Selecting an Applicable Cybersecurity Assessment Framework: Qualitative Metrics-Based Multiple-Factor Analysis

Rafał Leszczyna

Gdańsk University of Technology, Narutowicza 11/12, Gdańsk, 80-952, Poland.

Corresponding author(s). E-mail(s): rle@zie.pg.edu.pl;

Abstract

Recently a survey of cybersecurity assessment methods focused on general characteristics was conducted. Among its major findings, it revealed the methods' adoption issues. This paper presents a follow-up to the study. It provides an in-depth analysis of the methods' adoption-related properties based on qualitative metrics. As a result, the proposals which demonstrate a higher adoption potential were identified. The methods are good candidates for first-order improvements that would lead to obtaining solutions that would ultimately meet a broader application. The evaluations were performed by a single analyst, based on descriptions and individual observations. The major contribution of the study is related to providing a new view on method characteristics in reference to a systematic set of qualitative metrics and showing a path to selecting the method most suitable to a given context in terms of applicability and usability.

Keywords: security evaluation, usable cybersecurity, acceptance, organizational management, review

1 Introduction

Societies and economies rely on cyberspace and its core components. With the significantly increasing impact a cyberthreat can have on business nowadays [1–6], it is essential that cybersecurity measures deployed in organizations adequately respond to the risk context. In this respect, *cybersecurity assessments* play a crucial role.

Cybersecurity assessment is comprehensive examination of the entire cyber environment in an organization, including all computer devices, the communication infrastructure and software. It aims at determining if the organization is appropriately protected from cyberthreats or if there are vulnerabilities that may be potentially exploited. An important aspect of a cybersecurity assessment regards verification if cybersecurity controls have been implemented correctly and they work as intended [7–9]. The cybersecurity measures include technical, such as protection from malicious software or user authentication, but also organizational that are more focused on the human component and among the others refer to training and awareness raising.

Multiple methods that support the assessment have been proposed by scientific communities. This paper presents the results of the continuation of the study that aims at identifying the methods with the highest applicability potential i.e. the highest readiness for being directly applied in an organization. The research started with identifying the determinants of the applicability and introducing its taxonomy and metrics [10]. This was followed by a systematic literature analysis that led to the recognition of thirty-two methods proposed in academic and research environments. The methods were analyzed concerning the evaluation criteria that regarded the purpose, structure and selected applicability features (the documentation level of detail, required skills, real-world application, method's evaluation procedure and supporting tools) [11].

The follow-up study presented in this paper aimed at a more in-depth analysis of the methods based on qualitative metrics and eliciting the methods with the highest adoption potential. The methods could become good candidates for first-order improvements that would lead to obtaining solutions that would ultimately meet the broad application. The analysis is subjective, based on the method characteristics, literature descriptions, and the expertise and perceptions of one appraiser. The added component of qualitative metrics-based multiple-factor analysis aims at providing a new dimension to the methods' analysis to facilitate the selection of the method that is the most complementary to the analyzed environment in terms of usability and applicability. The main contributions of this study in reference to the previous research are summarized in Table 1.

The rest of the article is organized as follows. The research method applied in the study is explained in the next section. Section 3 describes the analysis of cybersecurity assessment methods based on 19 qualitative applicability metrics, including the construction of the methods' ranking according to values of complexity, usability, and acceptance metrics. This is followed by an in-depth

Table 1: The main contributions of the study in reference to the previous research.

Previous work	Ref.	The contribution of the current study
31 applicability determinants elicited Applicability taxonomy proposed 15 quantitative and 19 qualitative applicability metrics introduced	[10] [10] [10]	29 cybersecurity assessment methods subjected to a multiple factor analysis based on 19 qualitative applicability metrics
Dedicated questionnaire consisting of 22 questions of six different types designed	[10]	The methods with higher adoption potential elicited
Preliminary validation of internal reliability of the questionnaire	[10]	The ranking of methods according to applicability metrics' values developed
32 cybersecurity assessment methods proposed by scientific environments analyzed	[11]	The first ten methods from the ranking examined in more detail
Applicability control list developed	[35]	Findings and further research areas of improvement described
The checklist applied to evaluate EE-ISAC	[35]	A primary candidate method for direct use or further improvements indicated

study of the top ten methods in the ranking (Section 4). The main findings are presented in Section 5. The paper ends with concluding remarks.

2 Research method

The main activities involved in the research are summarized in Figure 1. There, the contribution of the study described in this paper is expressly depicted.

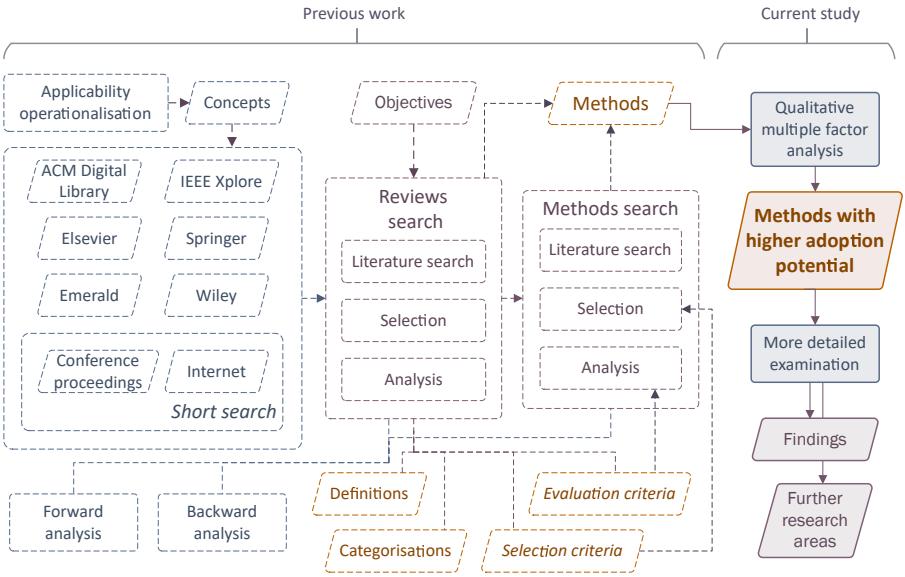

Fig. 1: The key tasks and data sources employed during the research with the demarcation between previous works and the study described in this paper.

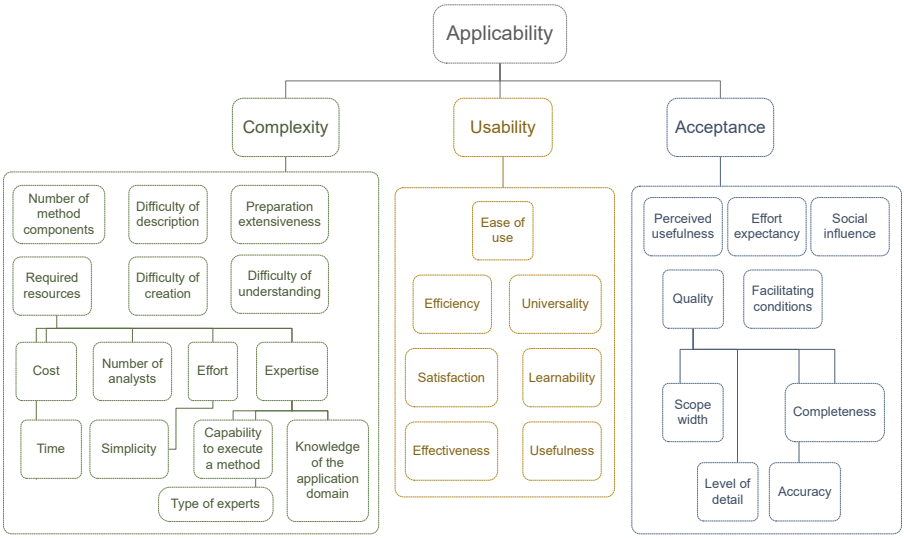

Fig. 2: Applicability taxonomy.

The research started with the operationalization of the applicability concept that led to the identification of three fundamental constituents of applicability, namely complexity, usability, and acceptance. Based on that, applicability determinants were distinguished. They enabled formulation of the applicability taxonomy (see Figure 2). Also, fifteen quantitative and nineteen qualitative applicability metrics were introduced and a dedicated questionnaire consisting of twenty-two questions in six different categories was designed and preliminarily validated[10]. With these conceptual grounds established, the analysis of cybersecurity assessment methods from the applicability perspective could commence.

The cybersecurity assessment methods were identified during a systematic literature review process that implemented Webster's and Watson's[12] as well as Kitchenham's and Brereton's[13] guidelines[11]. The two main components of the process embraced the *reviews search* which aimed at identifying potential alternative reviews and the *methods search* when individual proposals were searched for directly. Each of the stages contained three main activities i.e. the literature search, selection, and analysis, during which relevant criteria were applied. The data were grouped according to the *evaluation criteria* and analyzed[11].

In the follow-up study described in this paper, the methods were subjected to a multiple-factor analysis based on 19 qualitative applicability metrics. The choice of qualitative metrics before the quantitative ones was driven by the availability of data and the feasibility questions. At the same time, the evaluation based on the remaining quantitative 15 metrics, including the cost, time, quantified efficiency, and effectiveness, constitutes a prospective direction of future studies. However, it needs to be noted that it will call for substantial

resources as obtaining the proper values of the metrics requires dedicated, mostly complex experiments. The qualitative analysis enabled the elicitation of the best candidates for early adoption or promising improvements. These methods were analyzed more in detail. Findings and further research areas of improvement were described. A primary candidate method for direct use or further improvements was indicated.

3 Applicability of cybersecurity assessment methods

The general review of cybersecurity assessment methods[11] revealed that the application of the methods in practical environments was very limited. If a method was implemented, its deployment did not go beyond a pilot, a demonstrator, some hypothetical scenario, or other basic configuration. The initial analysis of selected applicability features of the methods, namely the documentation level of detail, required skills, real-world application, method's evaluation procedure, and supporting tools indicated that for a method to be more widely adopted, its applicability properties required better addressing. Applicability is the quality of being applicable or suitability to be implemented[10]. The taxonomy that shows primary determinants of applicability[10] is presented in Figure 2. This section describes further analysis of the methods based on 19 qualitative applicability metrics. The analysis was carried out to more precisely determine the areas of improvement and to identify the methods that demonstrate a higher adoption potential.

3.1 Qualitative metrics-based assessment

The metrics utilized during the analysis are summarized in Table 2. They include positive metrics that are positively correlated with applicability and negative ones, for which the correlation occurs but is negative. For instance, *accuracy* is a positive metric, because the more methods are accurate, the higher their chances of being applied. An example of a negative metric is preparation extensiveness. The more broad and labor-intensive preparation activities before using a method, the greater users' reluctance to apply the method.

For each metric, a subjective *quality value* in a 7-level scale was assigned. The outcome of the analysis is summarized in Tables 3 and 4. Table 3 groups the metrics associated with the complexity aspect of applicability, while Table 4 focuses on the usability and acceptance dimensions. The cell colors in the tables reflect the level of positive/negative influence on the applicability. The colors range from dark red, through yellow, to dark green. For positive metrics, dark red color indicates the lowest influence (quality value 1), while dark green illustrates the highest positive influence (quality value 7). For negative metrics, the dark red color shows the highest negative impact on the applicability (quality value 7), and the dark green depicts the lowest negative effect (quality value 1).

Table 2: Applicability qualitative metrics. Source: [10].

Metric	Description
Acceptance	
Perceived usefulness	Users' subjective perception of the likelihood that using the method will increase their performance within a specific context
Effort expectancy	Users' expectation of the effort required to utilize the method
Social influence	Users' perception of the importance that others assign to them using the method
Completeness	The degree of the method's comprehensiveness in tackling the entire addressed problem
Level of detail	The precision with which the method approaches the addressed problem
Scope width	The broadness of the application domain
Accuracy	The precision of results obtained with the method
Usability	
Satisfaction	Subjective opinions of experts regarding their impressions on using the method
Universality	The method's capacity to accommodate a diversity of users with different experience, knowledge and expertise
Ease of use	The method's capability to solve real problems in an acceptable way, it implies practical utility the method
Complexity	
Effort	The effort associated with applying the method
Expertise	Proficiency required for using the method
Simplicity	Straightforward usage of the method
Capability to execute a method	Experts' operational capabilities to apply the method
Knowledge of the application domain	Experts' familiarity with the problem area
Difficulty of creation	The degree of difficulty associated with constructing or duplicating a method
Difficulty of description	The degree to which a method is difficult to describe
Difficulty of understanding	The degree to which a method is difficult to comprehend
Preparation extensiveness	Broadness and labor intensity of preparation activities before using the method

3.2 Comparative analysis

To compare the methods a multiple factor analysis was carried out. The aggregation function M_A used in the analysis is presented in Equation 1. Its value is calculated by deducing the sum of the unweighted values for negative metrics from the sum of the unweighted values obtained with positive metrics.

$$M_A = \sum M_P - \sum M_N \tag{1}$$

Where: M_A – applicability metrics' aggregation function, M_P – positive metric, M_N' – negative' metric.

Table 5 summarizes the results of the calculations. There, the sums of values of positive and negative metrics and the relevant aggregators are provided separately for complexity, usability, and acceptance as well as usability. The compilation enables comparing the methods but also observing the contribution of methods' properties in different areas of applicability to the overall adoption potential. To facilitate the selection of methods, in Table 6 the methods are enlisted in order of decreasing values of the applicability metrics' aggregation function.

Table 3: Complexity values. Positive metrics are indicated with (+), and negative ones with (-). Scale: 1-very low, 2-low, 3-fairly low, 4-medium, 5-fairly high, 6-high and 7-very high. The cell colors reflect the level of positive/negative influence on the applicability. For positive metrics, dark red color indicates the lowest influence (quality value 1), while dark green illustrates the highest positive influence (quality value 7). For negative metrics, the dark red color shows the highest negative impact on the applicability (quality value 7), and the dark green depicts the lowest negative effect (quality value 1).

Method	Effort (-)	Expertize (-)	Simplicity (+)	Capability to execute a method (-)	Knowledge of the application domain (-)	Dificulty of creation (-)	Dificulty of description (-)	Dificulty of understanding (-)	Preparation extensiveness (-)
Checklist-based methods									
Advanced security measurement tailored to the organization's business profile [25]	5	6	4	5	5	3	4	5	4
Cyber-Physical IT Vulnerability Assessment for Semiconductor Companies [14]	4	5	5	3	5	3	3	2	3
Operational framework for security capability assessment [16]	5	4	4	3	5	3	3	3	3
Analytical Processing Approach to Supporting Cyber Security Compliance Assessment [17]	5	5	4	4	5	3	4	4	4
Rough set-based security assessment method [36]	6	7	2	6	5	5	6	6	5
Security compliance monitoring [37]	6	5	3	5	5	3	4	3	5
Security assessment approach for Internet banking services [38]	7	7	1	7	7	5	7	5	7
Vulnerability identification and analysis methods									
Work flow-oriented security assessment [39]	7	7	2	6	6	4	4	5	7
First principles vulnerabilities assessment [40]	7	7	3	7	7	5	5	5	7
Ovaldroid [41]	7	7	4	6	6	4	5	5	7
Bayesian attack graph-based quantitative assessment [42]	7	7	3	7	6	4	5	6	7
AI and Metrics-Based Vulnerability-Centric Cyber Security Assessment [43]	7	7	3	7	6	4	5	6	7
Ruckus [34]	6	7	3	7	7	4	3	2	6
Network security situation assessment method based on deep learning [44]	7	7	3	6	6	4	4	4	7
Online and offline security policy assessment [27]	6	6	4	6	6	5	4	4	6
Penetration testing methods									
Standardised method to cybersecurity assessments of critical infrastructures	6	7	2	6	6	3	3	2	6
Risk-based testing [23]	6	6	4	6	6	4	4	2	6
Structured Security Assessment Methodology for Manufacturers of Critical Infrastructure Components [18]	5	6	4	6	6	4	3	2	5
Cyberassessment method for SCADA security [45]	6	6	4	6	6	4	3	2	6
NetSecuritas [46]	7	6	2	6	6	5	5	5	7
Simulation-based methods									
Approach to security assessment of critical infrastructures [47]	7	7	2	6	6	3	3	2	7
Assessment/analysis platform for Multiple Interdependent Critical Infrastructures (AMICI) [48]	7	7	3	6	6	4	4	2	7
Cyber-physical security assessment [49]	7	7	3	6	6	3	3	3	7
Smart grids assessment through simulation [50]	7	7	3	6	6	4	5	5	7
Model-based methods									
Mission Oriented Network Analysis (MONA) [51]	7	6	2	6	6	5	6	6	7
Service-oriented approach for assessing critical infrastructure security [33]	6	6	4	5	6	5	5	4	6
General method for assessment of security in complex services [52]	7	7	1	7	6	7	7	7	7
Cybersecurity assessment of cyber-physical systems using Discrete Time Markov Chain model-based simulations [53]	6	6	2	6	6	5	6	6	6
Testing Security for Systems of Systems (TeSSoS) [54]	7	5	2	6	6	5	5	5	6

Table 4: Usability and acceptance values. Positive metrics are indicated with (+), and negative ones with (-). Scale: 1-very low, 2-low, 3-fairly low, 4-medium, 5-fairly high, 6-high and 7-very high. The cell colors reflect the level of positive/negative influence on the applicability. For positive metrics, dark red color indicates the lowest influence (quality value 1), while dark green illustrates the highest positive influence (quality value 7). For negative metrics, the dark red color shows the highest negative impact on the applicability (quality value 7), and the dark green depicts the lowest negative effect (quality value 1).

Method	Satisfaction (+)	Universality (+)	Ease of use (+)	Perceived usefulness(+)	Effort expectancy (-)	Social influence (+)	Completeness (+)	Level of detail (+)	Scope width (+)	Accuracy (+)
Checklist-based methods										
Advanced security measurement tailored to the organisation's business profile [25]	6	4	3	6	5	6	5	3	6	4
Cyber-Physical IT Vulnerability Assessment for Semiconductor Companies [14]	3	4	6	3	4	3	2	3	2	3
Operational framework for security capability assessment [16]	4	4	5	6	5	6	5	3	5	4
Analytical Processing Approach to Supporting Cyber Security Compliance Assessment [17]	6	4	5	6	5	6	6	3	6	4
Rough set-based security assessment method [36]	4	3	2	2	7	4	4	3	2	4
Security compliance monitoring [37]	3	4	3	3	6	5	4	3	6	4
Security assessment approach for Internet banking services [38]	5	1	3	7	4	6	4	4	1	7
Vulnerability identification and analysis methods										
Work flow-oriented security assessment [39]	5	3	3	4	6	5	5	6	6	5
First principles vulnerabilities assessment [40]	7	3	4	3	7	5	6	6	6	6
Ovaldroid [41]	5	3	4	5	6	4	5	6	3	6
Bayesian attack graph-based quantitative assessment [42]	5	3	3	5	6	4	5	5	5	5
AI and Metrics-Based Vulnerability-Centric Cyber Security Assessment [43]	5	3	3	5	6	4	6	5	5	5
Ruckus [34]	7	3	4	5	5	5	6	6	4	6
Network security situation assessment method based on deep learning [44]	4	3	4	5	6	4	6	6	5	4
Online and offline security policy assessment [27]	5	2	4	6	5	6	5	7	6	7
Penetration testing methods										
Standardised method to cybersecurity assessments of critical infrastructures [28]	7	3	4	6	6	5	6	6	3	6
Risk-based testing [23]	7	3	4	6	6	4	7	6	6	6
Structured Security Assessment Methodology for Manufacturers of Critical Infrastructure Components [18]	7	4	3	7	5	6	6	6	2	6
Cyberassessment method for SCADA security [45]	5	3	4	6	6	5	4	6	3	6
NetSecuritas [46]	4	3	3	4	6	4	7	6	6	6
Simulation-based methods										
Approach to security assessment of critical infrastructures [47]	6	3	3	7	6	5	7	7	7	7
Assessment/analysis platform for Multiple Interdependent Critical Infrastructures (AMICI) [48]	7	5	4	7	5	7	5	7	5	6
Cyber-physical security assessment [49]	5	4	5	6	5	7	5	6	5	4
Smart grids assessment through simulation [50]	7	1	5	6	5	7	5	6	1	4
Model-based methods										
Mission Oriented Network Analysis (MONA) [51]	4	3	3	4	6	4	6	5	5	5
Service-oriented approach for assessing critical infrastructure security [33]	5	3	4	5	5	5	7	6	6	6
General method for assessment of security in complex services [52]	3	1	1	1	7	5	6	4	4	4
Cybersecurity assessment of cyber-physical systems using Discrete Time Markov Chain model-based simulations [53]	4	3	3	4	6	4	5	5	2	5
Testing Security for Systems of Systems (TeSSoS) [54]	5	3	2	4	7	5	7	6	6	6

Table 5: Cumulative values of complexity, usability and acceptance metrics.

Method	Complexity			Usability			Acceptance			All		
	$\sum M_{PC}$	$\sum M_{NC}$	M_{AC}	$\sum M_{PU}$	$\sum M_{NU}$	M_{AU}	$\sum M_{PA}$	$\sum M_{NA}$	M_{AA}	$\sum M_P$	$\sum M_N$	M_A
Checklist-based methods												
Advanced security measurement tailored to the organisation's business profile [25]	4	37	-33	13	0	13	30	5	25	47	42	5
Cyber-Physical IT Vulnerability Assessment for Semiconductor Companies [14]	5	28	-23	13	0	13	16	4	12	34	32	2
Operational framework for security capability assessment [16]	4	29	-25	13	0	13	29	5	24	46	34	12
Analytical Processing Approach to Supporting Cyber Security Compliance Assessment [17]	4	34	-30	15	0	15	31	5	26	50	39	11
Rough set-based security assessment method [36]	2	46	-44	9	0	9	19	7	12	30	53	-23
Security compliance monitoring [37]	3	36	-33	10	0	10	25	6	19	38	42	-4
Security assessment approach for Internet banking services [38]	1	52	-51	9	0	9	29	4	25	39	56	-17
Vulnerability identification and analysis methods												
Work flow-oriented security assessment [39]	2	46	-44	11	0	11	31	6	25	44	52	-8
First principles vulnerabilities assessment [40]	3	50	-47	14	0	14	32	7	25	49	57	-8
Ovaldroid [41]	4	47	-43	12	0	12	29	6	23	45	53	-8
Bayesian attack graph-based quantitative assessment [42]	3	49	-46	11	0	11	29	6	23	43	55	-12
AI and Metrics-Based Vulnerability-Centric Cyber Security Assessment [43]	3	49	-46	11	0	11	30	6	24	44	55	-11
Ruckus [34]	3	42	-39	14	0	14	32	5	27	49	47	2
Network security situation assessment method based on deep learning [44]	3	45	-42	11	0	11	30	6	24	44	51	-7
Online and offline security policy assessment [27]	4	43	-39	11	0	11	37	5	32	52	48	4
Penetration testing methods												
Standardised method to cybersecurity assessments of critical infrastructures [28]	2	39	-37	14	0	14	32	6	26	48	45	3
Risk-based testing [23]	4	40	-36	14	0	14	35	6	29	53	46	7
Structured Security Assessment Methodology for Manufacturers of Critical Infrastructure Components [18]	4	37	-33	14	0	14	33	5	28	51	42	9
Cyberassessment method for SCADA security [45]	4	39	-35	12	0	12	30	6	24	46	45	1
NetSecuritas [46]	2	47	-45	10	0	10	33	6	27	45	53	-8
Simulation-based methods												
Approach to security assessment of critical infrastructures [47]	2	41	-39	14	0	14	29	6	23	45	47	-2
Assessment/analysis platform for Multiple Interdependent Critical Infrastructures (AMICI) [48]	3	43	-40	14	0	14	30	6	24	47	49	-2
Cyber-physical security assessment [49]	3	42	-39	11	0	11	29	6	23	43	48	-5
Smart grids assessment through simulation [50]	3	47	-44	11	0	11	27	6	21	41	53	-12
Model-based methods												
Mission Oriented Network Analysis (MONA) [51]	2	49	-47	10	0	10	29	6	23	41	55	-14
Service-oriented approach for assessing critical infrastructure security [33]	4	43	-39	12	0	12	35	5	30	51	48	3
General method for assessment of security in complex services [52]	1	55	-54	5	0	5	24	7	17	30	62	-32
Cybersecurity assessment of cyber-physical systems using Discrete Time Markov Chain model-based simulations [53]	2	47	-45	10	0	10	25	6	19	37	53	-16
Testing Security for Systems of Systems (TeSSoS) [54]	2	45	-43	10	0	10	34	7	27	46	52	-6

Table 6: Methods' ranking according to the cumulative values of complexity, usability and acceptance metrics. CB – Checklist-based methods, VI – Vulnerability identification and analysis methods, PT – Penetration testing methods, SB – Simulation-based methods, MB – Model-based methods

1.	Operational framework for security capability assessment [16]	CB	12
2.	Analytical Processing Approach to Supporting Cyber Security Compliance Assessment [17]	CB	11
3.	Structured Security Assessment Methodology for Manufacturers of Critical Infrastructure Components [18]	PT	9
4.	Risk-based testing [23]	PT	7
5.	Advanced security measurement tailored to the organisation's business profile [25]	CB	5
6.	Online and offline security policy assessment [27]	VI	4
7.	Standardised method to cybersecurity assessments of critical infrastructures [28]	PT	3
8.	Service-oriented approach for assessing critical infrastructure security [33]	MB	3
9.	Cyber-Physical IT Vulnerability Assessment for Semiconductor Companies [14]	CB	2
10.	Ruckus [34]	VI	2
11.	Cyberassessment method for SCADA security [45]	PT	1
12.	Approach to security assessment of critical infrastructures [47]	SB	-2
13.	Assessment/analysis platform for Multiple Interdependent Critical Infrastructures (AMICI) [48]	SB	-2
14.	Security compliance monitoring [37]	CB	-4
15.	Cyber-physical security assessment [49]	SB	-5
16.	Testing Security for Systems of Systems (TeSSoS) [54]	MB	-6
17.	Network security situation assessment method based on deep learning [44]	VI	-7
18.	Work flow-oriented security assessment [39]	VI	-8
19.	First principles vulnerabilities assessment [40]	VI	-8
20.	Ovaldroid [41]	VI	-8
21.	NetSecuritas [46]	PT	-8
22.	AI and Metrics-Based Vulnerability-Centric Cyber Security Assessment [43]	VI	-11
23.	Bayesian attack graph-based quantitative assessment [42]	VI	-12
24.	Smart grids assessment through simulation [50]	SB	-12
25.	Mission Oriented Network Analysis (MONA) [51]	MB	-14
26.	Cybersecurity assessment of cyber-physical systems using Discrete Time Markov Chain model-based simulations [53]	MB	-16
27.	Security assessment approach for Internet banking services [38]	CB	-17
28.	Rough set-based security assessment method [36]	CB	-23
29.	General method for assessment of security in complex services [52]	MB	-32

3.3 Results of the metric-based analysis

The analysis of the results shows that generally for all the methods, characteristics connected to complexity tend to introduce a major negative contribution to the adoption potential. The majority (∼75%) of negative metric values there are 6, 7, or 5 (∼31%, ∼25%, and ∼20% of values, consequently). Except for difficulty-related metrics (difficulty of creation, difficulty of description, and difficulty of understanding) and one method [14], the negative metrics scored above 3. This means that the complexity properties constitute the biggest obstacles to the methods' adoption. Above all, the methods require from their users a remarkable effort, great proficiency, and good familiarity with the problem area.

The usability and acceptance properties of the methods make a positive impact on applicability. More than half of the positive metric values in these areas are above average. Almost 24% of the values are 6, 23% – 5 and around

6% – 7. Specifically, metrics concerning the methods' completeness, accuracy, perceived usefulness, and users' satisfaction have medium to high impact values. At the same time, the results show that the methods target specialized professionals and do not accommodate well users with diverse expertise (universality). Also, the ease of use of the methods requires improvements.

Looking closely at the first 10 methods with the highest values of the aggregation function M_A (see Table 5), it becomes apparent that checklist-based methods lead the way. They take the first, second, and fifth position in the ranking, with the function values of 12, 11, and 5, respectively. Scrutinizing the individual metric values for the methods, it can be noted that the methods never score more than 5 in complexity, and never below 3 (for positive metrics) in usability and acceptance. When comparing their complexity, usability, and acceptance aggregators (the values of M_{AC}, M_{AU}, and M_{AA}) to other methods, it can be seen that the complexity-related characteristics contribute the most to the methods' high position in the ranking as there are other methods with similar values of M_{AU} and M_{AA}. Translating this observation into more simple terms – within the framework of applicability, the most straightforward methods exhibit the highest adoption potential.

The subsequent positions in the ranking are taken by penetration testing methods (3, 4, and 7 location). While being somewhere in the middle as far as their complexity aggregators are concerned, the methods stay out in terms of usability and acceptance. They received particularly high values for satisfaction, perceived usefulness, completeness, level of detail, and accuracy. From that point of view, they appear complementary to the checklist-based methods.

Two vulnerability identification and analysis methods fall in the "top ten" of the ranking. The first of them excels in the area of acceptance. Its aggregator M_{AA} is the highest in the entire comparison achieving the value of 32. This is because the values of completeness, level of detail, scope width, accuracy, and perceived usefulness metrics are very high. The second method exhibits higher complexity compared to other methods in the group, but usability and acceptance aggregators are high. They equal those of penetration testing methods. There is also one model-based method in the first ten. Looking at the numbers, its applicability features are similar to the former vulnerability identification and analysis method, with the acceptance aggregator M_{AA} equal to 30 which makes the method the second in this area. None of the simulation-based methods fell in the "top ten" group. The first ones in the ranking are located on the 12 and 13 position. Compared to the primary ten methods in the listing, they are more complex and less acceptable.

4 Top ten methods in the ranking

This section presents the results of the analysis of applicability features of the top ten methods in the ranking presented in Table 6.

4.1 Operational framework for security capability assessment

The framework for security capability assessment was presented as an extension to the earlier proposed Tactical Information Governance Security Model[15]. The model, dedicated to the medical environment was built upon the results of an action research that included a pilot exploratory study and semi-structured interviews with primary care practitioners. As a result, a domain-tailored version of a cybersecurity management framework focusing on risk assessment, policies and procedures, cybersecurity controls, capability assessment, reviews, and compliance monitoring was proposed. The model emphasizes the role of three prerequisites that need to be satisfied to render the governance process effective, namely the knowledge of relevant legal requirements, the awareness of ethical and professional responsibilities, and the appropriate assignment of roles and responsibilities. The model's primary goals were practicality, comprehensiveness, and easy implementation by personnel with little or no technical knowledge. The same principles guided the development of the operational framework for security capability assessment[16]. As a result, a simplified capability maturity model suitable for application by medical practices with little or no outside intervention was proposed. The application of the framework was illustrated in the context of data backup activity. Analyzing the applicability metrics, perceived usefulness, and social influence have particularly high values. Also, the ease of use, completeness, and scope width were highly ranked. This reflects the methods' good adjustment to an important sector and its particular specifics (including the non-technical environment). In the area of complexity, the method stands out in terms of the capability of execution, low difficulties associated with creation, description and understanding as well as preparation extensiveness. The findings may indicate that cybersecurity assessment frameworks tailored to specific application domains may have a higher chance of being adopted.

4.2 Analytical Processing Approach to Supporting Cyber Security Compliance Assessment

The Analytical Processing Approach to Supporting Cyber Security Compliance Assessment[17] facilitates broad compliance assessments not limited to one standard. It aims at addressing the complexity of such evaluations where normally a plethora of requirements need to be considered. The authors proposed a structured process of compliance analysis which starts with the analysis and specification of the subject of the evaluation (a service) and is followed by activities that result in assigning only the most relevant controls, standards, and security concerns. The compliance assessment is performed in reference to the selected set of requirements, thus the extensiveness of the entire evaluation is substantially reduced. The application of the approach is illustrated in the context of a credit card payment service. The method is slightly more complex ($M_{AC} = -30$) compared to the operational framework for security capability

assessment but extends the scope of the analysis to more than one reference document. As a result, the completeness of the assessment increases. At the same time, the description of the method application would require revision to support its easier comprehension.

4.3 Structured Security Assessment Methodology for Manufacturers of Critical Infrastructure Components

The Structured Security Assessment Methodology for Manufacturers of Critical Infrastructure Components[18] is a proprietary cybersecurity assessment framework used by Siemens – a well-recognized worldwide manufacturer of industrial products. The approach was developed with a strong emphasis on being "pragmatic, cost-efficient, generic, flexible, and built on relevant standards". Consequently, it consists of five main stages: pre-assessment, risk assessment, theoretical assessment, practical assessment, and post-assessment. The theoretical assessment is a checklist-based assessment conducted using a questionnaire produced in a semi-automated way from relevant standards. It is carried out in parallel with a risk assessment that implements the ISO/IEC[19] and NIST[20] guidelines, resulting in a facilitated process. In both stages, the relevant experts are being actively involved through interviews and workshops. The results constitute the input to the "practical assessment" that is vulnerability identification and penetration testing. The success in achieving the practicality and efficiency goals is confirmed by multiple applications to evaluations of Siemens products. The experiences proved its cost-effectiveness and reasonable resource requirements. Typically, an assessment involves one to three assessors and a few weeks. Analyzing the applicability metrics, the method has complexity only slightly higher than the two previous frameworks. This is due to the incorporation of penetration testing, which in turn requires expertise, larger capabilities, and knowledge of the application domain. At the same time, it is very well structured, comprising only the most substantial activities, and described in a very clear way, which reduces adoption difficulties and increases simplicity. As a result, the complexity aggregator ($M_{AC} = -33$) even compared to the most straightforward checklist-based methods is above average. Then, the method's usability and acceptance characteristics stand out from all the other frameworks. Among the others, because the completeness, level of detail, and accuracy of the framework are very high. The structure of the method seems to concur with the observation from this study (see Section 3.3), that checklist-based methods and penetration testing methods appear complementary to each other. It is also worth noting that the method adopts some aspects from the OSSTMM[21] – a well-established practical cybersecurity assessment framework and IEC/ISO 15408[22] – the most commonly applied standard for cybersecurity evaluation of products.

4.4 Risk-based testing

The cybersecurity assessment framework described by Rennoch et al.[23] was developed during two European research projects: DIAMONDS and RASEN. The main idea behind the overall approach is to connect the risk assessment to cybersecurity assessment, so its results can drive the test planning and the selection of appropriate tests. In that respect, the approach converges with the Siemens cybersecurity assessment methodology (see Section 4.3), which also uses risk assessment (and checklist-based assessment) as a driver for penetration testing. As a result, an extension to the cybersecurity testing process specified in ISO/IEC/IEEE 29119[24] was introduced. The approach is presented clearly and is well structured which results in complexity metrics' values similar to the Siemens' method. For details, project documentation needs to be studied and learned. This slightly increases the effort associated with using and preparing the method. Also, the usability and acceptance of the method are comparable. The scope width scored significantly higher because the framework was designed for diverse application domains. Several supportive tools are mentioned that are available openly or commercially.

4.5 Advanced security measurement tailored to the organisation's business profile

You et al.[25] described a checklist-based method that scales with various complexities of organizations. This is achieved by classifying cybersecurity requirements into three groups: mandatory, significant, and recommended. The requirements are adopted from a selected reference document, such as NIST SP 800-53[8] or ISO/IEC 27001[26]. The categorization into the middle group is based on the calculation of Pearson's correlation coefficients. The method emphasizes the involvement of the professionals that operate the equipment embraced by assessed cybersecurity controls. Questionnaires are distributed via various channels to reach the experts. Analyzing the metrics, the method has the complexity aggregator M_{AC} equal to -33 which as for the checklist-based method is considerable. This is because, among others, the effort, expertise, and difficulty of understanding received relatively high values. A revision of the method's description could potentially remove some issues. Also, the necessity of calculating the correlation coefficients has an impact on the complexity properties of the method. As far as usability and acceptance metrics are concerned, the cumulative values are similar to the best-ranking checklist-based methods. However, the ease of use and effort expectancy received relatively low values which reflects the additional activities introduced by the method to achieve the expected tailoring to a specific organization.

4.6 Online and offline security policy assessment

The framework proposed by Valenza et al.[27] enables the automated detection of configuration flaws in network-based security controls. Based on security

policies specified in a dedicated notation, test packets are generated together with the outputs expected from the target of the evaluation. The packets are sent to the target, which will process them according to the implemented policy. If a discrepancy in the policy implementation occurs, for instance, due to an attack, the output of the processing will not match the expected one. This will trigger an alert. As already mentioned (see Section 3.3), the method has outstanding acceptance properties ($M_{AA} = 32$). Within its scope, the method provides remarkable completeness and the level of detail. It is also broad in scope and accurate. At the same time, the complexity metrics' values are the lowest among all vulnerability identification and analysis methods (together with Ruckus, see Section 4.10). This is due to clear description and relative straightforwardness (supported by openly available tools).

4.7 Standardised method to cybersecurity assessments of critical infrastructures

The introduction of the cybersecurity assessment method for critical infrastructures[28] was preceded by an exploratory study involving sector stakeholders to identify the main challenges for cybersecurity assessment in the area. It showed that cost and time have a significant impact on the scope of practical evaluations. Also, operators perform various types of cybersecurity tests using different methodologies. The tests are performed mostly on-site and outside the daily operation of the system (e.g. during setup or a maintenance break). Thus, the main objective of the study was to provide a standardized reference model for conducting penetration testing in critical infrastructures[28] that among others would enable repeatable and comparable evaluations at reasonable cost and time. The authors did not intend to design a new methodology from scratch but to build on the previous work. As a result, a structured methodology that refers to NESCOR[29,30], OSSTMM[21], NIST SP 800-115[31], and ISSAF[32] was proposed. The framework consists of the most substantial activities composed in a two-level configuration that stemmed from the needs of stakeholders. All is described in a well-comprehensible way. Analyzing the applicability metrics, the values for complexity are comparable to risk-based testing with the exception of difficulty-related that scored better. Also, the values for usability and acceptance are very similar. There, the completeness, level of detail, and accuracy are at high levels, which is generally inherent to penetration testing. In a more general view, the proposal may resemble the the Siemens' cybersecurity assessment framework (see Section 4.3) without the checklist-based assessment stage. This might indicate that a specific composition of evaluation activities and stages as well as the involvement of the end-users' viewpoints during the design has a positive impact on applicability.

4.8 Service-oriented approach for assessing critical infrastructure security

The service-oriented approach for assessing critical infrastructure security[33] supports analyzing complex systems by employing the notions of services and dependencies. A service is defined as "a task performed by components or subsystems". During the initial stages, all the services present in the system as well as dependencies between them need to be identified and represented in the model of the system. Then, based on the model, the propagating effects of vulnerabilities, threats, and attacks of one system component on the other can be traced. In this way, vulnerability chains are determined, that show, for instance how a compound service can be affected by vulnerabilities in its low-level components and services. The threat analysis is facilitated by being vulnerability-driven i.e. only the threats that match a vulnerability are considered. Attack analyses are supported by focusing on disservice chains. The method is the least complex of the model-based methods analyzed in the study ($M_{AC} = -39$), specifically its simplicity and the difficulty of understanding stand out from the group. This is because the notions of a system service and system dependency are clearly described and are possible to be modeled in non-overcomplicated way. As already mentioned (see Section 3.3), the method has very good acceptance characteristics. By analyzing system dependencies and vulnerability, threat and attack chains, it achieves very high completeness. Also, the level of detail, accuracy, and scope broadness are high.

4.9 Cyber-Physical IT Vulnerability Assessment for Semiconductor Companies

This is a checklist-based method tailored to cybersecurity assessments of semiconductor manufacturers[14]. Based on consultations with IT security, audit, and data center teams as well as the Internet resources, a list of cybersecurity requirements for semiconductor companies and a tailored questionnaire with references to industry standards and procedures were developed. During an assessment, questionnaire-driven analyses and interviews with professionals in the organizations are carried out. The grade of satisfaction of a security requirement is denoted on a 4-level scale. The tool was applied to the assessment of four enterprises in China. Its use is very straightforward and little preparation is needed, thus the complexity parameters are satisfactory. At the same time, the scope of analyses is narrowed to the particular sector, and inherently for checklist-based methods, the precision and completeness are low, which has a visible impact on the acceptance of the method.

4.10 RUCKUS

RUCKUS is a methodology and a toolset that facilitates automated vulnerability identification in cyber-physical systems[34]. It is based on an innovative concept of software decomposition and correlation. During the knowledge

development, various versions of cyber-physical systems' firmware are decomposed into files and the files of interest are subject to semi-automated vulnerability discovery using static analysis, natural language processing, and fuzzing. The results, including affected library names and versions, vulnerability types, quantity, and ease of replication are introduced into a graph database. Then, when a new specific device needs to be evaluated, its firmware is also decomposed, but the vulnerability discovery activity is replaced with an automated correlation analysis with the data stored in the database. As a result, the scalability of the approach is remarkably improved. The practice shows that various devices share the same parts of code, such as libraries, configurations, and executables. The authors illustrated the effectiveness of the method in an automotive case study. Multiple vulnerabilities in a common cyber-physical system software have been identified in an automated way. The framework is an example of how an originally very complex process can be facilitated by introducing novel optimizations in its structure and the vast support of tools. As a consequence, RUCKUS has the lowest complexity of all vulnerability identification and analysis methods ($M_{AC} = -39$), together with online and offline security policy assessment, see Section 4.6). Its usability and acceptance are high. They are diminished mostly due to the application being narrowed to cyber-physical systems.

5 Findings from the analysis of the methods

This section denotes the main observations from the analysis of the "top ten". The primary learning is that methods that are straightforward and ready for immediate use have the strongest applicability potential and chances for broad adoption. The analysis shows that the desired characteristics of straightforwardness and instant application are inherent to well-designed checklist-based methods[14,15,17,25]. However, this is for the price of diminished completeness, the level of detail, and accuracy. The gap can be successfully filled in by complementing the checklist-based assessment with penetration testing. The latter normally requires high competencies, but delivering detailed and well-written documentation and supporting tools can relax the requirement (see RUCKUS described in Section 4.10). Also, the learning of the method can be substantially improved by providing tools and documentation. Moreover, the results show that an intuitive and uncomplicated composition of evaluation activities and stages as well as consulting the end-users during the design has a positive impact on applicability. The majority of the leading methods are described in a well comprehensible way. Only, for two of them[17,25] the descriptions require improvements.

Several methods[15,18,23] incorporate risk assessment into the cybersecurity evaluation stages. In risk-based testing[23] this concept is particularly emphasized. Such an approach enables focusing on the most relevant threats and assets. It results in the reduction of effort and resources, which is highlighted as a desired feature of a framework for its practical adoption. The

cost-effectiveness and reasonable resource demands (including time consumption) were primary objectives during the development of the Structured Security Assessment Methodology requirements[18] and Standardised method to cybersecurity assessments[28]. These methods were developed with a very strong orientation on being pragmatic and applicable. The success of the Siemens' method in this respect can be confirmed by multiple applications in assessments of its proprietary products.

The introduction of four methods in the "top ten"[14,15,18,28] was preceded by exploratory study and/or consultations with field experts. This is a standard step in requirements engineering but seems to be overlooked in many developments. This study shows its remarkable impact on the applicability of cybersecurity assessment methods. Several methods are adjusted to a particular domain[14,15,18,34]. However, it seems to be beneficial for only one of them[15], where the tailoring led to higher acceptance by the end-users. The other three methods could be directly adopted in other application areas, and the specialization does not result in higher applicability metrics' values. At the same time, it narrowed the scope, which resulted in a lower level of the associated metric.

Another positive characteristic of the leaders is that the majority of them did not intend to design a new methodology from scratch but to build on the previous work and to introduce demanded improvements[15,18,23,25,28]. In this way, the uncontrolled proliferation of methods that leads to the confusion of users unable to find their way in the multitude of proposals is avoided. Also, the idea of such an "incremental" approach is that the weaknesses of the previous work are reduced, while improvements are made.

Among the methods, the Structured Security Assessment Methodology for Manufacturers of Critical Infrastructure Components[18] (see Section 4.3) concurs with all these observations. It is a well-structured framework that combines checklist-based assessment with penetration testing and risk assessment to achieve a good focus on the most important aspects during the cybersecurity assessment. Consequently, the method is cost-effective and reasonably time-consuming which was proven in daily practice and the application to multiple evaluations. It is described in a comprehensible form, easy to learn, and straightforward. At the same time, the incorporation of penetration testing into the evaluation results in high completeness of the analysis and good precision. During the development of the method, the end-users were remarkably involved. On the other side, as the method targets manufacturers of critical infrastructure components, its scope width is diminished. However, as it represents generic steps, it should well transpose to a broader application domain. For instance, the sector-specific standards used for devising the checklists can be replaced with more universal documents or norms dedicated to other sectors. Taking this all into the account, the method is revealed as a primary candidate for direct use as well as further development.

The other innovative constructs introduced by the top ten methods can be taken as enhancements to the generic foundation. For example, when wishing

Table 7: Main findings: factors with a positive impact on applicability.

Factors with a positive impact on applicability
Straightforwardness and readiness for immediate use
Intuitive and uncomplicated composition of evaluation activities and stages
Detailed and well-written documentation and supporting tools
Complementing the checklist-based assessment with penetration testing
Incorporating risk assessment
Performing exploratory studies and/or consultations with field experts
Consulting the end-users during the design and development
Applying the incremental approach instead of devising new solutions

Table 8: Recommendations for developers.

Recommendations for developers
Use the Structured Security Assessment Methodology for Manufacturers of Critical Infrastructure Components[18] method as a basis for further developments
Apply the incremental approach
Assure straightforwardness and readiness for immediate use
Deliver detailed and well-written documentation and supporting tools to facilitate the application by less proficient users
Design the intuitive and uncomplicated composition of evaluation activities and stages
Perform exploratory studies and/or consult field experts
Consult the end-users during the design and development
Enable flexible enhancements of the method

to broaden compliance assessments to more than one standard, the approach from The Analytical Processing Approach to Supporting Cyber Security Compliance Assessment[17] can be borrowed. When tailoring to a specific complexity of an organization, then the procedure devised by You et al.[25] (see Section 4.5) can be followed. If looking for even higher precision and completeness of the analysis that takes into account cascading effects and propagation of vulnerabilities', threats' and attacks' consequences then system dependencies need to be explored. This can be achieved by adopting the Service-oriented approach for assessing critical infrastructure security[33]. Another extension can be including a stage dedicated to vulnerability and identification analysis in the cybersecurity assessment. For networking environments, the framework of Valenza et al.[27] (see Section 4.6) exhibits promising applicability properties. For software packages (such as a device firmware), the innovative methodology of RUCKUS[34] is worth to be applied.

The findings and resulting implications in the form of recommendations for developers and practitioners have been summarized in Tables 7 – 9.

6 Conclusion

The paper presented the results of the research that followed a general review of cybersecurity assessment methods. In the first stage, the methods identified in the previous study were subjected to more in-depth analysis based on 19 qualitative applicability metrics to more precisely determine the areas of

Table 9: Primary recommendations for practitioners.

Primary recommendations for practitioners
To achieve completeness and precision of analyses, complement checklist-based cybersecurity assessments with penetration testing
Connect cybersecurity assessment to risk assessment to save cost, time and other resources
Take the Structured Security Assessment Methodology for Manufacturers of Critical Infrastructure Components[18] method as a good starter
Depending on the needs, enhance the method with the methods of Buccafurri et al.[17], Masera and Fovino[33], Valenza et al.[27] or Potteiger et al.[34]

improvement and to identify the methods that demonstrate a higher adoption potential. This part of the study revealed that a good effort needs to be put into reducing the methods' complexity. In particular, the effort associated with the preparation and use of a method as well as the required competencies and familiarity with the problem area need to be reduced. Also, the ease of use of the methods and their readiness for being operated by users with different backgrounds demands further work. The effort and the ease of use can be reduced by the provision of supportive tools, while the other properties can be facilitated by documentation, including instructional videos and interactive exercises, that need to be continuously available to users. A ranking of methods according to their applicability metrics' values was constructed.

The second part of the study was based on the analysis of the primary ten methods from the ranking. While the detailed findings are presented in the two previous sections, the most important observation is that straightforward and ready-for-use methods are the most likely to be broadly adopted. Thus, checklist-based methods appear as the first candidates to be applied. However, the completeness and precision of the analyses supported by them are limited. This issue can be addressed by adding penetration testing to the evaluations. Also, connecting activities to the risk assessment appears to be beneficial as it leads to more focused analyses and consequently cost, time, and other resource savings. A method that incorporates all the observations is the Structured Security Assessment Methodology for Manufacturers of Critical Infrastructure Components developed by a large manufacturer of industrial products. On one side, it exhibits readiness for direct use, on the other – it can be subjected to further improvements described in this paper.

A limitation of the study is the fact that it was performed by a single analyst. This is due to the challenges in composing a group of experts familiar with or willing to learn all the presented methods. The subjective component had an impact on the evaluation of qualitative metrics which was based on methods' descriptions and individual observations. To a certain degree, it could have influenced the methods ranking. Thus, increasing the number of experts remains a potential direction of further research. Another prospective area of future projects regards the evaluation of methods based on quantitative metrics. As already mentioned, the study will demand considerable endeavor associated with proper preparation and realization of necessary experiments. At the same time, the current, qualitative study delivers a new view of the

methods within the framework of applicability metrics. Moreover, it should facilitate the selection of the method most suitable to a given context in terms of applicability and usability.

Declarations

The author states that there is no conflict of interest.

References

1. W.B. Jason Deane, L. Rees, Cybersecurity in supply chains: Quantifying risk. Journal of Computer Information Systems **63**(3), 507–521 (2023). https://doi.org/10.1080/08874417.2022.2081882. URL https://doi.org/10.1080/08874417.2022.2081882

2. I.F. Juan Carlos Fernandez de Arroyabe, Marta F. Arroyabe, C.F.A. Arranz, Cybersecurity resilience in smes. a machine learning approach. Journal of Computer Information Systems **0**(0), 1–17 (2023). https://doi.org/10.1080/08874417.2023.2248925. URL https://doi.org/10.1080/08874417.2023.2248925

3. D.P.B. Nan Liang, A. Luse, An empirical comparison of malicious insiders and benign insiders. Journal of Computer Information Systems **0**(0), 1–13 (2023). https://doi.org/10.1080/08874417.2023.2251427. URL https://doi.org/10.1080/08874417.2023.2251427

4. J.W. Obi Ogbanufe, F. Baucum, Towards a conceptual typology of darknet risks. Journal of Computer Information Systems **0**(0), 1–12 (2023). https://doi.org/10.1080/08874417.2023.2234323. URL https://doi.org/10.1080/08874417.2023.2234323

5. K.J. Smith, Bad employees: Examining deviant security behaviors. Journal of Computer Information Systems **0**(0), 1–14 (2023). https://doi.org/10.1080/08874417.2023.2175336. URL https://doi.org/10.1080/08874417.2023.2175336

6. D.B. Martin Wilson, Sharon McDonald, K. McGarry, It won't happen to me: Surveying sme attitudes to cyber-security. Journal of Computer Information Systems **63**(2), 397–409 (2023). https://doi.org/10.1080/08874417.2022.2067791. URL https://doi.org/10.1080/08874417.2022.2067791

7. National Institute of Standards and Technology (NIST), NIST SP 800-53A Rev. 5 Assessing Security and Privacy Controls in Information Systems and Organizations. Tech. Rep. January, 2022 (2022). https://doi.org/10.6028/NIST.SP.800-53Ar5

8. National Institute of Standards and Technology (NIST), NIST SP 800-53 Rev. 5 Security and Privacy Controls for Information Systems and Organizations. Tech. rep. (2020). https://doi.org/10.6028/NIST.SP.800-53r5

9. M. Chapple, J.M. Stewart, D. Gibson, *(ISC)² CISSP Certified Information Systems Security Professional Official Study Guide, 9th Edition* (2021)

10. R. Leszczyna, Aiming at methods' wider adoption: Applicability determinants and metrics. Computer Science Review **40**, 100,387 (2021). https://doi.org/https://doi.org/10.1016/j.cosrev.2021.100387. URL https://www.sciencedirect.com/science/article/pii/S1574013721000277

11. R. Leszczyna, Review of cybersecurity assessment methods: Applicability perspective. Computers & Security **108**, 102,376 (2021). https://doi.org/10.1016/J.COSE.2021.102376

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

13. B. Kitchenham, P. Brereton, A systematic review of systematic review process research in software engineering. Information and Software Technology **55**(12), 2049–2075 (2013). https://doi.org/https://doi.org/10.1016/j.infsof.2013.07.010. URL http://www.sciencedirect.com/science/article/pii/S0950584913001560

14. T.A. Cayetano, A. Dogao, C. Guipoc, T. Palaoag, in *Proceedings of the 2Nd International Conference on Cryptography, Security and Privacy* (ACM, New York, NY, USA, 2018), ICCSP 2018, pp. 67–71. https://doi.org/10.1145/3199478.3199482. URL http://doi.acm.org/10.1145/3199478.3199482

15. P. Williams, Information governance: A model for security in medical practice. Journal of Digital Forensics, Security and Law **2** (2007). https://doi.org/https://doi.org/10.15394/jdfsl.2007.1017

16. P. Williams, A practical application of CMM to medical security capability. Information Management and Computer Security **16**(1), 58–73 (2008). https://doi.org/10.1108/09685220810862751

17. F. Buccafurri, L. Fotia, A. Furfaro, A. Garro, M. Giacalone, A. Tundis, in *Proceedings of the 8th International Conference on Security of Information and Networks* (ACM, New York, NY, USA, 2015), SIN '15, pp. 46–53. https://doi.org/10.1145/2799979.2800007. URL http://doi.acm.org/10.1145/2799979.2800007

18. T. Brandstetter, K. Knorr, U. Rosenbaum, (Springer, Berlin, Heidelberg, 2009), pp. 248–258. https://doi.org/10.1007/978-3-642-01244-0_22. URL http://link.springer.com/10.1007/978-3-642-01244-0{_}22

19. ISO/IEC. ISO/IEC TR 13335-3:1998 Information technology – Guidelines for the management of IT Security – Part 3: Techniques for the management of IT Security (1998)

20. NIST. NIST SP 800-30 Risk Management Guide for Information Technology Systems (2002)

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

22. ISO/IEC, ISO/IEC 15408-1:2009 Information technology – Security techniques – Evaluation criteria for IT security – Part 1: Introduction and general model. Tech. rep. (2009). URL http://standards.iso.org/ittf/PubliclyAvailableStandards/index.html

23. A. Rennoch, I. Schieferdecker, J. Großmann, in *Communications in Computer and Information Science*, vol. 426 CCIS (Springer Verlag, 2014), pp. 397–406. https://doi.org/10.1007/978-3-662-43908-1_49

24. IEEE. ISO/IEC/IEEE International Standard – Software and systems engineering – Software testing – Part 2: Test processes (2013). https://doi.org/10.1109/IEEESTD.2013.6588540

25. Y. You, I. Cho, K. Lee, An advanced approach to security measurement system. Journal of Supercomputing **72**(9), 3443–3454 (2016). https://doi.org/10.1007/s11227-015-1585-7

26. ISO/IEC. ISO/IEC 27001:2013: Information technology – Security techniques – Information security management systems – Requirements (2013)

27. F. Valenza, M. Vallini, A. Lioy, in *Proceedings of the 8th ACM CCS International Workshop on Managing Insider Security Threats* (ACM, New York, NY, USA, 2016), MIST '16, pp. 101–104. https://doi.org/10.1145/2995959.2995970. URL http://doi.acm.org/10.1145/2995959.2995970

28. M. Caselli, F. Kargl, in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 8985 (Springer Verlag, 2016), pp. 332–343. https://doi.org/10.1007/978-3-319-31664-2_34

29. EPRI SmartGrid Resource Center - NESCOR (2023). URL https://smartgrid.epri.com/NESCOR.aspx

30. National Electric Sector Cybersecurity Organization Resource (NESCOR), NESCOR Guide to Penetration Testing for Electric Utilities Version 3. Tech. rep. (2013)

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

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

33. M. Masera, I.N. Fovino, in *Critical Infrastructure Protection*, ed. by E. Goetz, S. Shenoi (Springer US, Boston, MA, 2008), pp. 367–379

34. B. Potteiger, J. Mills, D. Cohen, P. Velez, in *Proceedings of the 7th Symposium on Hot Topics in the Science of Security* (Association for Computing Machinery, New York, NY, USA, 2020), HotSoS '20. https://doi.org/10.1145/3384217.3385622. URL https://doi.org/10.1145/3384217.3385622

35. T. Wallis, R. Leszczyna, Ee-isac - practical cybersecurity solution for the energy sector. Energies **15**(6) (2022). https://doi.org/10.3390/en15062170. URL https://www.mdpi.com/1996-1073/15/6/2170

36. W. Qiangmin, L. Mengquan, L. Jianhua, in *Proceedings - International Conference on Signal Image Technologies and Internet Based Systems, SITIS 2007* (2007), pp. 1041–1046. https://doi.org/10.1109/SITIS.2007.114

37. M. Vogel, V. Broer, in *ISSE 2013 Securing Electronic Business Processes* (Springer Fachmedien Wiesbaden, 2013), pp. 183–194. https://doi.org/10.1007/978-3-658-03371-2_16

38. S. Khattak, S. Jan, I. Ahmad, Z. Wadud, F.Q. Khan, An effective security assessment approach for Internet banking services via deep analysis of multimedia data. Multimedia Systems (2020). https://doi.org/10.1007/s00530-020-00680-7. URL https://doi.org/10.1007/s00530-020-00680-7

39. B. Chen, Z. Kalbarczyk, D.M. Nicol, W.H. Sanders, R. Tan, W.G. Temple, N.O. Tippenhauer, A.H. Vu, D.K. Yau, in *ACM International Conference Proceeding Series* (2013), pp. 65–76. https://doi.org/10.1145/2535813.2535821

40. J.A. Kupsch, B.P. Miller, E. Heymann, E. César, in *Proceedings of the ACM Conference on Computer and Communications Security* (2010), pp. 87–92. https://doi.org/10.1145/1866835.1866852

41. M. Barrère, G. Hurel, R. Badonnel, O. Festor, in *2013 9th International Conference on Network and Service Management, CNSM 2013 and its three collocated Workshops - ICQT 2013, SVM 2013 and SETM 2013* (IEEE Computer Society, 2013), pp. 235–242. https://doi.org/10.1109/CNSM.2013.6727842

42. C. Wang, Y. Wang, Y. Dong, T. Zhang, in *IEEE International Conference on Communications* (2011). https://doi.org/10.1109/icc.2011.5963092

43. I. Kotenko, E. Doynikova, A. Chechulin, A. Fedorchenko, in *Guide to Vulnerability Analysis for Computer Networks and Systems* (2018), pp. 101–130. https://doi.org/10.1007/978-3-319-92624-7_5

44. H. Yang, R. Zeng, G. Xu, L. Zhang, A network security situation assessment method based on adversarial deep learning. Applied Soft Computing **102**, 107,096 (2021). https://doi.org/https://doi.org/10.1016/j.asoc.2021.107096. URL https://www.sciencedirect.com/science/article/pii/S1568494621000193

45. M. Permann, K. Rohde, in *16th Annual Joint ISA POWID/EPRI Controls and Instrumentation Conference and 49th Annual ISA Power Industry Division, POWID Symposium 2006*, vol. 1 (2006), pp. 212–223

46. N. Ghosh, I. Chokshi, M. Sarkar, S.K. Ghosh, A.K. Kaushik, S.K. Das, in *ACM International Conference Proceeding Series*, vol. 04-07-Janu (Association for Computing Machinery, 2015). https://doi.org/10.1145/2684464.2684494

47. R. Leszczyna, I.N. Fovino, M. Masera, Approach to security assessment of critical infrastructures' information systems. IET Information Security **5**(3), 135 (2011). https://doi.org/10.1049/iet-ifs.2010.0261. URL https://doi.org/10.1049/iet-ifs.2010.0261

48. B. Genge, C. Siaterlis, M. Hohenadel, in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 7722 LNCS (2013), pp. 228–239. https://doi.org/10.1007/978-3-642-41485-5{_}20

49. N. Saxena, V. Chukwuka, L. Xiong, S. Grijalva, in *Proceedings of the 2017 Workshop on Cyber-Physical Systems Security and PrivaCy* (ACM, New York, NY, USA, 2017), CPS '17, pp. 69–79. https://doi.org/10.1145/3140241.3140246. URL http://doi.acm.org/10.1145/3140241.3140246

50. A. Tundis, R. Egert, M. Mühlhäuser, in *Proceedings of the 12th International Conference on Availability, Reliability and Security* (ACM, New York, NY, USA, 2017), ARES '17, pp. 13:1—-13:10. https://doi.org/10.1145/3098954.3098966. URL http://doi.acm.org/10.1145/3098954.

3098966

51. M. Lange, F. Kuhr, R. Möller, in *Proceedings of the 1st International Workshop on AI for Privacy and Security* (ACM, New York, NY, USA, 2016), PrAISe '16, pp. 6:1—-6:8. https://doi.org/10.1145/2970030.2970043. URL http://doi-1acm-1org-100005fkq0c6a.han.bg.pg.edu.pl/10.1145/2970030.2970043

52. L. Krautsevich, F. Martinelli, A. Yautsiukhin, in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 6994 LNCS (2011), pp. 153–164. https://doi.org/10.1007/978-3-642-24755-2_14

53. J. Zalewski, S. Drager, W. McKeever, A.J. Kornecki, in *Proceedings of the Eighth Annual Cyber Security and Information Intelligence Research Workshop* (ACM, New York, NY, USA, 2013), CSIIRW '13, pp. 10:1—-10:4. https://doi.org/10.1145/2459976.2459987. URL http://doi.acm.org/10.1145/2459976.2459987

54. M.A. Olivero, A. Bertolino, F.J. Dominguez-Mayo, M.J. Escalona, I. Matteucci, in *Proceedings of the 7th International Workshop on Software Engineering for Systems-of-Systems and 13th Workshop on Distributed Software Development, Software Ecosystems and Systems-of-Systems* (IEEE Press, Piscataway, NJ, USA, 2019), SESoS-WDES '19, pp. 62–65. https://doi.org/10.1109/SESoS/WDES.2019.00017. URL https://doi.org/10.1109/SESoS/WDES.2019.00017