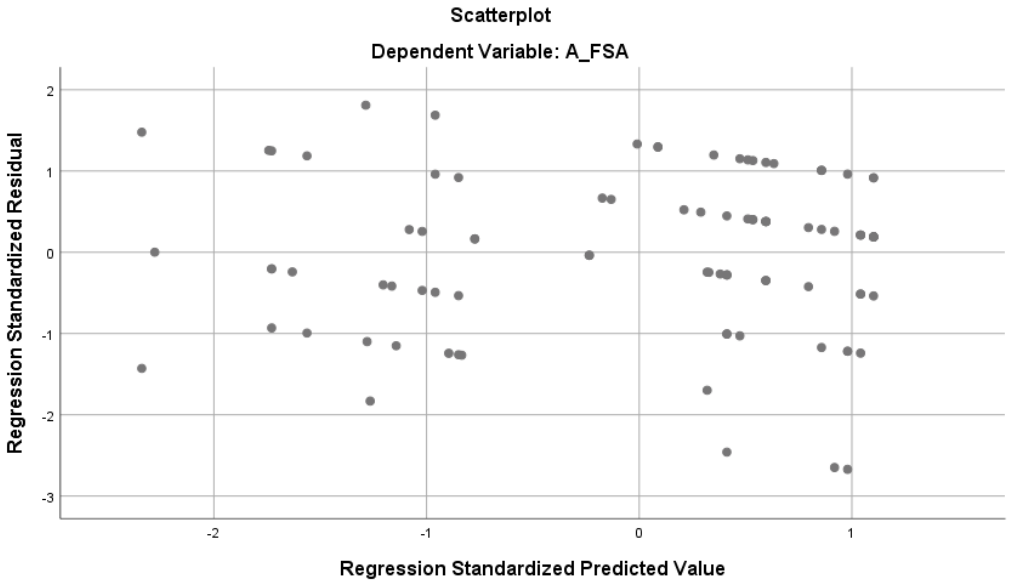
Model Summary[b]

Model	R	R square	Adjusted R Square	Std. Error of the Estimate	Durbin-Watson
1	.361[a]	.130	.070	.27521	1.728

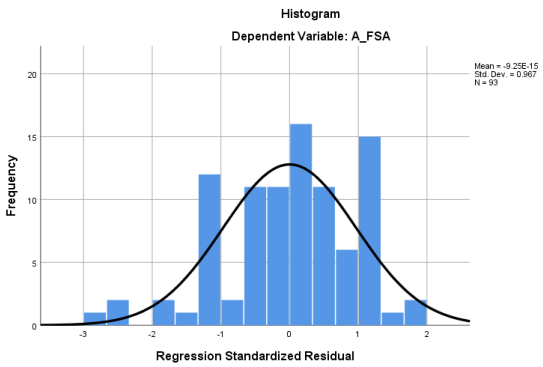
a. Predictors: (Constant), A_DSR, A_RAR, AUS

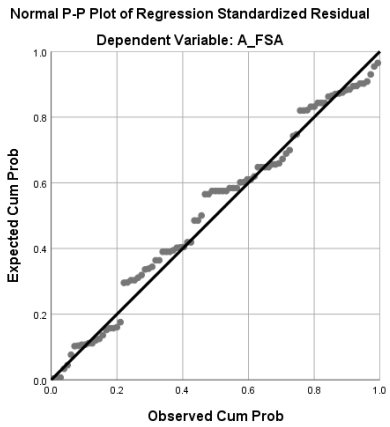
b. Dependent Variable: A_AUQ

Heteroscedasticity



Normality of residual





Equation 5: OAU = $\alpha_5 + \beta_{30}TCA_i + \beta_{31}BEM_i + \beta_{32}RGR_i + \beta_{33}AUS1_i + \beta_{34}AUS2_i + \beta_{35}AUS3_i + \beta_{36}AUS4_i + \varepsilon_5$

Interdependence of error term

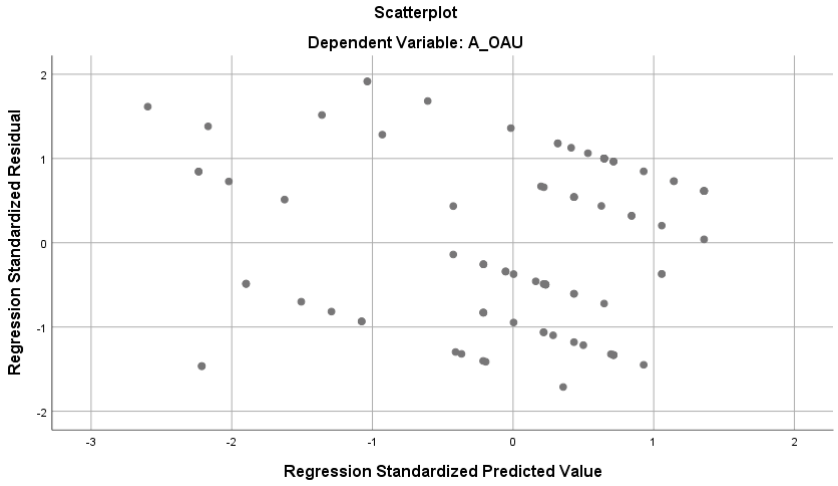
Model Summary[b]

Model	R	R square	Adjusted R Square	Std. Error of the Estimate	Durbin-Watson
1	.490[a]	.240	.187	.34834	2.066

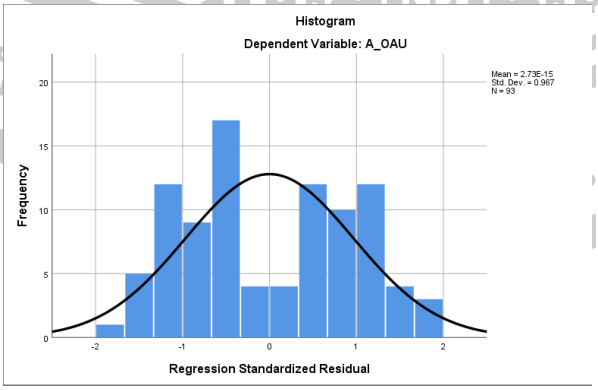
a. Predictors: (Constant), A_BEM, A_TCA, AUS, A_RGR

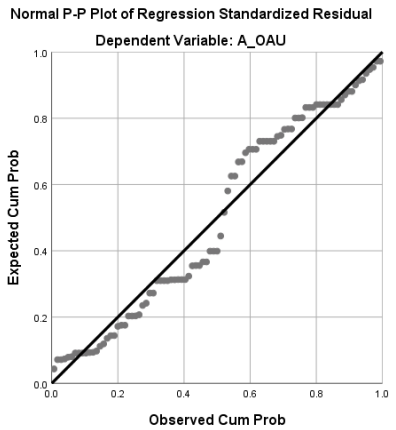
b. Dependent Variable: A_OAU

Heteroscedasticity



Normality of residual





Equation 6: CAU = $\alpha_6 + \beta_{37}TCA_i + \beta_{38}BEM_i + \beta_{39}RGR_i + \beta_{40}AUS1_i + \beta_{41}AUS2_i + \beta_{42}AUS3_i + \beta_{43}AUS4_i + \varepsilon_6$

Interdependence of error term

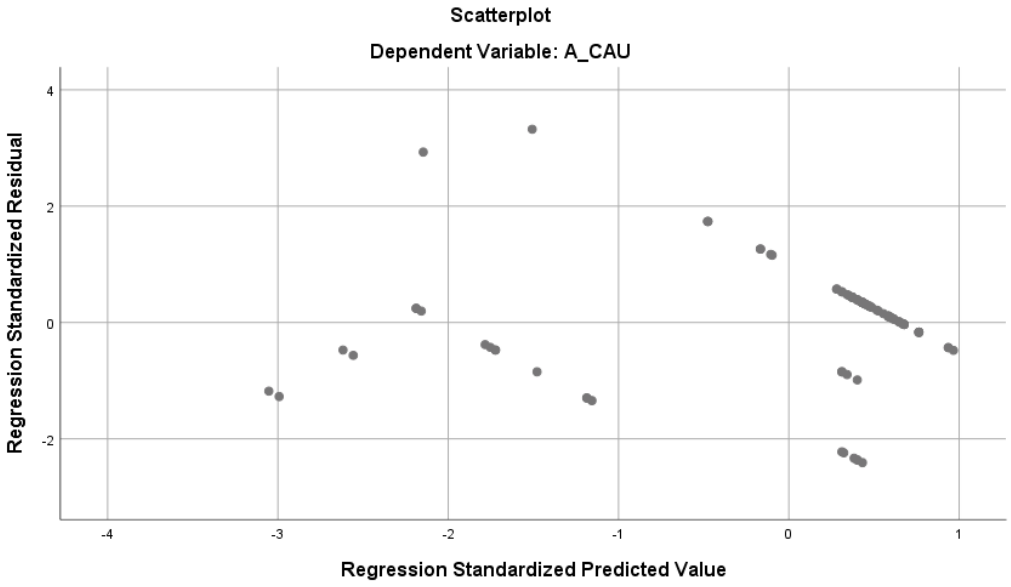
Model Summary[b]

Model	R	R square	Adjusted R Square	Std. Error of the Estimate	Durbin-Watson
1	.846[a]	.716	.697	.18174	1.581

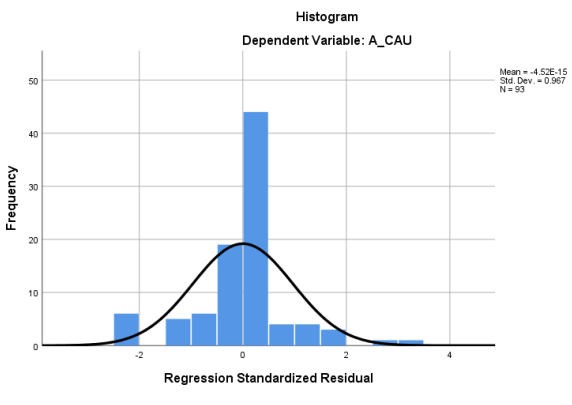
a. Dependent Variable: A_CAU

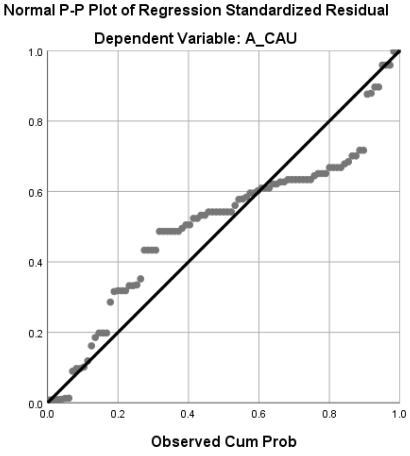
b. Predictors: (Constant), A_BEM, A_TCA, AUS, A_RGR

Heteroscedasticity



Normality of residual





Equation 7:ITC = $\alpha_7 + \beta_{44}TCA_i + \beta_{45}BEM_i + \beta_{46}RGR_i + \beta_{47}AUS1_i + \beta_{48}AUS2_i + \beta_{49}AUS3_i + \beta_{50}AUS4_i + \varepsilon_7$

Interdependence of error term

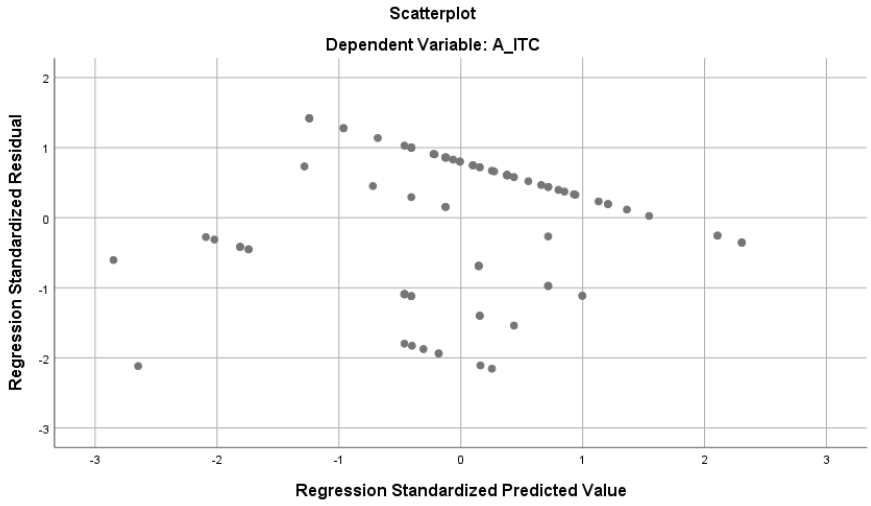
Model Summary[b]

Model	R	R square	Adjusted R Square	Std. Error of the Estimate	Durbin-Watson
1	.459[a]	.211	.156	.28318	2.318

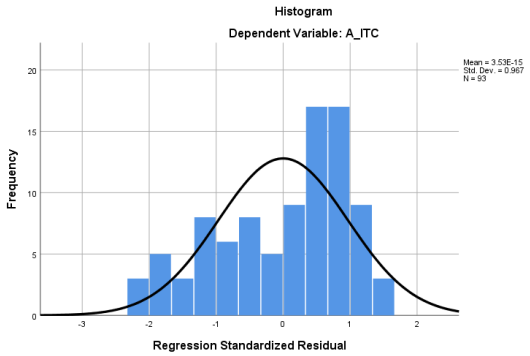
a. Predictors: (Constant), A_BEM, A_TCA, AUS, A_RGR

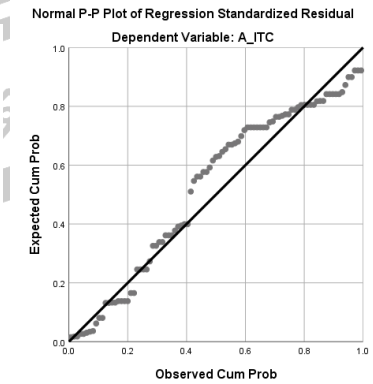
b. Dependent Variable: A_ITC

Heteroscedasticity



Normality of residual

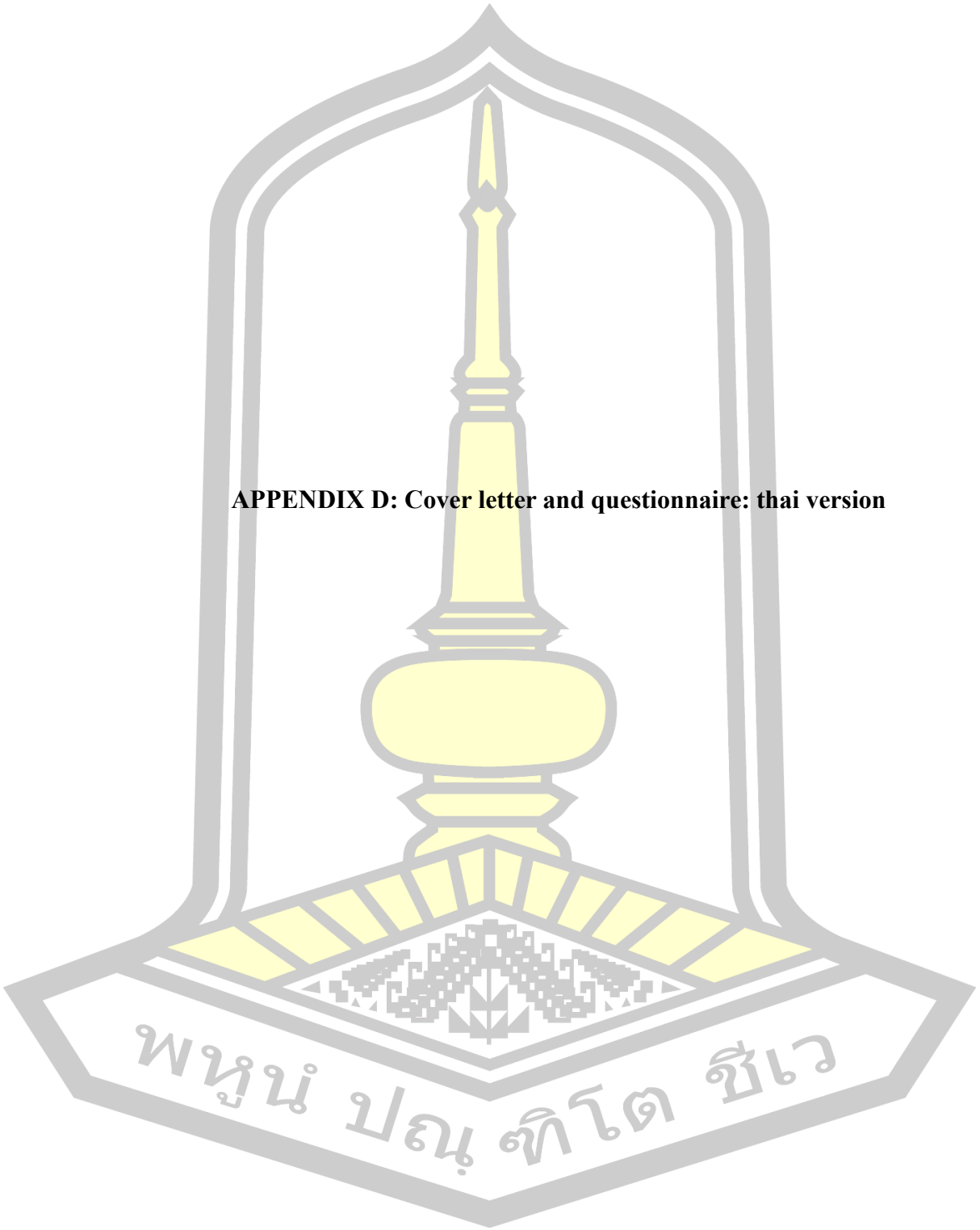




Multicollinearity

Equation	Maximum VIF
Equation 1	1.281
Equation 2	1.281
Equation 3	1.156
Equation 4	1.967
Equation 5	1.967
Equation 6	1.967
Equation 7	1.967

พหุน ปณ ฑิโต ชีเว



APPENDIX D: Cover letter and questionnaire: thai version

แบบสอบถามเพื่อการวิจัย

เรื่อง “ผลกระทบของการตรวจสอบเทคโนโลยีสารสนเทศที่มีต่อคุณภาพการตรวจสอบของผู้สอบบัญชีตลาดทุนในประเทศไทย”

<u>คำชี้แจง</u>

โครงการวิจัยนี้มีวัตถุประสงค์เพื่อศึกษาวิจัยเรื่อง “ผลกระทบของการตรวจสอบเทคโนโลยีสารสนเทศที่มีต่อคุณภาพการตรวจสอบของผู้สอบบัญชีตลาดทุนในประเทศไทย” เพื่อประกอบการศึกษาวิทยานิพนธ์ในระดับปริญญาเอกของผู้วิจัยในหลักสูตรปรัชญาดุษฎีบัณฑิต สาขาวิชาการบัญชี คณะการบัญชีและการจัดการ มหาวิทยาลัยมหาสารคาม โทรศัพท์ 043-754333

ผู้วิจัยขอความอนุเคราะห์จากท่านผู้ตอบแบบสอบถาม ได้โปรดตอบแบบสอบถามชุดนี้ โดยรายละเอียดแบบสอบถามประกอบด้วยส่วนคำถาม 6 ตอน ดังนี้

ตอนที่ 1 ข้อมูลทั่วไปเกี่ยวกับผู้สอบบัญชีตลาดทุนในประเทศไทย

ตอนที่ 2 ความคิดเห็นเกี่ยวกับการตรวจสอบเทคโนโลยีสารสนเทศของผู้สอบบัญชีตลาดทุนในประเทศไทย

ตอนที่ 3 ความคิดเห็นเกี่ยวกับคุณภาพการตรวจสอบของผู้สอบบัญชีตลาดทุนในประเทศไทย

ตอนที่ 4 ความคิดเห็นเกี่ยวกับปัจจัยภายในที่ส่งผลต่อการตรวจสอบเทคโนโลยีสารสนเทศของผู้สอบบัญชีตลาดทุนในประเทศไทย

ตอนที่ 5 ความคิดเห็นเกี่ยวกับปัจจัยภายนอกที่ส่งผลต่อการตรวจสอบเทคโนโลยีสารสนเทศของผู้สอบบัญชีตลาดทุน ในประเทศไทย

ตอนที่ 6 ข้อคิดเห็นและข้อเสนอแนะเกี่ยวกับการตรวจสอบเทคโนโลยีสารสนเทศของผู้สอบบัญชีตลาดทุนในประเทศไทย

คำตอบของท่านจะถูกเก็บรักษาเป็นความลับ และจะไม่มีการใช้ข้อมูลใด ๆ ที่เปิดเผยเกี่ยวกับธุรกิจของท่านในการรายงานข้อมูล รวมถึงจะไม่มีการร่วมใช้ข้อมูลดังกล่าว กับบุคคลภายนอกโดยไม่ได้รับอนุญาตจากท่าน หากท่านมีความประสงค์ที่จะรับข้อมูลสรุปผลการวิจัยโปรดระบุ E-mail Address ของท่านหรือแนบนามบัตรของท่านมาพร้อมกับแบบสอบถามชุดนี้

☐ ต้องการ e-mail _____ ☐ ไม่ต้องการ

ผู้วิจัยขอขอบพระคุณที่ท่านได้กรุณาเสียสละเวลาในการตอบแบบสอบถามได้อย่างถูกต้องครบถ้วน ข้อมูลที่ได้รับจากท่านจะเป็นประโยชน์อย่างยิ่งต่อการวิจัยในครั้งนี้ หากท่านมีข้อสงสัยประการใดเกี่ยวกับแบบสอบถามโปรดติดต่อผู้วิจัย นางสาวเมฑิณี เมษสุวรรณ โทรศัพท์ 083-2919016 หรือ E-mail: 64010991001@msu.ac.th

(นางสาวเมฑิณี เมษสุวรรณ)
นักศึกษาระดับปริญญาเอก สาขาการบัญชี
คณะการบัญชีและการจัดการ มหาวิทยาลัยมหาสารคาม

ตอนที่ 1 ข้อมูลทั่วไปเกี่ยวกับผู้สอบบัญชีตลาดทุนในประเทศไทย

1. เพศ

☐ ชาย ☐ หญิง

2. อายุ

☐ ไม่เกิน 30 ปี ☐ 31 - 40 ปี

☐ 41 – 50 ปี ☐ มากกว่า 50 ปี

3. สถานภาพ

☐ โสด ☐ สมรส

4. ระดับการศึกษา

☐ ปริญญาตรี ☐ สูงกว่าปริญญาตรี

5. ประสบการณ์ในการสอบบัญชีในตลาดหลักทรัพย์

☐ ไม่เกิน 5 ปี ☐ 6 - 10 ปี

☐ 11 - 15 ปี ☐ มากกว่า 15 ปี

6. รายได้เฉลี่ยต่อเดือน

☐ ไม่เกิน 100,000 บาท ☐ 100,001 - 150,000 บาท

☐ 150,001 - 200,000 บาท ☐ มากกว่า 200,000 บาท

พหุน ปณ ฑิโต ชีเว

ตอนที่ 2 ความคิดเห็นเกี่ยวกับการตรวจสอบเทคโนโลยีสารสนเทศของผู้สอบบัญชีตลาดทุนในประเทศไทย

การตรวจสอบเทคโนโลยีสารสนเทศ	มากที่สุด 5	มาก 4	ปานกลาง 3	น้อย 2	น้อยที่สุด 1
1) การตรวจสอบงบการเงิน					
1 ท่านให้ความสำคัญกับการตรวจสอบความถูกต้องของรายการที่เป็นสาระสำคัญในงบการเงิน					
2 ท่านตระหนักถึงความสามารถในการเปรียบเทียบกันได้ของข้อมูลในงบการเงิน					
3 ท่านมุ่งมั่นในการตรวจสอบข้อผิดพลาดที่เป็นสาระสำคัญในงบการเงิน					
4 ท่านให้ความสำคัญกับการตรวจสอบเพื่อพิสูจน์ยืนยันรายการบัญชีที่ปรากฏในงบการเงิน					
5 ท่านให้ความสำคัญกับการตรวจสอบเพื่อนำเสนอข้อมูลการเงินที่เกี่ยวข้องกับการตัดสินใจ					
2) การตรวจสอบการดำเนินงาน					
6 ท่านเชื่อว่าการปฏิบัติงานตามลำดับขั้นตอน จะช่วยให้การดำเนินงานบรรลุเป้าหมายที่กำหนดไว้					
7 ท่านตระหนักถึงการตรวจสอบวิธีการปฏิบัติงานตามที่กำหนดไเพื่อเพิ่มความน่าเชื่อถือในการดำเนินงานสอบบัญชีที่เป็นไปตามาตรฐานการสอบบัญชี					
8 ท่านตระหนักถึงการปฏิบัติงานตามขั้นตอนการปฏิบัติงานเพื่อเพิ่มประสิทธิภาพในการดำเนินงาน					
9 ท่านให้ความสำคัญกับการสอบทานภาระการปฏิบัติงานในองค์กรเพื่อให้การดำเนินงานขององค์กรมีประสิทธิภาพ					
10 ท่านให้ความสำคัญกับการปฏิบัติงานตามแผนที่วางไว้เพื่อให้การปฏิบัติงานมีประสิทธิภาพ					

ตอนที่ 2 ความคิดเห็นเกี่ยวกับการตรวจสอบเทคโนโลยีสารสนเทศของผู้สอบบัญชีตลาดทุนในประเทศไทย (ต่อ)

การตรวจสอบเทคโนโลยีสารสนเทศ	มากที่สุด 5	มาก 4	ปานกลาง 3	น้อย 2	น้อยที่สุด 1
3) การตรวจสอบการปฏิบัติงานตามกฎระเบียบ					
11 ท่านตระหนักถึงการปฏิบัติงานตามระเบียบ ข้อบังคับขององค์กร เพื่อให้การปฏิบัติงานมีความถูกต้องและครบถ้วน					
12 ท่านเชื่อว่าการตรวจสอบนโยบายและขอบเขตการปฏิบัติงานจะช่วยให้การปฏิบัติงานขององค์กรมีประสิทธิภาพ					
13 ท่านให้ความสำคัญกับการปฏิบัติงานตามกฎระเบียบขององค์เพื่อให้การปฏิบัติงานเป็นไปตามวัตถุประสงค์ที่วางไว้					
14 ท่านมุ่งมั่นที่จะตรวจสอบการปฏิบัติงานให้เป็นไปตามกฎระเบียบขององค์กร เพื่อให้มั่นใจว่าการปฏิบัติงานเป็นไปตามมาตรฐาน					
4) การควบคุมเทคโนโลยีสารสนเทศ					
15 ท่านเชื่อว่าการกำกับดูแลเทคโนโลยีสารสนเทศจะช่วยให้สารสนเทศมีความครบถ้วน สมบูรณ์ และใช้ในการแสดงความคิดเห็นที่เป็นไปตามมาตรฐานการรายงานทางการเงินและมาตรฐานการสอบบัญชี					
16 ท่านเชื่อว่าการควบคุมความปลอดภัยเทคโนโลยีสารสนเทศจะช่วยให้สารสนเทศมีความถูกต้อง และใช้ในการแสดงความคิดเห็นได้อย่างสมเหตุสมผล					
17 ท่านเชื่อว่าการกำหนดสิทธิ์การเข้าถึงเทคโนโลยีสารสนเทศจะช่วยให้ได้สารสนเทศที่มีความน่าเชื่อถือ เพื่อใช้ในการแสดงความคิดเห็นต่องบการเงินได้อย่างถูกต้อง					
18 ท่านเชื่อว่าการควบคุมการนำเข้าสารสนเทศ จะช่วยให้การประมวลผลมีประสิทธิภาพ และใช้ในการตรวจสอบที่สอดคล้องกับข้อเท็จจริง					
19 ท่านเชื่อว่าการการจัดเตรียมสารสนเทศและการตรวจสอบสารสนเทศก่อนนำเข้าเทคโนโลยีสารสนเทศจะช่วยป้องกันความเสียหายของระบบสารสนเทศ					

ตอนที่ 3 ความคิดเห็นเกี่ยวกับคุณภาพการตรวจสอบของผู้สอบบัญชีตลาดทุนในประเทศไทย

คุณภาพการสอบบัญชี	มากที่สุด 5	มาก 4	ปานกลาง 3	น้อย 2	น้อยที่สุด 1
1 ท่านเชื่อว่าการได้รับสารสนเทศที่น่าเชื่อถือ จะช่วยให้การแสดงความคิดเห็นต่องบการเงินเป็นไปตามมาตรฐานการสอบบัญชี					
2 ท่านให้ความสำคัญกับการรวบรวมหลักฐานการสอบบัญชีที่เพียงพอเพื่อแสดงความคิดเห็นต่องบการเงินที่ปราศจากข้อผิดพลาด					
3 ท่านเชื่อว่าการได้รับสารสนเทศที่เป็นปัจจุบันจะช่วยให้แสดงความคิดเห็นได้สอดคล้องกับข้อเท็จจริง					
4 ท่านเชื่อว่าการได้รับสารสนเทศที่มีความเป็นกลาง ปราศจากความลำเอียง จะช่วยให้การแสดงความคิดเห็นสอดคล้องกับข้อเท็จจริง					
5 ท่านตระหนักถึงการตรวจสอบและนำเสนอรายงานการสอบบัญที่เป็นไปตามความจริง					

ตอนที่ 4 ความคิดเห็นเกี่ยวกับปัจจัยภายในที่ส่งผลต่อการตรวจสอบเทคโนโลยีสารสนเทศของผู้สอบบัญชีตลาดทุนในประเทศไทย

ปัจจัยภายในที่ส่งผลต่อการตรวจสอบเทคโนโลยีสารสนเทศ	มากที่สุด 5	มาก 4	ปานกลาง 3	น้อย 2	น้อยที่สุด 1
การลดความเสี่ยงในการสอบบัญชี					
1 ท่านเชื่อว่าการวางแผนการตรวจสอบอย่างเหมาะสม จะช่วยลดข้อผิดพลาดจากการตรวจสอบได้					
2 ท่านเชื่อว่าการปฏิบัติงานด้วยความระมัดระวัง รอบคอบ จะช่วยให้การปฏิบัติงานมีความถูกต้อง					
3 ท่านตระหนักถึงการปฏิบัติงานที่ใช้เทคโนโลยีสารสนเทศที่เหมาะสม เพื่อลดความเสี่ยงในการตรวจสอบ					
4 ท่านให้ความสำคัญกับการปฏิบัติงานตามมาตรฐานการสอบบัญเพื่อลดข้อผิดพลาดในการปฏิบัติงาน					

ตอนที่ 4 ความคิดเห็นเกี่ยวกับปัจจัยภายในที่ส่งผลต่อการตรวจสอบเทคโนโลยีสารสนเทศของผู้สอบบัญชีตลาดทุนในประเทศไทย (ต่อ)

ปัจจัยภายในที่ส่งผลต่อการตรวจสอบเทคโนโลยีสารสนเทศ	มากที่สุด 5	มาก 4	ปานกลาง 3	น้อย 2	น้อยที่สุด 1
ความปลอดภัยของข้อมูล					
5 ท่านให้ความสำคัญกับการจัดเก็บสารสนเทศ เพื่อป้องกันความเสียหายของข้อมูล					
6 ท่านเชื่อว่าการตรวจสอบขั้นตอนการปฏิบัติงานจะช่วยให้สารสนเทศมีความน่าเชื่อถือและมีความถูกต้อง					
7 ท่านเชื่อว่าการกำหนดสิทธิ์การเข้าถึงข้อมูล จะช่วยให้ข้อมูลมีความปลอดภัยและสมบูรณ์					
8 ท่านเชื่อว่าการตรวจสอบการเข้าถึงระบบเครือข่ายจะช่วยให้ข้อมูลมีความปลอดภัย					
9 ท่านเชื่อว่าการควบคุมการใช้เทคโนโลยีสารสนเทศจะช่วยให้ข้อมูลมีความปลอดภัย					

ตอนที่ 5 ความคิดเห็นเกี่ยวกับปัจจัยภายนอกที่ส่งผลต่อการตรวจสอบเทคโนโลยีสารสนเทศของผู้สอบบัญชีตลาดทุนในประเทศไทย

ปัจจัยภายนอกที่ส่งผลต่อการตรวจสอบเทคโนโลยีสารสนเทศ	มากที่สุด 5	มาก 4	ปานกลาง 3	น้อย 2	น้อยที่สุด 1
การตระหนักถึงการเปลี่ยนแปลงทางเทคโนโลยี					
1 ท่านตระหนักถึงการประยุกต์ใช้เทคโนโลยีสารสนเทศ เพื่อเพิ่มศักยภาพในการปฏิบัติงาน					
2 ท่านให้ความสำคัญเกี่ยวกับการเรียนรู้เทคโนโลยีสารสนเทศเพื่อใช้ในการปฏิบัติงานให้มีประสิทธิภาพ					
3 ท่านมุ่งเน้นการแสวงหากระบวนการสอบบัญชีเพื่อรองรับเทคโนโลยีที่เปลี่ยนแปลงได้เป็นอย่างดี					
4 ท่านเชื่อว่าความก้าวหน้าทางเทคโนโลยีสารสนเทศและการเลือกใช้อย่างเหมาะสมและคุ้มค่าจะช่วยให้เกิดประสิทธิภาในการปฏิบัติงาน					

ตอนที่ 5 ความคิดเห็นเกี่ยวกับปัจจัยภายนอกที่ส่งผลต่อการตรวจสอบเทคโนโลยีสารสนเทศของผู้สอบบัญชีตลาดทุนในประเทศไทย (ต่อ)

ปัจจัยภายนอกที่ส่งผลต่อการตรวจสอบเทคโนโลยีสารสนเทศ		มากที่สุด 5	มาก 4	ปานกลาง 3	น้อย 2	น้อยที่สุด 1
	สภาพแวดล้อมทางธุรกิจ					
5	ท่านเชื่อว่าปัจจุบันสภาพแวดล้อมทางธุรกิจมีความผันผวน ทำให้ต้องเรียนรู้และเปลี่ยนแปลงการปฏิบัติงานตามสถานการณ์ที่เกิดขึ้น					
6	ท่านเชื่อว่าปัจจุบันมีความต้องการที่หลากหลาย ทำให้ต้องมุ่งเน้นในการตอบสนองความต้องการของลูกค้า					
7	ท่านเชื่อว่าคู่แข่งขันที่เพิ่มขึ้น เป็นแรงผลักดันที่ทำให้มีการเปลี่ยนแปลงและพัฒนาอย่างต่อเนื่องเพื่อให้สามารถอยู่รอดได้					
8	ท่านเชื่อว่าแรงผลักดันทางเทคโนโลยีสารสนเทศจะช่วยให้กระบวนการปฏิบัติงานเกิดการเปลี่ยนแปลง					
9	ท่านมุ่งมั่นในการแสวงหาขั้นตอนการปฏิบัติงานที่รองรับสภาพแวดล้อมที่เปลี่ยนแปลงไป					
	กฎระเบียบและข้อบังคับ					
10	ท่านเชื่อว่าข้อบังคับในการปฏิบัติงาน จะช่วยให้การปฏิบัติงาเป็นไปตามมาตรฐานการสอบบัญชี					
11	ท่านตระหนักถึงการปฏิบัติงานด้วยความระมัดระวัง รอบคอบเพื่อช่วยให้การปฏิบัติงานเป็นไปตามมาตรฐานการสอบบัญชีที่รับรองทั่วไป					
12	ท่านเชื่อว่าระเบียบ ข้อบังคับ และแนวทางการปฏิบัติงานจะช่วยให้การตรวจสอบมถูกต้องและครบถ้วน					
13	ท่านมุ่งเน้นการปฏิบัติงาน ที่เป็นไปด้วยความถูกต้องตามระเบียบและข้อบังคับ					
14	ท่านเชื่อว่าการกำหนดนโยบายที่ชัดเจน จะช่วยเพิ่มประสิทธิภาพการปฏิบัติงาน					

ตอนที่ 6 ความคิดเห็นและข้อเสนอแนะเพิ่มเติมเกี่ยวกับการตรวจสอบเทคโนโลยีสารสนเทศของผู้สอบบัญชีตลาดทุน

หากท่านมีข้อเสนอแนะเพิ่มเติมเกี่ยวกับแบบสอบถาม ได้โปรดเสนอแนะในช่องว่างข้างล่างนี้

.....

.....

.....

.....

สุดท้ายนี้ ขอขอบพระคุณท่านที่ได้สละเวลาตอบแบบสอบถามทุกข้อ โปรดพับแบบสอบถามและใส่ซองที่แนบมาพร้อมนี้ ส่งคืนตามที่อยู่ที่ระบุ หากท่านต้องการรายงานสรุปผลการวิจัยครั้งนี้ โปรดแนบนามบัตรหรือระบุ e-mail ของท่านมาพร้อมกับแบบสอบถาม ผู้วิจัยยินดีที่จะจัดส่งรายงานสรุปให้แก่ท่านภายหลังเสร็จสิ้นการวิเคราะห์ข้อมูล

พหุน ปณ ฑิโต ชีเว

APPENDIX E: Cover letters and questionnaire: english version

Questionnaire for Research

Subject: The effect of information technology audit on audit quality of auditors in the Capital Market in Thailand

Explanation:

This research project aims to study "The effect of information technology audit on audit quality of auditors in the Capital Market in Thailand" as part of the researcher's doctoral dissertation in the Doctor of Philosophy in Accounting program, Faculty of Accounting and Management, Mahasarakham University. Telephone: 043-754333.

The researcher kindly requests your assistance in answering this questionnaire. The questionnaire consists of six sections, as follows.

Section 1	General Information About auditors in the Capital Market in Thailand
Section 2	Opinions on Information Technology Audit by auditors in the Capital Market in Thailand
Section 3	Opinions on the Audit Quality by auditors in the Capital Market in Thailand.
Section 4	Opinion on internal environmental factors affects Information Technology Audits by auditors in the Capital Market in Thailand.
Section 5	Opinion on external environmental factors affects Information Technology Audits by auditors in the Capital Market in Thailand.
Section 6	Recommendations and suggestions about Information Technology Audits by auditors in the Capital Market in Thailand.

Your responses will be kept confidential, and no information about your business will be disclosed in the reporting of data. Additionally, this information will not be shared with any third party without your consent. If you wish to receive a summary of the research results, please provide your email address or attach your business card with this questionnaire.

☐ Requires email _____ ☐ Not Requires

The researcher would like to thank you for taking the time to answer the questionnaire accurately and thoroughly. The information you provide will be very valuable to this research. If you have any questions regarding the questionnaire, please contact the researcher, Ms. Metinee Maesuwan, at telephone 083-2919016 or E-mail: 64010991001@msu.ac.th

(Ms. Metinee Maesuwan)
Ph.D. Student
Mahasarakham Business School
Mahasarakham University, Thailand

Section 1: General Information About auditors in the Capital Market in Thailand

1. Gende

□ Male □ Female

2. Age

□ Not more than 30 years □ 31 - 40 years

□ 41 – 50 years □ More than 50 years

3. Status

□ Single □ Married

4. Education level

□ Bachelor's degree □ Higher than bachelor's degree

5. Experience in auditing in the capital market

□ Not more than 5 years □ 6 - 10 years

□ 11 - 15 years □ more than 15 years

6. Average monthly income

□ Not more than 100,000 baht □ 100,001 - 150,000 baht

□ 150,001 - 200,000 baht □ more than 200,000 baht

พหุน ปณ ฑิโต ชีเว

Section 2: Opinions on Information Technology Audit by auditors in the Capital Market in Thailand.

Information Technology Audit	Most 5	More 4	Moderate 3	Less 2	Least 1
1) Financial Statement Audit					
1 You place importance on the audit of material items in the financial statements					
2 You are aware of the comparability of data in the nancial statements					
3 You are committed to auditing material errors in the financial statements					
4 You place importance on auditing to verify the account items presented in the financial statements					
5 You place importance on auditing to present financial information relevant to decision-making					
2) Operational Audit					
6 You believe that following procedures will help achieve the set objectives					
7 You are aware of the need to audit procedures as specified to enhance the credibility of the audit process in accordance with auditing standards					
8 You are aware of the need to follow operational procedures to enhance efficiency in operations					
9 You place importance on reviewing the operational burden within the organization to ensure organizational efficiency					
10 You place importance on following the planned schedule to ensure operational efficiency					

พหุน ปณ ฑิโต ชีเว

Section 2: Opinions on Information Technology Audit by auditors in the Capital Market in Thailand (continue).

Information Technology Audit	Most 5	More 4	Moderate 3	Less 2	Least 1
3) Compliance Audit					
11 You are aware of the organization's rules and regulations to ensure that the work is correct and complete					
12 You believe that reviewing policies and scope of work will help the organization's operations be effective					
13 You prioritize adhering to the organization's regulations to ensure that operations align with the established objectives					
14 You are committed to monitoring operation to ensure they comply with the organizatior regulations, ensuring that the work meets the standards					
4) Information technology Control					
15 You believe that overseeing information technology will ensure that the information is complete, accurate, and used in a manner that complies with financial reporting standards and auditing standards					
16 You believe that information technology security controls will ensure the accuracy o information and enable reasonable opinions to be formed					
17 You believe that defining access rights to information technology will help ensure the reliability of information, allowing for accurate opinions on financial statements					
18 You believe that controlling the input of information will enhance processing efficiency and ensure that audits are conducted in alignment with the facts					
19 You believe that preparing and verifying information before inputting it into the information technology system will help prevent damage to the informatior system					

Section 3: Opinions on the Audit Quality by auditors in the Capital Market in Thailand.

Audit Quality	Most 5	More 4	Moderate 3	Less 2	Least 1
1 You believe that obtaining reliable information will ensure that opinions on financial statements comply with auditing standards					
2 You prioritize gathering sufficient audit evidence to express an opinion on financial statements that are free from errors					
3 You believe that receiving up to date information will help ensure that opinions ar consistent with the facts					
4 You believe that receiving information that is neutral and free from bias will help ensure th opinions are consistent with the facts					
5 You are aware of the importance of auditing and presenting audit reports that reflect the truth					

Section 4: Opinion on internal environmental factors affects Information Technology Audits by auditors in the Capital Market in Thailand.

Internal environmental factors affect Information Technology Audits	Most 5	More 4	Moderate 3	Less 2	Least 1
Reducing Audit Risk					
1 You believe that appropriate audit planning will help reduce errors in the audit					
2 You believe that performing work with caution and thoroughness will ensure accura in the operations					
3 You are aware of the importance of using appropriate information technology to reduc audit risk					
4 You prioritize adhering to auditing standards to reduce errors in the work					

Section 4: Opinion on internal environmental factors affects Information Technology Audits by auditors in the Capital Market in Thailand (continue).

	Internal environmental factors affect Information Technology Audits	Most 5	More 4	Moderate 3	Less 2	Least 1
	Data Security					
5	You prioritize the storage of information to prevent data loss					
6	You believe that reviewing operational procedures will help ensure the reliability an accuracy of information					
7	You believe that defining access rights to data will help ensure its security and integrit					
8	You believe that monitoring network access will help ensure the security of the data					
9	You believe that controlling the use of information technology will help ensure data security					

Section 5: Opinion on external environmental factors affects Information Technology Audits by auditors in the Capital Market in Thailand.

	External environmental factors affect Information Technology Audits	Most 5	More 4	Moderate 3	Less 2	Least 1
	Technological Change Awareness					
1	You recognize the importance of applying information technology to enhance operational efficiency					
2	You prioritize learning information technolo to improve work efficiency					
3	You focus on seeking audit processes that ca effectively adapt to changing technology					
4	You believe that advancements in informatio technology, along with its appropriate and cost-effective use, will enhance operational efficiency					

Section 5: Opinion on external environmental factors affects Information Technology Audits by auditors in the Capital Market in Thailand (continue).

	External environmental factors affect Information Technology Audits	Most 5	More 4	Moderate 3	Less 2	Least 1
	Business Environment					
5	You believe that the current business environment is volatile, necessitating continuous learning and adapting operation according to the circumstances					
6	You believe that the current diverse demand require a focus on meeting customer needs					
7	You believe that increased competition driv continuous change and development in order to survive					
8	You believe that technological advancemen will drive changes in operational processes					
9	You are committed to seeking operational procedures that can accommodate changing environments					
	Regulatory					
10	You believe that operational regulations will help ensure that operations comply wit auditing standards					
11	You are aware of the importance of performing work with caution and thoroughness to ensure that operations adhere to generally accept auditing standards					
12	You believe that regulations, rules, and guidelines will ensure that the audit is accurate and complete					
13	You focus on performing work that adheres to regulations and rules					
14	You believe that establishing clear policies will enhance operational efficiency					

Section 6: Opinions and Additional Suggestions Regarding the Information Technology Audit of auditors in the Capital Market.

If you have any additional suggestions regarding the questionnaire, please provide them in the space below.

……
……
……
……
……
……

Lastly, we would like to express our sincere gratitude to you for taking the time to answer all the questions in the survey. Please fold the survey and place it in the enclosed envelope and return it to the specified address. If you would like to receive a summary report of the research results, please include your business card or specify your email address with the survey. The researcher will be happy to send you the summary report after the data analysis is completed.

พหุน ปณ ฑิโต ชีเว

APPENDIX F: Letters to experts

ที่ อว 0605.10/๗๘๑

คณะการบัญชีและการจัดการ
มหาวิทยาลัยมหาสารคาม
ตำบลตลาดเรียง อำเภอกันทรวิชัย
จังหวัดมหาสารคาม
44150

9 พฤศจิกายน 2566

เรื่อง ขอเรียนเชิญเป็นผู้เชี่ยวชาญตรวจสอบเครื่องมือวิจัย

เรียน ผู้ช่วยศาสตราจารย์ ดร.สุมินทร เบ้าธรรม

ด้วย นางสาวเมพิณี เมษสุวรรณ รหัสนิสิต 64010991001 นิสิตหลักสูตรปรัชญาดุษฎีบัณฑิต (ปร.ด.) สาขาวิชาการบัญชี ระบบบนอกเวลาราชการ คณะการบัญชีและการจัดการ มหาวิทยาลัยมหาสารคาม กำลังศึกษาวิทยานิพนธ์ เรื่อง "ผลกระทบของการตรวจสอบเทคโนโลยีสารสนเทศต่อคุณภาพการตรวจสอบของผู้สอบบัญชีตลาดทุนในประเทศไทย" ซึ่งเป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปรัชญาดุษฎีบัณฑิต ดังนั้น เพื่อให้การดำเนินการเป็นไปด้วยความเรียบร้อยและบรรลุตามวัตถุประสงค์ คณะการบัญชีและการจัดการ มหาวิทยาลัยมหาสารคาม จึงขอความอนุเคราะห์ท่านเป็นผู้เชี่ยวชาญตรวจสอบเครื่องมือวิจัยและข้อเสนอแนะเพื่อนำข้อมูลที่ได้ไปดำเนินการทำวิทยานิพนธ์ต่อไป ตามแบบสอบถามที่แนบมาพร้อมนี้

คณะฯ หวังเป็นอย่างยิ่งว่า คงจะได้รับความอนุเคราะห์จากท่านด้วยดี และขอขอบคุณมา ณ โอกาสนี้

ขอแสดงความนับถือ

(อาจารย์ ดร.ชลธิชา ธรรมวิญญู)
คณบดีคณะการบัญชีและการจัดการ
มหาวิทยาลัยมหาสารคาม

งานบริหารหลักสูตรและการจัดการเรียนการสอนระดับบัณฑิตศึกษา
คณะการบัญชีและการจัดการ มหาวิทยาลัยมหาสารคาม
โทรศัพท์ 0-4375-4333 ต่อ 5630

ปณ ศิโต

APPENDIX G: Letter requesting to collect questionnaires

ที่ อว 0605.10/ 375

คณะการบัญชีและการจัดการ
มหาวิทยาลัยมหาสารคาม
ตำบลขามเรียง อำเภอกันทรวิชัย
จังหวัดมหาสารคาม
44150

31 มกราคม 2567

เรื่อง ขอความอนุเคราะห์กรอกแบบสอบถาม

เรียน ผู้สอบบัญชีตลาดทุนในประเทศไทย

ด้วย นางสาวเมทิณี เมษสุวรรณ รหัสนิสิต 64010991001 นิสิตหลักสูตรปรัชญาดุษฎีบัณฑิต (ปร.ด.) สาขาวิชาการบัญชี ระบบนอกเวลาราชการ คณะการบัญชีและการจัดการ มหาวิทยาลัยมหาสารคาม กำลังศึกษาวิทยานิพนธ์ เรื่อง "ผลกระทบของการตรวจสอบเทคโนโลยีสารสนเทศที่มีต่อคุณภาพการตรวจสอบของผู้สอบบัญชีตลาดทุนในประเทศไทย" ซึ่งเป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปรัชญาดุษฎีบัณฑิต (ปร.ด.) สาขาวิชาการบัญชี ดังนั้น เพื่อให้การดำเนินการเป็นไปด้วยความเรียบร้อยและบรรลุตามวัตถุประสงค์ คณะการบัญชีและการจัดการ มหาวิทยาลัยมหาสารคาม จึงขอความอนุเคราะห์ให้ นางสาวเมทิณี เมษสุวรรณ ศึกษาและเก็บรวบรวมในรายละเอียดตามแบบสอบถามที่แนบมาพร้อมนี้

คณะฯ หวังเป็นอย่างยิ่งว่า คงจะได้รับความอนุเคราะห์จากท่านด้วยดี และขอขอบคุณมา ณ โอกาสนี้

ขอแสดงความนับถือ

(ผู้ช่วยศาสตราจารย์ ดร.พันคม ศรีบุญลือ)
รองคณบดีฝ่ายโครงสร้างพื้นฐาน รักษาการแทน
คณบดีคณะการบัญชีและการจัดการ
มหาวิทยาลัยมหาสารคาม

คณะการบัญชีและการจัดการ มหาวิทยาลัยมหาสารคาม
โทรศัพท์ 0-4375-4333 ต่อ 5630 โทรสาร 0-4375-4425

APPENDIX H: Letter Ethics for Research Involving Human

MAHASARAKHAM UNIVERSITY ETHICS COMMITTEE FOR
RESEARCH INVOLVING HUMAN SUBJECTS

Certificate of Approval

Approval number: 071-617/2024

Title : The effect of information technology audit on audit quality of auditors in the capital market in Thailand.

Principal Investigator : Miss. Metinee Messuwan
Responsible Department : Faculty of Accountancy and Management
Research site : Faculty of Accountancy and Management Mahasarakham University

Review Method : Expedited Review

Date of Manufacture : 31 January 2024 **expire : 30 January 2025**

This research application has been reviewed and approved by the Ethics Committee for Research Involving Human Subjects, Mahasarakham University, Thailand. Approval is dependent on local ethical approval having been received. Any subsequent changes to the consent form must be re-submitted to the Committee.

.....
(Associate Professor Vorapoj Promasatayaprot)
Vice Chairman

Approval is granted subject to the following conditions: (see back of this Certificate)

BIOGRAPHY

NAME	
DATE OF BIRTH	26 May 1994
PLACE OF BIRTH	Kalasin Hospital.
ADDRESS	888/999 Phra Lap, Muang Khon kaen, Khon Kaen
POSITION	lecturer
PLACE OF WORK	Rajamangala University of Technology Isan Khon Kaen Campus 150 Sri Chant Rd, Mueang Khon Kaen District, Khon Kaen 40000
EDUCATION	2016 Bechalor of Accountancy 2019 Master of Accountancy Program 2025 Doctor of Philosophy Program in Accounting

พหุน ปณ ฑิโต ชีเว