RISCS

CYBER RISK QUANTIFICATION RESEARCH PROJECT

A Review of the General Risk Cyber Quantification Landscape

PROJECT TEAM:
Alpesh Bhudia, Anna Cartwright, Edward Cartwright, Frank Cremer, Tom Meurs, Phillip Samson, Jacob Seifert, Darren Shannon, and Barry Sheehan.

VERSION 1.0
31/01/24

OXFORD BROOKES UNIVERSITY
DE MONTFORT UNIVERSITY LEICESTER
UNIVERSITY OF LEICESTER
UNIVERSITY OF LIMERICK OLLSCOIL LUIMNIGH

RISCS

Table of Contents

Executive Summary

Cyber risk quantification provides a means to measure and subsequently communicate and manage the risk to an organisation from a cyber attack or breach. This requires evaluating the likelihood or probability of negative events and the loss that would be incurred as a result of those events. An overall measure of cyber risk to the organisation can then be estimated. Quantification can also be used as a means to evaluate potential interventions in terms of the negative or positive impact on cyber risk. Given that risk can be communicated in terms that are familiar to boards, it may help facilitate improved cyber security risk management.

Cyber risk quantification is, however, challenging to do well. Effective cyber risk quantification requires good, evidenced-based models of cyber risk. This involves evaluating complex threats and events, and about which, given the rapid evolution of cyber tactics, we may have relatively little quality data. Even a good model will inevitably result in significant uncertainty around overall risk. Quantification also requires resources and expertise to inform, conduct, and interpret the risk analysis. This can act as a barrier to effective use of cyber risk quantification. It can also result in organisations adopting 'flashy but ineffective' risk quantification tools that can negatively inform decision-making.

This report provides a comprehensive review of the academic literature on cyber risk quantification. We overview quantification approaches and discuss some of the dimensions on which they differ. We discuss the overall benefits and limitations of cyber risk quantification. We also identify gaps in the literature. Our key findings can be summarised:

1. There are over 200 cyber risk quantification methods, frameworks, standards and guidelines. The most frequently mentioned quantification approaches in the academic literature are (from most mentioned): ISO27005, ISO27001, OCTAVE, NIST SP800-30, CORAS, ISO27002, COBIT, ISO31000, FMEA, FAIR, and ISRAM.

2. There is little evidence on the comparative effectiveness of different methods and frameworks for cyber risk quantification. Moreover, there is no agreed benchmark for comparing methods. Many new methods being advertised in the private sector are not disclosed (for IP reasons) and so are less open to scrutiny.

3. There is no 'one size fits all' best method of cyber risk quantification. The optimal method or framework for a particular organisation will depend on its priorities and needs, reflecting, e.g., its risk profile, in-house expertise, financial resources, and time availability. Organisations need guidance on how to choose a cyber risk quantification approach.

4. Risk quantification methods can be systematically biased towards certain types of assets and risks, e.g. technical information, that are more 'easily' measured. This can neglect less tangible assets such as organisational knowledge.

5. Risk quantification assessment should be viewed as a continuous and routine process. This requires expertise (either in-house or external). New threats (e.g. deep fakes facilitated by AI) can make recent costly cyber security interventions ineffective while opening up new vulnerabilities. The need for constant updating of knowledge can overwhelm organisations.

6. There exist tested and trusted cyber risk quantification frameworks, guidelines, standards, and methods that are 'freely available to use and designed to be relatively accessible. While time and expertise are needed to implement such approaches, it can be beneficial for organisations to develop in-house capabilities rather than solely rely on external providers. This can be facilitated by starting with 'simpler' approaches and building up capability over time.

7. There is a sizable gap in the academic literature on cyber risk quantification around how organisations implement approaches and whether the assumptions underlying the approaches are a good fit with how they are being used. Future work could explore, through surveys and case studies, how organisations are implementing and learning from cyber risk quantification and whether the exercise is effective.

List of Abbreviations

AHP	Analytical Hierarchical Process
ANP	Analytic Network Process
ATA	Attack Tree Analysis
ATT&CK	Adversarial Tactics, Technologies, and Common Knowledge
BN	Bayesian Network
BPNN	BP Neural Network
CIRA	Cyber-Informed Risk Analysis
COBIT	Control Objectives for Information Technology
COBRA	Consultative Objective and Bi-Functional Risk Analysis
CORA	Compliance Risk Assessment
CORAS	Consultative Objective Risk Analysis System
CPTs	Conditional Probability Tables
CRAMM	CCTA Risk Analysis and Management Method
CRDF	Cloud Risk Decision Framework
CSF	Cybersecurity Framework
CVE	Common Vulnerabilities and Exposures
CVSS	Common Vulnerability Scoring System
CWE	Common Weaknesses Enumerations
DAG	Directed Acyclic Graphs
DDoS	Distributed Denial of Service
DEMATEL	Decision-Making Trial and Evaluation Laboratory
DREAD	Damage, Reproducibility, Exploitability, Affected users, and Discoverability
EBIOS	Expression of Needs and Identification of Security Objectives
ENISA	European Union Agency for Cybersecurity
ETA	Event Tree Analysis
FAHP	Fuzzy Analytic Hierarchy Process
FAIR	Factor Analysis of Information Risk

FMEA	Failure Mode and Effect Analysis
FMECA	Failure Mode, Effects, and Criticality Analysis
FRAP	Facilitated Risk Analysis Process
FTA	Fault Tree Analysis
HAZOP	Hazard and Operability Analysis
IS	IS Risk Analysis Method
ISO	International Organization for Standardization
ISRA	Information Security Risk Assessment
ISRAM	Information Security Risk Analysis Method
ITIL	Information Technology Infrastructure Library framework
MAGERIT	Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información
MCDM	Multi-Criteria Decision-Making
Mehari	Method for Harmonized Analysis of Risk
NIST	National Institute of Standards and Technology
NSM ROS	Norwegian National Security Authority Guidelines in Risk and Vulnerability Assessments
NVD	National Vulnerability Database
OCTAVE	Operationally Critical Threat, Asset and Vulnerability Evaluation
OVAL	Open Vulnerability and Assessment Language
PCI DSS	Payment Card Industry Data Security Standard
PRA	Probabilistic Risk Analysis
PRISMA	Preferred Reporting Items for Systematic Reviews and Meta-Analyses
RAIS	Risk Assessment Information System
STRIDE	Spoofing of user identity, Tampering, Repudiation, Information disclosure, Denial of service, and Elevation of privilege
TARA	Threat Agent Risk Assessment
TOPSIS	Technique for Order of Preference by Similarity to Ideal Solution
VIKOR	Multi-criteria Optimization and Compromise Solution

Introduction

Cyber risk quantification can be seen as a subset of the broader notion of information security risk assessment (ISRA). It enables organisations to identify security risks, outline risk scenarios, and identify the consequences and associated costs of such scenarios, as well as their frequency or likelihood and possible interventions. In general, there are three distinct phases: context establishment, risk identification and risk analysis (Shamala et al. 2013). Risk identification involves identifying assets, threats, existing controls, vulnerabilities and consequences (ISO/IEC 27005:2018). Risk analysis involves the assessment of consequences, the assessment of incident likelihood, and the determination of the resultant risk level (ISO/IEC 27005:2018). As we will discuss in more detail below, risk analysis can use a variety of different methods and approaches.

Cyber risk quantification, through risk identification and analysis, can inform risk evaluation and organisational strategy. For instance, the organisation can assess the priority of different risks and/or evaluate potential cybersecurity investments and interventions (Orlando 2021). While, in principle, cyber risk quantification can yield many benefits, there are also potential limitations and disadvantages. At the most basic level, a risk assessment can only be effective if there is accurate information to inform the assessment, the assessment methods make appropriate assumptions, and there is sufficient awareness to interpret findings (Böhme and Nowey 2008). There are many competing cyber risk quantification methods and frameworks and the effectiveness of these different methods is untested. The European Union Agency for Cyber Security (ENISA) recently criticised the lack of standard procedures for identifying, mitigating, and quantifying cyber risks (ENISA 2023a).

As part of a RISCS Cyber Risk Quantification Research Project, we were commissioned to produce a review of the general cyber risk quantification landscape. This includes an overview of quantification methodologies and their validity in addressing cyber risk challenges, including: risk analysis and prioritisation, risk communication, and cost-benefit analysis of security controls; the use cases and arguments for and against cyber risk quantification; the benefits and limits of cyber risk quantification; pre-requisites necessary for effective implementation of cyber risk quantification; gaps in the existing cyber risk quantification research literature.

In the report, we first provide some background information on cyber risk quantification, including a discussion of the dimensions on which quantification approaches can differ. We then discuss the methodology and findings from a systematic review of the literature we undertook for this project. This review is the most comprehensive cyber risk quantification study in the literature. Beginning with 1,900 relevant studies in the cybersecurity domain, 713 academic papers were forensically analysed and categorised according to the chosen scientific criteria. The analysis identifies 81 state-of-the-art risk assessment methodologies and 137 standards/frameworks/guidelines and provides a commentary on trends, best practices, and industry/sectoral applications. This study uses the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) method (Page et al. 2021) to obtain transparent and replicable systematic review results. We finish with a discussion of the arguments for and against cyber risk quantification.

Background on Cyber Quantification Methods

In this section, we provide a brief introduction to cyber risk quantification and the terminology we will use throughout the report. As we have already said there are many different cyber risk quantification methods, standards, frameworks and guidelines. Indeed, we identified well over 100 that are discussed within the academic literature. Alongside that are a growing number of tools and 'solutions' offered by the private sector, which are less accessible to academic study and remain something of a black box in terms of their precise methods.

To help clarify terminology, in Table 1, we delineate the realm of methods, standards, frameworks, and guidelines. The classification of these diverse approaches proves challenging, given that specific methodologies (e.g. OCTAVE) can be subdivided into multiple categories, leading to varied terminology across the academic literature. Moreover, a cyber risk quantification will optimally combine multiple elements. For instance, if a framework provides a structure, and guidelines provide guidance on how to implement the structure, then it is natural to combine framework and guideline. The delineation in Table 1 summarises the approach that we will use.

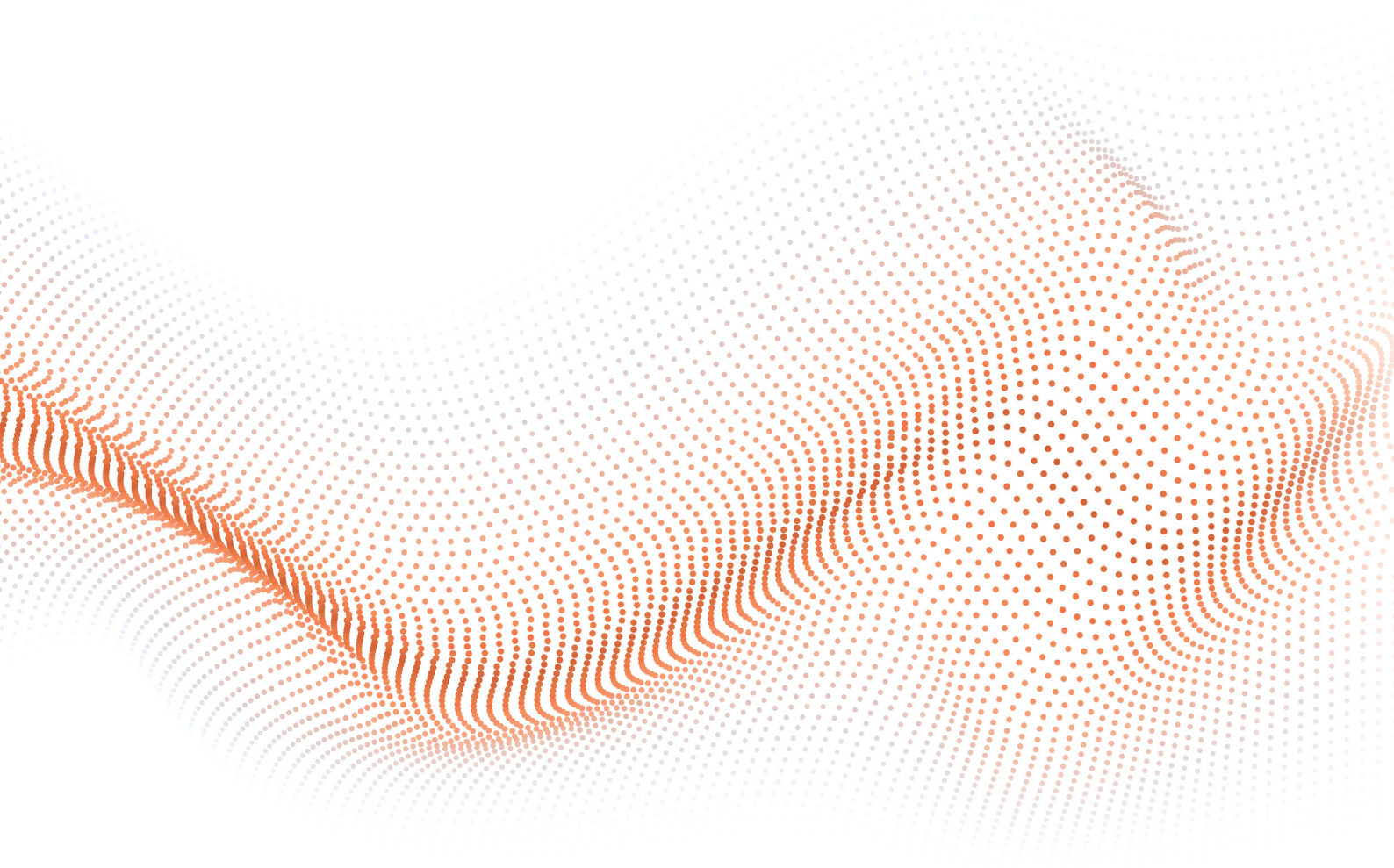


Table 1: Definition of terms that we will use in this report

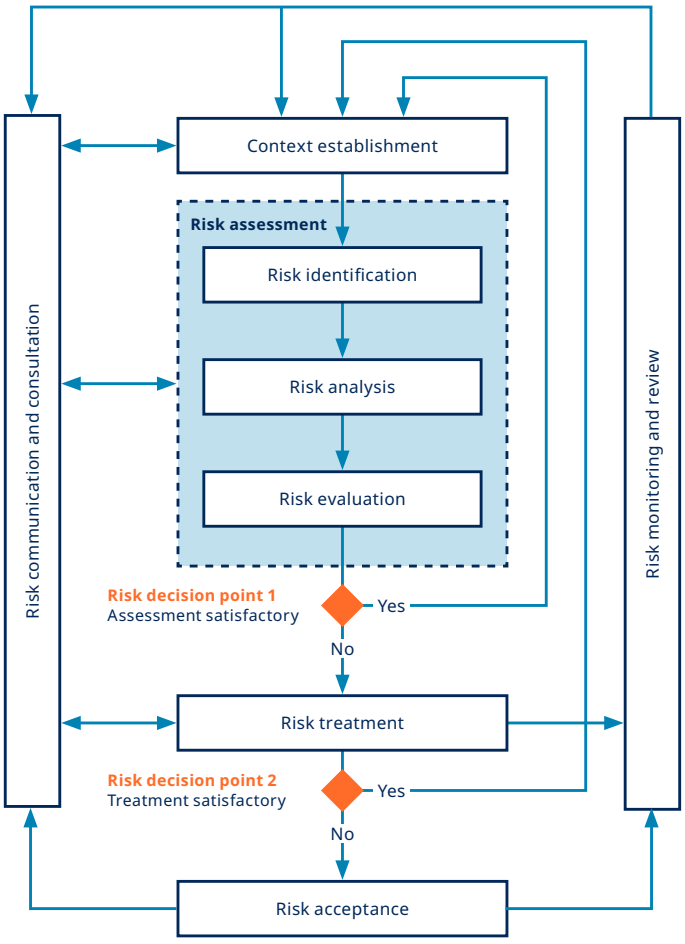
Term	Definition
Framework	A foundational structure that provides concepts, principles, and best practices. Its role is to assist organisations in establishing a starting point for risk assessment, forming a basis for further development. Moreover, a risk assessment framework can function as a tool facilitating effective risk communication with stakeholders. Notable examples of frameworks include NIST CSF, OCTAVE, COBIT, the ISO 3100 Family, and FAIR. For example the documentation around the NIST CSF says 'The Framework is based on existing standards, guidelines, and practices for organisations to better manage and reduce cybersecurity risk. In addition, it was designed to foster risk and cybersecurity management communications amongst both internal and external organisational stakeholders.' (NIST 2024a)
Guideline	An instructional or recommendatory document designed to guide users. It suggests steps to aid in the risk assessment process. Frequently referenced guidelines encompass NIST SP 800-30 and the ISO 3100 family. For instance, the documentation around ISO 31000 says 'ISO 31000 is an international standard that provides principles and guidelines for risk management. It outlines a comprehensive approach to identifying, analysing, evaluating, treating, monitoring and communicating risks across an organisation.' (ISO 2018)
Standard	Denotes a universally agreed-upon risk assessment procedure adopted by an organisation or community. Standardised requirements or criteria enable users to compare their risk assessment results with those of other organisations. Prominent examples in this category encompass the ISO 27005 and ISO 27001 standards, along with NIST SP 800-30. For certain standards, like ISO 27005, there are certifications, which may influence the business case for adopting the standard. As one example of a standard, the documentation around ISO 27005 says it 'provides guidance to assist organisations to: (a) fulfil the requirements of ISO/IEC 27001 concerning actions to address information security risks; (b) perform information security risk management activities, specifically information security risk assessment and treatment.' (ISO 2022)
Methods	A systematic, often mathematical, approach to assessing information security risks. This can encompass specific methodologies, examples include OCTAVE, MAGERIT, or Mehari, or the mathematical methods that are applied, examples including Fuzzy Theory, Bayesian Networks (BN), or Analytical Hierarchical Processes (AHP). For instance, the documentation around OCTAVE says 'It defines a comprehensive evaluation method that allows an organisation to identify the information assets that are important to the mission of the organisation, the threats to those assets, and the vulnerabilities that may expose those assets to the threats. By putting together the information assets, threats, and vulnerabilities, the organisation can begin to understand what information is at risk.' (Alberts et al., 1999).
Tool	Can be a generic term for any cyber risk quantification method or framework. Often, though, means a specific process that can be used to conduct risk assessment. This can be, for example, documents to work through (e.g. PRAM) or a computer led process (e.g. MetricStream). For instance, the documentation for NIST Privacy Risk Assessment Methodology (PRAM) states 'The PRAM is a tool that applies the risk model from NISTIR 8062 and helps organisations analyse, assess, and prioritise privacy risks to determine how to respond and select appropriate solutions. The PRAM can help drive collaboration and communication between various components of an organisation, including privacy, cybersecurity, business, and IT personnel.' (NIST 2024b)
Approach	We use cyber risk quantification approach as shorthand for cyber risk quantification framework, guideline, standard and/or method.

DIMENSIONS ALONG WHICH CYBER RISK QUANTIFICATION APPROACHES DIFFER

Given the very large number of frameworks, standards, guidelines, and methods for cyber risk quantification, we do not attempt to provide a summary of each approach here. For a more detailed comparison across some quantification approaches see Chen (2015), Wangen et al. (2018), Dixit et al. (2022), Sanchez-Garcia (2023) and ENISA (2024). Instead, by way of introduction to the literature on cyber risk quantification, we identify and give examples of the many dimensions on which cyber risk quantification approaches can differ.

In comparing across approaches, it is useful to consider a standard, such as ISO 27005, reproduced in Figure 1. This identifies the different components that go into a risk management process, including context establishment, risk identification and risk analysis (Sanchez-Garcia et al., 2022). Cyber risk quantification approaches can differ across any or all of these components, from the information needed as inputs into the process, the methods to identify, estimate, and evaluate risk, and the way output is presented with subsequent impact on communication and decision making.

Figure 1: The ISO/IEC 27005:2011 ISRM process (ISO, 2011)



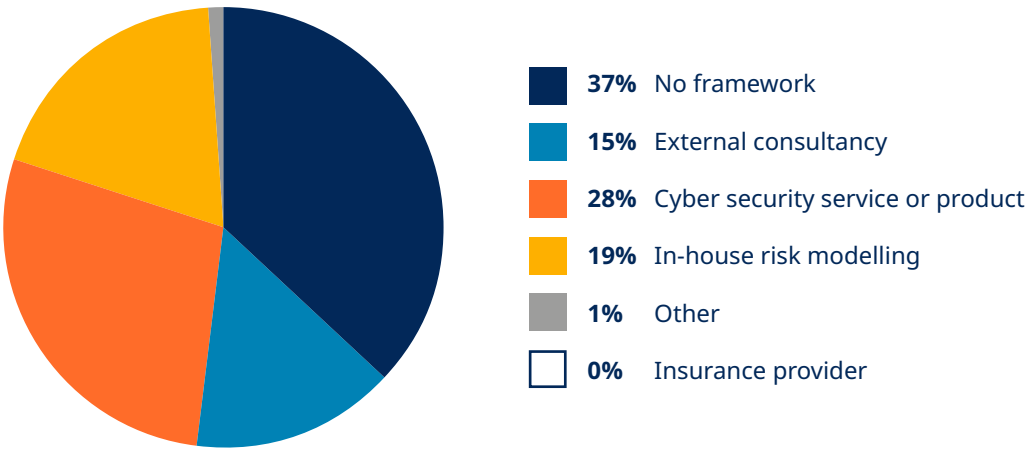
Drawing on the approach of Vorster and Labuschagne (2005), we distinguish and outline five important dimensions along which different cyber risk quantification approaches can differ:

a Self-directed (in-house) or provided as a service (external expertise). Some approaches are designed to be implemented by the organisation itself based on the framework, standards, guidelines, methods and/or tools provided. For instance, OCTAVE is a self-directed approach that is led by people within the organisation. This puts the organisation fully in control of the risk quantification but requires internal resources, namely time and expertise. Some approaches are designed to be implemented by an external service provider. There can be several variations on this theme, including:

- **i** An external risk assessment using a 'freely available' approach, such as OCTAVE. In this case, the organisation could have performed the risk assessment in-house but acquired the expertise to run the assessment.
- **ii** An external assessment using the provider's own tools and methods (which is typically company IP). In this case, the organisation is buying expertise and access to a different tool and/or method.
- **iii** The organisation effectively buys software/services that run a risk assessment process. This will still require internal expertise to input into the process and evaluate its outputs. The organisation is buying access to the software/service.

By way of context, we briefly comment on the results of a survey members of the project team conducted in 2023, which included questions on cyber risk quantification. A total of 205 medium and large businesses in the UK were surveyed. In Figure 2, we summarise the businesses' approach to cyber risk quantification. Here, we can see the split between in-house, external consultancy, or a service/product. You can see that all three options are commonly used.

Figure 2: Survey responses when a sample of medium and large businesses in the UK were asked, 'Which of the following best describes the framework you use to quantify cyber risk in your organisation?'



b Asset or scenario-based risk assessment. Some approaches are best suited to a risk assessment of individual assets. Specifically, approaches such as OCTAVE produce a threat profile for each asset. Other approaches are best adapted to assessment of overall risk. Specifically, approaches such as ISRAM identify how a threat scenario could impact across multiple assets within the organisation. The desirability of these different approaches will depend on the priorities of the organisation. For instance, whether the organisation wants to focus on the risk of specific assets or wants to focus on the risk from specific threats.

c The amount of information needed in preparation for the risk quantification. Approaches can differ on how much information is required prior to the risk analysis being performed. If the organisation want to perform a quick risk analysis, it would be better to adopt an approach that requires relatively less preparation and less information. By contrast, if accuracy is important, then it would be better to adopt an approach that requires more preparation and information. For instance, OCTAVE requires extensive preparation and so is not ideal for 'quick' results, while CORAS requires less preparation but is not ideal for 'accurate' results (Vorster & Labuschagne 2005).

d The complexity of the risk assessment and output. Some approaches are relatively simple to implement and subsequently interpret. For instance, OCTAVE and CORAS use no mathematical calculations and can be seen as relatively simple and transparent (even if they require considerable preparation and work). Often, these approaches use qualitative methods. Other approaches are more mathematical and, consequently, harder to interpret and less transparent. This is particularly the case for methods relying on complex methods such as Bayesian Networks and other AI approaches. While complexity can add accuracy, this needs to be balanced against the lack of transparency in how risk measures are calculated.

e The type of output produced, e.g. relative versus absolute risk and inter-operability. Some methods produce merely a ranking of risks, while some produce absolute measures of risk. For instance, OCTAVE, CORAS and ISRAM use qualitative methods and so are primarily about ranking risk and using low to high rankings. While such rankings may be seen as non-quantitative, they can still be an informative, approachable and transparent way to prioritise risk reduction. By contrast, methods such as IS Risk Analysis produce absolute methods of risk that allow statements such as one outcome having twice the negative impact of another. Such approaches allow more detailed prioritisation of risk. A related dimension on which to judge quantification approaches is how readily results can be compared. Comparison between results is important to check the robustness of different approaches. Indeed, an organisation may want to implement multiple methods. ENISA (2024) explores the interoperability of risk management frameworks; for instance, OCTAVE is seen as highly interoperable while MAGERIT and MEHARI are less so.

We highlight that this list of five dimensions is not exhaustive. For instance, approaches also differ in terms of the organisation who developed the approach: government, business sector, academic sector or voluntary sector. This can influence the transparency and cost of the approach.

It should be apparent, looking through the five dimensions (a-e) of variation, that there is no optimal one-size-fits-all approach to cyber risk quantification. Instead, there are a series of trade-offs in terms of cost and benefit. For instance, a simpler, quicker, and more transparent approach may work for one organization, while another prefers a more involved, complex and accurate risk assessment. These trade-offs are reflected in marketing. For example, 'OCTAVE Allegro is a methodology to streamline and optimise the process of assessing information security risks so that an organisation can obtain sufficient results with a small investment in time, people, and other limited resources'. We discuss the cost-benefit trade-offs of cyber risk quantification further in Section 5.

PRIOR ACADEMIC REVIEWS OF CYBER RISK QUANTIFICATION

Given the many different approaches to cyber risk quantification, the inherent complexity of the quantification exercise, and the trade-offs organisations face in choosing how to implement cyber risk quantification; academic research is essential to help us understand the process in more detail. Before providing our review of the literature, we briefly comment on existing reviews.

Companies, organisations, and government institutions face the challenge of identifying the most suitable cyber security risk assessment approach tailored to their specific requirements. As a result, numerous scientific studies have been published over the years to aid users in navigating this complex task. In the realm of scientific literature, one prevalent approach involves the comparison of diverse cyber risk assessment methodologies. Well-established methods such as OCTAVE, CORAS, ISRAM, CORA, IS, NIST SP 800-30, or ISO/IEC 27005 are frequently scrutinised based on specific criteria, thereby shedding light on the strengths and weaknesses of each approach. Noteworthy contributions to this comparative analysis include the works of Vorster and Labuschagne (2005), Derakhshandeh and Mikaeilvand (2011), Kiran et al. (2013), Shamala et al. (2013), Sayouti et al. (2014), Wangen et al. (2017), Alhajri et al. (2019), and Dixit et al. (2022). In addition to the comparative studies, there exist investigations within the realm of cyber risk assessment that focus on scrutinising specific assessment methods. Examples include examining Bayesian Networks (BN) and Multi-Criteria Decision-Making (MCDM).

Existing reviews have also identified the limitations of existing approaches and the lack of work comparing across approaches. Chockalingam et al. (2017) conducted a literature search in various databases to identify Bayesian Network (BN) models related to cyber or information security. After applying specific criteria, they identified 17 BN models and analysed them further regarding data sources, number of nodes, type of threat actor, the scope of variables, and purpose. They found that various combinations used expert knowledge and empirical data for Directed Acyclic Graphs (DAG) and conditional probability tables (CPTs). However, the specificity of threat actors was often lacking, and none of the models considered insider and outsider threats. The identified BNs fell into two categories: diagnostic and predictive models, with the majority being predictive. Similarly, Maček et al. (2020) conducted a systematic literature review on Information Security Risk Management and Multi-Criteria Decision-Making (MCDM). They extensively analysed MCDM methods, including AHP, FAHP, ANP, TOPSIS, and Delphi. The outcome indicated that no single method alone provides a compelling rationale for conducting a comprehensive assessment of IT security measures.

In anticipation of the systematic literature analysis on cyber security quantification, a thorough examination of the broader field of cyber security research was undertaken. Employing a meta-analytical approach, systematic literature analyses were scrutinised systematically using the PRISMA methodology. The purpose of this investigation was to enhance our understanding of the research landscape and to leverage the obtained insights to support subsequent analyses, such as refining search terms or identifying relevant databases. Apart from reaffirming the efficacy of the PRISMA method for conducting comprehensive literature analyses, a diverse array of reviews on various facets of cyber security were uncovered. A total of 206 studies were identified, encompassing the aforementioned work by Chockalingam et al. (2017). Other studies delved into cyber security within specific domains, including the automotive industry (Fernandez de Arroyabe et al. 2022), healthcare (Kruse et al. 2017), energy supply (Leszczyna 2018), and the banking sector (Vasquez Ubaldo et al. 2023), among others.

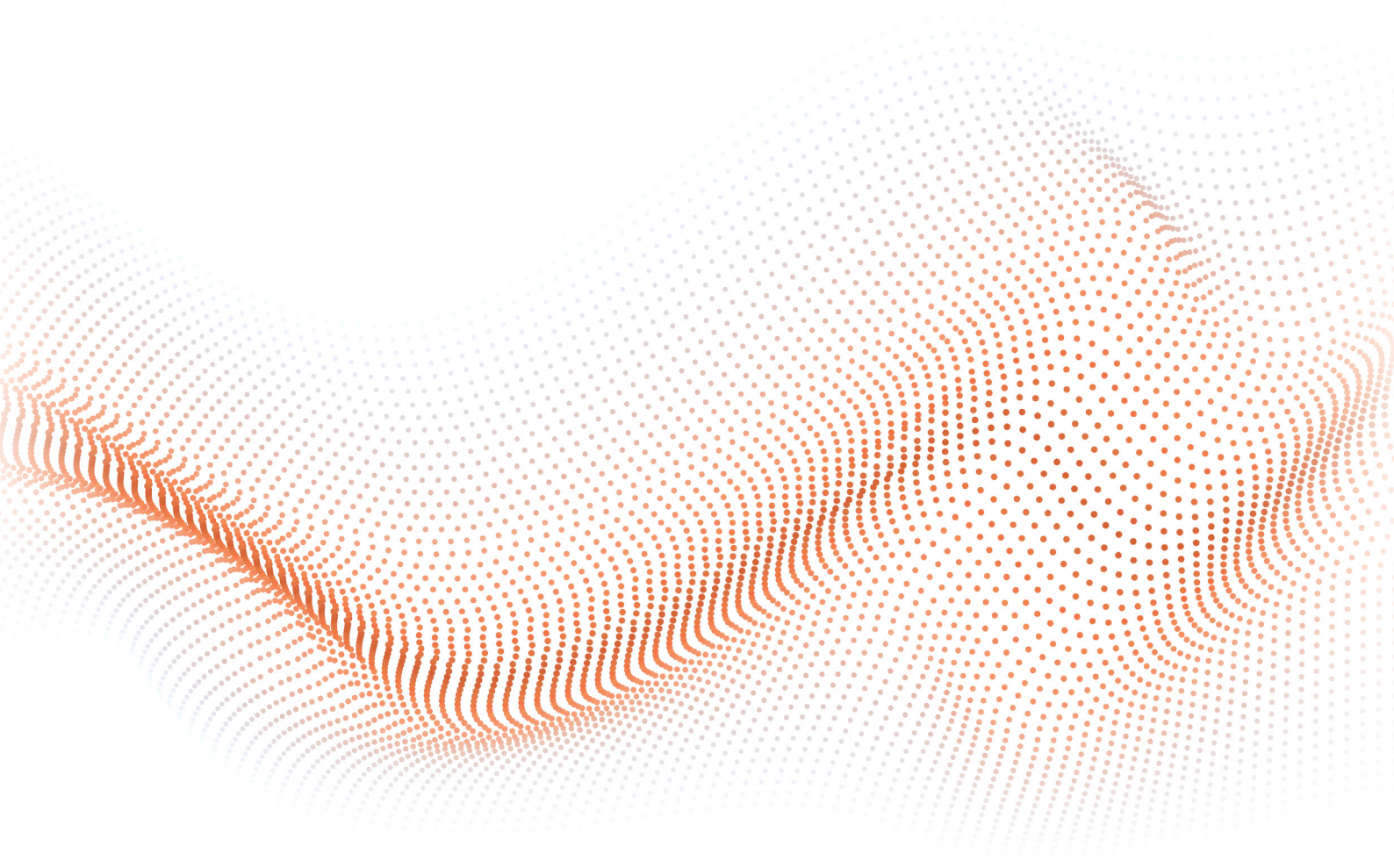
Two studies closely align with the focus of our investigation. In their exhaustive systematic literature review, Pan and Tomlinson (2016) delved into the methods employed for assessing information security risks. Out of the initial 107 research papers identified, 80 met the final relevance criteria. A significant finding of this study was the dearth of information on the collection of data required for risk assessment. However, the study suggests that Fuzzy Theory holds promise for enhancing the accuracy of calculations. Extending Pan and Tomlinson's investigation, Devi et al. (2022) focused on the period from 2016 to 2021. The initial search produced 1,641 potential results, a number refined to 593 papers through the application of specific criteria. From this subset, 25 studies were pinpointed as pertinent to the study's objectives. The authors conclude that no framework can be described as the best, as each must be adapted to the unique needs of the organisation.

Compared to the two studies above, our investigation employed a broader set of search terms and encompassed an extended time frame. Furthermore, the inclusion criteria were expanded to incorporate studies accessible to the University of Limerick, even requiring a fee. Consequently, the literature review conducted yielded an extensive pool of 1,900 studies, from which 713 were ultimately deemed relevant. This culminated in developing the most comprehensive systematic literature review within the realm of information security assessment to date, identifying 218 distinct approaches.

Methodology for Systematic Review of Cyber Risk Quantification Literature

This systematic review follows the structure of the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) framework proposed by Page et al. (2021). Figure 3 illustrates the complete analysis process.

Two fundamental questions must be answered to conduct a systematic literature review: i) which combinations of search terms should be used, and ii) which databases should be used? Systematic literature analyses already carried out in the cyber security context were examined using the PRISMA approach to identify best practices and literature gaps. For this purpose, the search terms “cyber security” OR “cybersecurity” OR “cyber assessment” OR “information security” OR “cyber risk”, AND “systematic review” were used in the respective combinations. Google Scholar was chosen as the database for the first search, as it generated the most results. A total of 234 literature reviews were identified, of which 206 remained after removal of duplicates. The overviews were then examined in terms of the search terms and databases used. The results mentioned most frequently in this context formed the basis for the next phase of this literature analysis.



A two-part search chain is employed, exploring all possible combinations between the search terms from the first part and those from the second part within the respective databases. The first part of the search chain was based on an analysis of reviews and resulted in the following terms: “Cyber Security,” “Cybersecurity,” “Information Security,” “Computer Security,” and “Data Security.” The last part of the search chain included the terms “vulnerability”, “threat assessment”, and “quantification”. Following Amin et al. (2022), the terms “Risk Assessment,” “Risk Identification,” “Risk Analysis,” and “Risk Evaluation” were also added to the latter part of the search chain.

Amin et al. (2022) introduced a methodology for performing a systematic literature review focused on cyber risk assessment. Following their approach, the authors recommended employing specific search terms such as “cyber risk” AND “assessment” OR “identification” OR “analysis” OR “evaluation.” They also advocated utilising online databases, including ACM Digital, Emerald Insight, IEEE Explore, Science Direct, Scopus, and Web of Science, alongside defined inclusion and exclusion criteria. In this study, we incorporate key elements from the methodology outlined in their paper.

This resulted in the following search chain:

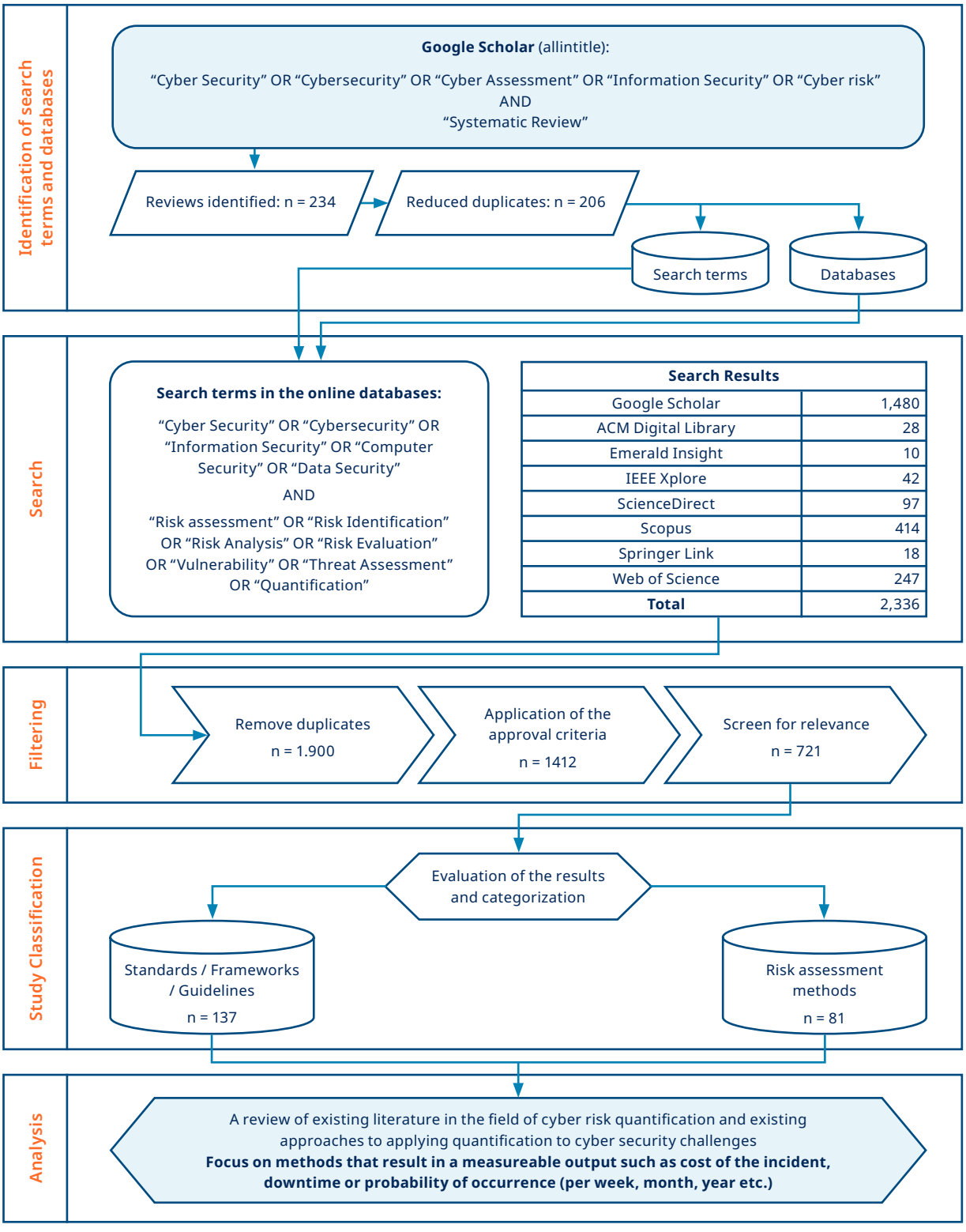
“Cyber Security” OR “Cyber-Security” OR “Cybersecurity” OR “Information Security” OR “Computer Security” OR “Data Security”

AND

“Risk Assessment” OR “Risk Identification” OR “Risk Analysis” OR “Risk Evaluation” OR “Vulnerability” OR “Threat Assessment” OR “Quantification”

In terms of databases, the following were identified as the most frequently mentioned: Google Scholar, ACM Digital Library, Emerald Insight, IEEE Xplore, ScienceDirect, Scopus, Springer Link, and Web of Science.

Figure 3: PRISMA systematic literature analysis methodology



PROCESS AND ELIGIBILITY CRITERIA

The inclusion and exclusion criteria selection leverages the work of Cremer et al. (2022) and Aziz (2020), as these reviews focus on cyber risk and cyber security and are, therefore, thematically consistent with our study. The search was conducted between 7 September 2023 and 13 September 2023.

Considering the continued development of cyber risks and new assessment methods, similar reviews were limited to an observation period of approximately 5-10 years. By contrast, we make no restrictions in this study, allowing us to examine the historical development of risk assessment approaches. Furthermore, only studies written in English and published in journals were considered. Regarding content, the studies were deemed eligible only if they addressed at least one standard, guideline, framework, or mathematical method to assess information security risks. A detailed summary of the above and other filtering criteria is described in Table 2.

Table 2: Inclusion and Exclusion Summary

CRITERIA SUMMARY	
Inclusion	**Exclusion**

• **The study was published in English.**
• **The study addressed at least one of the following areas in connection with information security:**
  • Method
  • Framework
  • Guideline
  • Standard
  • Method for risk assessment
• **The study was accessible in one of the following databases:**
  • ACM Digital Library
  • Emerald Insight
  • Google Scholar
  • IEEE Xplore
  • ScienceDirect
  • Scopus
  • Springer Link
  • Web of Science
	• **The search result was a bachelor / master thesis, white paper, magazine, newsletter, short article, or presentation.**
	• **Duplicates were removed.**

DATABASES

The following databases were scanned to ensure comprehensive and relevant results in the systematic literature search: ACM Digital Library, IEEE Xplore, ScienceDirect, Scopus, Springer Link, and Web of Science. ACM Digital Library is a platform for research, discovery, and networking, offering a full-text collection of ACM publications, curated publications from select publishers, a bibliographic database on computing, and connections among authors, works, institutions, and specialised communities (ACM Digital Library 2023). IEEE is the world's largest technical professional organisation focused on promoting technology for the betterment of humanity. IEEE Xplore's digital library has over 5 million documents and receives around 15 million monthly downloads (IEEE Xplore 2023). Scopus contains more than 27,100 peer-reviewed journals, with approximately 27% from the field of physical sciences (Scopus 2023). SpringerLink is one of the world's leading online information services for scientific, technical, and medical books and journals and currently contains 3825 journals (SpringerLink 2023). The Web of Science database is an extensive and comprehensive collection of academic resources that includes more than 9,500 journals in 182 categories (Web of Science 2023). Google Scholar is a search engine developed by Google that specialises in searching for scholarly literature, such as peer-reviewed articles, theses, books, and conference papers (Google Scholar 2023).

SEARCH STRATEGY

The previously determined search terms were entered into the respective databases to carry out the search. Appropriate search parameters were used to ensure that each search term had to be included in the result. Where possible, the search parameters were set to "language = English", "document type = article" and "search in title only". A total of 2,336 articles were identified:

Table 3: Number of articles identified by database

Google Scholar	1,480	**ScienceDirect**	97
ACM Digital Library	28	**Scopus**	414
Emerald Insight	10	**Springer Link**	18
IEEE Xplore	42	**Web of Science**	247

As Google Scholar partially referred to the other databases, there was a high number of duplicates, which were cleaned up in the next step. This reduced the number of studies found to 1,900. After applying the acceptance criteria, the number was reduced to 1,412.

SELECTION PROCESS

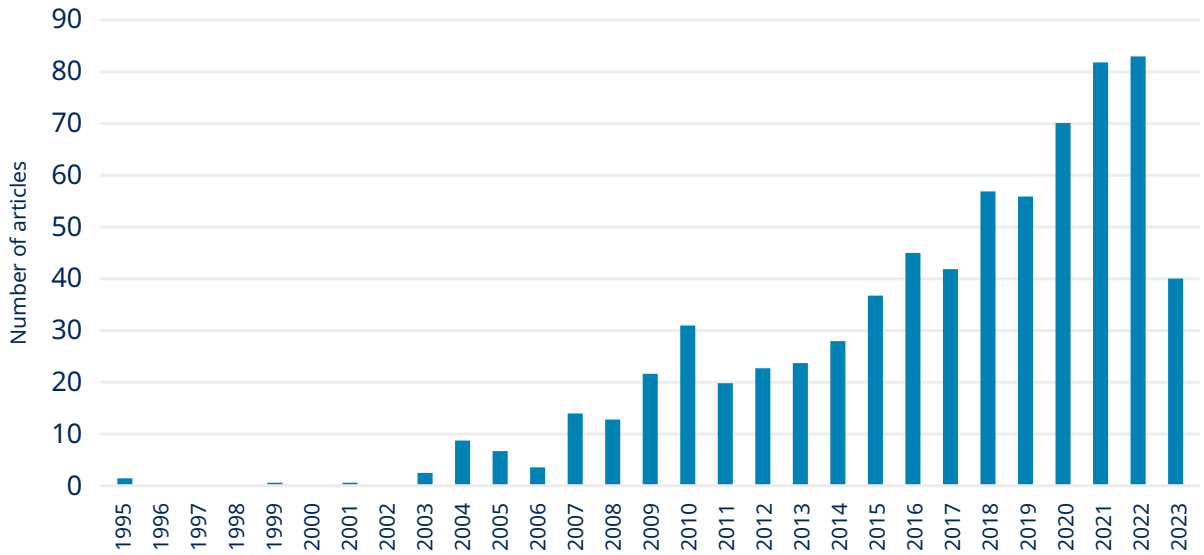
The 1,412 studies identified earlier underwent screening and verification for relevance. A study was deemed pertinent if it encompassed at least one method, guideline, standard, or approach related to information security assessment. Studies lacking these attributes or those inaccessible were excluded. Of the identified 1,412 studies, 713 aligned with the defined selection criteria.

Findings of the Systematic Review of Cyber Risk Quantification Literature

In this section, the findings of the systematic literature review are presented. During the screening process, all frameworks, guidelines, standards, risk assessment methods mentioned, and the field of application of the respective study were recorded for subsequent evaluation. A total of 218 approaches dealing with the topic of information risk assessment were found, whereby only those mentioned more than once were counted.

For a better overview, two categories were formed, with 81 approaches assigned to the "Risk Assessment Methods" category and the remaining 137 to the "Standards, Frameworks and Guidelines" category. Risk Assessment Methods are mathematical approaches used to calculate potential information security risks, such as Fuzzy Theory, Bayesian Networks (BN), or Analytical Hierarchical Processes (AHP). On the other hand, the "Standards, Frameworks, and Guidelines" category involves approaches that take a more comprehensive view of risk, such as the identification, calculation, management, communication, and monitoring of risks provided by the ISO 27005 standard.

Figure 4: Articles per year



The research on information security spans nearly three decades. For example, RAMeX, a prototype designed for analysing computer security risks in small and medium-sized enterprises, was introduced in 1995. From 2004 onward, there has been a consistent annual rise in publications, a trend that persists. (The 2023 number will be an underestimate because it takes time for articles to be indexed and the search was conducted in late 2023.) Figure 4 shows the number of scientific articles per year found in this search.

Table 4 provides an overview of the sectors examined in the identified studies. The industry, information technology, and energy sectors stand out prominently in this overview. This prominence may be attributed to the susceptibility of companies in these sectors to extensive repercussions from cyberattacks, such as production downtime or data loss.

Table 4: Frequency of articles by sector

Sector	Frequency
Industrials	288
Information Technology	130
Energy	105
Health Care	36
Consumer Discretionary	20
Financials	13
Real Estate	1
Consumer Staples	1

STANDARDS / FRAMEWORKS / GUIDELINES

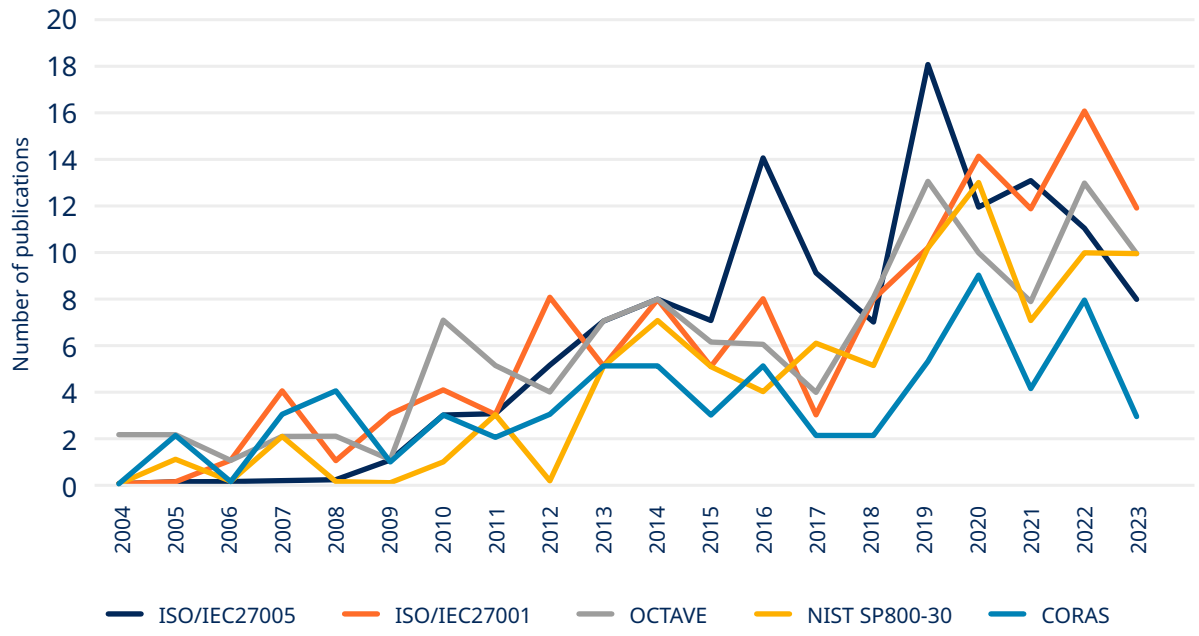
One of the objectives of this study was to identify the state-of-the-art information risk assessment approaches. However, establishing a definitive ranking proved challenging due to the diverse nature of these approaches in terms of their application areas and complexity. To address this, during the analysis of the 713 previously identified articles, we tallied the frequency of each approach being mentioned. It is important to note that an approach, even if highlighted as a category representative, may not have been the focus of an article. The count provided insights into which approaches garnered attention in the scientific community in recent years, indicating popularity and general mentions. The resulting list, comprising 865 entries, represents the most comprehensive overview of information security risk assessment approaches. For clarity, this article enumerates only those approaches mentioned in at least ten different articles. These are summarised in Table 5.

Table 5: Frequency with which Standards, Frameworks, and Guidelines are mentioned in the literature. Price at time of writing

#	Abbreviation	Name (long)	Price (approx.)	Freq.
1	ISO/IEC 27005	Information security, cybersecurity, and privacy protection - Guidance on managing information security risks	£177	126
2	ISO/IEC 27001	Information security, cybersecurity, and privacy protection - Information security management systems	£118	125
3	OCTAVE	Operationally Critical Threat, Asset, and Vulnerability Evaluation	Free	119
4	NIST SP 800-30	Guide for Conducting Risk Assessments	Free	89
5	CORAS	Consultative Objective Risk Analysis System	Free	69
6	ISO/IEC 27002	Information security, cybersecurity, and privacy protection - Information security controls	£197	50
7	COBIT	Control Objectives for Information Technology	Unknown	48
8	ISO 31000	Risk management - Guidelines	£88	46
9	FMEA	Failure mode and effect analysis	Free	43
10	FAIR	Factor Analysis of Information Risk	Unknown	32
11	ISRAM	Information Security Risk Analysis Method	Free	30
12	GB/T 20984-2022	National standard of the People's Republic of China - Information security technology - Risk assessment method for information security	Unknown	28
13	MAGERIT	Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información	Unknown	24
14	Mehari	Method for Harmonized Analysis of Risk	Free	24
15	NIST SP 800-53	Security and Privacy Controls for Information Systems and Organizations	Unknown	23
16	OCTAVE Allegro	Operationally Critical Threat, Asset, and Vulnerability Evaluation	Free	22
17	IEC 62443	Industrial Communication Networks – Networks and System Security	Unknown	22
18	MITRE ATT&CK	Adversarial Tactics, Technologies, and Common Knowledge	Unknown	20
19	ISO/IEC 15408	Information security, cybersecurity, and privacy protection — Evaluation criteria for IT security	Up to £817*	18
20	TARA	Threat Agent Risk Assessment	Unknown	17
21	PCI DSS	Payment Card Industry Data Security Standard	Unknown	13
22	ISO/SAE 21434	Road vehicles — Cybersecurity engineering	£197	13
23	IEC 61850	Communication networks and systems for power utility automation	Unknown	13
24	NIST SP 800-39	Managing Information Security Risk - Organization, Mission, and Information System View	Free	12
25	NIST SP 800-37	Risk Management Framework for Information Systems and Organizations - A System Life Cycle Approach for Security and Privacy	Unknown	11
26	ITIL	Information Technology Infrastructure Library framework	TBD	10
27	ISO 26262	Road vehicles - Functional safety	Up to £1,584	10

In Figure 5, we plot the frequency with which the top 5 standards, frameworks and guidelines are mentioned since 2004. You can see that there is a general rise in frequency across all five methods with no one standard, framework or guideline dominating in the academic literature.

Figure 5: Frequency with which top 5 standards, frameworks and guidelines are mentioned over time



RISK ASSESSMENT METHOD

This section presents the findings from analysing 713 articles categorised under risk assessment methods. As indicated in the preceding paragraph, terms like risk assessment method, framework, etc., are frequently employed interchangeably in various articles. Within the scope of this study, the term "risk assessment method" refers to an approach primarily associated with evaluating information security risks, typically employing a mathematical methodology. This study's most frequently referenced approaches include Fuzzy Theory, CVSS, AHP, BN, and FTA. In Table 6, we provide a brief overview of some of the key cyber risk quantification methods.

Table 6: Summary description of some cyber risk quantification methods

Method	Description
Fuzzy Theory	Fuzzy theory, also known as fuzzy logic, originates from pattern recognition. In contrast to Boolean logic, fuzzy logic is grounded in fuzzy sets that can assume any actual number between 0 and 1. This methodology proves particularly pertinent where risk factors are challenging to quantify or exhibit ambiguity.
CVSS	CVSS (Common Vulnerability Scoring System) is an industry-standard wherein vulnerabilities in IT systems receive assigned values. Upon discovering a vulnerability, its severity can be assessed, with a higher value indicating a more severe impact. This simplifies decision-making regarding prioritisation and necessary measures for responsible parties.
AHP	AHP (Analytical Hierarchical Process) represents a mathematical approach applicable in information security risk assessment to organise criteria and sub-criteria based on their weighting. This aids decision-makers in the process of making informed decisions.
Bayesian Networks	Bayesian Networks (BN) provide a probabilistic method for modelling uncertainty and dependencies among various variables. BNs can calculate probabilities associated with security events and their consequences in assessing information security risks. A key advantage of BN lies in its capacity to compensate for missing information through experiential input, such as expert knowledge.
FTA	FTA (Fault Tree Analysis) is as a method for analysing the causes of risk events and failures. It allows for the graphical representation of logical event chains and the subsequent evaluation of their effects. Primarily, this facilitates effective communication of safety risks with stakeholders.

In Table 7, we detail the frequency with which different methods are mentioned in the academic literature. We remind that there were well over 100 methods mentioned. You can see in the Table that Fuzzy Theory, CVSS and AHP stand out as the most frequent methods. We remark that these methods are not mutually exclusive. For instance, there is interest in combining Fuzzy Theory with CVSS (Saulaiman et al. 2021). Moreover, the same mathematical method (e.g. Fuzzy Theory) can be applied in very different ways.

Table 7: Frequency (number of articles) mentioning cyber risk quantification methods

#	Abbreviation	Name (long)	Freq.
1	Fuzzy Theory		102
2	CVSS	Common Vulnerability Scoring System	98
3	AHP	Analytical Hierarchical Process	97
4	BN	Bayesian Networks	47
5	FTA	Fault Tree Analysis	36
6	ISRA	Information Security Risk Assessment	28
7	STRIDE	Spoofing of user identity, Tampering, Repudiation, Information disclosure, Denial of service, and Elevation of privilege	27
8	HAZOP	Hazard and Operability Analysis	26
9	Delphi		22
10	ISRAM	Information Security Risk Analysis Method	22
11	EBIOS	Expression of Needs and Identification of Security Objectives	22
12	MCDM	Multi-Criteria Decision-Making	20
13	FAHP	Fuzzy Analytic Hierarchy Process	20
14	ATA	Attack Tree Analysis	19
15	FRAP	Facilitated Risk Analysis Process	19
16	TOPSIS	Technique for Order of Preference by Similarity to Ideal Solution	18
17	PRA	Probabilistic Risk Analysis	14
18	DEMATEL	Decision-Making Trial and Evaluation Laboratory	14
19	COBRA	Consultative Objective and Bi-Functional Risk Analysis	14
20	Markov model		12
21	DREAD	Damage, Reproducibility, Exploitability, Affected users, and Discoverability	12
22	IS	IS Risk Analysis Method	12
23	Grey Theory		12
24	ANP	Analytic Network Process	11
25	ETA	Event Tree Analysis	11
26	FMECA	Failure Mode, Effects, and Criticality Analysis	11
27	VIKOR	Multi-criteria Optimization and Compromise Solution	10
28	BPNN	BP Neural Network	10
29	CIRA	Cyber-Informed Risk Analysis	10

Discussion of Cyber Risk Quantification Methods

RISK ANALYSIS AND PRIORITISATION

One of the main objectives of this study was to identify the approaches that are particularly suitable for assessing information security risks. To this end, the studies were analysed to determine how often the respective approaches were mentioned. This step investigates whether the frequency of individual approaches also correlates with their relevance. To this end, comparative studies identified in the literature analysis are examined.

In their study, Wangen et al (2018) examined the completeness of risk assessment methods. The approaches CIRA, CORAS, CRAMM, FAIR, NSM ROS, OCTAVE Allegro, ISO 27005, NIST SP 800-30, RISK IT, RAIS and CRDF were compared. The reference point was ISO 27005, compared with the other approaches. As a result, the authors stated that ISO 27005 generally fulfilled the most criteria and was the most complete. In terms of pure risk assessment, FAIR fulfilled the most criteria. Apart from NSM ROS and the niche approaches RAIS and CRDF, each mentioned less than ten times, all of the compared approaches are included in our ranking. ISO 27005, which the authors named the most complete, corresponds to our ranking. Although CRAMM was counted 75 times in our survey, this approach is no longer available, so it has been removed from our ranking.

Dixit et al. (2022) compared the OCTAVE, ISRAM, CORAS, CRAMM, CIRA, IS, NIST, and Mehari approaches in their framework. The study focused on whether the approaches were qualitative or quantitative, the complexity of implementation, and the acquisition costs. Concerning costs, the authors stated that all techniques, except for CRAMM, are free of charge. It is also noticeable in this study that the approaches examined there occupy a relatively high position within the ranking compiled as part of this study.

Conducting a systematic mapping review, Sánchez-García et al. (2022) analysed tools for automating cybersecurity risk assessment, comparing a total of 35. The research found that the ISO 27000 family and the NIST CSF were the most widely accepted international models and that smaller companies tend to use qualitative assessment methods and switch to quantitative models with appropriate size and internal organisation at a later stage.

As the same risk assessment approaches were often compared in the studies examined, and these were each given a high position in the ranking presented herein in our review, it can be assumed that there is a correlation between the frequency of mention and the degree of maturity of the respective approaches.

RISK COMMUNICATION

Assessing information risk accurately is often just the initial step in a successful information security risk strategy. After completing the assessment, it is crucial to communicate the results to relevant stakeholders for appropriate action. In this context, different risk assessment methods exhibit variations.

In certain risk assessment methodologies like Mehari or ISO 27005, effective risk communication is seamlessly integrated into the broader risk management process. As per the ISO 27005:2018 standard, risk communication is characterised as an activity focused on attaining consensus regarding risk handling through exchanging and sharing information among decision-makers and other stakeholders. Within this context, information encompasses the understanding, characteristics, manifestation, probability, severity, treatment, and acceptance of risks. In NIST SP 800-30, the perspective on risk communication aligns closely with the ISO 27005 standard. NIST emphasises that for optimal effectiveness, the communication of information security risks should harmonise with other modes of risk communication existing within the organisation. Internal policies, procedures, and mechanisms are pivotal in ensuring the collected information can be utilised effectively (National Institute of Standards and Technology 2012).

According to a study by Agrawal (2017), methods like CORAS and CIRA are collaborative, requiring cooperation between system stakeholders and risk assessment experts. This collaborative nature can be initially expensive, particularly for larger companies, due to the time-consuming and cost-intensive knowledge transfer involved. On the other hand, ISRAM is a method that demands less expert knowledge for implementation, allowing non-expert employees to participate in the assessment. This not only reduces costs but also facilitates risk communication, eliminating language barriers between experts and decision-makers.

In their study, Alohali et al. (2018) advocate for the precise application of risk communication, suggesting that messages should encompass both technical and non-technical contexts. Moreover, it is essential to assess the impact and appeal of the communication on users. The authors emphasise that messages not comprehended may detrimentally affect the overall communication between experts and users. Accordingly, the authors recommend categorising users based on their IT knowledge and tailoring the communication for optimal effectiveness.

ARGUMENTS FOR AND AGAINST CYBER RISK QUANTIFICATION

Cyber risk quantification can yield tangible benefits in terms of information cyber security investment and prioritising the protection of organisational assets. Govender et al. (2021) identify four main benefits: (1) Cost justification: advise senior management on critical technology risks to focus security spend. (2) Increased productivity because of less downtime. (3) Breaking barriers: It exposes risks in systems, technology and processes. (4) Self-analysis: allows for introspection of the IT department. Moreover, there are, as we have discussed, many frameworks, standards, guidelines, and methods that can be implemented. We, therefore, take it as given in this report that an organisation should have an ongoing process of cyber risk quantification. The more relevant questions are:

a How much should an organisation invest, particularly in terms of time and effort, in cyber risk quantification?

b What cyber risk quantification approach should an organisation adopt both in terms of methods, frameworks, standards and/or guidelines and also whether to use in-house or external expertise?

As discussed in Section 2, there are a variety of factors the organisation will want to consider, such as the simplicity/complexity of the approach, its accuracy, transparency, and the amount of resources needed to input into the process.

Making a general cost/benefit analysis of risk assessment approaches is complicated. This is not necessarily because the acquisition of the respective approaches is expensive. Apart from the ISO standards, which generally cost a small three-figure sum, many of the frameworks are available free of charge. However, the actual cost driver is associated with implementation in the form of staff time and opportunity cost. Another factor is the certification cost, for example, for ISO 27001.

Cyber risk quantification should be a dynamic and ongoing process that evolves over time. For instance, an organisation may start with relatively simple and transparent approaches and then progress to more complex approaches over time (ISO 27005). Each organisation will need to determine its own trade-offs. Here, we summarise some relevant factors from our review of the literature:

Decision-Making Aids for Management

Evaluating information security risks is the foundation for determining how to address the previously identified risks. Depending on the severity of these identified risks, prioritisation is essential to optimise the allocation of organisational resources. This study identified Analytic Hierarchy Process (AHP) as a method that systematically presents risks in a structured manner, streamlining the decision-making process. Quantitative models such as ISRAM, CORA, or IS offer a precise depiction of risks, facilitating a mathematical assessment of their consequences. On the other hand, qualitative approaches like OCTAVE or CORAS provide a relatively simple and cost-effective analysis of risks, describing them using adjectives rather than relying on mathematical models. The selection of the appropriate approach depends on factors such as the target audience, company size, or the expertise of decision-makers (Zabawi et al, 2015).

Risk Transfer Through Cyber Insurance

After identifying information security risks, there are various approaches to managing them. One avenue involves risk reduction, such as enhanced encryption techniques, firewalls, access controls, and similar measures. Alternatively, organisations can mitigate the financial risk of a potential security breach by securing cyber insurance (Gordon et al. 2003). Cyber insurance offers additional benefits through assistance services. Insurers often provide support in proactively minimising risks before any insured event occurs. Moreover, they offer loss mitigation measures typically unavailable to policyholders in other forms, such as assistance with data recovery or negotiation support in the aftermath of a ransomware incident. However, insurers only extend their expertise and services when the risk is quantifiable. This underscores the importance of a risk assessment, as it is a prerequisite for obtaining cyber insurance coverage.

The Constant Change in Cyber Risks

Cyber risks constantly evolve. As a consequence, a cyber risk quantification exercise can quickly be out of date. For instance, ransomware has exploded over the last five years. Attacks on cloud services are increasing in the context of pandemic-related behavioural changes, such as working-from-home initiatives. New trends, such as deep fakes or other uses of artificial intelligence, are not yet widely factored into threat analysis. The need to constantly evolve can make cyber risk quantification an overwhelming exercise. On the one hand, employees would have to be retrained every year to be able to recognise threats effectively; on the other hand, a vulnerability that has been closed at great expense may no longer be the main target of cybercriminals next year. Precise calculations of future threats are so difficult that the question arises as to whether the financial outlay corresponds to the potential benefit.

Data Availability

One of the main problems in assessing information security risks is the lack of sufficient data sets (Cremer et al. 2022). On the one hand, a large number of cyber security incidents are required to be able to make reliable forecasts for future events. On the other hand, the risk parameters are necessary within the organisation. Small and medium-sized companies, in particular, often do not have sufficient IT expertise, meaning that an assessment can either not be carried out at all or only by external service providers.

Unforeseeable Events

Further limits of risk assessment lie in events that cannot be predicted. Examples of this are geopolitical conflicts and hacktivism. Attacks driven by ideological motivations fall under the category of hacktivism. While typically associated with state or state-affiliated entities in geopolitical conflicts, hacktivism can extend beyond these boundaries. Since the start of the Russia-Ukraine war, attacks on the availability of critical data, services, and other critical resources using DDoS or ransomware have been observed in more significant. In addition to financial gain, espionage, disruption, or destruction, the ideological motivation of the attackers must also be considered (ENISA 2022). A notable and early instance of hacktivism involves the clash between Wikileaks and financial service providers like PostFinance, PayPal, MasterCard, Visa, and Moneybookers.com. Following Wikileaks' release of confidential US government documents in November 2010, the mentioned companies ceased their services, allowing money transfers to Wikileaks. DDoS attacks on the companies followed. Intentional inundation of requests aimed at overwhelming their servers resulted in the temporary unavailability of the companies' services (Pras et al. 2010).

Evaluating Risks of Third Parties

Another aspect of the limitation of cyber risk quantification involves the reliance on external resources or services. Like risk assessment, software development incorporates standards or code libraries, which may be accessible to the public either freely or for a fee. One notable example is Log4j, a widely used library. In December 2021, a vulnerability, CVE-2021-44228 (also known as Log4Shell), in Log4j enabled attackers to execute remote software code. NIST classified this threat as a critical vulnerability, assigning it the highest severity level. Given its status as a standard library, a race ensued between system administrators tasked with updating systems and attackers seeking to exploit the vulnerability. Merely a day after the official disclosure of the vulnerability, botnets like Mirai initiated the exploitation of this vulnerability (Hiesgen et al. 2022).

In this context, another crucial aspect to consider is the phenomenon known as supply chain attacks. For instance, when a company cannot conduct IT or IT security in-house, it often resorts to outsourcing these activities to third-party providers. However, if the systems of these external providers are compromised, it opens the door for attackers to infiltrate the service provider's customer base. The SolarWinds incident serves as a notable example, where the attackers successfully implanted a backdoor in over 18,000 systems, affecting 40 public institutions. This clandestine access granted them external entry to the targeted victims' data (Martínez and Durán 2021).

Potential Bias in Risk Quantification

Risk assessment can be biased towards certain types of assets, e.g. technical information rather than organisational knowledge. Shedden et al. (2011), for instance, provide a case study of an Australian business. The RISA focussed on technical issues such as backups. Follow-up interviews revealed the RISA did not account for organisational tacit knowledge, in other words, people knowing things that 'are not written down'. Given that the backup process is subtle and depends on tacit, informal knowledge, people are critical assets. This criticality was not recognised in the risk management process. More generally, risk quantification can focus on tangible assets that are easier to quantify.

The Need for Organisational Skills and Expertise

Govender et al. (2021) emphasise the importance of IT staff members' correct behaviour and values and strengthening their ability to do risk assessments. Risk assessment needs to be a continuous, routine part of what IT staff do. This, though, requires resources and illustrates how the costs of cyber risk quantification extend beyond the direct cost of running an assessment. We explore this in more detail in the next section.

THE PRE-REQUISITES NECESSARY FOR AN EFFECTIVE IMPLEMENTATION OF CYBER RISK QUANTIFICATION

As we have discussed, cyber risk quantification is a multi-stage process that includes risk identification, estimation, evaluation, and communication. Each stage of that process needs to be implemented well in order to be effective. Here, we highlight some of the most important factors.

One of the essential prerequisites for effectively implementing cyber risk quantification is a deep understanding of the threat. In their study, Rocchetto et al. (2019) described ways through which users of assessment models can acquire information concerning cyber risks. In particular, the authors referred to important sources, including the National Vulnerability Database (NVD), the Common Vulnerability Scoring System (CVSS), Common Vulnerability and Exposures (CVE), Open Vulnerability and Assessment Language (OVAL), and Common Weaknesses Enumerations (CWE), which are explained in the following.

The NVD, a publicly accessible database provided by NIST, offers a comprehensive overview of every known system vulnerability. It details how such attacks are carried out and under what conditions a vulnerability can be exploited. Additionally, the vulnerabilities are evaluated based on the CVSS, an industry standard that gauges the complexity of an attack and its potential impact. Each entry in the NVD is assigned a CVE identifier, which is managed by the MITRE organisation in the CVE database. OVAL serves as an automated vulnerability assessment tool. The structured nature of OVAL descriptions enables an automatic verification of whether a CVE impacts a system. CWE provides illustrations of faulty implementation or programming, which can subsequently be correlated with one or more CVEs. The overarching goal of various databases and organisations is to standardise vulnerabilities, facilitating smoother information exchange. An illustrative instance of this effective communication has been mentioned previously with CVE-2021-44228 (Log4Shell). Thanks to these mechanisms, affected organisations could swiftly respond and promptly address the identified vulnerability.

In addition to knowledge of possible threats, users must take further measures and make decisions before an assessment of these risks can begin. The first steps are often described in the standards, frameworks, and guidelines in the context of information security risk management. In the following, the most frequently mentioned representatives of this category, ISO, NIST, and OCTAVE, are examined in terms of how they prepare the user for the risk assessment:

ISO 27001

In the initiation phase of implementing the Information Security Management System (ISMS), the standard advises users to delineate the system's scope and limitations precisely. Simultaneously, it is crucial to delineate the overarching objectives to pursue and identify any pertinent requirements tied to business, legal, regulatory, or contractual obligations. Once the objectives and associated requirements are clearly defined, a suitable risk assessment approach must be identified, accounting for these parameters. Subsequently, criteria should be established to determine when risks are acceptable and the methodology for conducting such assessments. The entire process should be meticulously structured to ensure repeatability, allowing the results of individual iterations to be compared over time (International Organization for Standardization 2018).

NIST SP 800-30

Per the NIST standard, the risk assessment process necessitates a meticulous analysis of threats and vulnerabilities to ascertain their potential impact on the user and the probability of occurrence. Users can select an assessment approach, such as quantitative, qualitative, or semi-qualitative, each with its associated advantages and drawbacks.

As mentioned in the standard, quantitative methods typically employ methodologies, principles, or rules grounded in numerical data. This proves especially beneficial for conducting cost-benefit analyses concerning alternative risk responses or courses of action. Another advantage lies in the repeatability of studies, ensuring reproducible results. Nonetheless, a potential drawback may arise in presenting results, necessitating interpretation or clarification for decision-makers. In certain scenarios, using quantitative models may entail elevated costs due to the substantial time and effort the expert demands. Therefore, a judicious evaluation of disadvantages against advantages is essential.

In comparison to quantitative methods, qualitative assessments typically abstain from employing numerical categories, opting instead for categories like "low," "average," or "high" risk levels. This approach significantly facilitates result interpretation. However, when relying on expert knowledge rather than mathematical functions for risk assessment, it is crucial to define values precisely. This ensures consistency, preventing divergent results from arising from individual interpretations among experts.

Semi-quantitative assessments adeptly merge the advantages of both methods by converting a spectrum of values, such as a scale of 1-100, into easily comprehensible explanations for decision-makers. The granularity of the chosen ranges within this scale, for instance, 0-20, 21-40, 41-60, 61-80, and 81-100, determines the comparability of results and facilitates more effective prioritisation. Like the qualitative method, there exists a potential for subjective evaluations if the values lack precise definitions.

Another critical consideration for users of risk assessment methods is the choice of analysis approach. The NIST standard outlines three distinctive approaches: threat-oriented, asset- and impact-oriented, and vulnerability-oriented. Threat-oriented methodologies initiate with the identification of threat sources and events, exploring their potential development, including discerning the attacker's intent. Value and impact-oriented approaches scrutinise the potential consequences arising from a threat event and assess their implications for the user. In contrast, a vulnerability-oriented approach centres on the weaknesses within the user's organisation or environment, elucidating the potential repercussions resulting from their exploitation (National Institute of Standards and Technology 2012).

OCTAVE Allegro

Prior to embarking on a risk assessment with OCTAVE Allegro, the creators advocate for several essential preparatory activities. These activities encompass securing management support, allocating resources (such as staff with ample time and expertise), and delineating a framework for the assessment activities. Subsequently, the focus shifts to identifying the information resources critical to the user's organisation. This is succeeded by a comprehensive sequence of eight steps constituting the OCTAVE Allegro risk assessment, with Steps 1-6 viewed as preparatory measures within this context.

The first step is determining the organisational factors used to assess a risk's impact on the user's organisation. In doing so, it should be considered that the effects could be realised differently depending on the organisational area, so prioritisation must be made. In the second step, the information assets are described in detail so that the security requirements can be defined based on the characteristics, qualities, properties, and value of each. In step three, the areas where the information is located are identified. These can be service providers or the company's own IT infrastructure, for example. In the next step, the user should identify particularly vulnerable areas within the organisation and find possible scenarios or conditions that could threaten these areas. In step six, the threat analysis is extended to all other areas. The threats are divided into four areas: "Human actors using technical means", "Human actors using physical access", "Technical problems" and "Other problems" (Caralli et al. 2007).

Key Findings

This report provides a comprehensive review of the academic literature on cyber risk quantification. We overview quantification approaches and discuss some of the dimensions on which they differ. We also provide a discussion on the overall benefits and limitations of cyber risk quantification. Our key findings can be summarised:

1 There are well over 100 cyber risk quantification methods, frameworks, standards and guidelines. The most frequently mentioned quantification approaches in the academic literature are (from most mentioned): ISO27005, ISO27001, OCTAVE, NIST SP800-30, CORAS, ISO27002, COBIT, ISO31000, FMEA, FAIR, and ISRAM.

2 There is little evidence on the comparative effectiveness of different methods and frameworks for cyber risk quantification. Moreover, there is no agreed benchmark for comparing methods. Many new methods being advertised in the private sector are not disclosed (for IP reasons) and so are less open to scrutiny.

3 There is no 'one size fits all' best method of cyber risk quantification. The optimal method or framework for a particular organisation will depend on its priorities and needs, reflecting, e.g., its risk profile, in-house expertise, financial resources, and time availability. Organisations need guidance on how to choose a cyber risk quantification approach.

4 Risk quantification methods can be systematically biased towards certain types of assets and risks, e.g. technical information, that are more 'easily' measured. This can neglect less tangible assets such as organisational knowledge.

5 Risk quantification assessment should be viewed as a continuous and routine process. This requires expertise (either in-house or external). New threats (e.g. deep fakes facilitated by AI) can make recent costly cyber security interventions ineffective while opening up new vulnerabilities. The need for constant updating of knowledge can overwhelm organisations.

6 There exist tested and trusted cyber risk quantification frameworks, guidelines, standards, and methods that are 'freely available to use and designed to be relatively accessible. While time and expertise are needed to implement such approaches, it can be beneficial for organisations to develop in-house capabilities rather than solely rely on external providers. This can be facilitated by starting with 'simpler' approaches and building up capability over time.

Gaps in the Literature

There are many gaps in the existing literature on cyber risk quantification. First and foremost, we need more evidence on whether different approaches work at a technical level (i.e., the assumptions underlying the methods are sound) and an implementation level (i.e., organisations can effectively implement the approach). We summarise as follows:

a There needs to be more work to analyse, compare, and contrast the assumptions underlying different frameworks, standards, guidelines, and methods. As we previously highlighted, approaches can differ across the implementation of the management process, including context establishment, risk identification, and risk analysis, as well as communication. A wide range of qualitative and quantitative methods are also being used for the risk analysis. There is a lack of current research analysing the modelling assumptions of different approaches and their advantages and limitations. This gap in understanding will only get worse as new approaches are developed by the private sector, for which we have limited information on underlying assumptions. Current work tends to focus on comparing differences between approaches in terms of implementations (e.g., Wangen 2018; Sanchez-Garcia et al. 2022).

b There needs to be more work to analyse the implementation of different risk approaches within organisations. At a most basic level, would two different teams within an organisation implementing a particular risk quantification approach end up with similar conclusions? If not, then there is a problem with the approach. To explore this question, we need to analyse and observe how organisations implement approaches. Work of this nature, e.g. Shedden et al. (2011) with a case study, has identified potential bias in approaches and implementation. Ideally, therefore, there would be more work observing and following the cyber risk quantification process within organisations and evaluating consistency in implementation.

c There is a need for more work analysing the methods currently being used by organisations. Our review focuses on the academic literature with the implicit assumption that approaches discussed more frequently in the academic literature are used more frequently in the wild. There is, though, a need for more work exploring the approaches that organisations are adopting. The survey results we provide in section 2 on a sample of medium and large businesses are a step in that direction, documenting the proportion of businesses using cyber risk quantification and whether they buy in services or use in-house modelling. Further research is needed to obtain more detail on specific approaches used, resources devoted to cyber risk quantification, etc.

d The focus of the located studies has been on areas such as industry, energy production, information technology, or the healthcare sector. Future research could, for instance, concentrate on small and medium-sized enterprises as well as governmental institutions.

Conclusion

The objective of this study was to provide a comprehensive overview of the cyber risk quantification landscape and assess its validity and usefulness in addressing the challenges associated with cyber risk. A systematic literature review was conducted to encompass the landscape, identifying over 1,900 studies, with 713 deemed relevant to the context of cyber risk quantification. In total, 137 frameworks, guidelines, and standards, along with 81 risk assessment methods, were identified to assist users in diverse ways in evaluating cyber threats. The subsequent sections elaborate on the findings of the systematic review.

Our investigation yielded diverse approaches that users can employ to evaluate potential cyber risks. We categorised these approaches into two main groups: "Risk Assessment Methods" and "Standards, Frameworks, and Guidelines." The first category encompasses 81 methods exclusively focused on risk assessment, employing quantitative, qualitative, or semi-quantitative methodologies. Notably, methods like Fuzzy Theory, Analytical Hierarchical Process, CVSS, Bayesian Networks, and Fault Tree Analysis were frequently mentioned. These approaches within the category serve varied objectives, including predicting probabilities of occurrence, supporting decision-making processes, and conducting monetary assessments of attack consequences. Additionally, we observed in the reviewed studies that authors often combined different approaches to explore potential enhancements in predictive outcomes.

Within the second category, we compiled a total of 137 standards, guidelines, and frameworks. This amalgamation is partly due to the frequent use of these terms interchangeably and because these approaches extend beyond mere risk assessment. They aid users in activities such as identifying, monitoring, communicating, and managing risks. In the evaluation of risks, some approaches either referenced individually suitable risk assessment methods or provided them. Prominent representatives in this category include the ISO/IEC standards 27005 and 27001, along with OCTAVE, NIST SP 800-30, and CORAS, which were consistently cited.

The ISO 27001, OCTAVE, and NIST SP 800-30 approaches were chosen in this study to delineate the diverse requirements for conducting a comprehensive cyber risk assessment. Users must deliberate on the objectives guiding risk management, the business, legal, and regulatory obligations, and the methodology employed for risk assessment. Additionally, users should pinpoint relevant information assets and identify vulnerable areas within the organisation. It's noteworthy that proficiency in handling cyber risks is often presumed, encompassing knowledge of potential risk scenarios, attacks, and the execution of risk assessment methods. Challenges may arise for many companies, particularly small and medium-sized enterprises, due to the overall scarcity of skilled personnel in the cybersecurity sector. It's crucial to recognise that there is no standardised approach for all companies, and comparing different approaches can be challenging. Throughout the study, no universally superior approach was identified. The choice of a risk assessment approach depends on individual factors such as company size, data confidentiality, user expertise, geopolitical considerations, industry specifics, or compliance requirements from official or contractual obligations. Different risk assessment approaches may confer advantages based on these distinctive user characteristics.

References

ACM Digital Library. (2023). About ACM DL, available at: https://dl.acm.org/about [Accessed 05.07.2023]

AGCS Global. (2022). Allianz Risk Barometer 2023 | AGCS, available at: https://www.agcs.allianz.com/news-and-insights/news/allianz-risk-barometer-2023-press.html [Accessed 05.07.2023]

Agrawal, V. (2017). A Comparative Study on Information Security Risk Analysis Methods. Journal of Computers, 12(1), 57-67. Available at: http://dx.doi.org/10.17706/jcp.12.1.57-67

Alberts, C. J., Behrens, S. G., Pethia, R. D., & Wilson, W. R. (1999). Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) Framework, Version 1.0

Alhajri, R.M., Alsunaidi, S.J., Zagrouba, R., Almuhaideb, A.M. & Alqahtani, M.A. (2019). Dynamic Interpretation Approaches for Information Security Risk Assessment. In (2019) International Conference on Computer and Information Sciences (ICCIS), 3-4 April 2019, 1-6. Available at: http://dx.doi.org/10.1109/ICCISci.2019.8716399

Amin, Z. (2017). A Practical Road Map for Assessing Cyber Risk', Journal of Risk Research, 22(1), 32-43. Available at: http://dx.doi.org/10.1080/13669877.2017.1351467

Amin, Z.M., Anwar, N., Mohd Shoid, M.S. & Samuri, S. (2022). Method for Conducting Systematic Literature Review (SLR) for Cyber Risk Assessment, Environment-Behaviour Proceedings Journal, 7(SI10), 255-260. Available at: http://dx.doi.org/10.21834/ebpj.v7iSI10.4130

Aziz, B. (2020). A systematic literature review of cyber insurance challenges. In 2020 International Conference on Information Technology Systems and Innovation (ICITSI), IEEE, 357-363. Available at: http://dx.doi.org/10.1109/ICITSI50517.2020.9264966

Böhme, R. & Nowey, T. (2008). Economic Security Metrics. Dependability Metrics: Advanced Lectures, 176-187

Chen, F. (2015). An Investigation and Evaluation of Risk Assessment Methods in Information Systems

Chockalingam, S., Pieters, W., Teixeira, A. & van Gelder, P. (2017). Bayesian Network Models in Cyber Security: A Systematic Review. In Lipmaa, H., Mitrokotsa, A. and Matulevičius, R., eds., Secure IT Systems, 105-122. Cham: Springer International Publishing

Cremer, F., Sheehan, B., Fortmann, M., Kia, A.N., Mullins, M., Murphy, F. & Materne, S. (2022). Cyber Risk and Cybersecurity: A Systematic Review of Data Availability, Geneva Pap Risk Insur Issues Pract, 47(3), 698-736. Available at: http://dx.doi.org/10.1057/s41288-022-00266-6

Derakhshandeh, S. & Mikaeilvand, N. (2011). New Framework for Comparing Information Security Risk Assessment Methodologies. Australian Journal of Basic and Applied Sciences, 5

Devi, R.K., Sensuse, D.I., Kautsarina & Suryono, R.R. (2022). Information Security Risk Assessment (ISRA): A Systematic Literature Review', Journal of Information Systems Engineering and Business Intelligence, 8(2), 207-217, available: http://dx.doi.org/10.20473/jisebi.8.2.207-217

Dixit, K., Singh, U.K. and Pandya, B.K. (2022). Comparative Framework for Information Security Risk Assessment Model. In Proceedings of the International Conference on Innovative Computing & Communication (ICICC) 2022. Available at: http://dx.doi.org/10.2139/ssrn.4121814

ENISA. (2019). ENISA Threat Landscape Report 2018. Available at: https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018 [Accessed 05.07.2023]

ENISA. (2022). ENISA Threat Landscape 2022. Available at: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022 [Accessed 17.01.2024].

ENISA. (2023a). Demand Side of Cyber Insurance in the EU. Available at: https://www.enisa.europa.eu/publications/demand-side-of-cyber-insurance-in-the-eu [Accessed 05.07.2023]

ENISA. (2023b). ENISA Threat Landscape 2023. Available at: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023 [Accessed 05.07.2023]

ENISA. (2024). ENISA Interoperable EU Risk Management Framework. Available at: https://www.enisa.europa.eu/publications/interoperable-eu-risk-management-framework

Fernandez de Arroyabe, I., Watson, T. & Angelopoulou, O. (2022). Cybersecurity in the Automotive Industry: A Systematic Literature Review (SLR). Journal of Computer Information Systems, 63(3), 716-734. Available at: http://dx.doi.org/10.1080/08874417.2022.2103853

Google Scholar. (2023). Stand on the Shoulders of Giants. Available at: https://scholar.google.com/intl/de/scholar/about.html [Accessed 05.07.2023]

Gordon, L.A., Loeb, M.P. & Sohail, T. (2003). A Framework for Using Insurance for Cyber-Risk Management. Communications of the ACM, 46(3), 81-85. Available at: http://dx.doi.org/10.1145/636772.636774

Hiesgen, R., Nawrocki, M., Schmidt, T.C. & Wählisch, M. (2022). The Race to the Vulnerable: Measuring the Log4j Shell Incident. arXiv preprint arXiv:2205.02544

IEEE Xplore. (2023). IEEE at a Glance. Available at: https://www.ieee.org/about/at-a-glance.html [Accessed 05.07.2023]

ISO. 2011. ISO/IEC 27005:2011 Second edition, Information Technology - Security Techniques - Information Security Risk Management, International Organization for Standardization

ISO. 2018. International Organization for Standardization ISO 31000:2018 Risk Management - Guidelines. Available at: https://www.iso.org/standard/65694.html [Accessed on 26.01.2024]

ISO. 2022. ISO/IEC 27005:2022, Information Security - Cybersecurity and Privacy Protection - Guidance on Managing Information Security, International Organization for Standardization

Kiran, K., Reddy, L. & Haritha, N.L. (2013). A Comparative Analysis on Risk Assessment Information Security Models. International Journal of Computer Applications, 82(9)

Kruse, C.S., Frederick, B., Jacobson, T. & Monticone, D.K. (2017). Cybersecurity in Healthcare: A Systematic Review of Modern Threats and Trends. Technol Health Care, 25(1), 1-10. Available at: http://dx.doi.org/10.3233/THC-161263

Leszczyna, R. (2018). A Review of Standards with Cybersecurity Requirements for Smart Grid. Computers & Security, 77, 262-276. Available at: http://dx.doi.org/10.1016/j.cose.2018.03.011

Maček, D., Magdalenić, I. & Ređep, N. (2020). A Systematic Literature Review on the Application of Multicriteria Decision Making Methods for Information Security Risk Assessment. International Journal of Safety and Security Engineering, 10(2), 161-174. Available at: http://dx.doi.org/10.18280/ijsse.100202

Macher, G., Armengaud, E., Brenner, E. & Kreiner, C. (2016). A Review of Threat Analysis and Risk Assessment Methods in the Automotive Context. In Skavhaug, A., Guiochet, J. & Bitsch, F., eds., Computer Safety, Reliability, and Security, 130-141. Cham: Springer International Publishing

Malekos Smith, Z., Lewis, J.A. & Lostri, E. (2020). The Hidden Costs of Cybercrime. Available at: https://www.mcafee.com/de-de/consumer-corporate/newsroom/press-releases/press-release.html?news_id=6859bd8c-9304-4147-bdab-32b35457e629&tab=detect [Accessed 05.07.2023]

Martínez, J. & Durán, J.M. (2021). Software Supply Chain Attacks, A Threat to Global Cybersecurity: SolarWinds' Sase Study. International Journal of Safety and Security Engineering, 11(5), 537-545

NIST. 2024a. National Institute of Standards and Technology (NIST) 'Cybersecurity Framework, Framework Basics. US Department of Commerce. Available at: https://www.nist.gov/cyberframework/frequently-asked-questions/framework-basics [Accessed 26.01.2024]

NIST. 2024b. National Institute of Standards and Technology (NIST) 'Risk Assessment Tools', US Department of Commerce. Available at: https://www.nist.gov/itl/applied-cybersecurity/privacy-engineering/collaboration- space/browse/risk-assessment-tools [Accessed 26.01.2024]

Orlando, A. (2021). Cyber Risk Quantification: Investigating the Role of Cyber Value at Risk. Risks, 9(10), 184

Page, M.J., McKenzie, J.E., Bossuyt, P.M., Boutron, I., Hoffmann, T.C., Mulrow, C.D., Shamseer, L., Tetzlaff, J.M., Akl, E.A., Brennan, S.E., Chou, R., Glanville, J., Grimshaw, J.M., Hrobjartsson, A., Lalu, M.M., Li, T., Loder, E.W., Mayo-Wilson, E., McDonald, S., McGuinness, L.A., Stewart, L.A., Thomas, J., Tricco, A.C., Welch, V.A., Whiting, P. & Moher, D. (2021). The PRISMA 2020 Statement: An Updated Guideline for Reporting Systematic Reviews', Syst Rev, 10(1), 89. Available at: http://dx.doi.org/10.1186/s13643-021-01626-4.

Pan, L. & Tomlinson, A. (2016). A Systematic Review of Information Security Risk Assessment. International Journal of Safety and Security Engineering, 6(2), 270-281

Pras, A., Sperotto, A., Moura, G.C., Drago, I., Barbosa, R., Sadre, R., Schmidt, R. & Hofstede, R. (2010). Attacks by "Anonymous" WikiLeaks Proponents Not Anonymous. Design and Analysis of Communication Systems Group (DACS) CTIT Technical Report, 1-10

Sánchez-García, I.D., Mejía, J. & San Feliu Gilabert, T. (2022). Cybersecurity Risk Assessment: A Systematic Mapping Review, Proposal, and Validation. Applied Sciences, 13(1). Available at: http://dx.doi.org/10.3390/app13010395

Sayouti, A., Medromi, H., Faris, S. & Ghazouani, M. (2014). Information Security Risk Assessment A Practical Approach with a Mathematical Formulation of Risk. International Journal of Computer Applications, 103(8), 36-42. Available at: http://dx.doi.org/10.5120/18097-9155

Saulaiman, M., Takács, M., Kozlovszky, M., & Csilling, A. (2021). Fuzzy Model for Common Vulnerability Scoring System. In 2021 IEEE 15th International Symposium on Applied Computational Intelligence and Informatics (SACI) (pp. 419-424)

Scopus. (2023). Factsheet. Available at: https://www.elsevier.com/solutions/scopus [Accessed 05.07.2023]

Shamala, P., Ahmad, R. & Yusoff, M. (2013). A Conceptual Framework of Info Structure for Information Security Risk assessment (ISRA). Journal of Information Security and Applications, 18(1), 45-52. Available at: http://dx.doi.org/10.1016/j.jisa.2013.07.002

SpringerLink. (2023). Result(s) for Journal. Available at: https://link.springer.com/search?facet-content-type=%22Journal%22 [05.07.2023]

Vasquez Ubaldo, A.L., Gutierrez Barreto, V.Y., Berrios Albines, J.A., Andrade-Arenas, L. & Bellido-García, R.S. (2023). Information Security in the Banking Sector: A Systematic Literature Review on Current Trends, Issues, and Challenges

Vorster, A. & Labuschagne, L. (2005). A Framework for Comparing Different Information Security Risk Analysis Methodologies. Pages, 95-103

Wangen, G., Hallstensen, C. & Snekkenes, E. (2017). A Framework for Estimating Information Security Risk Assessment Method Completeness. International Journal of Information Security, 17(6), 681-699. Available at: http://dx.doi.org/10.1007/s10207-017-0382-0

Web of Science. (2023). Discovery and Workflow Solutions – Web of Science. Available at: https://clarivate.com/products/scientific-and-academic-research/research-discovery-and-workflow-solutions/web-of-science/web-of-science-core-collection/science-citation-index-expanded/ [Accessed 05.07.2023]

World Economic Forum. (2023). Global Risks Report 2023: 18th Edition. Available at: https://www3.weforum.org/docs/WEF_Global_Risks_Report_2023.pdf [Accessed 05.07.2023]

Zabawi, A.Y., Ahmad, R. & Abdul-Latip, S.F. (2015). A Comparative Study for Risk Analysis Tools in Information Security, 10, 17672-17678