Indexed in Clarivate Analytics WoS, and ScienceOPEN

E-B Environment - Behaviour Proceedings Journal

ITMAHuB2023

https://kppim.uitm.edu.my/research/conferences/itmahub-2023

2nd International Conference on Information Science, Technology, Management, Humanities, and Business

Hotel UiTM, Shah Alam, Malaysia, 26-27 Sep. 2023

Organised by College of Computing, Informatics and Mathematics, UiTM, Malaysia

Systematic Literature Review for Modeling a Cyber Risk Assessment Framework

Zahari Mohd Amin[1], Norizan Anwar[1], Mohd Shamsul Mohd Shoid[1], Suzaliana Samuri[2]

[1] Senior Lecturer, School of Information Science, College of Computing, Informatics and Mathematics, Universiti Teknologi MARA, Selangor, Malaysia

[2] Senior Manager, Malaysia Airports Holding Berhad, KLIA, Sepang, Selangor, Malaysia

zahari1483@uitm.edu.my, norizan8027@uitm.edu.my, shamsulshoid@uitm.edu.my, suzalianasamuri@malaysiaairports.com.my
Tel: +60173018626

Abstract

This paper presents a framework for cyber risk assessment using a systematic literature review (SLR). A three-staged systematic review was used in this SLR planning, conducting, and reporting the review. Results screening was done by applying inclusion and exclusion criteria. EndNote software and the PRISMA flow diagram were helpful tools during this screening process. The SLR helps the researcher to discover the variables and dimensions in assessing cyber risk. Its findings helped the researcher to produce a framework model of cyber risk assessment. The framework created is expected to give an overview of a more standardized and controlled method of assessing cyber risk to be adopted by organizations.

Keywords: Cyber security, Systematic literature review, cyber risk assessment framework

DOI: https://doi.org/10.21834/e-bpj.v9iSI18.5481

1.0 Introduction

It is fair to say that internet technologies have become a compulsory element and are a must for not only organizations, but individuals to run their businesses. Technologies such as Knowledge Management systems (KMS) allow organizations to gain vast business intelligence (Baharuddin et al., 2016). Organizational agility has also become a necessary capability for organizations to compete and cope with the unprecedented changes in the business environment (Zaini et al., 2020). With this increase in online business transactions, organizations are exposed to various online threats that may harm their business operations. This cyber threat can impact all areas of business operations, whether technically, harming the IT infrastructure or economically, which means a loss in terms of profit and cost to recover the harm done. Patel and Zaveri (2010) outlined that the possible losses to the business caused by cyber risk are mainly loss of revenues, including a loss in controls, products, staff time, equipment damage, and loss in prevention (Patel & Zaveri, 2010). This situation is a risk in business, and this risk, which appears via an online network, is what we call cyber risk, and anything connected to the internet is potentially exposed to these risks. To control this risk, it needs to be assessed properly before another process of controlling can further proceed.

In combating or minimizing cyber risk, we need to know the risk. According to RSA (2016), cyber risk is exposure to harm or loss resulting from breaches of or attacks on information systems (RSA, 2016). We would be unable to manage these hazards and threats if

eISSN: 2398-4287 © 2024. The Authors. Published for AMER and cE-Bs by e-International Publishing House, Ltd., UK. This is an open access article under the CC BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/4.0/). Peer–review under responsibility of AMER (Association of Malaysian Environment-Behaviour Researchers and cE-Bs (Centre for Environment-Behaviour Studies), College of Built Environment, Universiti Teknologi MARA, Malaysia.
DOI: https://doi.org/10.21834/e-bpj.v9iSI18.5481

we did not know it. Assessing is the initial and earliest process of managing risk. At this stage, organizations will get to know the available risk, know its nature, and define its severity, whether it is tolerable or not to the organizations. Cyber risk assessment is one of the stages in the risk management process. At this stage, the risk of the cyber-related area will be assessed through various methods and criteria to determine the level of harm caused (or may cause) and the order of tackling it. There are Standards provided for applying risk management controls in organizations, such as the ISO/IEC 27005, National Institute of Standards and Technology (NIST) Special Publication 800-30, and British Standards 31000-2018. There are also policies produced for managing risk. Somehow, there is a lack of a specific methodology or concept for handling this risk. During the literature review phase, the researcher faces difficulty in retrieving literature that relates to cyber risk assessment. The literature found was mostly non-empirical papers that would not represent the conduct of the cyber risk assessment process in-depth. Most searches return conceptual papers that discuss cyber risk in general but not much on the assessment application of it. The guidelines and policies are general breakdowns that are being extracted from the standards mentioned above. Organizations may apply it differently by looking at their controlling resource or capability to do it. However, it is hard to find how organizations assess cyber risk as it will depend on their policy of risk management or the best practices of the organizations. It is best if a specific guideline is given in assessing the cyber risk to be used by organizations in a standard manner. These various ways of assessing risk may impose problems in getting a precise idea of how cyber risk is being handled and may not provide the best and most comprehensive method for standard in assessing cyber risk.

These factors have motivated the researcher to find specific papers about the conduct of cyber risk assessment and the method used in the assessing process. Therefore, a systematic literature review (SLR) is needed. The main objectives of the SLR are:
1) to explore literature published in cyber risk assessment that specifically discussed cyber risk assessment and the matters of conduct involved in assessing cyber risk,
2) to identify the variables and dimensions involved in assessing cyber risk, and
3) to develop a framework based on the variables and dimensions identified.

The researcher expected that at the end of the research, the framework developed will produce the variables and dimensions that are usually being used in assessing cyber risk. The framework will give an idea of a more standardized and controlled method in assessing cyber risk to be adopted by organizations in quest of minimizing or mitigating the risk of cyber-criminal-related issues. The breakdown of more specific stages in the assessment would benefit organizations in managing the risk of cyber during the assessment phase of the risk management process.

2.0 Methodology

The initial idea was developed during the traditional literature review, and the gap found was a lack of literature published specifically on cyber risk assessment. The researcher tends to investigate cybersecurity-related risk assessment as this is a current topic, and the least amount of published literature has been produced. To further view the topic, a systematic review is considered the best way to get the best idea about the research topic. Guidelines suggested by Kitchenham (2007) are best to be used in this systematic review. She mentioned that there are three phases of SLR which are planning the review, conducting the review, and reporting the review. A systematic review is a method of making sense of large bodies of information and a means of contributing to the answers to questions about what works and what does not (Petticrew & Roberts, 2008). It is a methodical way to identify, evaluate, and interpret the available studies conducted on a topic, research question, or phenomenon of interest (Kitchenham & Charters, 2007).

Stages of the systematic review were developed in this research. According to Joanna Briggs Institute (JBI), SLR entails a three-stage approach, (*Introduction to JBI Systematic Reviews - JBI Manual for Evidence Synthesis - JBI Global Wiki*, n.d.). These stages are the same as mentioned in the SLR phases by Kitchenham (2007). Table 1 shows the stages of systematic review in this research based on the JBI model.

Table 1: Stages of Systematic Review

Stages	Details
Planning the review	Specifying the search terms
	Selection of the most popular online database
Conducting the review	Apply search terms on the selected online database
	Apply the inclusion and exclusion criteria to get a precise finding
Reporting the review	Evaluating the result

A systematic review flow diagram from PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) is used in conducting the review (*PRISMA*, n.d.). PRISMA listed three main phases in conducting a review, which are identification, screening, and inclusion. It maps out the number of records identified, included, and excluded from the systematic review. The reasons for exclusions can also be added to the flow diagram.

3.0 Planning the Review

3.1 Search Terms

The initial traditional literature review provides an idea of defining the best search terms related to cyber risk assessment. Choosing the correct terms is vital in making sure the research is going in the right direction in achieving the objective of the systematic review. There

are four keywords identified as best to be used to search papers related to cyber risk assessment. According to ISO27001, the risk assessment process consists of three phases, namely, risk identification, risk analysis, and risk evaluation (ISO 27001, 2013). These phases are being used to determine different types of risk. Therefore, these three risk keywords will also be used for the search terms together with risk assessment. As this research tends to look at the risk in cyber, the search keywords in the systematic review are cyber risk assessment, cyber risk identification, cyber risk analysis, and cyber risk evaluation.

Table 2: Definition of the Search Terms

Search term	**Definition**
Cyber risk assessment	Cyber risk assessment is the process of identifying, analyzing, and evaluating risk (*Cybersecurity Risk Assessment*, n.d.)
Cyber risk identification	the process of determining what could happen to cause a potential loss, and gaining insight into how, where, and why the loss might happen (I S O ISO, 2011)
Cyber risk analysis	Steps in looking at the likelihood of it happening or its occurrence probability (McNeil et al., 2018)
Cyber risk evaluation	Process of giving a score on the risk's severity and likelihood (International Standards Organisation ISO et al., 2008)

These terms will be used individually as the researcher tends to find specific literature related to each term.

3.2 Literature Retrieval

This study focuses on articles from journals and proceedings. This is because the researcher tends to look for research-related cyber risk assessment papers. Online databases chosen for the retrieval are aligned with the focus articles and popularity. The list of online databases selected for the search is listed below:

Table 3: Literature and Online Databases

Focused literature	Online Databases
Journals and Proceedings	ACM Digital Library, Emerald Insight, IEEE Explore, Science Direct, Scopus, Web of Science

During the search, all the search terms as Table 2 are applied to each online database. The initial search results are accepted as the number considered as the initial finding of the review. At this stage, the numbers are big as no screening has been done for the results yet. Statistics for the number of searches were produced for each search term applied.

4.0 Conducting the Review

4.1 Search Strategy

Searching for the terms was using quotation marks (" ") to search for the exact match of the phrase. An exact match is chosen for the research as it would be more specific and to avoid any unwanted literature from being included in the search results as the researcher tends to look for specific literature based on the search terms used. The researcher did a trial search run by applying a general search using the same search terms, and the results were a vast amount of search results. The results somehow provide articles that do not really in cyber risk assessment, but a very general thing related to information security and cyber security.

In this research, the same search terms were applied to each online database to ensure the uniformity of the searches and to avoid biases between searchings. These results during the first initial search process were recorded and extracted into EndNote software.

4.2 Inclusion and Exclusion

Inclusion and exclusion criteria ensure the selected studies are relevant and related to the current study. This criterion is vital to systematic review as it will determine the most accurate literature being accessed in this SLR. The consideration was only for articles in journals or proceedings written in the English language. The papers must also be published after the year 2000 as, during this period, cybersecurity and the activities of cyber criminals started to evolve, and so many types of cyber criminals surfaced. The growth of the internet was huge during this period, and the first hacker group was also developed during this time (*History of Cyber Security - Cyber Security Degree*, n.d.)

Table 4: Inclusion and Exclusion Criteria

Criteria	Decision
Keywords existed in the title, abstract, or content of the paper	Inclusion
Papers from Journals article	Inclusion
Full-text article	Inclusion
The paper was published in scientific peer-reviewed journals	Inclusion
Papers that are duplicated within the searched documents and sources	Exclusion
Papers that are not accessible	Exclusion
Papers are written other than in the English language	Exclusion
Papers that are not primary/ original research	Exclusion

Papers published before the year 2000	Exclusion

The screened results were further filtered to make sure the most suitable papers were selected for the review. According to Anwar (2015), result filtering can be done by applying the relevance criteria (Anwar, 2015). The papers are considered not relevant if it has at least one of the following criteria:

Table 5: Relevance Criteria

Criteria	Decision
1 Its main focus is not on the assessment of cyber risk	Exclude
2 It does not mention any assessment part of cyber risk, either identification, analysis, or evaluation of cyber risk	Exclude
3 It does not have any explanation of the cyber risk being addressed in its content	Exclude
4 The risk assessment is not in a cyber-related area	Exclude
5 Short papers with 2 pages or less	Exclude
6 It has no author	Exclude

The researcher tends to look for papers that discuss the conduct of cyber risk assessment and the process involved. Papers that do not have these criteria (as shown in criteria 1 – 4 in Table 5) will be excluded from the SLR. Papers that have less than 2 pages would be considered as the researcher to be insufficient in the data and explanation given. Meanwhile, papers with no author are doubtful of their authority and the accuracy of the data provided.

5.0 Reporting the Review

Based on the PRISMA flow diagram for systematic reviews, below are the overall results of the systematic literature review for cyber risk assessment.

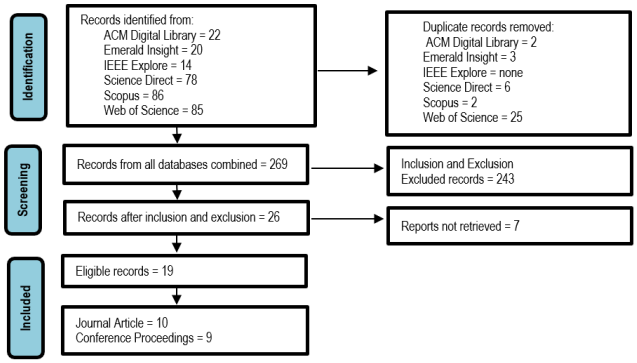

Figure 1: SLR Flow Diagram for Cyber Risk Assessment

The diagram shows a significant reduction in numbers after duplicated records were removed and after the exclusion based on the criteria given in Table 4 and Table 5.

6.0 SLR findings

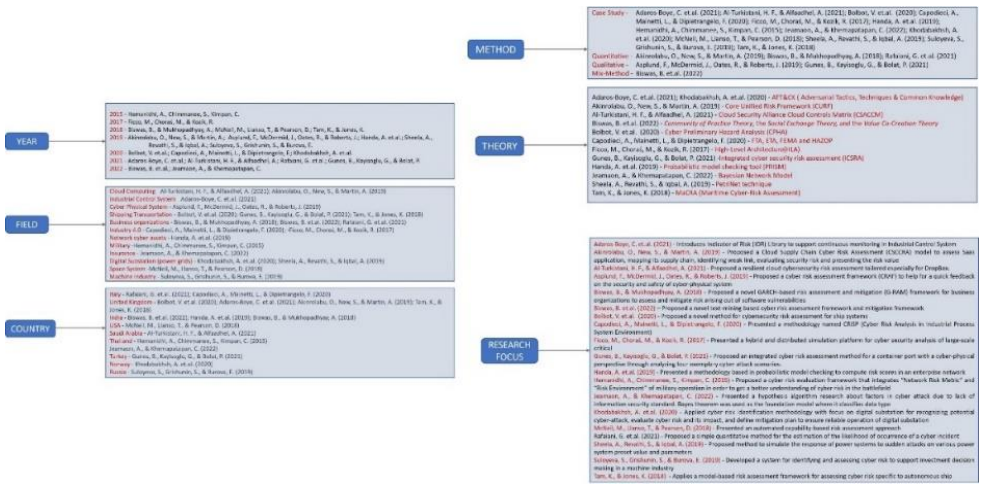

Figure 2: SLR Summary

The final papers found from the SLR were read through and were categorized into several areas; year of study, research field, country of origin, method of research, theory used, and research focus. The figure below presents a summary of the findings.

The result summary above is useful to get a better insight into the papers and provide good details references on research done on cyber risk assessment. Going further, 3 main variables were found used in these papers in assessing cyber risk which are cyber risk identification, cyber risk analysis, and cyber risk evaluation. The table below presents the summary of the variables from each author and their dimensions.

Table 6: Summary of Dimension of Independent Variable (IV)

	Cyber Risk Identification					Cyber Risk Analysis				Cyber Risk Evaluation	
Authors	Assets (People, Process, Technology)	Vulnerability	Type of threat (Offensive Capability)	Attack Vector	Available Control (Defensive Capability)	Likelihood	Severity/ Impact to Business	Risk Criteria	Risk Rating	Risk Score	Risk Control
Adaros-Boye, C. et.al., 2021	√							√	√	√	
Akinrolabu & Martin, 2019											
Al-Turkistani, & Alfaadhel, 2021	√										
Asplund, et.al., 2019		√	√				√				
Biswas & Mukhopadhyay, 2018		√					√				
Biswas, B. et.al. 2022			√			√					
Bolbot, V. et.al. 2020			√	√		√		√	√	√	√
Capodieci, A. et.al., 2020							√				
Ficco, M., et.al., 2017									√	√	√
Gunes, B. et.al., 2021					√			√		√	√
Handa, A. et.al. 2019											
Hemanidhi, A. et.al., 2015		√								√	√
Jeamaon & Khemapatapan, 2022						√				√	√
Khodabakhsh, A. et.al. 2020				√				√	√		
McNeil, M. et.al., 2018					√			√	√		
Rafaiani, G. et.al. 2021		√				√					
Sheela, A. et.al., 2019										√	√
Suloyeva, S. et.al., 2019	√					√		√	√		
Tam & Jones, 2018			√								

This led the author to form a basic research model for cyber risk assessment based on the results found from the above tables as figure below.

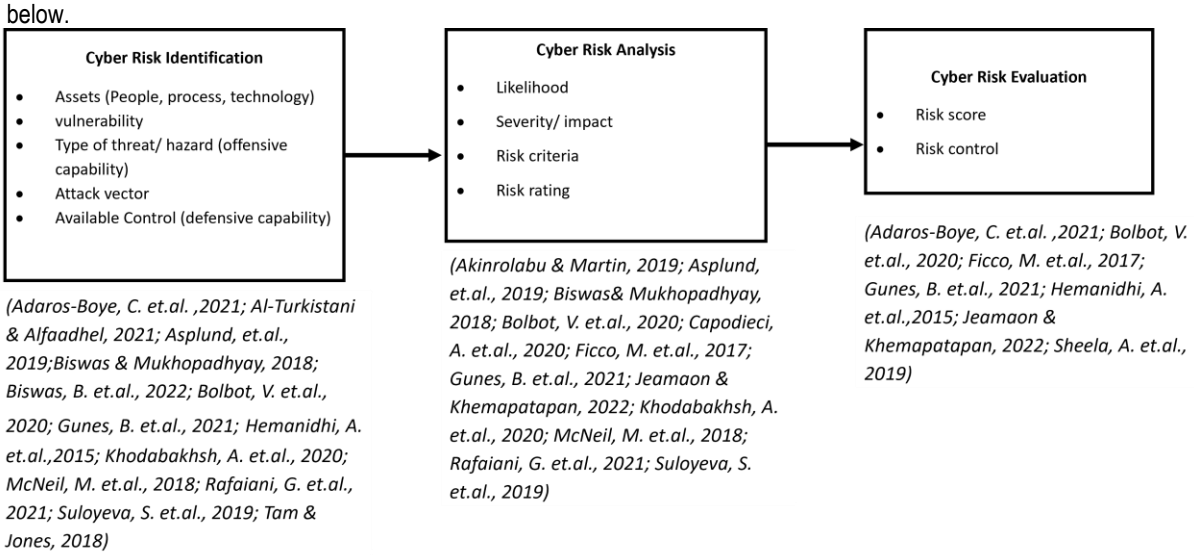

Figure 3: Research Framework for Cyber Risk Assessment

In cyber risk identification, risks are identified mainly from the three elements of people, process, and technology, which these elements are considered assets to organizations (Adaros-Boye, 2021). In any organization, people, processes, and technologies are the elements that would drive their performance and productivity. It is considered an asset, and any harm to it will cause losses. The type of threat would define the vulnerability level of the assets to the possibility of cyber-attacks (Al-Turkistani, 2021). Vulnerable assets would easily be exposed to harm by cyber attackers and need to be identified before further action to overcome the possibilities of cyber-criminal activities. The attack vector is a path or means by which an attacker or hacker can gain access to a computer or network server to deliver a payload or malicious outcome. It is interrelated with the vulnerability of the assets. McNeil (2018) in his work listed available control as a defensive capability that needs to be identified for mitigating the issues of cyber risk.

Cyber risk analysis is a process after identification in defining the likelihood of a cyber-attack and its severity. Likelihood in the framework of cyber risk analysis was conceptualized by Biswas (2022). It stated in the research that the likelihood of cyber-attacks is

needed in mitigating the cyber risk issue. This can be done by rating the risk and defining its severity. The ranking is the risk rating under the cyber risk analysis process.

Cyber risk evaluation in the framework was conceptualized mainly from the theory by Hemanidhi (2015). Hemanidhi in its research came up with a risk metric that produces risk score. The score is used to determine how an organization can cope by accepting the risk and mapping with the best control for each risk.

7.0 Conclusion

The lack of a specific methodology for assessing cyber risk leads the author to look for the best approach to assessing cyber risk. SLR is the best way to look for papers in cyber risk assessment, as limited papers are produced on this topic. This article shows the steps in conducting a systematic literature review for cyber risk assessment. After some extensive and detailed search, the result returned numbers of the most relevant papers in the related area. The process involved in assessing cyber risk based on various research papers done in various fields was discovered from this literature. The findings help to produce a simple framework based on variables and dimensions found in the conduct of cyber risk assessment. Through this SLR, the main variables in cyber risk assessment in the risk management process are seen as the same in identification, analysis, and evaluation. Somehow, the dimensions in each variable appear to vary according to the preferred cyber risk assessing process done by each organization. This framework, however, might be useful in discovering all the different dimensions that should be considered in all the stages of identifying, analyzing, and evaluating cyber risk. Although organizations may not be able to go through all the processes as shown in the framework because of factors such as resource capability, it may guide them to consider the dimensions that are related to their operation in assessing cyber risk.

This research, however, is limited to the assessment part of the overall risk management process. It is at the phase of assessing cyber risk but not on the treatment of the risk. The terms used in the SLR are specific based on the risk assessment process according to the standards from ISO27005. An exact match search method was used to find papers from the exact terms. This would not allow any keywords outside of the terms used to appear in the searched results. Although the search results came back specific and very precise to the related field, it may miss related papers in cyber risk assessment that are being used with different keywords. The online databases used for the search were limited to the mentioned 6 major online databases. It may provide more data if more online databases are used in the SLR.

Acknowledgement

The author would like to thank the College of Computing, Informatics, and Mathematics, University Teknologi MARA for supporting this paper..

References

Anwar, N. (2015). The Impact of Information Technology Infrastructure Flexibility on Strategic Use of Information Systems. *Pacific Asia Conference on Information Systems (PACIS)*, *3*, Paper 271.

Baharuddin, M. F., Tengku, T. A., Mohamad, A. N., & Hasnol, W. M. H. W. (2016). A Framework-based Knowledge Management System (KMS) for Dynamic Decision-Making (DDM). *International Journal of Academic Research in Business and Social Sciences*, *6*(4). https://doi.org/10.6007/ijarbss/v6-i4/2107

Cybersecurity Risk Assessment. (n.d.). Retrieved January 6, 2022, from https://www.itgovernance.asia/cyber-security-risk-assessments-10-steps-to-cyber-security

(Gough et al., (2012). *An introduction to systemic reviews*.

History of Cyber Security - Cyber Security Degree. (n.d.). Retrieved January 16, 2022, from https://cyber-security.degree/resources/history-of-cyber-security/

Introduction to JBI Systematic Reviews - JBI Manual for Evidence Synthesis - JBI Global Wiki. (n.d.). Retrieved June 21, 2022, from https://jbi-global-wiki.refined.site/space/MANUAL/4687241/1.1+Introduction+to+JBI+Systematic+reviews

ISO 27001. (2013). INTERNATIONAL STANDARD ISO / IEC Information technology — Security techniques — Information security management systems — Requirements. *Information Technology — Security Techniques — Information Security Management Systems — Requirements*, *2014*(ISO/IEC 27001:2013), 38.

ISO, I S O. (2011). IEC 27005: Information technology–security techniques–information security risk management. *Iso/Iec*, *44*(0).

ISO, International Standards Organisation, 1, J. T. C. I. J., Technology, I., & Subcommittee SC 27, I. S. techniques. (2008). *Iso/Iec 27005:2008*. *3*, 61. http://www.iso.org

Kitchenham, B. A., & Charters, S. (2007). *Guidelines for performing Systematic Literature Reviews in Software Engineering. EBSE Technical Report EBSE-2007-01. School of Computer Science and Mathematics, Keele University*. *January*, 1–57.

McNeil, M., Llanso, T., & Pearson, D. (2018, April 10). Application of capability-based cyber risk assessment methodology to a space system. *ACM International Conference Proceeding Series*. https://doi.org/10.1145/3190619.3190644

Patel, S., & Zaveri, J. (2010). A risk-assessment model for cyber attacks on information systems. *Journal of Computers*, *5*(3), 352–359. https://doi.org/10.4304/jcp.5.3.352-359

Petticrew, M., & Roberts, H. (2008). Systematic Reviews in the Social Sciences: A Practical Guide. In *Systematic Reviews in the Social Sciences: A Practical Guide*.

https://doi.org/10.1002/9780470754887

PRISMA. (n.d.). Retrieved June 21, 2022, from https://prisma-statement.org//prismastatement/flowdiagram.aspx

Purssell, E., & McCrae, N. (2020). How to Perform a Systematic Literature Review. In *How to Perform a Systematic Literature Review*. https://doi.org/10.1007/978-3-030-49672-2

RSA. (2016). Cyber Risk Appetite: Defining and Understanding Risk in the Modern Enterprise. *Rsa*, 1–4. http://www.reuters.com/article/us-nasdaq-halt-glitch-idUSBRE97S11420130829%0Ahttp://www.reuters.com/article/us-nasdaq-halt-glitch-idUSBRE97S11420130829%0Ahttp://www.reuters.com/article/us-nasdaq-haltglitch-idUSBRE97S11420130829%0Ahttps://www.rsa.com/cont

Zaini, M. K., Masrek, M. N., & Abdullah Sani, M. K. J. (2020). The impact of information security management practices on organizational agility. *Information and Computer Security*, *28*(5), 681–700. https://doi.org/10.1108/ICS-02-2020-0020