THE RELATIONSHIP BETWEEN INTERNAL AUDITOR'S ROLE AND CYBERSECURITY IN MALAYSIA

SADIQAH AISYAH BINTI OTHMAN

Thesis Submitted to

Tunku Puteri Intan Safinaz School of Accountancy

Universiti Utara Malaysia,

in Partial Fulfillment of the Requirement for the Master of Science (International Accounting)

2023

Kolej Perniagaan
(College of Business)
Universiti Utara Malaysia

PERAKUAN KERJA DISERTASI/KERTAS PENYELIDIKAN/KERTAS PROJEK
(Certification of thesis / dissertation)

Kami, yang bertandatangan, memperakukan bahawa
(We, the undersigned, certify that)

SADIQAH AISYAH BINTI OTHMAN (828663)

calon untuk Ijazah
(candidate for the degree of) MASTER OF SCIENCE (INTERNATIONAL ACCOUNTING)

telah mengemukakan tesis / disertasi yang bertajuk:
(has presented his/her thesis / dissertation of the following title):

THE RELATIONSHIP BETWEEN INTERNAL AUDITOR'S ROLE AND CYBERSECURITY IN MALAYSIA

seperti yang tercatat di muka surat tajuk dan kulit tesis / disertasi.
(as it appears on the title page and front cover of the thesis / dissertation).

Bahawa tesis/disertasi tersebut boleh diterima dari segi bentuk serta kandungan dan meliputi bidang ilmu dengan memuaskan, sebagaimana yang ditunjukkan oleh calon dalam ujian lisan yang diadakan pada:

.

(That the said thesis/dissertation is acceptable in form and content and displays a satisfactory knowledge of the field of study as demonstrated by the candidate through an oral examination held on:

'

Pengerusi Viva *(Chairman for Viva)*	:		Tandatangan *(Signature)*	
Pemeriksa Dalam *(Internal Examiner)*	:	DR. MOHD. AMIR BIN MAT SAMSUDIN @ MOHD. SHAM	Tandatangan *(Signature)*	

Tarikh: 30 APRIL 2023
(Date)

Nama Pelajar (Name of Student)	:	SADIQAH AISYAH BINTI OTHMAN (828663)
Tajuk Tesis / Disertasi *(Title of the Thesis / Dissertation)*	:	THE RE**LATIONSHIP BETWEEN INTERNAL AUDITOR'S ROLE AND** CYBERSECURITY IN MALAYSIA
Program Pengajian *(Programme of Study)*	:	M20D **–** MASTER OF SCIENCE (INTERNATIONAL ACCOUNTING)
Nama Penyelia/Penyelia-penyelia *(Name of Supervisor/Supervisors)*	:	DR. MOHAMAD ZULKURNAI BIN GHAZALI

Tandatangan

PERMISSION TO USE

In presenting this dissertation/project paper in partial fulfillment of the requirements for a Post Graduate degree from the Universiti Utara Malaysia (UUM), I agree that the library of this university may make it freely available for inspection. I further agree that permission for copying this dissertation/project paper in any manner, in whole or in part, for scholarly purposes may be granted by my supervisor(s) or in their absence, by the Dean of Tunku Puteri Intan Safinaz School of Accountancy where I did my dissertation/project paper. It is understood that any copying or publication or use of this dissertation/project paper parts of it for financial gain shall not be allowed without my written permission. It is also understood that due recognition shall be given to me and to the UUM in any scholarly use which may be made of any material in my dissertation/project paper.

Request for permission to copy or to make other use of materials in this dissertation/project paper in whole or in part should be addressed to:

Dean of Tunku Puteri Intan Safinaz School of Accountancy

Universiti Utara Malaysia

06010 UUM Sintok

Kedah Darul Aman

ABSTRACT

Information technology (IT) is rapidly being integrated into various fields, particularly finance. Although IT helps run daily operations quickly, effectively, and competitively but the transformation has exposed businesses and companies to the risk of cyberattacks such as data theft, software corruption and disruption of business operations. The Institute of Internal Auditors (IIA) has launched the Three Lines Model which has proven effective in mitigating cybersecurity risks through the first and second lines of defense. Nonetheless, the specific role of internal auditors as the third line of defense in preventing cyberattacks in Malaysia remains unclear and requires further clarification. Therefore, the objectives of this study are to (i) examine the relationship between the internal auditor's role and the internal audit principles in providing assurance to the organization's cybersecurity, (ii) examine the relationship between the internal auditor's role and cybersecurity of the organization's governance, risk, and control and (iii) examine the relationship between internal auditor's role and the competency to assess and mitigate cybersecurity risk. A total of seven participants with diverse backgrounds in the industry were interviewed using open-ended questions. The study revealed a positive correlation between the role of internal auditors and the internal audit principles in providing cybersecurity assurance to the organizations. Furthermore, there is a significant relationship between the internal auditor's role and the cybersecurity of the organization's governance, risk, and control. Additionally, the study found a positive relationship between the internal auditor's role and their ability to assess and mitigate cybersecurity risk. These findings provide valuable insight into the contributions of internal auditors towards cybersecurity in Malaysia.

Keywords: Information technology, internal auditor, cybersecurity, Three Lines Model, cyberattacks

Hubungan antara Peranan Juruaudit Dalaman dan Keselamatan Siber di Malaysia

ABSTRAK

Teknologi maklumat (IT) sedang pesat diintegrasikan dalam pelbagai bidang, khususnya kewangan. Walaupun IT membantu menjalankan operasi harian dengan cepat, berkesan dan berdaya saing tetapi transformasi ini telah mendedahkan perniagaan dan syarikat tersebut kepada risiko serangan siber seperti kecurian data, kerosakan perisian dan gangguan kepada operasi perniagaan. Institut Juruaudit Dalaman (IIA) telah melancarkan Model Tiga Baris IIA yang telah terbukti berkesan dalam mengurangkan risiko keselamatan siber melalui barisan pertahanan pertama dan kedua. Namun begitu, peranan khusus juruaudit dalaman sebagai barisan pertahanan ketiga dalam mencegah serangan siber di Malaysia masih tidak jelas dan memerlukan penjelasan lanjut. Oleh sebab itu, objektif kajian ini adalah untuk (i) mengkaji hubungan antara peranan juruaudit dalaman dan prinsip audit dalaman dalam menjamin keselamatan siber sesebuah organisasi, (ii) mengkaji hubungan antara peranan juruaudit dalaman dan keselamatan siber terhadap tadbir urus, risiko dan kawalan organisasi dan (iii) mengkaji hubungan antara peranan juruaudit dalaman dan kecekapan untuk menilai dan mengurangkan risiko keselamatan siber. Seramai tujuh peserta dengan pelbagai latar belakang dalam industri telah ditemu bual menggunakan soalan terbuka. Kajian ini telah mendedahkan korelasi positif antara peranan juruaudit dalaman dan prinsip audit dalaman dalam menjamin keselamatan siber sesebuah organisasi. Tambahan pula, terdapat hubungan yang signifikan antara peranan juruaudit dalaman dan keselamatan siber tadbir urus, risiko dan kawalan organisasi. Selain itu, kajian ini mendapati adanya hubungan positif antara peranan juruaudit dalaman dan keupayaan mereka untuk menilai dan mengurangkan risiko keselamatan siber. Hasil kajian ini memberikan sudut

pandangan yang berharga tentang sumbangan juruaudit dalaman terhadap keselamatan siber di Malaysia.

Kata kunci: *Teknologi maklumat, juruaudit dalaman, keselamatan siber, Model Tiga Baris, serangan siber*

DECLARATION

I certify that except where due acknowledgment has been made, the work is that of the author alone; the work has not been submitted previously, in whole or in part, to qualify for any other academic award; the content of the thesis is the result of work which has been carried out since the official commencement date of the approved research program; and any editorial work, paid or unpaid, carried out by a third party is acknowledged.

ACKNOWLEDGEMENT

First, I would like to thanks to Allah for helping me and giving me strength from the beginning until I managed to finish the project paper. Besides, I would like to thank my supervisor, Dr. Mohamad Zulkurnai Bin Ghazali, a great lecturer that have continuously taught me, encouraged, and stimulated me with his words during my project paper and hard time. I would like to thank all my lecturers that have taught me and not forgetting my family that always encourage me.

I would like to thank all my classmate and work colleague that have always helping and guide me in writing the project paper. Not forgotten, thanks to my interviewee that help me with my project paper data. I would also like to express my thanks to my boss for the advice provided in guiding me to conduct the interview.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

AC	Audit Committee
AI	Artificial Intelligence
AICPA	American Institute of Certified Public Accountants
BARC	Bhabha Atomic Research Center
BCP	Business Continuity Plan
BIM	Building Information Modelling
BOD	Board of Directors
CAE	Certified Audit Executive
CI	Critical Infrastructures
CISO	Chief Information Security Officers
CMA	Communications Multimedia Act
CNII	Critical National Information Infrastructure
COBIT	Control Objectives for Information Technologies
CPA	Certified Public Accountant
CRI	Cyber Risk Index
CRO	Chief Risk Officer
CS	Cyber Security
CSA	Cyber Security Audit
CSAM	Cybersecurity Audit Model
CYRVM	Cyber Risk and Vulnerability Management
DOS	Denial of Service
ECIIA	European Confederation of Institute of Internal Auditors
ERM	Enterprise Risk Management

GRC	Governance, Risk and Control
HCI	Human-Computer Interface
IAF	Internal Audit Function
ICS-CERT	Industrial Control Systems Cyber Emergency Response Team
IIA	Institute of Internal Auditors
IIARF	Institute of Internal Auditors Research Foundation
IMTA	Information Management and Technology Assurance
IPPF	International Professional Practices Framework
IRS	Internal Revenue Service
IS	Information Security
ISACA	Information Systems Audit and Control Association
ISO	International Organisation for Standardisation
ISRA	Information Security Risk Assessment
IT	Information Technology
MOSTI	Ministry of Science, Technology, and Innovation
NACSA	National Cyber Security Agency
NCSC	National Cybersecurity Centre
NCSP	National Cyber Security Policy
NISER	National Security Emergency Response Centre
NIST	National Institute of Standards and Technology
PRC	Privacy Rights Clearinghouse
SEC	Securities and Exchange Commission
SME	Small and Medium-sized Enterprises
SNI	Systems of National Interest
TMT	Top-Level Management

CHAPTER 1

INTRODUCTION

1 Introduction

In this chapter, brief background of study related to cybersecurity and internal auditor will be explained. Problem statements will be introduced in this chapter including research objectives and research questions. This chapter also includes scope of research and significance of research. Lastly, key terms used in this study will be explained in this chapter.

1.1 Background of Study

Organisations must embrace digitisation and maintain connectivity in the current fast-paced business environment (Ozkaya, 2019). Many companies have adopted information technology (IT) to enable their organisation in running operations quickly, effectively, and competitively. People are using IT more frequently for financial duties and business deals, changing the perception of the conventional economy and ushering in the so-called digital economy (Ozkaya & Aslaner, 2019). The expansion of the internet of things and the use of cloud-based networks have exposed businesses to the threat of cyberattacks, which refer to external attempts to pilfer data, damage software, disrupt operations and cause harm to hardware and network infrastructures. This poses a significant challenge for the field of internet security (Wilson, 2021). According to Australian Cyber Security Centre (2016), a cyberattack is defined as an action to manipulate, disrupt, or destroy devices or information networks related to cyberspace to cause instability in economic and national security. Cyberattacks frequently cause irreparable financial and reputational losses

REFERENCES

Ahmad, M. Z., Azman, N. A., May, O. S., Omar, A., & Norman, M. A. R. (Eds.) (2020). Sustaining Global Strategic Partnership in the Age of Uncertainties. Proceedings of the 8th International Conference on International Studies (ICIS 2020), 5-6 December 2020. School of International Studies: Sintok.

Alina, C. M., Cerasela, S. E., & Gabriela, G. (2017). Internal audit role in cybersecurity. *Ovidius University Annals: Economic Sciences Series*, *17*(2), 510-513.

Al-Matari, O. M., Helal, I. M., Mazen, S. A., & Elhennawy, S. (2021). Integrated framework for cybersecurity auditing. *Information Security Journal: A Global Perspective*, *30*(4), 189-204.

Altwairqi, A. F., AlZain, M. A., Soh, B., Masud, M., & Al-Amri, J. (2019). Four most famous cyber attacks for financial gains. *International Journal of Engineering and Advance Technology*, *9*(2), 2131-2139.

Anderson, D.J. & Eubanks, G. (2015). "Leveraging COSO across the three lines of defense". *Committee of Sponsoring Organizations of the Treadway Commission*, pp.1-32. https://www.iia-ru.ru/upload/documents/professional_practice/position_papers/COSO-2015-3LOD-PDF.PDF

Australian Cyber Security Centre (2016). *ASCS threat report 2016*. Australian Government. Retrieved from https://www.cyber.gov.au/acsc/view-all-content/reports-and-statistics/acsc-threat-report-2016 on 3 December 2022.

Bansal, M. (2018). An Overview of Cyber Security in Malaysia. *International Journal of Emerging Technologies and Innovative Research (Www.jetir.org)*, *5*(8).

Bao Ngo, T. N., & Tick, A. (2021). Cyber-security Risks Assessments by External Auditors. *Interdisciplinary Description of Complex Systems: INDECS*, *19*(3), 375-390.

Betti, N., Sarens, G., & Poncin, I. (2021). Effects of digitalisation of organisations on internal audit activities and practices. *Managerial Auditing Journal*.

Bozkus Kahyaoglu & Caliyurt (2018). Cyber security assurance process from the internal audit perspective. *Managerial Auditing Journal*, *33*(4), 360-376.

Center for Internet Security (2019). *CIS controls*. Version 7.1. https://learn.cisecurity.org/cis-controls-download (Accessed: 2022-11-30).

Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining cybersecurity. *Technology Innovation Management Review*, *4*(10), 13-21.

Deloitte (2017). *Cybersecurity and the role of internal audit: an urgent call to action.* www2.deloitte.com/us/en/pages/risk/articles/cybersecurity-internal-audit-role.html (Accessed: 2022-11-30).

European Confederation of Institutes of Internal Auditors (2020). *Risk in focus 2021. Hot topics for internal auditors*. Retrieved from https://www.eciia.eu/2020/09/risk-in-focus-2021-hot-topics-for-internal-auditors/ on 2 December 2022.

Fairburn, N., Shelton, A., Ackroyd, F., & Selfe, R. (2021, July). Beyond Murphy's Law: Applying Wider Human Factors Behavioural Science Approaches in Cyber-Security Resilience.

In *International Conference on Human-Computer Interaction* (pp. 123-138). Springer, Cham.

Gandhi, R., Sharma, A., Mahoney, W., Sousan, W., Zhu, Q., & Laplante, P. (2011). Dimensions of cyber-attack: Social, political, economic and cultural. *IEEE Technology and Society Magazine*, *30*(1), 28-38.

Ganesin, A., Supayah, L., & Ibrahim, J. (2016). An Overview of Cyber Security in Malaysia. *Kuwait Chapter of the Arabian Journal of Business and Management Review*, *6*(4), 12.

Gao, L., Calderon, T. G., & Tang, F. (2020). Public companies' cybersecurity risk disclosures. *International Journal of Accounting Information Systems*, *38*, 100468.

Ghosh, S. G. (2022, June 19). *An analysis of cybersecurity in Malaysia*. ETCIO.com. Retrieved December 4, 2022, from https://ciosea.economictimes.indiatimes.com/news/security/an-analysis-of-cybersecurity-in-malaysia/92301366

Gulzira, M., Gulmira, B., Altynbek, S., & Assel, O. (2020, September). The audit method of enterprise's Information security. In *Proceedings of the 6th International Conference on Engineering & MIS 2020* (pp. 1-5).

Haapamäki & Sihvonen (2019).

Hashim, M. S. B. (2011). Malaysia's national cyber security policy: The country's cyber defence initiatives. *Second Worldwide Cybersecurity Summit*, 1-7.

Hassanzadeh, A., Rasekh, A., Galelli, S., Aghashahi, M., Taormina, R., Ostfeld, A., & Banks, M. K. (2020). A review of cybersecurity incidents in the water sector. *Journal of Environmental Engineering*, *146*(5), 1-13.

Ho, A. (2018, July 1). *Roles of three lines of Defense for Information Security and governance*. ISACA. Retrieved December 8, 2022, from https://www.isaca.org/resources/isaca-journal/issues/2018/volume-4/roles-of-three-lines-of-defense-for-information-security-and-governance

IBM. (n.d.). *What is cybersecurity?* Retrieved December 2, 2022, from https://www.ibm.com/my-en/topics/cybersecurity

International Trade Administration. (n.d.). *Malaysia Cybersecurity*. Market Intelligence. Retrieved December 2, 2022, from https://www.trade.gov/market-intelligence/malaysia-cybersecurity

Irwin, L. (2022, May 17). *What is a cyber security audit and why is it important?: It governance*. IT Governance UK Blog. Retrieved December 2, 2022, from https://www.itgovernance.co.uk/blog/what-is-a-cyber-security-audit-and-why-is-it-important#:~:text=A%20cyber%20security%20audit%20is,result%20in%20a%20data%20breach.

Islam, M. S., Farah, N., & Stafford, T. F. (2018). Factors associated with security/cybersecurity audit by internal audit function: An international study. *Managerial Auditing Journal*.

Jayabalan, P., Ibrahim, R., & Manaf, A. A. (2014). Understanding cybercrime in Malaysia: an overview. *Sains Humanika*, *2*(2).

Kahyaoglu, S. B., & Caliyurt, K. (2018). Cyber security assurance process from the internal audit perspective. *Managerial Auditing Journal*.

Kaspersky Security Bulletin. (2013). *Statistics*. Retrieved from http://report.kaspersky.com/#the-overall-statistics-for-2013 on 4 December 2022.

Kaur, D. (2022). *Kaspersky: Malaysia needs to take a more active stance in cybersecurity*. Retrieved from https://techwireasia.com/2022/10/kaspersky-malaysia-needs-to-take-a-more-active-stance-in-cybersecurity/ on 4 December 2022.

Li, H., No, W. G., & Boritz, J. E. (2020). Are external auditors concerned about cyber incidents? Evidence from audit fees. *Auditing: A Journal of Practice & Theory*, *39*(1), 151-171.

Lois, P., Drogalas, G., Karagiorgos, A., Thrassou, A., & Vrontis, D. (2021). Internal auditing and cyber security: audit role and procedural contribution. *International Journal of Managerial and Financial Accounting*, *13*(1), 25-47.

Munir, A. B., & Yasin, S. H. M. (2010). *Information and Communication Technology Law*. Petaling Jaya, Malaysia: Sweet & Maxwell Asia.

Murugiah, S. (2022). AirAsia hit by ransomware attack, five million passenger and employee data compromised. Retrieved from https://www.theedgemarkets.com/article/airasia-hit-ransomware-attack-5-million-passenger-and-employee-data-compromised on 5 December 2022.

Newman, H, L., (2021). The worst hacks of 2021. It was a year of ransomware, surveillance, data breaches, and yes, more ransomware. *Wired,* 24th December. https://www.wired.com/story/worst-hacks-2021/

Ozkaya, E & Aslaner, M., (2019). *Hands-on cybersecurity for finance, Identify vulnerabilities and secure your financial services from security breaches.* Packet publishing, Mumbai, India.

Ozkaya, E. (2019). *Cybersecurity: The Beginner's Guide: A Comprehensive Guide to Getting Started in Cybersecurity*, Packt Publishing, Limited, Birmingham.

Priyadarshini, I. (2019). Introduction on cybersecurity. In Le, D., Kumar, R., Mishra, B. K., Khari, M., & Chatterjee, J. M. (Eds.). *Cyber Security in Parallel and Distributed Computing: Concepts, Techniques, Applications and Case Studies* (1-37). Beverly, USA: Scrivener Publishing.

Quader, F., & Janeja, V. P. (2021). Insights into organizational security readiness: Lessons learned from cyber-attack case studies. *Journal of Cybersecurity and Privacy*, *1*(4), 638-659.

Ramamoorti, S. (2003). Internal auditing: History, evolution, and prospects. In Bailey, A. D., Gramling, A. A., & Ramamoorti, S. (Eds.). *Research Opportunities in Internal Auditing*. Florida, USA: Institute of Internal Auditors Research Foundation.

Rainer, R. K., & Prince, B. (2021). *Introduction to Information Systems*. New York, USA: John Wiley & Sons.

Raju, R., Rahman, N. H. A., & Ahmad, A. (2022). Cyber security awareness in using digital platforms among students in a higher learning institution. *Asian Journal of University Education*, *18*(3), 756-766.

Rosati, P., Gogolin, F., & Lynn, T. (2019). Audit firm assessments of cyber-security risk: evidence from audit fees and SEC comment letters. *The International Journal of Accounting*, *54*(03), 1950013.

Rosati, P., Gogolin, F., & Lynn, T. (2022). Cyber-security incidents and audit quality. *European Accounting Review*, *31*(3), 701-728.

Roussy, M. & Perron, A. (2018). "New Perspectives in Internal Audit Research: A Structured Literature Review", *Accounting perspectives,* 17(3), pp. 345-385.

Russo, P., Caponi, A., Leuti, M., & Bianchi, G. (2019). A web platform for integrated vulnerability assessment and cyber risk management. *Information*, *10*(7), 242.

Sabillon, R. (2019). Audits in cybersecurity. In Management Associations (Eds.). *Research Anthology on Business Aspects of Cybersecurity*. Pahang, Malaysia: IGI Global.

Sabillon, R., Serra-Ruiz, J., Cavaller, V., & Cano, J. (2017, November). A comprehensive cybersecurity audit model to improve cybersecurity assurance: The cybersecurity audit model (CSAM). In *2017 International Conference on Information Systems and Computer Science (INCISCOS)* (pp. 253-259). IEEE.

Salihu, A., & Berisha-Hoti, X. (2019). The Effect of IT Audit on Security Incidents. *International Journal of Scientific & Technology Research*, *8*(8), 1342-1347.

Shaikh, F. A., & Siponen, M. (2023). Information security risk assessments following cybersecurity breaches: The mediating role of top management attention to cybersecurity. *Computers & Security*, *124*, 102974.

Shameli-Sendi, A., Ezzati-Jivan, N., & Jabbarifar, M. (2012). Intrusion response systems: Survey and taxonomy. *International Journal of Computer Science and Network Security, 12*(1), 1-14.

Simić, N. (2022). The Internal Auditor's Role in Cybersecurity Governance: A qualitative study about the internal auditor's influence on the people factor of cybersecurity.

Slapničar, S., Vuko, T., Čular, M., & Drašček, M. (2022). Effectiveness of cybersecurity audit. *International Journal of Accounting Information Systems*, *44*, 100548.

Stafford, T., Deitz, G., & Li, Y. (2018). The role of internal audit and user training in information security policy compliance. *Managerial Auditing Journal*.

Steinbart, P. J., Raschke, R. L., Gal, G., & Dilla, W. N. (2012). The relationship between internal audit and information security: An exploratory investigation. *International Journal of Accounting Information Systems*, *13*(3), 228-243.

Steinbart, P. J., Raschke, R. L., Gal, G., & Dilla, W. N. (2018). The influence of a good relationship between the internal audit and information security functions on information security outcomes. *Accounting, Organizations and Society*, *71*, 15-29.

Supayah, G., & Ibrahim, J. (2016). An overview of cyber security in Malaysia. *Arabian Journal of Business and Management Review*, *6*(4), 12-20.

Sulaiman, N. S., Fauzi, M. A., Hussain, S., & Wider, W. (2022). Cybersecurity behaviour among government employees: The role of protection motivation theory and responsibility in mitigating cyberattacks. *Information*, *13*, 1-17.

Tamyez, P. F. (2019). The challenges and solutions of cybersecurity among Malaysian companies. In Management Associations (Eds.). *Research Anthology on Business Aspects of Cybersecurity*. Pahang, Malaysia: IGI Global.

Tawfik, O. I., Al Tahat, S., Jasim, A. L., & Abd Almonem, O. (2021). INTELLECTUAL IMPACT OF CYBER GOVERNANCE IN THE CORRECT APPLICATION OF CLOUD ACCOUNTING IN JORDANIAN COMMERCIAL BANKS-FROM THE POINT OF VIEW OF JORDANIAN AUDITORS. *Journal of Management Information and Decision Sciences*, *24*(5), 1-14.

Tharshini, N. K., Mas'ud, F. H., & Hassan, Z. (2022). Level of cybercrime threat during the outbreak of COVID-19 pandemic: A study in Malaysia. *International Journal of Academic Research in Business and Social Sciences*, *12*(5), 40-51.

The Institute of Internal Auditors (IIA) (2017). *International Professional Practice Framework (IPPF) (2017 edition).* The Institute of Internal Auditors.

Turk, Ž., Sonkor, M. S., & Klinc, R. (2022). Cybersecurity assessment of BIM/CDE design environment using cyber assessment framework. *Journal of Civil Engineering and Management*, *28*(5), 349-364.

US, D. (2022, August 16). *Cybersecurity and internal audit*. Deloitte United States. Retrieved December 8, 2022, from https://www2.deloitte.com/us/en/pages/risk/articles/cybersecurity-internal-audit-role.html

Walton, S., Wheeler, P., Zhang, Y. & Zhao, X. (2021). "An Integrative Review and Analysis of Cybersecurity Research: Current State and Future Directions", *The Journal of information systems,* 35(1), pp. 155-186.

Wilson, C. D., (2021). *Cybersecurity: The MIT press essential knowledge series,* The Mit press, Cambridge, Massachusetts.

Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., & Basim, H. N. (2022). Cyber security awareness, knowledge and behavior: a comparative study. *Journal of Computer Information Systems*, *62*(1), 8

APPENDICES

Interview Question:

#	**Question**
Background	
Q1	What is your role in the company?
Q2	How long have you worked in the company?
Q3	How long have you worked with internal auditing?
Role of Internal Auditor	
Q4	What would you say is essential within your position as an internal auditor?
Q5	How does the internal audit process look like in a company? a. How does the process look like regarding cybersecurity?
Q6	Is the internal audit process based on a specific framework or from a specific regulatory organisation?
Q7	How would you describe assurance?
Q8	How do you, as an internal auditor, promote assurance within governance, risk, and control? a. How do you provide assurance within cybersecurity?
Q9	How would you describe your relationship with other important roles within the company, such as with top management, board of directors and managers?
Q10	Do you believe cybersecurity has changed the role of internal audit in organisations, if so how and why?
Q11	Is the internal audit activity capable of assessing processes and controls to mitigate cyber threats, or does the IA need to consider additional resources with cyber security expertise?
Governance	
Q12	How does your work with internal auditing influence the employees and the organisation?
Q13	With your current position, do you have any relation with those co-workers working with cybersecurity? Is there a specific cybersecurity unit in your organisation? / How would you describe the relationship internal auditors have with people working with cybersecurity?
Q14	What is your opinion about internal auditing promoting cybersecurity risk disclosures? / In what way do you think internal auditing helps improving organisation's public disclosures regarding cybersecurity towards the stakeholders?
Q15	In what way do you believe internal audit influences on organisation's cybersecurity governance? / In what way do you believe internal audit strengthen on organisation's cybersecurity governance?
Q16	How do you think internal audit helps to prevent attacks from cyberhackers where employees are being tricked to release confidential information? a. What kind of procedures can internal auditors take regarding internal control?