Choosing the Right Cybersecurity Solution: A Review of Selection and Evaluation Criteria

Rafał Leszczyna[1][0000−0001−7293−2956]

[1] Gdańsk University of Technology, Faculty of Management and Economics, Gdańsk, Poland
rle@zie.pg.edu.pl

Abstract. Information technologies evolve continuously reaching pioneering areas that bring in new cybersecurity challenges. Security engineering needs to keep pace with the advancing cyberthreats by providing innovative solutions. At the same time, the foundations that include security and risk assessment methodologies should remain stable. Experts are offered with an extensive portfolio of solutions and an informed choice of a particular one becomes problematic. Transparent criteria are the instrument that answers this issue by laying the ground for evidence-based justifications. Within the framework of systematic literature analysis, this study reviews the criteria proposed in the relevant literature. Based on the outcome, a consolidated set of criteria that should help in choosing a cybersecurity solution is proposed. Ethical questions posed by certain cybersecurity assessment activities are discussed. Consequently, new criteria related to the ethical application of a solution are introduced in the consolidated set.

Keywords: cybersecurity, management, solutions, methods, ethics, organisation management

1 Introduction

Information technologies evolve continuously demarcating new areas of applications and solutions. Edge computing, Software 2.0, digital twins, remote working at a massive scale, broad AI application or 5G are only selected examples of emerging technology trends (Accenture, 2021b; Deloitte Insights, 2021; Duggal, 2021; McKinsey & Company, 2021). Together with great opportunities, these changes bring in new challenges. Innovative hardware and software architectures open new paths for cyberattacks. The contemporary cyberthreat landscape is marked by phenomena such as cybercrime as a service (ENISA, 2021), commodity malware (Accenture, 2021a), and the ransomware crisis (Accenture, 2021a; Sophos, 2021) or refined supply chain infringements (ENISA, 2021). Cybersecurity needs to keep pace with the advancing cyberthreats by providing innovative solutions. The developments include situational awareness (Alcaraz & Lopez, 2013; Bolzoni et al., 2016; Tadda & Salerno, 2010) and threat intelligence platforms (Leszczyna & Wróbel, 2019), facilitated cyberincident

information sharing (Leszczyna et al., 2019) or embedding artificial intelligence into defensive mechanisms.

In parallel, there are elements of cybersecurity that independently of the complexity or innovativeness of the technology shall remain stable. One of them is *risk assessment* – the process devoted to the identification, analysis and evaluation of cybersecurity risks (ISO/IEC, 2018; NIST, 2011; Wangen et al., 2018) – that constitutes the central part of cybersecurity management (ISO/IEC, 2013). Also, *cybersecurity assessment* should be a solid and steady component. It investigates the cybersecurity state of an assessed entity (Dalalana Bertoglio & Zorzo, 2017; Qassim et al., 2019; Rogers & Syngress Media, 2004) and determines how effectively the entity fulfils specific security objectives (Scarfone et al., 2008).

Experts are offered an extensive portfolio of solutions, both the innovative ones and related to the fundamental risk and cybersecurity assessment activities (Gritzalis et al., 2018; Ionita & Hartel, 2013; Leszczyna, 2021; Wangen et al., 2018). In this regard, an informed choice of a particular solution becomes challenging. Transparent criteria are the instrument that answers this issue by laying the ground for evidence-based justifications. *Selection criteria* enable identifying the methods applicable to a specific area, while *evaluation criteria* facilitate comparing the identified methods and eliciting the most suitable one.

This study reviews the criteria proposed in the relevant literature during a systematic process that implements the (Webster & Watson, 2002) and (Kitchenham & Brereton, 2013) guidelines. Based on the outcome a consolidated set of criteria that should help in choosing a cybersecurity solution is proposed. Because cybersecurity management and cybersecurity assessments, in particular, may include activities that pose ethical questions, the collection is extended with criteria related to the ethical application of a solution.

The main contributions of the research are as follows:

- Criteria proposed in the relevant literature are identified during a systematic review process.
- A consolidated set of criteria that should facilitate informed decisions on the choice of cybersecurity solution is proposed.
- The collection is extended with criteria related to the ethical application of a solution.

The paper is organised as follows. Section 2 presents the research method applied in the study. The outcome of the analysis i.e. the identified criteria are presented in Section 3. After that, the ethical questions related to cybersecurity management are discussed (Section 4) and the consolidated set of criteria is introduced (Section 5). The paper closes with concluding remarks.

2 Research method

This study adopts the approaches of Webster & Watson, 2002 and Kitchenham & Brereton, 2013 to systematic literature surveys. Its main components are presented in Figure 1. During the *literature search*, relevant publications were searched for using

the keywords “security assessment”, “review” and “survey”. To reduce the number of results this step was repeated several times. Also, selection and evaluation criteria were applied to facilitate the process. Depending on the functionalities provided by a search engine, the initial iterations focused on titles, abstracts, keywords or other metadata. Then, the descriptions of the publications were read (*manual search*), to finally browse the contents of the documents in the concluding iteration (*in-depth analysis*). When possible, the search was restricted to computer science or a cognate domain.

The literature sources included journals, books and the databases of established publishers that address the topics of cybersecurity, communication systems, computer science and related i.e. the ACM Digital Library, Elsevier, Emerald, IEEE Xplore, Springer and Wiley. Also, collective databases that contain records of various publishers – EBSCOhost, Scopus and Web of Science were utilised. In addition to that, the search was completed with a short search of conference proceedings and the Internet. When discovered papers mentioned other relevant articles, also the latter were subject to the analysis (*backward analysis* (Webster & Watson, 2002)).

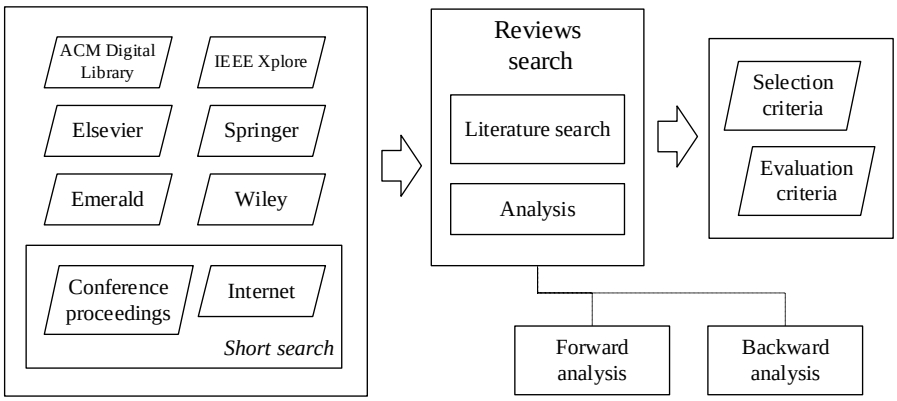

Fig. 1. The key tasks and data sources employed during the review process.

3 Identified criteria

Qassim et al., 2019 apply basic criteria to depict a standard or a guideline as most relevant to the topic of the study: availability free of charge, English documentation, publication by a standard body or governmental agency, implementation or application in the context of industrial control systems and the presence of detailed descriptions. The documents’ analysis criteria regard the method’s coverage of cybersecurity management processes, the assessment mode (active or passive), and compliance to the NERC CIP requirements.

Cherdantseva et al., 2016 took advantage of an adaptation of the literature review approach of Kitchenham & Brereton, 2013 to obtain a structured search. As inclusion criteria, the authors utilised the method’s coverage of risk assessment processes, its industrial control systems-specific design and scientific, cybersecurity-related origin.

The analysis criteria embraced the method's aim, its application domain, addressed phases and concepts of risk management, the impact assessment scheme, sources of data for deriving probabilities, the method's evaluation procedure and availability of supporting tools. Based on the analysis criteria a series of methods' categorisations have been introduced, comprising, for instance, formula-based and model-based, low-level and high-level detail coverage or qualitative and quantitative, the latter including probabilistic, non-probabilistic and undefined. Also, a content coverage-related criterion is applied by Hahn & Govindarasu, 2011 who compared assessment methods based on the coverage of 13 NERC CIP requirements relevant to cybersecurity assessment. Shahriar & Zulkernine, 2009 defined seven criteria for comparing testing methods. The criteria encompass vulnerability coverage, source of test cases, test generation method, test level, the granularity of test cases, tool automation and application domain.

A structured method for comparing and evaluating risk assessment techniques is applied by Gritzalis et al., 2018. The authors thoroughly analysed the criteria utilised in earlier studies to derive a set of common criteria that were discussed by industry experts and contain a strong practical component. The criteria are categorised into four groups, namely validity, compliance, cost and usefulness. They are presented in Table 1. In addition, as selection criteria, the presence of a risk assessment method description, the focus on information security risks and the availability of English documentation are used.

Table 1. Gritzalis et al., 2018 evaluation and comparison criteria for risk assessment methods.

Validity	Compliance	Cost	Usefulness
Completeness			**Ease of use**
Preparation (1)			
Risk identification (2)			Usability (Interface, handle errors, documentation)
Risk analysis (3)			
Risk evaluation (4)			
Type of analysis			**Scope**
Qualitative	Compliance with standards	Support cost	Target organisation (type, size), Focus
Quantitative		Software cost	
Risk calculation class			**Life cycle**
Class A			Release
Class B			Last update
Class C			**Adaptability**
Class D			**Software support**
Class E			**Training**

Wangen et al., 2018 developed a dedicated framework for comparing risk assessment methods and evaluating their completeness as far risk assessment

constituent tasks are concerned. The development process was bottom-up and incremental, based on extracting and combining tasks specified in the methods. Consequently, more than 40 tasks and 10 associated concepts are distinguished, coverage of which pertains to the frameworks' criteria. The tasks are grouped into three descriptive categories related to the incumbent stages of risk assessment (risk identification, estimation and evaluation). As selection criteria, the large number of citations (exceeding 50), the coverage of particular risk subjects (incentives risk, cloud risk and privacy risk), the coverage of three compulsory risk assessment processes, timeliness (published during the last 15 years) and availability of English or Norwegian documentation were utilised.

Ionita & Hartel, 2013 advocate deriving selection criteria directly from the scope and assumptions of the research. As a result, introduced inclusion criteria include the presence of a method description that comprises all obligatory risk assessment stages, application to an existing system or a system design, specific audience (chief security officers or other decisive personnel), the focus on information security risks, the availability of comprehensive English documentation as well as practical application in more than one country. Exclusion criteria embraced certification purpose, orientation towards a concrete product or system and only high-level (managerial or governance) specifications. When comparing risk assessment methods the authors apply the following criteria: method class (from one to five), method type (quantitative or qualitative), sponsor, focus, supported risk assessment phases, release date, price, type of target users (management, operational or technical), required skills, availability of supporting tools (paid, free), availability of a standalone version and the target organisation type (government agency, large company, small or medium enterprise). Besides that, a categorisation of methods is proposed based on risk measurement (quantitative and qualitative), risk model (five classes) and goal (e.g. certification, audit or internal control).

Felderer et al., 2016 performed an extensive analysis of existing evaluation criteria and classifications of security testing methods to construct a taxonomy of model-based security testing techniques. Based on the research, the authors proposed a structured set of classification criteria presented in Figure 2. The criteria are divided between filter and evidence types. The former validated the existence of a system security model, an environment security model and explicit test selection criteria. The latter focused on examining the maturity of the assessment object, evidence measures and the evidence level. The selection criteria used in the study embraced the documentation in a peer-reviewed paper written in English and the coverage of a model-based security testing approach. Earlier on, Felderer & Schieferdecker, 2014 presented a compound taxonomy focused on risk-based testing that distinguishes three top-level classes related to risk drivers, risk assessment and the risk-based test process. It contains more than 40 classification criteria. Giannopoulos et al., 2012 propose analysis criteria that result from the practice of conducting multiple impact assessments, namely the method's scope, objectives, target users, applied techniques and standards, the coverage of interdependencies, addressing of cross-sectoral risks and relevance to resilience.

To compare risk analysis methods, Meriah & Rabai, 2018 use the following criteria: purpose, inputs, outcome, the structure of the security management process, supporting

tools and type of system application. Fabisiak et al., 2012 proposed a substantial set of comparison criteria that are used to evaluate methods that support various aspects of cybersecurity management, including cybersecurity assessment and risk assessment. The criteria are presented in Table 2. Shah & Mehtre, 2015 classify vulnerability discovery techniques into manual testing, automated testing, static analysis and fuzz testing. A taxonomy of automated cybersecurity assessment based on D^3 (Discovery, Description, and Detection) approach is proposed by Barrere et al., 2014. Steffen Weiss (Weiss, 2008) introduces a basic categorisation of cybersecurity assessment methods into measurement approaches and combines approaches depending on the breadth of evaluation (components – organisation), as well as based on the meticulousness' level of measurements – algorithmic approaches and guidelines. For instance, algorithmic measurement approaches include vulnerability analysis.

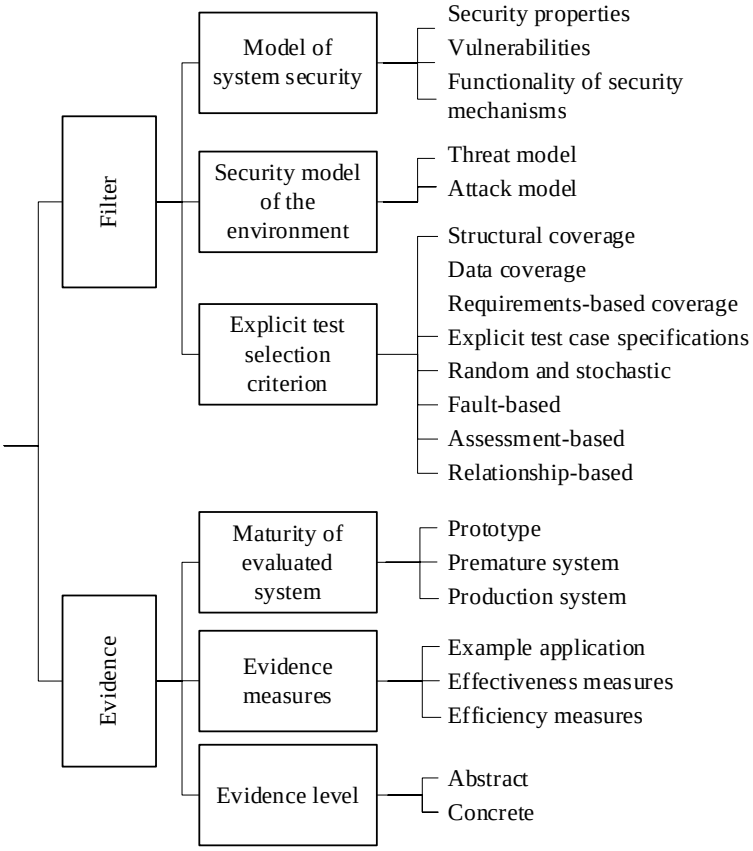

Fig. 2. Classification criteria for security testing methods proposed by (Felderer et al., 2016).

The study of Li et al., 2019 focuses on the software used in vulnerability identification. Thus, selection criteria, besides the availability free of charge, are strictly

technical. They refer to stand-alone, self-contained operation, detection of Java code vulnerabilities and identification of security weaknesses extending beyond code bugs. Similarly, the metrics applied to compare the applications are software-oriented. They comprise the vulnerability coverage (the number of detected flaws), the recall, precision, and discrimination rates as well as 15 usability measures including the tool output quality, the averaged false positive rate or extendability. The analogous study of Holm et al., 2011 concentrated on the tools' functionality and accuracy. 12 metrics associated with the former attribute embraced software flaws detection, configuration errors detection, scanning mode (active or passive), ports coverage, patch deployment ability and others. The latter property was linked to the number of false negatives. Lykou et al., 2019 compare vulnerability identification tools using 13 metrics, namely the tool type, its developer, origin, description, the number of stages in the evaluation process, survey method, required security expertise, standards compliance, presence of standards' compliance checking functionality, database of industry available cybersecurity practices, sector average score, presence of a recommendation list and the type of result.

Table 2. Comparison criteria for cybersecurity assessment, risk assessment and cybersecurity management methods introduced by Fabisiak et al., 2012.

Cost	Number of standard scenarios	Risk metric
English documentation	Analysis of scenarios dependencies	Choice of countermeasures
National standard	Data gathering method	Analysis of countermeasures' dependencies
International standard	Data verification	Analysis of countermeasures' influence
Declared compliance with standards	Basis for risk calculation	Estimation of risk treatment efficiency
Target group	Number of risk levels	Risk monitoring
Sophistication of usage/implementation	Basis for probability estimation	Detection of new risks
Popularity	Number of probability levels	Automatic correction of dependant risk for security policy framework
Flexibility	Basis for cause estimation	Procedures generation support
Method's scope of action	Number of cause levels	
Method of risk identification	Cause metric	
Risk completeness verification	Probability metric	

The selection and analysis criteria applied in the studies (besides the criteria of Felderer et al., 2016 and Gritzalis et al., 2018 which are presented in Figure 2 and Table 1) are summarised in Tables 3 and 4. Based on them, common criteria for choosing a cybersecurity management solution were derived. The criteria are presented in Section 5.

Table 3. Method selection criteria from several studies (Cherdantseva et al., 2016; Felderer et al., 2016; Gritzalis et al., 2018; Ionita & Hartel, 2013; Qassim et al., 2019; Wangen et al., 2018).

(Qassim et al., 2019)	(Cherdantseva et al., 2016)	(Gritzalis et al., 2018)	(Wangen et al., 2018)	(Ionita & Hartel, 2013)	(Felderer et al., 2016)
Availability free of charge	Coverage of risk assessment processes	English documentation	Large number of citations	English documentation	English documentation
English documentation	Industrial control systems-specific design	Focus on information security risks	English or Norwegian documentation	Practical application in more than one country	Documentation in a peer-reviewed paper
Publication by a standard body or governmental agency	Scientific, cybersecurity-related origin	Presence of a risk assessment method description	Coverage of particular risk subjects	Application to an existing system or a system design	Coverage of a model-based security testing approach
Implementation or application in the context of industrial control systems			Coverage of three compulsory risk assessment processes	Presence of a method description that comprises all obligatory risk assessment stages	
Detailed descriptions			Timeliness	Specific audience	
				Focus on information security risks	

4 Ethical questions

Cybersecurity management is perceived as an ethical process. By protecting cyberassets, security of human beings that depend on them is improved. Moreover, this is an ethical obligation for cybersecurity professionals to protect their organisations' infrastructure from intrusions and attacks (Vallor & Rewak, 2018). Consequently, cybersecurity assessments, as a constituent of a cybersecurity management process should be perceived as ethical. During assessments, the overall level of protection is determined and vulnerabilities are discovered (Dalalana Bertoglio & Zorzo, 2017; Qassim et al., 2019; Scarfone et al., 2008). This, in turn, enables the introduction of controls that aim at improving the recognised situation.

One of the techniques, broadly instructed in cybersecurity guidelines is the emulation of hacking techniques. There, the analysts employ the same tactics and tools as hackers do (Harper et al., 2018). Already this poses ethical questions, as hacking is generally considered unethical (Best, 2006; Falk, 2004), but the situation gets even more complicated when the analyses are directed toward the human component. *Social engineering* refers to manipulating individuals to perform specific actions or to reveal sensitive information (Lohani, 2019; Sargent & Webb, 2020). Social engineering attacks intertwine human interactions and technical measures (Klimburg-Witjes & Wentland, 2021). In cybersecurity assessment, social engineering exercises aim at testing the resistance of the human element in an organisation to this type of hacking technique. It facilitates determining the level of cybersecurity awareness and enables identifying weaknesses in user behaviour, including not following cybersecurity policies (Scarfone et al., 2008).

Table 4. Evaluation and comparison criteria from several studies (Cherdantseva et al., 2016; Giannopoulos et al., 2012; Ionita & Hartel, 2013; Meriah & Rabai, 2018; Qassim et al., 2019; Shahriar & Zulkernine, 2009).

(Qassim et al., 2019)	(Cherdantseva et al., 2016)	(Shahriar & Zulkernine, 2009)	(Ionita & Hartel, 2013)	(Giannopoulos et al., 2012)	(Meriah & Rabai, 2018)
Assessment mode (active or passive)	Aim	Test level	Class	Scope	Purpose
	Application domain	Source of test cases	Type (quantitative or qualitative)	Objectives	Outcome
Compliance to the NERC CIP requirements	Addressed phases and concepts of risk management	Test generation method	Type of target users (management, operational or technical)	Applied techniques and standards	Type of system application
Coverage of cybersecurity management processes	Impact assessment scheme	Vulnerability coverage	Supported risk assessment phases	Coverage of interdependencies	Inputs
	Sources of data for deriving probabilities	Granularity of test cases	Availability of supporting tools (paid, free)	Addressing of cross-sectoral risks	structure of the security management process
	Evaluation procedure	Tool automation	Release date	Target users	
	Availability of supporting tools	Application domain	Availability of a standalone version	Relevance to resilience	Supporting tools
			Price		
			Required skills		
			Sponsor		
			Focus		

Commonly adopted cybersecurity assessment frameworks describe social-engineering-related testing operations. The Information Systems Security Assessment Framework (ISSAF) explains several social engineering techniques to be applied during cybersecurity assessment. When evaluating compliance with *handling sensitive information* or *password storage* policies, testers are instructed to look for documents left on users' desktops, around office devices or to seek written down passwords, notepapers, or keys attached to monitors that enable opening lockers that often contain message pads with passwords. Also, they should approach users' workstations and check if they can access them due to users' negligence. Another technique recommended for detecting cybersecurity "incompliance" of employees is "shoulder surfing" i.e. stealthy observing users when they type in passwords on keyboards. Also, the fundamental social engineering activity i.e. wastepaper analysis is indicated to be performed during cybersecurity assessments (Rathore et al., 2006).

On a weekly basis, evaluators should call users and impersonate IT Helpdesk analysts to identify employees who would disclose their passwords. According to the framework, the employees should be dismissed from their work or at least severely sanctioned. The auditors can phone the audited organisation and present themselves as an employee requesting assistance. They may also act as a monitoring or maintenance unit and offer help in resolving some fictional problem. They may even cause a real system disruption to make the situation more realistic. In all the cases sensitive information from administrators or personnel in charge would be required (Rathore et al., 2006). The ISSAF framework instructs the evaluators not to inform the employees about the social engineering activities. Only the necessary personnel indicated in the organisation's procedures will be briefed on them. This is explained by the potential presence of "malicious insiders" in the organisation i.e. male employees that collaborate with attackers or are attackers themselves (Rathore et al., 2006).

Similarly the NIST Special Publication 800-115 "Technical Guide to Information Security Testing and Assessment" (Scarfone et al., 2008) indicates misrepresentation as a help desk worker or an employee that requests assistance to be employed during assessments. Also, phishing or sending e-mail with a malicious attachment is indicated in the guideline. The document reflects on the delicate nature of the exercise in the sense that it may cause unwanted bias and negative emotions among workers. Thus, the demand for conducting experiments in an indiscriminating way is emphasised.

The Open Source Security Testing Methodology Manual (OSSTMM) (Herzog, 2010) devotes Chapter 7 to testing human security. There, in section 7.6 *Trust Verification*, impersonating a member of the internal support or delivery personnel, a manager or external support or delivery agent is thought to determine users' susceptibility to reveal sensitive data based on social engineering attacks. Also, phishing exercises need to be performed in this respect. What is more, evaluating the organisation's resistance to extreme or mass reactions, such as revolt, violence or chaos caused by disruption of personnel and the use of misinformation or other psychological abuse is discussed. The Open Web Application Security Project (OWASP, 2020) Testing Guide points out social engineering steps when testing a web application's security. The Penetration Testing Execution Standard (PTES) (*PTES Technical Guidelines – The Penetration Testing Execution Standard*, 2019) directs to the Social-

Engineering Toolkit (SET) as a means for simulating social-engineering attacks and determining their effectiveness in a given environment.

These testing activities may raise serious doubts as to their ethical dimension. To address them, certain requirements to the analysis procedure are introduced. One of them is performing experiments in a controlled and secure way (Harper et al., 2018), so no damage is incurred. Another requires obtaining the authorisation for carrying out the tests from the analysed organisation and involved parties (e.g. employees or contractors) (Oriyano, 2017). Within the latter boundaries, the activity should become an *"ethical" hacking*. The former is associated with so-called *penetration testing* (Dalalana Bertoglio & Zorzo, 2017; Gordon, 2016; Oriyano, 2017). Penetration testers use the techniques of malicious attackers, but in a controlled and safe manner (Harper et al., 2018). These "ethicising" operations influence the course of experiments and may have an impact on the results. While the ethical component needs to be considered when planning the testing exercises, a proper balance between these two dimensions needs to be found by each individual organisation. The decision can be facilitated by providing the ethical "parameters" of a cybersecurity assessment framework. Such parameters, for instance, could take the form of an ethical discussion of each assessment activity. The presence of the ethical attributes needs to be taken into account when selecting a specific solution.

5 Criteria for choosing a cybersecurity solution

In this section, a consolidated set of criteria derived from the publications identified during the literature review is proposed. The criteria should help in choosing a cybersecurity solution. They are presented in Tables 5-11. Table 5 comprises selection criteria that facilitate a quick decision on a method choice. The criteria include the presence of the discussion of ethical questions in the documentation of a method.

Table 5. Selection criteria.

Focus and scope	Release	Documentation	Application
Particular focus	Publication by a standard body or governmental agency	Documentation in a specific language	Implementation or application in a particular sector or domain
Specific audience	Scientific, cybersecurity-related origin	Detailed descriptions	Application to an existing system or a system design
Coverage of particular risk subjects	Timeliness	Documentation in a peer-reviewed paper	Practical application in more than one country
Coverage of all assessment processes	Availability free of charge	Discussion of ethical questions	
Coverage of specific assessment processes		Large number of citations	
Coverage of a model-based security testing approach			

Tables 6-11 contain criteria that enable more detailed analyses and comparisons between various frameworks. They are related to the scope, application, design, compliance and specific features of the solutions. The criteria are provided with literature references, where their definitions and descriptions can be found. Based on the discussion presented in Section 4, the ethical criterion related to the discussion of security assessment activities has been introduced into the group of application-related criteria.

Table 6. Scope-related criteria.

Criterion	Reference
Aim	(Cherdantseva et al., 2016)
Scope	(Fabisiak et al., 2012; Giannopoulos et al., 2012; Gritzalis et al., 2018)
Objectives	(Giannopoulos et al., 2012)
Purpose	(Meriah & Rabai, 2018)
Focus	(Gritzalis et al., 2018; Ionita & Hartel, 2013)
Inputs	(Meriah & Rabai, 2018)
Outcome	(Meriah & Rabai, 2018)
Type (quantitative or qualitative)	(Fabisiak et al., 2012; Ionita & Hartel, 2013)

Table 7. Application-related criteria.

Criterion	Reference
Release (date)	(Gritzalis et al., 2018; Ionita & Hartel, 2013)
Last update	(Gritzalis et al., 2018)
Application domain	(Cherdantseva et al., 2016; Shahriar & Zulkernine, 2009)
Type of system application	(Meriah & Rabai, 2018)
Target users	(Fabisiak et al., 2012; Giannopoulos et al., 2012; Ionita & Hartel, 2013)
Target organisation (type, size)	(Gritzalis et al., 2018)
Availability of a standalone version	(Ionita & Hartel, 2013)
Availability of supporting tools (paid, free)	(Cherdantseva et al., 2016; Ionita & Hartel, 2013; Meriah & Rabai, 2018)
Software support	(Gritzalis et al., 2018)
Tool automation	(Shahriar & Zulkernine, 2009)
Required skills	(Ionita & Hartel, 2013)
Training	(Gritzalis et al., 2018)
Popularity	(Fabisiak et al., 2012)
National standard	(Fabisiak et al., 2012)

International standard	(Fabisiak et al., 2012)
English documentation	(Fabisiak et al., 2012)
Ethical discussion of individual assessment activities	
Cost	(Fabisiak et al., 2012; Gritzalis et al., 2018)
Price	(Ionita & Hartel, 2013)
Support cost	(Fabisiak et al., 2012)
Software cost	(Fabisiak et al., 2012)
Sponsor	(Ionita & Hartel, 2013)

Table 8. Criteria related to detailed design features of a solution.

Criterion	Reference	Criterion	Reference
Impact assessment scheme	(Cherdantseva et al., 2016)	Number of probability levels	(Fabisiak et al., 2012)
Sources of data for deriving probabilities		Basis for cause estimation	
Evaluation procedure		Number of cause levels	
Source of test cases	(Shahriar & Zulkernine, 2009)	Cause metric	
Test generation method		Probability metric	
Vulnerability coverage		Risk metric	
Method of risk identification	(Fabisiak et al., 2012)	Choice of countermeasures	
Risk completeness verification		Analysis of countermeasures' dependencies	
Number of standard scenarios		Analysis of countermeasures' influence	
Analysis of scenarios dependencies		Estimation of risk treatment efficiency	
Data gathering method		Detection of new risks	
Data verification		Automatic correction of dependent risk	
Basis for risk calculation		Structure of the security management process	(Meriah & Rabai, 2018)
Number of risk levels		Addressed phases and concepts of risk management	(Cherdantseva et al., 2016; Gritzalis et al., 2018; Ionita & Hartel, 2013; Qassim et al., 2019)
Basis for probability estimation		Risk calculation class	(Gritzalis et al., 2018; Ionita & Hartel, 2013)

Table 9. Compliance criteria.

Criterion	Reference
Declared compliance with standards	(Fabisiak et al., 2012; Gritzalis et al., 2018)
Applied techniques and standards	(Giannopoulos et al., 2012)
Compliance to the NERC CIP requirements	(Qassim et al., 2019)

Table 10. Criteria related to general characteristics of a solution.

Criterion	Reference
Completeness	(Gritzalis et al., 2018)
Adaptability	(Fabisiak et al., 2012; Gritzalis et al., 2018)
Usability (Interface, handle errors, documentation)	(Gritzalis et al., 2018)
Ease of use	(Gritzalis et al., 2018)
Sophistication of usage/implementation	(Fabisiak et al., 2012)
Flexibility	(Fabisiak et al., 2012)
Validity	(Gritzalis et al., 2018)
Usefulness	(Gritzalis et al., 2018)

Table 11. Criteria related to additional features of a solution.

Criterion	Reference
Coverage of interdependencies	(Giannopoulos et al., 2012)
Addressing of cross-sectoral risks	(Giannopoulos et al., 2012)
Support for security policy framework generation	(Fabisiak et al., 2012)
Procedures generation support	(Fabisiak et al., 2012)
Risk monitoring	(Fabisiak et al., 2012)

6 Conclusions

Based on a systematic literature review process around ninety criteria that facilitate an informed choice of a cybersecurity management solution have been identified. The criteria have been consolidated into selection criteria that enable a quick choice of a framework primarily based on its scope and applicability to a specific domain. In addition, six groups of attributes have been distinguished that support thorough analyses and comparisons between different solutions. The six categories are related to the scope, application (including the cost), design features, compliance, general characteristics and supplementary features of a proposal. Around eighty different criteria have been classified into the categories.

Cybersecurity assessment methodologies may include activities that raise ethical questions. Widely used cybersecurity guidelines instruct to emulate hacking techniques to identify vulnerabilities in the organisation's cybersecurity posture. Even more, with the aim of verifying the resistance of employees to social engineering, exercises that employ this hacking technique are advised. Namely, the testers should try to manipulate individuals to perform specific actions or to reveal sensitive information. In this way, the level of cybersecurity awareness and the weaknesses in user behaviour can be identified. Although valuable from the point of cybersecurity, it can have a negative impact on social relations, the level of trust in the organisation and individual situations of employees. For these reasons, the ethically questionable activities need to be

transparently indicated in cybersecurity assessment frameworks and the associated ethical component discussed. Consequently, criteria related to the ethical application of a methodology have been proposed and included in the consolidated set.

References

Accenture. (2021a). *2021 Cyber Threat Intelligence Report* (Issue July). Accenture.

Accenture. (2021b). *Technology Vision 2021*.

Alcaraz, C., & Lopez, J. (2013). Wide-area situational awareness for critical infrastructure protection. *Computer*, *46*(4), 30–37. https://doi.org/10.1109/MC.2013.72

Barrere, M., Badonnel, R., & Festor, O. (2014). Vulnerability assessment in autonomic networks and services: A survey. *IEEE Communications Surveys and Tutorials*, *16*(2), 988–1004. https://doi.org/10.1109/SURV.2013.082713.00154

Bolzoni, D., Leszczyna, R., Wróbel, M. R., & Wrobel, M. R. (2016). Situational Awareness Network for the electric power system: The architecture and testing metrics. In M. Ganzha, L. Maciaszek, & M. Paprzycki (Eds.), *Proceedings of the 2016 Federated Conference on Computer Science and Information Systems, FedCSIS 2016* (pp. 743–749). IEEE. https://doi.org/10.15439/2016F50

Cherdantseva, Y., Burnap, P., Blyth, A., Eden, P., Jones, K., Soulsby, H., & Stoddart, K. (2016). A review of cyber security risk assessment methods for SCADA systems. *Computers & Security*, *56*, 1–27. https://doi.org/https://doi.org/10.1016/j.cose.2015.09.009

Dalalana Bertoglio, D., & Zorzo, A. F. (2017). Overview and open issues on penetration test. *Journal of the Brazilian Computer Society*, *23*(1), 1–16. https://doi.org/10.1186/s13173-017-0051-1

Deloitte Insights. (2021). *Tech Trends 2022*.

Duggal, N. (2021, December 7). *Top 9 New Technology Trends for 2022*. https://www.simplilearn.com/top-technology-trends-and-jobs-article#9_cyber_security

ENISA. (2021). *ENISA Threat Landscape 2021* (Issue October). ENISA. https://doi.org/10.2824/324797

Fabisiak, L., Hyla, T., & Klasa, T. (2012). Comparative Analysis of Information Security Assessment and Management Methods. *Studia i Materialy Polskiego Stowarzyszenia Zarzadzania Wiedza / Studies & Proceedings Polish Association for Knowledge Management*, *60*, 55–70.

Felderer, M., & Schieferdecker, I. (2014). A taxonomy of risk-based testing. *International Journal on Software Tools for Technology Transfer*, *16*(5), 559–568. https://doi.org/10.1007/s10009-014-0332-3

Felderer, M., Zech, P., Breu, R., Büchler, M., & Pretschner, A. (2016). Model-based security testing: A taxonomy and systematic classification. *Software Testing Verification and*

Reliability, *26*(2), 119–148. https://doi.org/10.1002/stvr.1580

Giannopoulos, G., Filippini, R., & Schimmer, M. (2012). Risk assessment methodologies for Critical Infrastructure Protection. Part I: A state of the art. In *European Commission JRC (Joint Research Center) Technical notes.* https://doi.org/10.2788/22260

Gordon, A. (2016). The Official (ISC) 2® Guide to the CCSP SM CBK ®. In *The Official (ISC) 2® Guide to the CCSP SM CBK ®*. John Wiley & Sons, Inc. https://doi.org/10.1002/9781119419198

Gritzalis, D., Iseppi, G., Mylonas, A., & Stavrou, V. (2018). Exiting the risk assessment maze: A meta-survey. *ACM Computing Surveys*, *51*(1), 1–30. https://doi.org/10.1145/3145905

Hahn, A., & Govindarasu, M. (2011). An evaluation of cybersecurity assessment tools on a SCADA environment. *IEEE Power and Energy Society General Meeting*. https://doi.org/10.1109/PES.2011.6039845

Harper, A., Regalado, D., Linn, R., Sims, S., Spasojevic, B., Martinez, L., Baucom, M., Eagle, C., & Harris, S. (2018). *Gray hat hacking: the ethical hacker's handbook* (Fifth). McGraw-Hill Education.

Herzog, P. (2010). *OSSTMM 3 - The Open Source Security Testing Methodology Manual*. http://www.isecom.org/mirror/OSSTMM.3.pdf

Holm, H., Sommestad, T., Almroth, J., & Persson, M. (2011). A quantitative evaluation of vulnerability scanning. *Information Management and Computer Security*, *19*(4), 231–247. https://doi.org/10.1108/09685221111173058

Ionita, D., & Hartel, P. (2013). *Current Established Risk Assessment Methodologies and Tools*.

ISO/IEC. (2013). ISO/IEC 27001:2013: Information technology -- Security techniques -- Information security management systems -- Requirements. In *ISO/IEC 27001* (p. 23).

ISO/IEC. (2018). *ISO/IEC:2018 Information technology — Security techniques — Information security management systems — Overview and: Vol. 5th edit* (p. 38).

Kitchenham, B., & Brereton, P. (2013). A systematic review of systematic review process research in software engineering. *Information and Software Technology*, *55*(12), 2049–2075. https://doi.org/https://doi.org/10.1016/j.infsof.2013.07.010

Klimburg-Witjes, N., & Wentland, A. (2021). Hacking Humans? Social Engineering and the Construction of the "Deficient User" in Cybersecurity Discourses. *Science, Technology & Human Values*, *46*(6), 1316–1339. https://search.ebscohost.com/login.aspx?direct=true&db=bsu&AN=152626306&lang=pl&site=ehost-live&scope=site

Leszczyna, R. (2021). Review of cybersecurity assessment methods: Applicability perspective. *Computers & Security*, *108*, 102376. https://doi.org/10.1016/J.COSE.2021.102376

Leszczyna, R., Wallis, T., & Wróbel, M. R. (2019). Developing novel solutions to realise the European Energy – Information Sharing & Analysis Centre. *Decision Support Systems*, *122*. https://doi.org/10.1016/j.dss.2019.05.007

Leszczyna, R., & Wróbel, M. R. (2019). Threat intelligence platform for the energy sector. *Software: Practice & Experience*.

Li, J., Beba, S., & Karlsen, M. M. (2019). Evaluation of open-source IDE plugins for detecting security vulnerabilities. *ACM International Conference Proceeding Series*, 200–209. https://doi.org/10.1145/3319008.3319011

Lohani, S. (2019). Social Engineering: Hacking into Humans. *International Journal of Advanced Studies of Scientific Research*, *4*(1).

Lykou, G., Anagnostopoulou, A., Stergiopoulos, G., & Gritzalis, D. (2019). Cybersecurity self-assessment tools: Evaluating the importance for securing industrial control systems in critical infrastructures. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 11260 LNCS*, 129–142. https://doi.org/10.1007/978-3-030-05849-4_10

McKinsey & Company. (2021). *The top trends in tech - executive summary*.

Meriah, I., & Rabai, L. B. A. (2018). A survey of quantitative security risk analysis models for computer systems. *Proceedings of the 2nd International Conference on Advances in Artificial Intelligence (ICAAI 2018)*, 36–40. https://doi.org/10.1145/3292448.3292456

NIST. (2011). NIST SP 800-39 Managing Information Security Risk Organization, Mission, and Information System View. In *Nist Special Publication* (Issue March). http://csrc.nist.gov/publications/nistpubs/800-39/SP800-39-final.pdf

Oriyano, S.-P. (2017). Penetration Testing Essentials. In *Penetration Testing Essentials*. John Wiley & Sons, Inc. https://doi.org/10.1002/9781119419358

OWASP. (2020). *OWASP Testing Guide v4.2*. https://github.com/OWASP/wstg/releases/download/v4.2/wstg-v4.2.pdf

PTES Technical Guidelines -- The Penetration Testing Execution Standard. (2019). http://www.pentest-standard.org

Qassim, Q. S., Jamil, N., Daud, M., Patel, A., & Ja'affar, N. (2019). A review of security assessment methodologies in industrial control systems. *Information and Computer Security*, *27*(1), 47–61. https://doi.org/10.1108/ICS-04-2018-0048

Rathore, B., Brunner, M., Dilaj, M., Herrera, O., Brunati, P., Subramaniam, R. K., Raman, S., & Chavan, U. (2006). *Information Systems Security Assessment Framework (ISSAF) Draft 0.2.1B*.

Rogers, R., & Syngress Media, I. (2004). *Security assessment: case studies for implementing the NSA IAM*. Syngress.

Sargent, S. A., & Webb, J. P. (2020). The Key to Trust: Social Engineering Fraud and Modern Threat Detection. *Benefits Magazine*, *57*(1).

Scarfone, K., Souppaya, M., Cody, A., & Orebaugh, A. (2008). *NIST SP 800-115 Technical Guide to Information Security Testing and Assessment*. NIST.

Shah, S., & Mehtre, B. M. (2015). An overview of vulnerability assessment and penetration

testing techniques. *Journal of Computer Virology and Hacking Techniques*, *11*(1), 27–49. https://doi.org/10.1007/s11416-014-0231-x

Shahriar, H., & Zulkernine, M. (2009). Automatic testing of program security vulnerabilities. *Proceedings - International Computer Software and Applications Conference*, *2*, 550–555. https://doi.org/10.1109/COMPSAC.2009.191

Sophos. (2021). *The State of Ransomware 2021* (Issue April). Sophos. https://doi.org/10.2824/324797

Tadda, G. P., & Salerno, J. S. (2010). Overview of Cyber Situational Awareness. In S. Jajodia, P. Liu, V. Swarup, & C. Wang (Eds.), *Cyber Situational Awareness* (Vol. 46, pp. 15–35). Springer US. https://doi.org/10.1007/978-1-4419-0140-8

Vallor, S., & Rewak, W. J. (2018). *An Introduction to Cybersecurity Ethics*. https://www.scu.edu/ethics/focus-areas/technology-ethics/resources/an-introduction-to-cybersecurity-ethics/

Wangen, G., Hallstensen, C., & Snekkenes, E. (2018). A framework for estimating information security risk assessment method completeness: Core Unified Risk Framework, CURF. *International Journal of Information Security*, *17*(6), 681–699. https://doi.org/10.1007/s10207-017-0382-0

Webster, J., & Watson, R. T. (2002). Analyzing the past to prepare for the future: writing a literature review. *MIS Quarterly*, *26*(2), xiii–xxiii.

Weiss, S. (2008). Industrial approaches and standards for security assessment. In I. Eusgeld, F. C. Freiling, & R. Reussner (Eds.), *Dependability Metrics: Vol. 4909 LNCS* (pp. 166–175). https://doi.org/10.1007/978-3-540-68947-8_14