Available Online at www.e-iph.co.uk
Indexed in Clarivate Analytics WoS, and ScienceOPEN
https://www.amerabra.org

E-B Environment - Behaviour Proceedings Journal

ICIS2022Penang
https://fim.uitm.edu.my/index.php/research/conference/342-icis-2022
5th International Conference on Information Science
Royale Chulan, Penang, Malaysia, 19-21 Sep 2022
Organised by Faculty of Information Management, UiTM, Malaysia

e-IPH e-International Publishing House Ltd., United Kingdom

Method for Conducting Systematic Literature Review (SLR) for Cyber Risk Assessment

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

[1] Senior Lecturer, Faculty of Information Management, UiTM Selangor, Shah Alam, 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 method for conducting a systematic literature review (SLR) on cyber risk assessment. 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 PRISMA flow diagram were used as useful tools during this screening process. This SLR method helps to get systematic and in-depth way to get the accurate and precise numbers of literature. It would be useful for researchers to have a new way of finding literature apart from the traditional literature review.

Keywords: Systematic literature review, cyber risk assessment, risk management

DOI: https://doi.org/10.21834/ebpj.v7iSI10.4130

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 organisations to gain vast business intelligence (Baharuddin et al., 2016). Organisational agility has also become a necessary capability for organisations to compete and cope with the unprecedented changes in the business environment (Zaini et al., 2020). With this increase in online business transactions, organisations are exposed to various online threats that may harm their business operations. This cyber threat can impact all areas of business operations, whether technically, by 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 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 minimising 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 not be unable to manage these hazards and threats if we did not know it. Assessing is the initial and earliest process of managing risk. At this stage, organisations will get to know the available risk, know its nature, and define its severity whether it is something that is tolerable or not to the organisations. 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 by looking using

eISSN: 2398-4287 © 2022. The Authors. Published for AMER ABRA 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-Behavior Researchers), ABRA (Association of Behavioral Researchers on Asians), and cE-Bs (Centre for Environment-Behavior Studies), Faculty of Architecture, Planning & Surveying, Universiti Teknologi MARA, Malaysia.
DOI: https://doi.org/10.21834/ebpj.v7iSI10.4130

various methods and criteria to determine the level of harm caused (or may cause) and the order of tackling it. There are Standards provided in applying risk management controls in organisations, 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 are lacking of a specific methodology or concept for handling this risk. During the literature review phase, the researcher faces difficulty in retrieving literature that relate to cyber risk assessment. The literature found was mostly non-empirical papers that would not represent the conduct of cyber risk assessment process in-depth. Most searches return conceptual paper which discusses cyber risk in general but not much on the assessment application of it. The guidelines and policies are general breakdowns which are much being extracted from the standards mentioned above. Organisations may apply it differently by looking at their controlling resource or capability to do it. However, it is hard to find how organisations assess cyber risk as it will depend on their policy of risk management or best practices of the organisations. It is best if a specific guideline is given in assessing the cyber risk to be used by organisations in a standard manner. These various ways of assessing risk may impose problems in getting the 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.

To find the specific papers about the conduct of cyber risk assessment and the method used in the assessing process, a systematic literature review (SLR) is needed. The main objective of the SLR is to find literature published in cyber risk assessment and to discover papers that specifically discussed on cyber risk assessment and the matters of conduct involved in assessing cyber risk. Another objective is to find framework and steps of assessing cyber risk in detail from these papers. It would be very useful by discovering various way of assessing cyber risk, standard guideline for cyber risk assessment is potentially to be produced in the future base on the processes discovered. SLR is a logical, linear process where each part is informed by that preceding it. (Purssell & McCrae, 2020). Meanwhile, SLR is define as a review of research literature using systematic and explicit, accountable methods' (Gough et al., 2012). Detailed steps in conducting the SLR will be presented to show the method of getting into literature that relates to cyber risk assessment.

2.0 Methodology

The researcher started to get into the idea by doing a traditional literature review. The initial idea was developed during the traditional literature review, and the gap found was a lack of literature published specifically in cyber risk assessment. Risk assessment is vastly written in many fields. Still, 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. This was further supported by the fact that there was a lack of studies done in cyber risk assessment found during the traditional literature review. Guidelines suggested by Kitchenham (2007) is best to be used in this systematic 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 (*1.1 Introduction to JBI Systematic Reviews - JBI Manual for Evidence Synthesis - JBI Global Wiki*, n.d.). 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 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 is 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. The process is done by identifying the initial keywords to be searched and then looking at these early papers to look for other terms that they have used that might be useful. 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. 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, analysing, and evaluating risk (*Cybersecurity Risk Assessment*, n.d.)
Cyber risk identification	the process of determining what could happen to cause a potential loss, and to gain 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)

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, the search terms are applied to each online database. The initial search results are accepted as the number consider as the initial finding of the review. At this stage, the numbers are big as no screening is done for the results yet. Statistic for the number of searches was 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 make sure the uniformity of the searches and to avoid biases between searching. These results during the first initial searching 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 a 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 on 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

4.3 Data Screening

PRISMA flow diagram of the screening model was used as a guide for filtering. EndNote software was used as a tool to filter the results by removing duplicated data. All the search results from online databases were saved as RIS file extension and imported to EndNote. The imported data were separated according to online databases searched. The initial result number was recorded for reference before the further screening. These results were then grouped to remove the duplicated title.

4.4 Identification

An exact match searching method is used using (" ") to search for the exact match for the phrases in all databases. During this stage, duplicated papers were identified and removed from the list. The table below shows the results of each database during this process.

Table 6: Initial Search Results by Online Databases

	Online Database					
Search term	ACM Digital Library	Emerald Insight	IEEE Explore	Science Direct	Scopus	Web of Science
"Cyber risk assessment"	14	12	4	55	48	49
Cyber risk identification"	1	0	0	2	3	1
Cyber risk analysis"	4	5	14	11	32	9
Cyber risk evaluation"	1	0	1	3	1	1
Total	20	17	19	71	84	60

The results from all the online databases were then compiled together to further manually removed duplicated papers. Out of 269 of the results combined, 53 duplicated papers were found, which brings the total to 216 remaining papers during this identification process.

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.

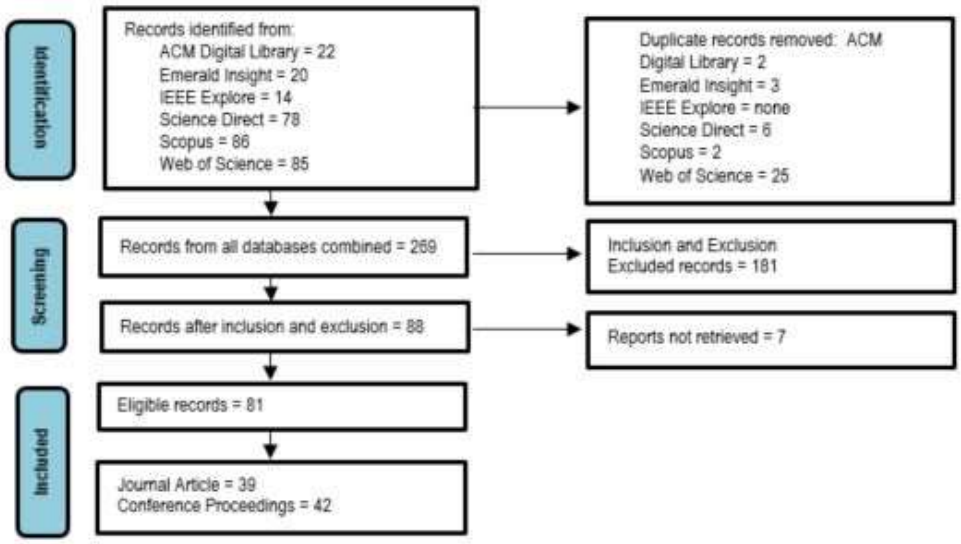

Figure 1: SLR Flow Diagram for Cyber Risk Assessment

Based on the flow diagram above, initial records found from all databases were listed in the identification phase. These are raw records numbers which did yet to be screened and sorted out. The total numbers from each online database were the combination of searches of all the search terms for the systematic review. Each search term of this systematic review which is "cyber risk assessment", "cyber risk identification", cyber risk analysis", and "cyber risk evaluation" was uniformly applied to each of the online databases. These records were then looked for duplication during the later stage of identification. At this stage, EndNote software was used and became a very useful tool in removing duplicated records. It can be seen from the flow diagram there are some changes in the record number, although there was no duplication in IEEE Explore as it shows the same numbers of records.

During the screening stage, all the records are combined as one folder in EndNote. The researcher did a manual duplication removal of the records as it was mentioned that some duplicated records might not be detected in EndNote's *find duplicate* function. This is due to the reference may not being updated for it to detect the same record. At this stage, the inclusion and exclusion criteria were applied together with the filtering criteria. A significant reduction in the number of records was seen after this process was done. Filtering criteria were applied to look for an ineligible record. Records that were not accessible or without an author were filtered out, and the records were further reduced by 7 from the total records. The new total of records is now considered eligible to be accessed. Of the total number of eligible records, 39 were from journal articles and 42 from conference proceedings. This final number of records also shows the final numbers of literature related to cyber risk assessment.

5.0 Quality Assessment

According to David Gough (2012), quality assessment is a tool of scale or other methods to assist with an assessment of the quality and relevance of the study in a review (Gough et al., 2012). This SLR was evaluated using the following criteria based on three quality assessment (QA) questions.

QA1. Are the review's inclusion and exclusion criteria well-described and appropriate?
QA2. Is the literature search likely to have covered all relevant studies on the topic?
QA3. Was the cyber risk assessment mentioned in the publication described adequately?

To address the SLR objective which to find literature published in cyber risk assessment, the quality assessment questions were applied. It was seen that each stage of the SLR has answered all the questions in the quality assessment criteria.

6.0 Conclusion

To sum things up, this article shows the basic steps in conducting a systematic literature review for cyber risk assessment. The steps were elaborate in a very simple way of doing SLR. The findings at the end are aligned with the initial objective of the SLR, which was to find literature published in cyber risk assessment. Although there are few methods and models used in SLR, this research presents the SLR process used by Kitchenham (2007) with some combination with other tools such as PRISMA systematic flow diagram and the use of EndNote software for result filtering. It gives an idea of how cyber risk assessment literature can be accessed, and its accuracy is guaranteed. This method can help to get a very systematic and in-depth way to get the accurate and precise numbers of literature in the form of journal articles and proceedings that have been published in the area related to cyber risk assessment. This would help researchers to explore further the related topics or any other research area to get the most accurate research publication.

Acknowledgements

The authors would like to acknowledge the Faculty of Information Management, Selangor branch and Research Nexus UiTM (ReNeU), Office of Deputy Vice-Chancellor (Research & Innovation) Universiti Teknologi MARA for funding and support.

Paper Contribution to Related Field of Study

This research paper contributes to the field of Library and Information Management

References

1.1 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

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/

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-halt-glitch-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 organisational agility. *Information and Computer Security*, *28*(5), 681–700. https://doi.org/10.1108/ICS-02-2020-0020