Front. Comput. Sci., 2024, 18(3): 183808
https://doi.org/10.1007/s11704-023-1582-6

REVIEW ARTICLE

# Towards an integrated risk analysis security framework according to a systematic analysis of existing proposals

**Antonio SANTOS-OLMO (✉)[1,2], Luis Enrique SÁNCHEZ[1,2], David G. ROSADO[1], Manuel A. SERRANO[3], Carlos BLANCO[4], Haralambos MOURATIDIS[2], Eduardo FERNÁNDEZ-MEDINA[1]**

1 GSyA Research Group, University of Castilla-La Mancha, Ciudad Real 13071, Spain
2 Institute for Analytics and Data Science, University of Essex, Colchester CO4 3SQ, UK
3 Alarcos Research Group, University of Castilla-La Mancha, Ciudad Real 13071, Spain
4 ISTR Research group, Department of Computer Science and Electronics, University of Cantabria, Santander 39005, Spain

**Abstract** The information society depends increasingly on risk assessment and management systems as means to adequately protect its key information assets. The availability of these systems is now vital for the protection and evolution of companies. However, several factors have led to an increasing need for more accurate risk analysis approaches. These are: the speed at which technologies evolve, their global impact and the growing requirement for companies to collaborate. Risk analysis processes must consequently adapt to these new circumstances and new technological paradigms. The objective of this paper is, therefore, to present the results of an exhaustive analysis of the techniques and methods offered by the scientific community with the aim of identifying their main weaknesses and providing a new risk assessment and management process. This analysis was carried out using the systematic review protocol and found that these proposals do not fully meet these new needs. The paper also presents a summary of MARISMA, the risk analysis and management framework designed by our research group. The basis of our framework is the main existing risk standards and proposals, and it seeks to address the weaknesses found in these proposals. MARISMA is in a process of continuous improvement, as is being applied by customers in several European and American countries. It consists of a risk data management module, a methodology for its systematic application and a tool that automates the process.

**Keywords** information security management, security system, security risk assessment and management

## 1 Introduction

Cyber security is a real and increasingly critical need in a digitised society in which the number of threats and their impacts are constantly growing [1,2] and which requires information systems that are adequately protected [3,4]. Security management and threat mitigation within information systems have, therefore, implicitly become a fundamental aspect for citizens (to preserve their privacy), for enterprises (to protect digital assets and transactions) and for states (to protect their critical infrastructures and ensure the continuity of government and government services, etc.) [5−7].

More specifically, companies in the present-day globalised and competitive business environment are increasingly dependent on their information systems, since they have proved to be a factor of great importance as regards increasing competitiveness [8,9]. Companies are consequently now aware that the information and processes that support systems and networks are their most important assets [10,11], and that these assets are subject to a wide variety of risks, which may critically affect the company [12−14]. It is, therefore, crucial for companies to implement security controls that allow them to discover and control the risks to which they may be subjected [15,16]. But the implementation of these controls is not sufficient, and systems with which to manage security over time are required that will make it possible to react quickly to new risks, vulnerabilities, threats, etc.[17]. However, the security systems of most companies (and especially small and medium-sized enterprises - SMEs) have been developed without adequate guidelines, without documentation, with insufficient resources [18,19] and with a low security culture [10,20]. Moreover, the security tools on the market help to solve part of the security problems, but often do not address the problem in a comprehensive and integrated manner [21].

Reality has, therefore, shown that for companies to be able to use information and communication technologies with guarantees, it is necessary to have guides, metrics and tools that will allow them to identify their security level and any vulnerabilities not yet covered [22]. However, the level of successful implementation of these security systems is currently very low. This problem is particularly accentuated in

Received October 2, 2022; accepted February 7, 2023

E-mail: antonio.santosolmo@uclm.es

the case of SMEs, which have the additional limitation of not having sufficient human and economic resources for proper management [23]. It is consequently necessary to implement mechanisms that will allow companies to be able to understand their cyber security, and in particular, the risks associated with it. Moreover, these mechanisms must be sufficiently simple to be adaptable to all types of companies [24].

The concept of security management emerged as a solution to these problems [25,26] in an attempt to improve the information security of companies. This was done by employing an approach based on correct risk management [27−30], since risk management is an essential process in any business management model, and all the activities of a company involve risks [31]. An effective risk assessment, therefore, helps the top management of an organisation to make optimal decisions and avoid losses [32,33]. It is consequently necessary to select and implement safeguards in order to ascertain, prevent, impede, reduce or control the risks identified [34].

The classic risk analysis models did not, however, frequently consider some the new characteristics that appeared as the result of technological evolution [35]. But it is now necessary to consider the risks that may appear because of the relationship that the company has with its environment, its circumstances and with other companies. These other companies may be technological partners, third parties in a service provided by the company or co-participants in multi-company projects [36]. The treatment of these hierarchical and associative risks also acquires special relevance with the emergence of new scenarios, such as Cloud Computing [37,38], the Internet of Things (IoT) [39,40], Big Data [41] or Cyber-Physical Systems (CPS) [42,43] associated with Industry 4.0, all of which have drastically altered the perception of the infrastructure of Information Systems. This rapid transition to new technologies means that, from a security perspective, unknown risks and vulnerabilities may emerge as a result of this relocation of Information Systems, with the consequent deterioration of a large part of the effectiveness of traditional protection mechanisms [44,45].

It should also be noted that risk analysis is a costly process, and current approaches are not designed to repeat the process every time a change is made. This means that companies are not aware of their real risks at all times, but rather have a static image of the risks they had months or even years ago. This detracts from the value of the analysis and its use by third parties. It is, therefore, important to develop specific methodologies that make it possible to maintain the results of risk analysis without increasing costs [46,47], i.e., dynamic risk analysis methodologies that evolve on the basis of security events (incidents) and that can be adapted to any type of company, regardless of its size and sector [48].

The need for this feature has been stated by several researchers, who have highlighted the importance of dynamic risk systems [49]. This is owing to the fact that the application of risk analysis and management processes is a common practice in the field of information systems, since it allows the timely planning of preventive actions against risks. This is done in the short, medium or long term, but a considerable potential to facilitate real-time decision making in the face of security events or incidents is currently untapped [50,51]. Moreover, risk is not fixed in time, and dynamism is, therefore, required in its treatment [50].

This paper presents the result of a systematic review of the existing literature on research in the field of risk analysis and management.

The key contributions of this paper are summarised as follows:

- A systematic review carried out in order to identify the main weaknesses of the existing risk analysis and management models with respect to the new market needs. This systematic review was performed using the guidelines for systematic reviews proposed by Kitchenham. These are based on directives developed for medical research [52,53], and were subsequently adapted for use by a team of researchers in the field of information systems [54,55].
- A summary of the MARISMA framework built, after observing the main weaknesses found in the proposals analysed, and which attempts to solve these shortcomings by employing a methodological and technological perspective.

The remainder of the paper is structured as follows: Section 2 shows the research question defined, while Section 3 provides an explanation of the review method, which is based on the research protocol. It is here that the search strategy and study selection is defined. Section 4 shows the data to be extracted and presented in the summary of relevant studies, and Section 5 presents the results of the review and an analysis of the results obtained. The framework that has been developed and that seeks to provide a solution to the problems identified above is presented in Section 6. Finally, the last section shows a description of the main conclusions obtained.

## 2 Review planning

In this section, the research question is formulated. It focuses on the area of interest of the work and defines both the problem to be addressed and its main characteristics.

### 2.1 Scope of the research question

The expected outcome of this review is to gain knowledge on existing proposals for associative and hierarchical risk analysis that are oriented towards SMEs (low-cost generation) and dynamic aspects. They will subsequently be analysed in order to discover what aspects they share and how they differ, and to identify research needs.

The research question defined for this paper is, therefore, the following:

> What work has been carried out to develop risk analysis systems by taking into account hierarchical, associative, dynamic and low-cost risks?

The keywords and related concepts that were used to formulate this question and during the execution of the review are the following:

Risk analysis: risk analysis model, risk analysis methodology

Risk management: risk management model, risk management methodology

Risk assessment: risk assessment model, risk assessment methodology

Risks: Associative risks, hierarchical risks

Dynamic: dynamic risk, dynamic assessment, knowledge reuse

The existing proposals on risk analysis models and methodologies have, therefore, been sought. Emphasis was placed on those oriented towards dealing with associative risks, hierarchical risks, dynamic assessment and/or oriented towards SMEs. The most important were extracted and subsequently analysed and compared. The population analysed comprised the publications present in the repositories of the data sources selected that were related to the objective of this review.

## 3 Review method

The review method was based on the research protocol. At this stage, we defined: the search strategy, the sources that would be used to identify the primary studies, any potential restrictions, the inclusion and exclusion criteria, the criteria used to assess the quality of the primary studies, and the way in which the data from the studies would be extracted and synthesized.

### 3.1 Sources selection

The objective of this phase was to select the sources that would be used to search for primary studies.

The criteria employed to select the search sources made it possible to consult documents on the Internet or in the digital library appertaining to the University of Castilla-La Mancha. This repository contains electronic books, in addition to providing access to the following digital libraries: ACM, IEEE, Elsevier, Springer, Taylor&Francis and Wiley Online Library, among others. Access is also provided to search engines that allow advanced queries and search by keywords, in addition to publishers, books, journals and conferences recommended by experts in the field.

The search for primary studies was conducted using web search engines, electronic databases and manual searches, such as searches in a specific journal/conference/book/publication or in research publications recommended by experts in the field.

```
(methodology OR model)
AND
(associative OR hierarchical)
AND
(“risk analysis” OR “risk management” OR “risk
assessment")
AND
(“dynamic” OR “knowledge reuse”)
```

### 3.2 Studies selection

Having defined the sources, it is now necessary to describe the process and criteria employed during the execution of this review in order to select and evaluate the studies.

First, the selected keywords were combined with “AND” and “OR” connectors to obtain the search string shown above:

The first step in the study selection procedure was to adapt the search string to the source search engine and run the query, limiting the search to papers published in the last 11 years (2011−2022). Inclusion and exclusion criteria should be based on the research question. The inclusion criterion acts on the results obtained when running the search on the source, thus making it possible to carry out an initial selection of papers considered in the context of the review as candidates to become primary studies. The main inclusion criterion was an analysis of the title, keywords and abstract of each document. This made it possible to see how these words were related and why the study was selected. This criterion located and eliminated most of the results obtained that did not contribute to risk analysis in the field of information systems.

The exclusion criterion acted on the subset of relevant studies obtained and made it possible to obtain the set of primary studies. In this phase, we focused mainly on reading and analysing the summary of the document and its conclusions. In some cases, it was necessary to study the document in greater depth and carry out a more detailed reading of other parts of it. This allowed us to carry out a more detailed analysis of what each study was about, consider the actual relationship it had with the objectives pursued and, if it was truly relevant to the review, select it as a primary study.

### 3.3 Execution of the selection

At this point, the search was executed in each of the selected sources in order to obtain an initial list of studies for subsequent evaluation by applying all of the specified criteria.

The study selection procedures were applied to all the papers obtained. The execution of the query initially yielded a total of 6,635 results for the period 2011−2022, from which 30 studies corresponding exactly to all the previously defined inclusion and exclusion criteria were eventually selected.

In order to structure the results of the selection process, the studies were grouped by initiative. Four specific categories and a generic category that included the remaining proposals were created:

- Process: Set of activities planned in successive phases with the aim of achieving a given objective.
- Framework: Layered structure, whose function is to support or guide the construction of a risk management framework, encompassing a set of functions within the system, along with the relationships between them.
- Model: Specific artefact that provides a representation of a complex system in order to facilitate its understanding.
- Methodology: Set of procedures and techniques that are applied in an orderly and systematic manner in the resolution of a problem, in our case, in order to carry out a correct risk management in an organisation. They integrate the concepts of Process and Model.

- Others: Proposals that do not completely fit into the previous typologies, but that contain interesting concepts for research.

The different proposals selected are studied in the following section in order to extract their main contributions and adapt them to the desired characteristics.

## 4 Information collection

The information obtained from the studies had to contain the techniques, methods, processes, measures, strategies or any type of initiative with which to adapt the analysis, management or evaluation of risks to a scope feasible for SMEs, or to manage associative or hierarchical risks.

The reporting forms defined for this systematic review contained the identification of the study, the study methodology or model, the study results, the study issues, and general impressions of the study.

The following is a brief review of each of the selected studies shown in the previous section, according to the information extracted by employing the information forms.

### 4.1 Processes

#### 4.1.1 Process 1 (P1[1)]): A hybrid information security risk assessment procedure considering interdependences between controls [56].

The authors propose a hybrid procedure with which to evaluate information security risk levels in the face of different security controls. The procedure is composed of different phases: i) The DEMATEL (Decision Making Trial and Evaluation Laboratory) method is applied in order to build the interrelationships between security control areas, and ii) the Analytic Network Process (ANP) method is used to obtain the risk ratings, thus allowing interdependence and feedback between security control families to be detected.

In this approach, the authors focus on three security control areas of ISO/IEC 27001 and their corresponding control families in order to formulate the risk assessment criteria. The proposed risk assessment procedure is organised in the following steps: i) System characterisation; ii) Identification of threats and vulnerabilities; iii) Risk assessment; iv) Impact analysis; v) Risk determination, and vi) Control recommendations.

The proposed procedure is not very flexible and is fundamentally theoretical. It is applied to a practical case, but is, therefore, complex to apply and evaluate, and does not take into account associative and hierarchical factors.

#### 4.1.2 Process 2 (P2): A fuzzy logic-based system for risk analysis and evaluation within enterprise collaborations [57].

The authors propose a fuzzy logic-based system for risk analysis and assessment, focusing on the identification and management of risks in network-based enterprise collaborations. Risk factors are identified with respect to the four stages of a collaboration life cycle: pre-creation, creation, operation and termination, and the development of a fuzzy logic-based algorithm for collaboration risk assessment in order to evaluate these perceived risk factors. Each risk is described by a risk probability and a risk impact.

The authors have built a prototype web service, the Collaboration Risk Evaluator (CRE), which they have validated using real use cases.

However, they do not consider aspects that facilitate their applicability to all types of companies and sectors, nor do they have mechanisms that allow the reuse of knowledge.

#### 4.1.3 Process 3 (P3): A software defined network information security risk assessment based on pythagorean fuzzy sets [58].

The authors propose an information systems risk assessment process based on the construction of a model using the Software Defined Network (SDN). Their objective is, therefore, to define a mechanism with which to determine the information risk associated with SDN or based on SDN architecture, taking into account uncertainty. To this end, they intend to develop a multi-criteria decision-making method (MCDM) composed of a Fuzzy Decision Making and Evaluation Laboratory method in order to determine the influences between SDN properties and vulnerabilities. They propose to do this by implementing a Pythagorean Analytical Hierarchical Process to evaluate the priority of the severity weights of SDN properties, along with their vulnerabilities. This process, by its very nature, allows associative factors to be taken into account when performing the risk assessment using fuzzy techniques.

However, this is a fundamentally theoretical study, whose results are not contrasted by applying the proposal in complex practical cases.

#### 4.1.4 Process 4 (P4): An integrated approach to risk assessment for special line shunting via fuzzy theory [59].

The authors present a risk assessment process based on fuzzy techniques with the main objective of obtaining reliable risk values in environments subject to environmental factors that tend to obtain incomplete risk results or involve high levels of uncertainty.

Although the study is specifically applied to the field of railways, its concepts could easily be extrapolated to the IT field, in which uncertainty is also a key factor in risk analysis processes. The importance of reducing uncertainty in order to obtain reliable results is, therefore, emphasised, as are other very interesting concepts, such as the use of both qualitative and quantitative techniques. The study also stresses the need to take into account hierarchical relationships and defines a case study in order to apply this process.

However, this is a fundamentally theoretical study, whose results are not contrasted by applying the proposal in complex practical cases.

### 4.2 Frameworks

#### 4.2.1 Framework 1 (F1): A new comprehensive framework for enterprise information security risk management [60].

The authors present a comprehensive framework for information system risk management, with the objective of

[1)] This kind of abbreviations will be employed for the sake of the legibility of the table.

enabling the effective establishment of a secure environment and focusing on the framework for electronic transactions in enterprises.

The framework has two structural and two procedural dimensions. The structural dimensions include scope and evaluation criteria, while the procedural dimensions include process and evaluation tools.

The structural scope of the framework is based on the STOPE (Strategy, Technology, Organization, People, Environment) view, while the management process is associated with the cyclical phases of the well-known six sigma DMAIC (Define, Measure, Analyse, Improve, Control).

This is a theoretical study, whose results are not contrasted by applying the methodology in practical cases.

#### 4.2.2 Framework 2 (F2): Knowledge-based risk management framework for information technology project [61].

The authors submit a conceptual framework denominated as Knowledge-Based Risk Management (KBRM) that employs Knowledge Management (KM) processes to improve the effectiveness of risk management and increase the probability of success in information technology projects.

The authors consequently consider that KM processes have become a strategic resource for organisations and can have a great influence on reducing risks in them. The following activities are defined: 1) Knowledge-based risk identification; 2) Knowledge-based risk capture; 3) Knowledge-based risk sharing; 4) Knowledge-based risk assessment; 5) Knowledge-based risk education.

This is a theoretical study, whose results are not contrasted by applying the methodology in practical cases.

#### 4.2.3 Framework 3 (F3): A conceptual framework of info-structure for information security risk assessment (ISRA) [62].

The authors present a new conceptual framework whose objective is to structure the information required for the enterprise to select, understand and undertake the risk management methodology that may be most appropriate for it.

The objective of the Information Systems Risk Analysis (ISRA) info-structure is, therefore, to help organisations to obtain an overview of the process flow and gather information on the requirements that must be met before the risk assessment can be carried out successfully. This information structure can be used by organisations to complete all necessary planning and to select appropriate methods with which to undertake the risk analysis.

It is a theoretical study, whose results are not contrasted by applying the methodology in practical cases. Furthermore, it takes into account only the major risk analysis methodologies, which are difficult to apply in SMEs, although it stresses the importance of the fact that the methodology chosen must be dynamic and take into account relational aspects.

#### 4.2.4 Framework 4 (F4): Dynamic risk management: a contemporary approach to process safety management [63].

The authors propose a framework for dynamic risk management, the cornerstone of which is a dynamic risk assessment process based on a Plan-Do-Check-Act (PDCA) strategy. This, therefore, allows the definition of an initial risk assessment, after which a PDCA cycle of continuous assessment begins.

The proposed framework is still at a very early stage, but the most interesting aspect of this proposal is the growing importance of the concept of dynamism within risk assessment processes.

This is a theoretical study, whose results are not contrasted by applying the proposal in practical cases.

#### 4.2.5 Framework 5 (F5): Towards an efficient risk assessment in software projects–Fuzzy reinforcement paradigm [64].

The authors propose an approach based on fuzzy techniques as a basis for the future development of a risk assessment framework with which to manage uncertainty and efficiently assess risks in the field of software project development. This will make it possible to guide a decision-making process throughout the project life cycle.

This is a theoretical study, whose results are not contrasted by applying the proposal in practical cases.

#### 4.2.6 Framework 6 (F6): Information Security Risk Assessment: A Method Comparison [21].

The authors propose a framework denominated as CURF (Core Unified Risk Framework) whose objective is to compare information systems risk assessment methods.

The proposal is interesting because it states the need for this framework to be dynamic, thus allowing it to adapt to the new characteristics and tasks of the methods reviewed. In addition, the criteria employed in order to compare risk analysis methods include the key factors that they should be adapted to cloud computing and take into account the reuse of knowledge.

However, other than the comparative method, no new proposal by which to adapt to new needs in risk analysis processes is provided.

#### 4.2.7 Framework 7 (F7): A new fuzzy methodology-based structured framework for RAM and risk analysis [65].

The authors propose a framework with which to conduct risk analysis whose processes are based on FMEA (Failure Mode and Effect Analysis) techniques, and particularly rule-based approaches and fuzzy techniques.

The main objective is to use these techniques to reduce arbitrariness, and thus uncertainty, in risk analysis. A Fuzzy Lambda-Tau (FLT) approach is accordingly used to calculate the Reliability, Availability and Maintainability (RAM) parameters of the system.

The study focuses on the scope of a chemical processing plant, although it is sufficiently generic to be adapted to any type of Information System. Whatever the case may be, it reinforces the growing importance of specific risk analysis processes for critical infrastructures.

This is a theoretical study, whose results are not contrasted by applying the proposal in practical cases.

#### 4.2.8 Framework 8 (F8): LiSRA: Lightweight security risk assessment for decision support in information security [66].

The authors present a risk assessment framework with the main objective of guiding security decision-making in all types of organisations, specifically with a view to adapting it to the needs of SMEs.

They also highlight the importance of evaluating security actions by taking into account existing security activities, in addition to considering the dependencies between other activities or elements that may affect security depending on the context of the company. The importance of associative relationships is, therefore, emphasised, as is the importance of obtaining initial assessments quickly and easily through the use of qualitative techniques.

The study also highlights the importance of having mechanisms with which to take advantage of knowledge from previous implementations.

However, this is a theoretical study, whose results are not contrasted by applying the proposal in practical cases.

#### 4.2.9 Framework 9 (F9): BPRIM: An integrated framework for business process management and risk management [67].

The authors present a comprehensive framework called BPRIM (Business Process-Risk Integrated Method) with the main objective of integrating risk management and business process management. The contribution is very interesting, since one of the main objectives of safety governance is to ensure that safety management processes are perfectly aligned with an organisation’s business objectives.

To this end, a life cycle is designed on the basis of coupling the stages of the life cycles of both BPM (Business Process Management) and ERM (Enterprise Risk Management). There are also a risk metamodel, which has been defined at a generic level, thus allowing it to be adapted to different areas, and a semi-formal graphic modelling language. The framework also has a support tool, although it is specific only to process modelling, with no support for the risk version. In its current version it is, therefore, closer to business process management than to risk management.

The framework has been tested in some practical cases related to the healthcare sector, although its effectiveness has not yet been analysed in other sectors.

### 4.3 Models

#### 4.3.1 Model 1 (MO1): An information systems security risk assessment model under uncertain environment [68].

The authors propose a model for risk assessment in information security systems based on the theory of evidence (a generalisation of the Bayesian theory of subjective probability). In so doing, they assume that, since there is a great deal of uncertainty in the information security systems (ISS) risk assessment process, the management of uncertainty is of great importance for the effectiveness of risk assessment.

The model provides a new way in which to define BBAs (Basic Belief Assignment) using fuzzy measures, with the objective of addressing the evidence of uncertainty in ISS risk assessment. The model also provides a method with which to check the consistency of evidence, which can reduce the uncertainty arising from conflicts between evidence predicted by experts.

Uncertainty management can be very interesting when applying the results of the model to Cloud computing environments. The model is contrasted with a practical case study, but it is very generic and is not supported by any kind of software tool.

#### 4.3.2 Model 2 (MO2): A VIKOR technique based on DEMATEL and ANP for information security risk control assessment [69].

The authors propose an information security risk assessment model. The proposed model is an MCDM model that combines VIKOR (VIseKriterijumskaOptimizacija I KompromisnoResenje- Multicriteria Optimization and Compromise Solution), DEMATEL and ANP in order to resolve conflicts among conflicting criteria that may show dependency and feedback to each other.

The proposed model has four phases: 1) risk assessment, 2) risk remediation, 3) risk monitoring and review, and 4) risk management improvement. The process has been developed using a PDCA strategy, defining a continuous cycle of assessment, treatment, risk monitoring and safety improvement.

The authors define a case study in order to apply and refine this model, but it is very generic and is not supported by any kind of software tool.

#### 4.3.3 Model 3 (MO3): A security risk analysis model for information systems: Causal relationships of risk factors and vulnerability propagation analysis [70].

The authors present a security risk analysis model with the objective of identifying the causal relationships between risk factors and analysing the complexity and uncertainty of the propagation of vulnerabilities. It is based on the fact that the security risks in information systems are caused by various interrelated internal and external factors. A security vulnerability could, therefore, also propagate and escalate through the causal chains of risk factors via different pathways.

The authors develop a Bayesian network in order to simultaneously define risk factors and their causal relationships on the basis of knowledge obtained from observed cases and domain experts.

This is a theoretical study, whose results are not contrasted by applying the proposal in practical cases.

The use of Bayesian networks as a technique for information systems risk assessment and analysis is also used in the work of Wang et al. “Research the information security risk assessment technique based on Bayesian network” [71], in which an architecture for the use of this type of network in risk analysis processes is defined, although principally from a theoretical point of view.

#### 4.3.4 Model 4 (MO4): A situation awareness model for information security risk management [72].

The authors propose a Risk Analysis Model for Information Awareness of the Situation (SA-ISRM) in order to complement the information security risk management process. Its objective is to alleviate the deficiencies in the practice of information security risk assessment that inevitably lead to poor decision making and inadequate or inappropriate security strategies.

The proposed model, therefore, seeks to address these deficiencies through the collection, analysis and communication of information related to the risks of the company as a whole. The model has been refined by means of a case study in the U.S. national security intelligence enterprise.

However, the authors do not consider aspects that facilitate applicability to all types of companies and sectors, nor are there mechanisms that allow the reuse of knowledge.

#### 4.3.5 Model 5 (MO5): An efficient security data-driven approach for implementing risk assessment [26].

The author proposes a risk management model oriented towards the processes that make up an organisation's data lifecycle (creation, editing, visualization, processing, transfer, storage), and its adaptation to the asset layers (logical, physical and human) through a series of predefined patterns. To this end, a pyramid of the security needs of various organisations is defined, with each pyramid being a hierarchical multilayer, including security concerns, related business processes, security data extracted, assets involved, risks identified and the optimal combination of security controls.

The author defines a simple comparative case study in order to apply this model, but it is very generic and is not supported by any kind of software tool.

#### 4.3.6 Model 6 (MO6): Improving information security risk analysis by including threat-occurrence predictive models [73].

The authors present a risk assessment model with the main objective of obtaining a more realistic risk estimate, which would lead to results closer to reality when making security decisions, and greater efficiency when selecting the most appropriate controls in each improvement cycle. This increase in efficiency is based on a predictive model that allows the calculation of risk by replacing historical threat frequencies with probabilities of future threats, taking into account the current vulnerabilities of an information system. The relevance of dynamic adaptation, in this case through the predictive model designed using a logistic regression approach, to the real conditions and to the changes that occur in the context of the organisation, is very interesting.

Furthermore, the importance of adapting the models to all types of companies, especially SMEs, is highlighted. The authors define a case study in order to apply and refine this model.

However, they do not consider aspects that facilitate dynamic adaptation, nor do they have mechanisms that allow the reuse of knowledge.

#### 4.3.7 Model 7 (MO7): Data breach management: an integrated risk model [74].

The authors propose a risk assessment model focused on the security of the data in an organisation, with the objective of managing security incidents and learning about data breach management in dynamic security environments.

The paper highlights the importance of a holistic approach to risk but focuses its application specifically on data breach risks and related management. It also stresses the need to apply heuristic techniques in order to adapt to the dynamic capabilities of the organisation itself, its technological architecture and changes in the context.

The study also stresses the need to take into account hierarchical relationships and defines a case study in order to apply this process.

This is a theoretical study, whose results are not contrasted by applying the proposal in practical cases.

#### 4.3.8 Model 8 (MO8): Risk management for cyber-infrastructure protection: A bi-objective integer programming approach [75].

The authors propose a stochastic-deterministic risk assessment model whose objective is to select a set of security controls from each review and improvement cycle in order to optimise the residual risk according to a given organisational budget. The technical part of decision-making is, therefore, integrated with the economic part by starting from a frequent practical scenario, such as the limitation of the budget available for security aspects.

The authors propose a dual stochastic and deterministic approach with which to take uncertainty into account for effective risk reduction and aim to facilitate decision- making in safety issues. The application of the model is focused on an IT-based supply chain, but the way in which it is defined would allow it to be applied to other areas.

This is a theoretical study, whose results are not contrasted by applying the proposal in practical cases.

#### 4.3.9 Model 9 (MO9): A Configurable Dependency Model of a SCADA System for Goal-Oriented Risk Assessment [76].

The authors propose a goal-oriented risk analysis model specifically intended for ICS (Industrial Control Systems). More specifically, the model focuses on identifying and dynamically assessing the risks associated with the multiple dependencies between the different technical and non-technical sub-elements that may be involved in the security of SCADA (Supervisory Control and Data Acquisition) devices.

The proposal, therefore, highlights the importance of having dynamic and adaptive models that allow the assessment of risk by taking into account the specific dependencies existing in the particular context of each system, in addition to allowing adaptation to changing circumstances. It also stresses the importance of implementing risk analysis processes adapted to specific sectors or technologies, in this case highlighting the need for ICS and the increasingly used IoT technologies. The authors also present a case study focusing on a water control system.

Although the need for adaptation is highlighted, the dependencies between elements must be reconfigured manually, and domain experts are required for proper tuning. Moreover, it is difficult to extrapolate to systems other than purely Operational Technologies environments.

### 4.4 Methodologies

#### 4.4.1 Methodology 1 (ME1): Risk analysis in information systems: A fuzzification of the MAGERIT methodology [77].

The authors present an extension of the MAGERIT methodology based on fuzzy computational models with the objective of reducing the degree of uncertainty in the measurement techniques of traditional methodologies.

They consequently present a scale of linguistic terms with which to represent the measurement values, their dependencies and frequencies and the degradation of assets in information systems environments.

These techniques are applied by also taking into account the fact that the relationship among IS assets can be both internal and dependent on third parties, which supports the need to work with associative factors for risk assessment and management.

This is a theoretical study, whose results are not contrasted by applying the proposal in practical cases.

#### 4.4.2 Methodology 2 (ME2): Risk analysis using FMEA: Fuzzy similarity value and possibility theory based approach [78].

The authors propose a methodology that incorporates FMEA techniques, particularly rule-based approaches and fuzzy techniques, into risk analysis processes.

The main objective is to use these techniques to reduce arbitrariness, and thus uncertainty, in risk analysis by integrating concepts of similarity of measurement values of fuzzy numbers and possibility theories.

This is a theoretical study whose results are not contrasted by applying the proposal in practical cases.

#### 4.4.3 Methodology 3 (ME3): Functional quantitative security risk analysis (QSRA) to assist in protecting critical process infrastructure [79].

The authors propose a quantitative security risk assessment methodology oriented towards critical infrastructures. They start from a concurrent threat and vulnerability assessment approach and introduce a Bow Tie risk model mapped onto a Bayesian network model that allows different logical assumptions. Finally, risk/vulnerability probabilities are integrated with potential loss values in order to quantify risk.

The importance of risk analysis processes adapted to critical infrastructures by following a “Bow Tie” model is also presented by Abdo et al. in “A safety/security risk analysis approach of industrial control systems: A cyber bowtie - combining new version of attack tree with bowtie analysis” [80].

Although both starting points are focused on chemical facilities (in order to prepare real case studies), the methodologies can be adapted to any critical infrastructure by configuring and customising their elements, although expert knowledge is necessary in order to carry this out.

The authors have defined a case study in order to apply and refine this methodology, but it is very generic and is not supported by any kind of software tool.

#### 4.4.4 Methodology 4 (ME4): A risk assessment methodology for the Internet of Things [81].

The authors propose a risk analysis and management methodology that is applicable to IoT environments. The proposed method (which is both qualitative and quantitative) is based on the construction of an attack tree adapted to each scenario and on a criterion denominated as an exploitability value. The evaluation of this value is initially obtained in a qualitative manner by considering the levels of difficulty of performing an attack against the system. These qualitative levels are then translated into concrete quantitative values. The overall exploitability value of the system is eventually calculated on the basis of a graph showing the dependency among the vulnerabilities identified.

The proposed procedure is essentially theoretical. It is applied in a practical case, but it is too global, and the authors do not provide many details of the processes carried out to obtain the results. Moreover, it requires a high degree of expert knowledge for its maintenance and focuses mainly on the risk of attack on physical components, thus making it too specific.

#### 4.4.5 Methodology5 (ME5): A dynamic simulation approach to support the evaluation of cyber risks and security investments in SMEs [82].

The authors propose a methodology whose objective is cyber risk assessment, and which is oriented towards SMEs. They define a series of indicators and dynamic metrics oriented towards supporting decision making in cyber security investments, while being simple to apply in small companies. They additionally address the need to adapt to a dynamic organisational complexity and, therefore, to assess cyber risks and related dynamics over time.

The authors also provide a tool called SMECRA (SME Cyber Risk Assessment) with which to support the application of the proposed methodology. This methodology is focused mainly on the simulation of risk scenarios from an economic point of view but does not support global risk management.

#### 4.4.6 Methodology 6 (ME6): A fuzzy based model proposal on risk analysis for human-robot interactive systems[83].

The authors propose a specific risk analysis methodology with which to adapt to a new operational paradigm, such as the growing interdependence between humans and robots in any kind of technological field.

The paper, therefore, highlights the importance of having specific risk analysis processes for changing and often unpredictable environments such as human-robot interactive systems (HMI – Human-Machine Interfaces), in which a high degree of uncertainty and sometimes potentially dangerous situations for operators must be considered. A methodology for risk analysis based on fuzzy set theory and MCDM using z-numbers, which can take into account the uncertainty of the data, is consequently presented.

However, it is a fundamentally theoretical study, which has not been tested in practical cases and which has no supporting tools for its application. Moreover, mechanisms for knowledge re-use are not taken into account and the methodology can be difficult to apply without considerable expert knowledge.

### 4.5 Others

#### 4.5.1 Others 1 (O1): A new formula of information security risk analysis that takes risk improvement factor into account [84].

The author proposes a qualitative approach for the organisations' information security risk analysis processes, taking into account the factor of progressive improvement to risk levels.

He also proposes that the results of this new formula can be considered as an important factor in decision making. This is a theoretical study, whose results are not contrasted by applying the proposal in practical cases.

#### 4.5.2 Others 2 (O2): Munodawafa, F. et al. "Security risk assessment within hybrid data centers: A case study of delay sensitive applications" [85].

The authors present a discursive study on the need for risk analysis and management processes in the specific field of data centres. No specific mechanism is proposed or defined, but relevant concepts, such as the need for the risks to which not only physical but also virtual servers are subjected to be included in the security of these data centres, are mentioned. This new scenario ties in with the new needs in the area of cloud computing, with the need for the coexistence of classic physical systems with virtual systems, and with the associative risks derived from virtualisation.

The study presents an initial selection of risks and vulnerabilities focused on data centres, including some specific to virtual servers. A case study specifically focused on the evaluation of availability aspects on a Voice over IP (VoIP) service is also presented, although it is still very sketchy and not very detailed.

## 5 Analysis of results

The results of the systematic review are shown in Table 1, which summarises the number of studies by initiative:

As illustrated in Table 1, the scientific community is producing many ongoing research projects concerning new frameworks, processes, models and methodologies. These attempt to facilitate risk management, assessment and/or analysis. They take into account factors such as the flexibility or simplicity of their application (which are necessary for their application to any type of company, regardless of the size), or consider the importance of managing hierarchical and associative risks, which is essential for, i.e., Cloud Computing or IoT.

Table 2 shows an analysis of the different proposals selected, considering their main contributions and characteristics, which are aligned with the objectives of the systematic review. Each of the aspects analysed is described below:

- Scope: Scope of application of the proposal with a view to its application in an information system. It can be global (applicable to the information system as a whole) or applicable only to a specific aspect.
- Technique/Base Model: Indicates the main scientific techniques, disciplines or methods used as a basis for the proposal.
- Main contributions: Most significant contributions of the proposal aligned with the object of this research.

**Table 1** Results by initiative

| Initiative type | Studies # | Initiatives |
|---|---|---|
| **Process** | 4 | P1, P2, P.3, P.4 |
| **Framework** | 9 | F1, F2, F3, F4, F5, F6, F7, F8, F9 |
| **Model** | 9 | MO1, MO2, MO3, MO4, MO5, MO6, MO7, MO8, MO9 |
| **Methodology** | 6 | ME1, ME2, ME3, ME4, ME5, ME6 |
| **Others** | 2 | O1, O2 |
| **Total** | 30 | – |

As Table 2 shows, after the analysis it was concluded that each of the selected initiatives, while not completely solving the problem identified, deals with very interesting aspects related to the requirements of risk analysis in information systems. These are features that can be used as a basis for new methodologies / processes / frameworks / techniques, or as extensions to existing ones. They can, in particular, be employed as a reference for the development of a methodology that includes all the desired characteristics.

Table 3 shows a comparison of the different proposals analysed, considering a specific set of criteria that researchers have identified as desirable for the performance of a correct risk analysis. It is considered that the aspects assessed can be fully, partially or not addressed by the model. Each of the aspects analysed is described below:

- AC — Need for Adaptive Catalogues: information security has become an essential element for organisations, but the existence of numerous different types of risk assessment methods, standards, guidelines and specifications makes it daunting for organisations to confront the task of determining the most appropriate method to meet their needs [39]. One of the problems related to risk analysis recently identified by the scientific community is, therefore, the need for adaptive catalogues that would allow greater flexibility in risk analysis [81,86].
- HA — Hierarchy and Associativity: The need for risk analyses to be able to contemplate associative and hierarchical structures is emphasised. The treatment of these associative types of risks also takes on particular relevance with the emergence of Cloud computing. This is because the rapid transition to the Cloud has meant that, from a security perspective, a number of unknown risks and vulnerabilities have appeared [87–89].
- RKL — Reuse Knowledge and Learning: Another group of researchers highlight the importance of being able to reuse the knowledge acquired during previous risk analyses. This will allow the system to learn to perform a better risk analysis [90] and to use decision support techniques [73,91,92].
- DY — Dynamic and Evolutionary: It is important to consider that risk analysis is a costly process, and that current methodologies were not designed to repeat the process every time a modification is made. The need for this feature is stated by several researchers, for whom risk analysis studies generally provide a static picture of the state of the site, while the system is constantly evolving or degrading, signifying that it is important to be able to have dynamic risk systems [49].
- CC — Collaborative Capability: Another fundamental

**Table 2** Main contributions of the selected proposals

| Type | Initiat. | Scope | Technique | Main contributions |
|---|---|---|---|---|
| **Process** | P1 | Limited ISO27001 | DEMATEL, ANP | −Interrelationships between risks according to control areas |
| | P2 | Networks | Fuzzy techniques | −Risks associated with networked business collaborations<br>−Prototyping and application in real cases |
| | P3 | Software defined networks (SDN) | Fuzzy techniques, DEMATEL | −Reduction of the degree of uncertainty<br>−Associative risk management |
| | P4 | Railways | Fuzzy techniques | −Reduction in the degree of uncertainty<br>−Hierarchical factors for risk probability and impact assessment |
| **Framework** | F1 | Electronic transactions | STOPE, DMAIC | −Risks associated with networked business collaborations |
| | F2 | IT projects | KM | −Application of knowledge management techniques to risk analysis |
| | F3 | Global | – | −Structuring of information prior to risk analysis<br>−Knowledge reuse |
| | F4 | Global | – | −Dynamic risk assessment |
| | F5 | Software development | Fuzzy techniques | −Reduction in the degree of uncertainty |
| | F6 | Global | – | −Knowledge reuse<br>−Importance of Dynamic Risk and Cloud Environments |
| | F7 | Critical Infrastructure | FMEA | −Reduction inf the degree of uncertainty |
| | F8 | Global | Logic trees | −Decision-making processes<br>−Knowledge reuse<br>−Targeting SMEs & Associative risk management |
| | F9 | Business processes | – | −Integration of BPM with risk management<br>−Risk metamodel |
| **Model** | MO1 | Global | Theory of evidence<br>Fuzzy measures | −Management of uncertainty in results<br>−Consistency evidence<br>−Case study |
| | MO2 | Global | VIKOR, DEMATEL, ANP | −Interdependence and feedback of risk criteria<br>−PDCA risk assessment process |
| | MO3 | Global | Bayesian Networks | −Weakness propagation uncertainty analysis |
| | MO4 | Global | – | −Decision-making processes<br>−Improved processes with which to analyse risk information<br>−Case study |
| | MO5 | Data | – | −Use of risk patterns<br>−Associative risk management<br>−Case study |
| | MO6 | Global | Logistic regression models | −Predictive techniques<br>−Dynamic risk assessment<br>−Focus on SMEs |
| | MO7 | Data | Heuristic techniques | −Dynamic risk assessment<br>−Importance of the environment and third parties in risk |
| | MO8 | Supply chains | Stochastic & Deterministic techniques | −Mixed application of stochastic and deterministic techniques<br>−Reduction in the degree of uncertainty<br>−Decision-making processes |
| | MO9 | ICS | Mind Maps | −Dynamic risk assessment<br>−Associative risk management<br>−Case study |
| **Methodology** | ME1 | Global | Fuzzy techniques | −Reduction in the degree of uncertainty<br>−Importance of the environment and third parties in risk |
| | ME2 | Global | FMEA | −Reduction of uncertainty |
| | ME3 | Critical Infrastructure | Bow Tie Models, Bayesian Networks | −Concurrent analysis of risks and vulnerabilities<br>−Case study |
| | ME4 | IoT | – | −Exploitability value of vulnerabilities.<br>−Degrees of vulnerability |
| | ME5 | Financial | – | −Adaptation to dynamic scenarios<br>−Focus on SMEs<br>−Prototyping and application in real cases |
| | ME6 | I4.0 - HMI | VIKOR, DEMATEL, ANP<br>Fuzzy techniques | −Reduction in the degree of uncertainty<br>−Importance of the environment in risk |
| **Others** | O1 | Global | – | −Progressive improvement of risk levels |
| | O2 | Data Centre | – | −Risk analysis in virtualisation<br>−Risks in data centres outside but part of the IS |

aspect is that of taking into account the concept of collaborative risk, i.e., enabling several companies to align their risk systems in order to manage risks more efficiently [93,94].

- AE — Valuation of Elements: Some researchers have placed the focus of the problem of current risk analysis methodologies on the lack of quantitative valuation mechanisms for the different elements associated with risk [95], which do not allow costs to be calculated correctly [96].
- DM — Dynamic Metrics: Another group of researchers has focused their studies on the need for methodologies with which to advance in the development and automation of dynamic risk metrics [97], highlighting the need for current risk analysis systems to have adequate metrics [98].

**Table 3** Comparison of the selected proposals

| Type | Initiative | AC | HA | RKL | DY | CC | AE | DM | LLS | SLC | TS | GS | PC |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Process** | **P1** | No | Part. | No | No | No | Part. | No | No | No | No | No | No |
| | **P2** | No | Part. | No | No | No | Part. | No | No | No | Yes | No | Yes |
| | **P3** | No | Part. | No | No | No | Part. | No | Part. | No | No | No | Part. |
| | **P4** | No | Part. | No | No | No | Part. | No | Part. | No | No | No | No |
| **Framework** | **F1** | No | Part. | No | No | No | No | No | No | No | No | No | No |
| | **F2** | No | No | Yes | No | No | No | No | No | No | No | No | No |
| | **F3** | No | Part. | Yes | No | No | No | No | No | No | No | Yes | No |
| | **F4** | No | No | Part. | No | No | No | No | Part. | No | No | Yes | No |
| | **F5** | No | No | No | No | No | Part. | No | Part. | No | No | No | No |
| | **F6** | No | Part. | Yes | Part. | No | No | No | No | No | No | Yes | No |
| | **F7** | No | No | No | No | No | Part. | No | Part. | No | No | Yes | No |
| | **F8** | No | Part. | Yes | No | No | Part. | No | No | Yes | Yes | Yes | No |
| | **F9** | Part. | No | No | No | No | No | No | No | No | Part. | Yes | Part. |
| **Model** | **MO1** | No | Part. | No | Part. | No | Part. | No | Part. | No | No | Yes | Yes |
| | **MO2** | No | No | Part. | No | No | Part. | No | No | No | No | Yes | Yes |
| | **MO3** | No | Part. | No | No | No | Part. | No | Part. | No | No | Yes | No |
| | **MO4** | No | Part. | Part. | No | No | No | No | No | No | No | Yes | Yes |
| | **MO5** | Part. | Part. | No | No | No | Part. | No | No | No | No | No | Part. |
| | **MO6** | No | No | No | Part. | No | No | No | Part. | Part. | No | Yes | Yes |
| | **MO7** | No | Part. | No | Part. | No | No | No | No | No | No | No | No |
| | **MO8** | No | No | No | Part. | No | Part. | No | No | No | No | No | No |
| | **MO9** | Part. | Yes | No | Yes | No | Part. | No | No | No | No | No | Yes |
| **Methodology** | **ME1** | No | Part. | No | Part. | No | Part. | No | Part. | No | No | Yes | No |
| | **ME2** | No | Part. | No | No | No | Part. | No | Part. | No | No | Yes | No |
| | **ME3** | No | No | No | No | No | No | No | No | No | No | No | Yes |
| | **ME4** | No | No | No | No | No | Part. | No | No | No | No | No | Yes |
| | **ME5** | No | No. | No | Yes | No | Part. | Yes | No | Yes | Yes | No | Yes |
| | **ME6** | No | Parc. | No | No | No | No | No | Yes | No | No | No | No |
| **Others** | **O1** | No | No | Yes | No | No | Part. | No | No | No | No | Yes | No |
| | **O2** | No | Part. | No | Part. | No | No | No | No | No | No | No | Part. |

- LLS — Low Level of Subjectivity: Other researchers highlight the problem of the number of subjective aspects that must be defined when generating a risk analysis. This means that the results are limited to internal use by the company but cannot be taken into account by third parties interested in objective and replicable results regardless of the consultant who performs them [99,100].
- SLC — Simplicity and Low Cost: Another problem highlighted by researchers is the high complexity of many current risk analysis methodologies, making simplicity and practical orientation of risk analysis critical for companies [101,102], and particularly SMEs [103−106].
- TS — Supported by Tools: Some researchers and institutions such as NATO emphasise that one of the fundamental points in risk analysis methodologies is to be able to rely on tools that support it, allow the automation of tasks and facilitate compliance with the methodologies [60,107].

Two new characteristics have been added to these desirable characteristics. These were obtained by applying the action research method to real cases on the basis of the authors' experience of real companies' needs. Specifically:

- GS — Scope of application (Global Scope): whether the model is applied globally to the security of a company's information systems, or only to a subset of them. It is desirable for its scope of application to be global.
- PC — Practical Cases: The model should be developed and refined on the basis of practical cases. This is necessary in order to reinforce its real applicability.

It is considered that each of these aspects can be totally fulfilled (Yes), partially fulfilled (Part) or not taken into account by the model (No).

As Table 3 shows, very few papers describe complex case studies that show the possibility of applying the proposed model or methodology in practice, and the benefits that could be attained from doing so. Moreover, although some of them attempt to develop dynamic low-cost processes, they have a high level of complexity as regards their implementation. It will be noted that none of the proposals studied has all the characteristics required for them to be implemented in any type of company, regardless of its characteristics and size.

The analysis of Table 3, therefore, makes it possible to conclude the following:

- AC — Adaptive Catalogues: Practically no proposal orients part of its operation towards the existence of element catalogues that can vary over time without altering the methodology.
- HA — Hierarchy and Associativity: None of the proposals fully takes into account the concepts of hierarchy and associativity among risk analyses, leaving aside fundamental concepts such as shared assets or dependencies among different risk analyses. However,

many have already begun to consider that this aspect is fundamental.

- RKL — Knowledge Reuse and Learning: Only a few proposals highlight the need to be able to reuse knowledge for future implementations. But few of them implement adequate processes for knowledge reuse, and especially for learning from experience.
- DY — Dynamic and evolutionary: Some proposals highlight the need for risk analysis to be dynamic, but without providing complete solutions with which to make the system dynamic. The remaining proposals do not consider this characteristic.
- CC — Collaborative Capacity: None of the proposals studied considers the concept of collaborative networks among companies as a solution by which to better protect companies from external threats.
- AE — Valuation of Elements: Not all the proposals contemplate the valuation of elements as part of this, i.e., taking into account aspects such as the quantitative value of assets, impacts, etc. However, quite a few of them do analyse some of these aspects.
- DM — Dynamic Metrics: Although many of the proposals include formulas with which to calculate risk, none of them consider the possibility of these formulas being dynamic, i.e., that they could be sufficiently versatile to calculate risk in different ways from the basic elements of the risk analysis.
- LLS — Low Level of Subjectivity: With regard to the development of additional mechanisms with which to reduce the level of subjectivity, some proposals have made efforts in this direction, albeit at a conceptual level.
- SLC — Simplicity and Low Cost: The orientation towards simple methodologies and models that can be applied by SMEs has barely been taken into account as a differentiating factor in the proposals studied, signifying that no real mechanisms have been developed that would allow these proposals to be really useful for SMEs.
- TS — Supported by Tools: Some proposals have already identified the need to be supported by tools in order to automate part of their processes. Other proposals have developed partial tools that support part of the process.
- GS — Scope of application: Although some proposals are already oriented towards their application in the scope of an Information System as a whole, there are still many that are focused on specific areas. This signifies that they should be complemented with other mechanisms in order to achieve a risk analysis with a complete scope.
- PC — Practical Cases: Most of the proposals contemplate risk analysis from a theoretical point of view, without establishing concrete risk-management mechanisms based on practical cases.

## 6 The MARISMA framework

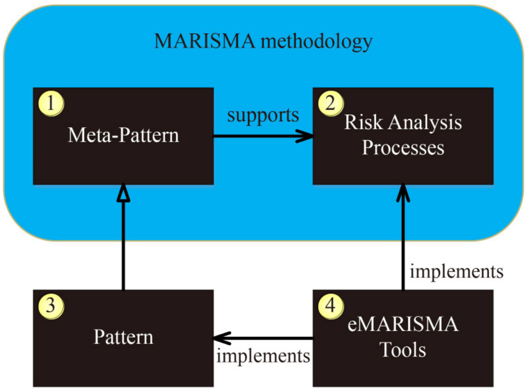

**Fig. 1** MARISMA methodology

The shortcomings identified during the systematic review have been used as the basis on which to propose the development of a framework called MARISMA (Methodology for the Analysis of Risks on Information Systems, using Meta-pattern and Adaptability). This framework consists of the four elements shown in Fig. 1, i.e., a structure denominated as a meta-pattern, a set of processes, a knowledge base and a tool that supports the aforementioned elements:

- The first two elements form the core of the methodology: i) The first of these elements is a structure denominated as a meta-pattern (number 1 in Fig. 1), whose objective is to support the different information models of the methodology, and which contains the elements required in order to be able to perform a risk analysis and its subsequent management. This meta-pattern is made up of three base elements, denominated as Control-Asset-Threat (CAT) (see Fig. 2), and two matrices connecting these elements. The meta-pattern is a common structure for all the patterns (normative schemes in which to perform the risk analysis) that are applied in the methodology. ii) The second element is the set of processes of which the methodology is composed (number 2 in Fig. 1) and comprises three processes that deal with the risk analysis and management life cycle (see Fig. 3), since they make the system dynamic, thus allowing it to evolve over time. These three processes are: i) the RPG (Risk Pattern Generator) Process , whose objective is the Generation of patterns for risk analysis, including their relationships and the knowledge acquired in the different implementations; ii) the RAMG (Risk

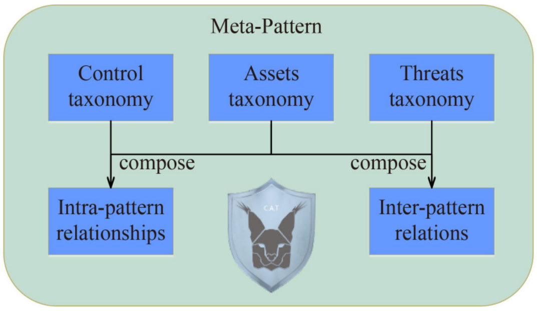

**Fig. 2** CAT meta-pattern

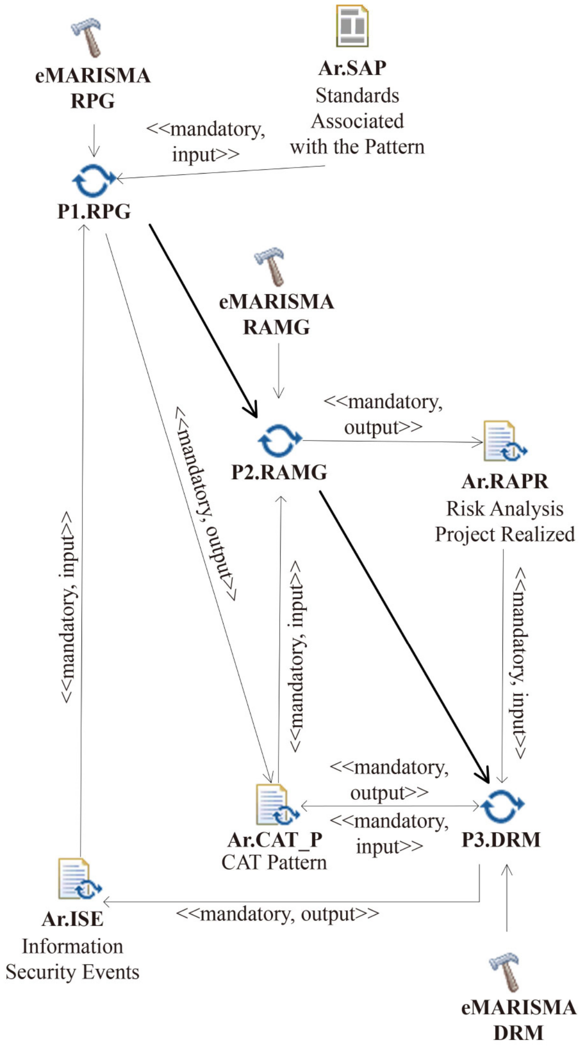

**Fig. 3** Overview in SPEM of the processes in the methodology

Analysis and Management Generator) Process, which deals with the Generation of risk analysis and management through the instantiation of the most appropriate pattern. It also allows the definition of dynamic metrics with which to value assets and the risk calculation formula itself, thus making it possible to solve the problems of AE - Valuation of Elements and DM - Dynamic Metrics, and iii) the DRM (Dynamic Risk Management) Process, which deals with the dynamic maintenance of risk analysis through the use of the matrices that interconnect the different artefacts, and that allow the system to recalculate the risk as security incidents occur, the defined metrics fail, or the expert systems generate suggestions.

- This framework also has a third element. This is a knowledge base of patterns (number 3 in Fig. 1) that allows the maintenance of different normative patterns, along with the knowledge acquired from their instantiation in the different risk analyses.
- Finally, the fourth element is the tool (number 4 Fig. 1) that supports the entire methodology, allowing its use to be automated (see Fig. 4).

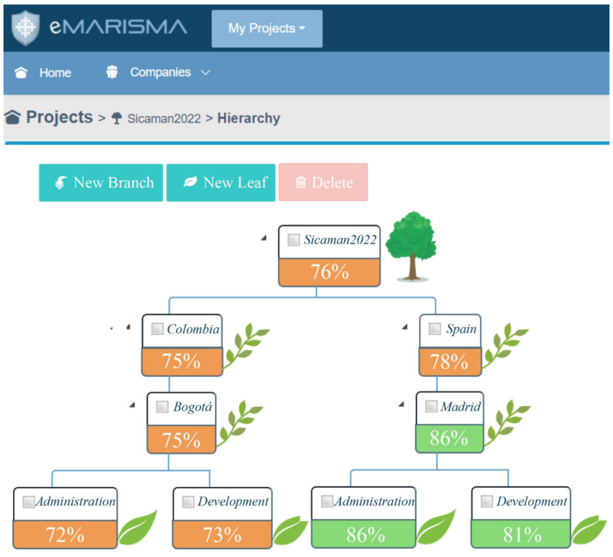

**Fig. 4** Example of audits tree of eMARISMA tool

- Each of the elements in the framework was created with the objective of solving one or more of the problems identified throughout the systematic review:
- The use of the Meta-pattern makes it possible to solve the problem of having "AC - Adaptive Catalogues", by providing a knowledge base with different patterns that can evolve, and in which controls have been included as an integrated element. Most existing methodologies do not, however, consider controls or safeguards until the risk management phase, considering it an independent element of assets, threats and vulnerabilities, and thus complicating the development and monitoring of risk analysis.
- Furthermore, the ability to learn from these patterns, along with the concept of legacy, which is implemented through the use of inter-pattern relationships, both make it possible to fulfil the need for "RKL - Reuse of Knowledge and Learning", since this structure allows this knowledge to be stored and the patterns to evolve over time.
- The "DY - Dynamic and evolutionary" problem is solved by using the three processes of the methodology. These processes exchange information in order to make the system learn and evolve: i) The generation of an event in the DRM process causes: ii) The instance associated with the event to evolve by changing aspects such as the level of coverage of a control, or the probability of occurrence of a threat associated with the RAMG process; and iii) Changes in the pattern associated with the instance that was created by the RPG process, thus allowing it to readjust the relationships between its elements, and to readjust elements associated with the temporary external risk, thereby helping to create a global security shield among the companies that use that pattern; iv) Furthermore, when a pattern undergoes changes as a result of the learning of the instances, these also evolve by means of the legacy principle, and the acquired knowledge is

transmitted, and v) The changes that produce evolution in the patterns are eventually transmitted to all the instances in order to help them to improve, thus producing an evolution in them.

- The problem of "LLS - Low Level of Subjectivity" has been solved by implementing different methods: on the one hand, in the RAMG process we perform a pre-audit with a higher level of accuracy that reduces the initial level of ambiguity, and on the other, in the DRM process we have implemented an expert system of suggestions that learns from the events in order to make the system tend towards reality as security events occur.
- The "CC - Collaborative Capacity" problem is solved through the use of pattern legacy, along with the ability to acquire and share the information obtained in the DRM process among the different instances of a pattern, or its ascendants-descendants.
- In order to automate all the tasks and take advantage of the learning and dynamism capabilities, the eMARISMA tool has been implemented, thus providing a solution to the problems of "SLC - Simplicity and Low Cost" and "TS - Supported by Tools".
- The tool also makes it possible to support the knowledge base, allowing specialised patterns to be obtained for different application scopes. This, therefore, provides a solution to the problem of "GS - Scope of application", in addition to having a wide base of practical cases that allow the system to learn and evolve in the face of changing circumstances and technologies. A solution to the problem of "PC - Practical Cases" is, therefore, provided.

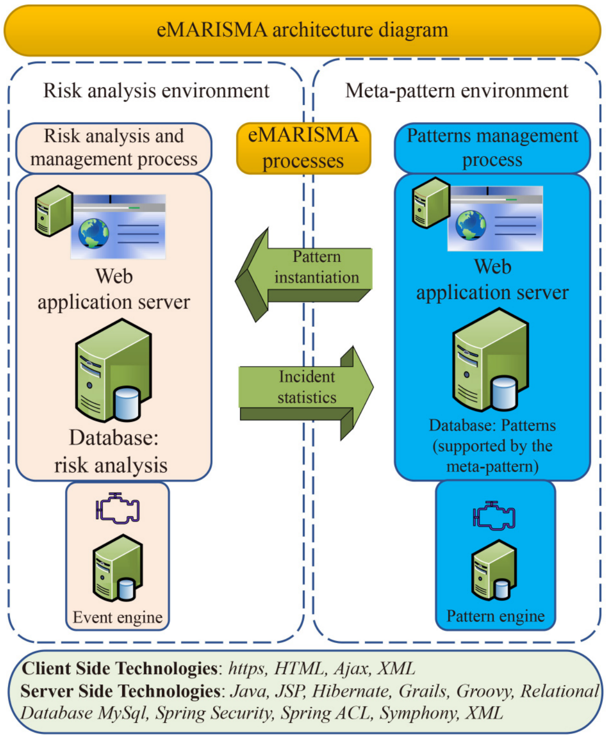
eMARISMA architecture diagram
Risk analysis environment
Meta-pattern environment
Risk analysis and management process
eMARISMA processes
Patterns management process
Web application server
Pattern instantiation
Web application server
Incident statistics
Database: risk analysis
Database: Patterns (supported by the meta-pattern)
Event engine
Pattern engine
Client Side Technologies: https, HTML, Ajax, XML
Server Side Technologies: Java, JSP, Hibernate, Grails, Groovy, Relational Database MySql, Spring Security, Spring ACL, Symphony, XML

**Fig. 5** Diagram of eMARISMA architecture

The MARISMA framework originated as the main result of several PhD theses of members of our research team. It has been developed using an iterative and incremental process and is directly applied to customers of our spin-offs. We are specifically applying MARISMA in order to carry out the risk analysis and management of dozens of companies in Spain, Colombia, Ecuador, and Argentina and from different sectors, such as government, critical infrastructures, hydrocarbons, chemical, and naval. This has allowed us to evaluate and improve each component of the risk analysis and management framework. The eMARISMA tool is based on cloud computing and was developed using an open architecture based on Java technology under Grails. Its security layers are based on Spring Security and ACL (Access Control List) and its relational schema is supported by MySQL. It is divided into two independent parts (see Fig. 5). On the one hand, there is the pattern generator, which functions as a pattern repository and a knowledge repository. On the other, there is the risk and event analysis manager, which can be located on different servers, and which communicates with the pattern module in order to instantiate patterns and send new knowledge to it.

## 7 Conclusions

This paper presents a systematic review of the different processes, frameworks, models and methodologies for risk analysis and management, with the aim of determining their main shortcomings with respect to the current technological state of the art.

As a result of this review, it has been possible to establish the importance of the management and analysis of information systems security risks in the performance and sustainable evolution of companies. This is a basic requirement in order to achieve the organisational mission and objectives in a highly competitive environment.

A large number of processes, frameworks and methods for risk management have been analysed in detail. It was consequently possible to discover that the need for their use in order to effectively protect a company's assets is being increasingly recognised and considered by organisations. However, as demonstrated, despite their value, they do not fully cover the current needs of companies, which is hindering the development of proper security management within organisations. Ten shortcomings or weaknesses were identified during the systematic review, and these need to be reinforced in order to make these systems more effective. These shortcomings have been addressed through the development of a specific framework for risk analysis and management denominated as MARISMA. This has, through the use of different techniques and artefacts, made it possible to provide a total or partial solution to these shortcomings.

As future work, we intend to continue evolving the framework in order to further optimise the solutions to each of the shortcomings identified. This will be done by employing the knowledge base that is being obtained using current implementations, which will be achieved through the use of artificial intelligence techniques.

**Acknowledgements** This work has been developed within the AETHER-UCLM (PID2020-112540RB-C42) funded by MCIN/AEI/10.13039/501100011033, Spain, ALBA-UCLM (TED2021-130355B-C31, id.4809130355-130355-28-521) and ALBA-UC (TED2021-130355B- C33, id.3611130630-130630-28-521) funded by the "Ministerio de Ciencia e Innovacion", Spain, and supported by the European Union's Horizon 2020 Project "CyberSANE" under Grant Agreement No. 833683. We are grateful to the following companies for their support: Sicaman Nuevas Tecnologías S.L. and Marisma Shield S.L., since they have facilitated the validation of case studies and the use of the eMARISMA tool.

**Funding note** Open Access funding provided thanks to the CRUE-CSIC agreement with Springer Nature

# References

1. Hussain A, Mohamed A, Razali S. A review on cybersecurity: challenges & emerging threats. In: Proceedings of the 3rd International Conference on Networking, Information Systems & Security, 2020, 28
2. Hölbl M, Welzer T. Experience with teaching cybersecurity. In: Proceedings of the 27th EAEEIE Annual Conference (EAEEIE). 2017, 1−4
3. Toapanta S M T, Gurumendi A J, Gallegos L E M. An approach of national and international cybersecurity laws and standards to mitigate information risks in public organizations of Ecuador. In: Proceedings of the 2nd International Conference on Education Technology Management. 2019, 61−66
4. Shamala P, Ahmad R, Zolait A, Sedek M. Integrating information quality dimensions into information security risk management (ISRM). Journal of Information Security and Applications, 2017, 36: 1–10
5. Mirtsch M, Blind K, Koch C, Dudek G. Information security management in ICT and non-ICT sector companies: a preventive innovation perspective. Computers & Security, 2021, 109: 102383
6. Hentea M. Security management. In: Hentea M, ed. Building an Effective Security Program for Distributed Energy Resources and Systems: Understanding Security for Smart Grid and Distributed Energy Resources and Systems, Volume 1. Wiley, 2021, 405–436
7. Kumah P. The role of human resource management in enhancing organizational information systems security. In: Misra S, Adewumi A, eds. Handbook of Research on the Role of Human Factors in IT Project Management. Hershey, PA, USA: IGI Global, 2019, 278–303
8. Lee H, Han C, Yoo T. The application of mistake-proofing to organisational security management. Total Quality Management & Business Excellence, 2019, 30(9–10): 1151–1166
9. Li F, Chen T, Wang B, Zhang J, Qing S. Research on information security technology of mobile application in electric power industry. In: Proceedings of 2020 Asia-Pacific Conference on Image Processing, Electronics and Computers (IPEC). 2020, 51−54
10. Nasir A, Arshah R A, Hamid M R A, Fahmy S. An analysis on the dimensions of information security culture concept: a review. Journal of Information Security and Applications, 2019, 44: 12–22
11. Khando K, Gao S, Islam S M, Salman A. Enhancing employees information security awareness in private and public organisations: a systematic literature review. Computers & Security, 2021, 106: 102267
12. Ganin A A, Quach P, Panwar M, Collier Z A, Keisler J M, Marchese D, Linkov I. Multicriteria decision framework for cybersecurity risk assessment and management. Risk Analysis, 2020, 40(1): 183–199
13. van der Schyff K, Flowerday S. Mediating effects of information security awareness. Computers & Security, 2021, 106: 102313
14. Prajanti A D, Ramli K. A proposed framework for ranking critical information assets in information security risk assessment using the OCTAVE allegro method with decision support system methods. In: Proceedings of the 34th International Technical Conference on Circuits/Systems, Computers and Communications (ITC-CSCC). 2019, 1−4
15. Chopra A, Chaudhary M. The need for information security. In: Chopra A, Chaudhary M, eds. Implementing an Information Security Management System: Security Management Based on ISO 27001 Guidelines. Berkeley, CA: Apress, 2020, 1−20
16. Grishaeva S A, Borzov V I. Information security risk management. In: Proceedings of 2020 International Conference Quality Management, Transport and Information Security, Information Technologies (IT&QM&IS). 2020, 96−98
17. Zaini M K, Masrek M N, Abdullah Sani M K J. The impact of information security management practices on organisational agility. Information and Computer Security, 2020, 28(5): 681–700
18. Kiedrowicz M, Stanik J. Method for assessing efficiency of the information security management system. MATEC Web of Conferences, 2018, 210: 04011
19. Sánchez L E, Santos-Olmo A, Fernandez-Medina E, Piattini M. ISMS building for SMEs through the reuse of knowledge. In: Management Association I R, ed. Small and Medium Enterprises: Concepts, Methodologies, Tools, and Applications. Hershey, PA, USA: IGI Global, 2013, 394−419
20. Santos-Olmo A, Sánchez L E, Caballero I, Camacho S, Fernandez-Medina E. The importance of the security culture in SMEs as regards the correct management of the security of their assets. Future Internet, 2016, 8(3): 30
21. Wangen G, Hallstensen C, Snekkenes E. A framework for estimating information security risk assessment method completeness. International Journal of Information Security, 2018, 17(6): 681–699
22. Achmadi D, Suryanto Y, Ramli K. On developing information security management system (ISMS) framework for ISO 27001-based data center. In: Proceedings of 2018 International Workshop on Big Data and Information Security (IWBIS). 2018, 149−157
23. Jeong C Y, Lee S Y T, Lim J H. Information security breaches and IT security investments: impacts on competitors. Information & Management, 2019, 56(5): 681–695
24. Uchendu B, Nurse J R C, Bada M, Furnell S. Developing a Cyber Security culture: current practices and future needs. Computers & Security, 2021, 109: 102387
25. Casola V, Catelli R, De Benedictis A. A first step towards an ISO-based information security domain ontology. In: Proceedings of the 28th IEEE International Conference on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE). 2019, 334−339
26. Shameli-Sendi A. An efficient security data-driven approach for implementing risk assessment. Journal of Information Security and Applications, 2020, 54: 102593
27. Putra I M M, Mutijarsa K. Designing information security risk management on Bali regional police command center based on ISO 27005. In: Proceedings of the 3rd East Indonesia Conference on Computer and Information Technology (EIConCIT). 2021, 14−19
28. Hariyanti E, Djunaidy A, Siahaan D O. A conceptual model for information security risk considering business process perspective. In: Proceedings of the 4th International Conference on Science and Technology (ICST). 2018, 1−6

29. Szwaczyk S, Wrona K, Amanowicz M. Applicability of risk analysis methods to risk-aware routing in software-defined networks. In: Proceedings of 2018 International Conference on Military Communications and Information Systems (ICMCIS). 2018, 1−7
30. Ruan K. Introducing cybernomics: a unifying economic framework for measuring cyber risk. Computers & Security, 2017, 65: 77–89
31. Dobaj J, Schmittner C, Krisper M, Macher G. Towards integrated quantitative security and safety risk assessment. In: Proceedings of 2019 International Conference on Computer Safety, Reliability, and Security. 2019, 102−116
32. Sönmez F Ö, Kılıç B G. A decision support system for optimal selection of enterprise information security preventative actions. IEEE Transactions on Network and Service Management, 2021, 18(3): 3260–3279
33. Tiganoaia B, Niculescu A, Negoita O, Popescu M. A new sustainable model for risk management—RiMM. Sustainability, 2019, 11(4): 1178
34. Amutio M A, Candau J, Manas J A. MAGERIT-version 3.0 Methodology for information systems risk analysis and management. Ministry of Finance and Public Administration, 2014
35. Ali M L, Thakur K, Atobatele B. Challenges of cyber security and the emerging trends. In: Proceedings of 2019 ACM International Symposium on Blockchain and Secure Critical Infrastructure. 2019, 107−112
36. Khambhammettu H, Boulares S, Adi K, Logrippo L. A framework for risk assessment in access control systems. Computers & Security, 2013, 39: 86–103
37. Jouini M, Rabai L B A. A security risk management model for cloud computing systems: infrastructure as a service. In: Proceedings of the10th International Conference on Security, Privacy, and Anonymity in Computation, Communication, and Storage. 2017, 594−608
38. Weil T. Risk assessment methods for cloud computing platforms. In: Proceedings of the 43rd IEEE Annual Computer Software and Applications Conference (COMPSAC). 2019, 545−547
39. Brunner M, Sauerwein C, Felderer M, Breu R. Risk management practices in information security: exploring the status quo in the DACH region. Computers & Security, 2020, 92: 101776
40. Zakaria H, Abu Bakar N A, Hassan N H, Yaacob S. IoT security risk management model for secured practice in healthcare environment. Procedia Computer Science, 2019, 161: 1241–1248
41. Zhang Z. A new method for information security risk management in big data environment. In: Proceedings of the 2nd International Conference on Information Technology and Computer Application (ITCA). 2020, 1−4
42. Fu Y, Zhu J, Gao S. CPS information security risk evaluation system based on petri net. In: Proceedings of the 2nd IEEE International Conference on Data Science in Cyberspace (DSC). 2017, 541−548
43. Mokalled H, Pragliola C, Debertol D, Meda E, Zunino R. A comprehensive framework for the security risk management of cyber-physical systems. In: Flammini F, ed. Resilience of Cyber-Physical Systems: From Risk Modelling to Threat Counteraction. Cham: Springer International Publishing, 2019, 49−68
44. Chen J, Zhu Q. Interdependent strategic security risk management with bounded rationality in the internet of things. IEEE Transactions on Information Forensics and Security, 2019, 14(11): 2958–2971
45. Capodieci A, Mainetti L, Dipietrangelo F. Model-driven approach to cyber risk analysis in industry 4.0. In: Proceedings of the 10th International Conference on Information Systems and Technologies. 2020, 33
46. Malik V, Singh S. Security risk management in IoT environment. Journal of Discrete Mathematical Sciences and Cryptography, 2019, 22(4): 697–709
47. Govender S G, Kritzinger E, Loock M. A framework and tool for the assessment of information security risk, the reduction of information security cost and the sustainability of information security culture. Personal and Ubiquitous Computing, 2021, 25(5): 927–940
48. Javaid M I, Iqbal M M W. A comprehensive people, process and technology (PPT) application model for Information Systems (IS) risk management in small/medium enterprises (SME). In: Proceedings of 2017 International Conference on Communication Technologies (ComTech). 2017, 78−90
49. Paltrinieri N, Reniers G. Dynamic risk analysis for Seveso sites. Journal of Loss Prevention in the Process Industries, 2017, 49: 111–119
50. Affia A A O, Matulevičius R, Nolte A. Security risk management in cooperative intelligent transportation systems: a systematic literature review. In: Proceedings of 2019 OTM Confederated International Conferences “On the Move to Meaningful Internet Systems”. 2019, 282−300
51. Genchev P G. Analysis of changes in the probability of an incident with information security. In: Proceedings of the 56th International Scientific Conference on Information, Communication and Energy Systems and Technologies (ICEST). 2021, 119−122
52. Kitchenham B, Charters S. Guidelines for performing systematic literature reviews in software engineering. 2007
53. Kitchenham B, Brereton P. A systematic review of systematic review process research in software engineering. Information and Software Technology, 2013, 55(12): 2049–2075
54. Barat S, Clark T, Barn B, Kulkarni V. A model-based approach to systematic review of research literature. In: Proceedings of the 10th Innovations in Software Engineering Conference. 2017, 15−25
55. Barn B, Barat S, Clark T. Conducting systematic literature reviews and systematic mapping studies. In: Proceedings of the 10th Innovations in Software Engineering Conference. 2017, 212−213
56. Lo C C, Chen W J. A hybrid information security risk assessment procedure considering interdependences between controls. Expert Systems with Applications, 2012, 39(1): 247–257
57. Wulan M, Petrovic D. A fuzzy logic based system for risk analysis and evaluation within enterprise collaborations. Computers in Industry, 2012, 63(8): 739–748
58. Deb R, Roy S. A Software Defined Network information security risk assessment based on Pythagorean fuzzy sets. Expert Systems with Applications, 2021, 183: 115383
59. Zhang H, Sun Q. An integrated approach to risk assessment for special line shunting via fuzzy theory. Symmetry, 2018, 10(11): 599
60. Saleh M S, Alfantookh A. A new comprehensive framework for enterprise information security risk management. Applied Computing and Informatics, 2011, 9(2): 107–118
61. Alhawari S, Karadsheh L, Nehari Talet A, Mansour E. Knowledge-based risk management framework for information technology project. International Journal of Information Management, 2012, 32(1): 50–65
62. Shamala P, Ahmad R, Yusoff M. A conceptual framework of info structure for information security risk assessment (ISRA). Journal of Information Security and Applications, 2013, 18(1): 45–52
63. Khan F, Hashemi S J, Paltrinieri N, Amyotte P, Cozzani V, Reniers G. Dynamic risk management: a contemporary approach to process safety management. Current Opinion in Chemical Engineering, 2016, 14: 9–17
64. Sangaiah A K, Samuel O W, Li X, Abdel-Basset M, Wang H. Towards an efficient risk assessment in software projects−Fuzzy reinforcement paradigm. Computers & Electrical Engineering, 2018, 71: 833–846
65. Panchal D, Singh A K, Chatterjee P, Zavadskas E K, Keshavarz-Ghorabaee M. A new fuzzy methodology-based structured framework for RAM and risk analysis. Applied Soft Computing, 2019, 74: 242–254
66. Schmitz C, Pape S. LiSRA: Lightweight Security Risk Assessment for decision support in information security. Computers & Security, 2020, 90: 101656
67. Lamine E, Thabet R, Sienou A, Bork D, Fontanili F, Pingaud H.

BPRIM: an integrated framework for business process management and risk management. Computers in Industry, 2020, 117: 103199

68. Feng N, Li M. An information systems security risk assessment model under uncertain environment. Applied Soft Computing, 2011, 11(7): 4332–4340

69. Ou Yang Y P, Shieh H M, Tzeng G H. A VIKOR technique based on DEMATEL and ANP for information security risk control assessment. Information Sciences, 2013, 232: 482–500

70. Feng N, Wang H J, Li M. A security risk analysis model for information systems: causal relationships of risk factors and vulnerability propagation analysis. Information Sciences, 2014, 256: 57–73

71. Wang L, Wang B, Peng Y. Research the information security risk assessment technique based on Bayesian network. In: Proceedings of the 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE). 2010

72. Webb J, Ahmad A, Maynard S B, Shanks G. A situation awareness model for information security risk management. Computers & Security, 2014, 44: 1–15

73. Tubío Figueira P, López Bravo C, Rivas López J L. Improving information security risk analysis by including threat-occurrence predictive models. Computers & Security, 2020, 88: 101609

74. Khan F, Kim J H, Mathiassen L, Moore R. Data breach management: an integrated risk model. Information & Management, 2021, 58(1): 103392

75. Schmidt A, Albert L A, Zheng K. Risk management for cyber-infrastructure protection: a bi-objective integer programming approach. Reliability Engineering & System Safety, 2021, 205: 107093

76. Cherdantseva Y, Burnap P, Nadjm-Tehrani S, Jones K. A configurable dependency model of a SCADA system for goal-oriented risk assessment. Applied Sciences, 2022, 12(10): 4880

77. Vicente E, Mateos A, Jiménez-Martín A. Risk analysis in information systems: a fuzzification of the MAGERIT methodology. Knowledge-Based Systems, 2014, 66: 1–12

78. Mandal S, Maiti J. Risk analysis using FMEA: fuzzy similarity value and possibility theory based approach. Expert Systems with Applications, 2014, 41(7): 3527–3537

79. van Staalduinen M A, Khan F, Gadag V, Reniers G. Functional quantitative security risk analysis (QSRA) to assist in protecting critical process infrastructure. Reliability Engineering & System Safety, 2017, 157: 23–34

80. Abdo H, Kaouk M, Flaus J M, Masse F. A safety/security risk analysis approach of Industrial Control Systems: a Cyber Bowtie − combining new version of attack tree with bowtie analysis. Computers & Security, 2018, 72: 175–195

81. Sicari S, Rizzardi A, Miorandi D, Coen-Porisini A. A risk assessment methodology for the Internet of Things. Computer Communications, 2018, 129: 67–79

82. Armenia S, Angelini M, Nonino F, Palombi G, Schlitzer M F. A dynamic simulation approach to support the evaluation of cyber risks and security investments in SMEs. Decision Support Systems, 2021, 147: 113580

83. Bozkuş E, Kaya İ, Yakut M. A fuzzy based model proposal on risk analysis for human-robot interactive systems. In: Proceedings of 2022 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA). 2022, 1−6

84. Sato H. A new formula of security risk analysis that takes risk improvement factor into account. In: Proceedings of the IEEE Third International Conference on Privacy, Security, Risk and Trust and 2011 IEEE Third International Conference on Social Computing. 2011, 1243−1248

85. Munodawafa F, Awad A I. Security risk assessment within hybrid data centers: a case study of delay sensitive applications. Journal of Information Security and Applications, 2018, 43: 61–72

86. Scala N M, Reilly A C, Goethals P L, Cukier M. Risk and the five hard problems of Cybersecurity. Risk Analysis, 2019, 39(10): 2119–2126

87. Li Q, Lv P, Wang M, Zhang Z, Wang S, Fang P, Gao L. A risk assessment method of smart grid in cloud computing environment based on game theory. In: Proceedings of the 5th IEEE International Conference on Cloud Computing and Big Data Analytics (ICCCBDA). 2020, 67−72

88. Malik V, Singh S. Intelligent strategies for cloud computing risk management and testing. In: Proceedings of ICMDE 2020 Computational Methods and Data Engineering. 2020, 101−114

89. Volkov A I, Semin V G, Khakimullin E R. Modeling the structures of threats to information security risks based on a fuzzy approach. In: Proceedings of 2020 International Conference Quality Management, Transport and Information Security, Information Technologies (IT&QM&IS). 2020, 132−135

90. Petrescu A G, Postole M A, Ciobanasu M. The international experience in security risk analysis methods. In: Oncioiu I, ed. Network Security and its Impact on Business Strategy. Hershey, PA, USA: IGI Global, 2019, 157–169

91. Khosravi-Farmad M, Ghaemi-Bafghi A. Bayesian decision network-based security risk management framework. Journal of Network and Systems Management, 2020, 28(4): 1794–1819

92. Genchev P. An approach to support information security risk assessment. In: Proceedings of 2020 International Conference on Biomedical Innovations and Applications (BIA). 2020, 125−128

93. Burnap P, Cherdantseva Y, Blyth A, Eden P, Jones K, Soulsby H, Stoddart K. Determining and sharing risk data in distributed interdependent systems. Computer, 2017, 50(4): 72–79

94. Tagarev T. Towards the design of a collaborative cybersecurity networked organisation: identification and prioritisation of governance needs and objectives. Future Internet, 2020, 12(4): 62

95. Kuzminykh I, Ghita B, Sokolov V, Bakhshi T. Information security risk assessment. Encyclopedia, 2021, 1(3): 602–617

96. Lee I. Cybersecurity: risk management framework and investment cost analysis. Business Horizons, 2021, 64(5): 659–671

97. Arafah M, Bakry S H, Al-Dayel R, Faheem O. Exploring cybersecurity metrics for strategic units: a generic framework for future work. In: Proceedings of 2019 Future of Information and Communication Conference on Information and Communication. 2020, 881−891

98. Kotenko I, Doynikova E, Chechulin A, Fedorchenko A. AI- and metrics-based vulnerability-centric cyber security assessment and countermeasure selection. In: Parkinson S, Crampton A, Hill R, eds. Guide to Vulnerability Analysis for Computer Networks and Systems: An Artificial Intelligence Approach. Cham: Springer International Publishing, 2018, 101−130

99. Piromsopa K, Klima T, Pavlik L. Designing model for calculating the amount of cyber risk insurance. In: Proceedings of the 4th International Conference on Mathematics and Computers in Sciences and in Industry (MCSI). 2017, 196−200

100. Stergiopoulos G, Gritzalis D, Kouktzoglou V. Using formal distributions for threat likelihood estimation in cloud-enabled IT risk assessment. Computer Networks, 2018, 134: 23–45

101. Abbass W, Baina A, Bellafkih M. Using EBIOS for risk management in critical information infrastructure. In: Proceedings of the 5th World Congress on Information and Communication Technologies (WICT). 2015, 107−112

102. Oppliger R, Pernul G, Katsikas S. New frontiers: assessing and managing security risks. Computer, 2017, 50(4): 48–51

103. García-Porras C, Huamani-Pastor S, Armas-Aguirre J. Information security risk management model for Peruvian SMEs. In: Proceedings of 2018 IEEE Sciences and Humanities International Research Conference (SHIRCON). 2018, 1−5

104. Wagner P, Hansch G, Konrad C, John K H, Bauer J, Franke J. Applicability of security standards for operational technology by

SMEs and large enterprises. In: Proceedings of the 25th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA). 2020, 1544−1551

105. Skrodelis H K, Strebko J, Romanovs A. The information system security governance tasks in small and medium enterprises. In: Proceedings of the 61st International Scientific Conference on Information Technology and Management Science of Riga Technical University (ITMS). 2020, 1−4

106. Antunes M, Maximiano M, Gomes R, Pinto D. Information security and cybersecurity management: a case study with SMEs in Portugal. Journal of Cybersecurity and Privacy, 2021, 1(2): 219–238

107. Gill A K, Zavarsky P, Swar B. Automation of security and privacy controls for efficient information security management. In: Proceedings of the 2nd International Conference on Secure Cyber Computing and Communications (ICSCCC). 2021, 371−375

Antonio Santos-Olmo holds a PhD in Computer Science from the University of Castilla-La Mancha, Spain and an MSc in Information Systems Audit from the Polytechnic University of Madrid, Spain. He is also an ISACA Certified Information System Auditor. He is an Assistant Professor at the Escuela Superior de Informática of the University of Castilla-La Mancha in Ciudad Real, Spain. His research activities are management security system, security metrics, data mining, data cleaning, and business intelligence. He is a member of the GSyA research group at the University of Castilla-La Mancha.

Luis Enrique Sánchez holds a PhD in Computer Science from the University of Castilla-La Mancha, Spain, and an MSc in Computer Information Systems Audit from the Polytechnic University of Madrid, Spain. He is an Associate Professor at the Escuela Superior de Informática of the University of Castilla-La Mancha in Ciudad Real, Spain. His research lines are focused on cybersecurity and risk assessment and management. He is a member of the GSyA research group at the University of Castilla-La Mancha.

David G. Rosado has an MSc and a PhD in Computer Science from the University of Málaga, Spain and from the University of Castilla-La Mancha, Spain, respectively. He is an Associate Professor at the Escuela Superior de Informática of Castilla-La Mancha University in Ciudad Real, Spain. His research activities are focused on security for Information Systems and Cloud Computing. He is a member of the GSyA research group at the University of Castilla-La Mancha.

Manuel A. Serrano holds an MSc and a PhD in Computer Science from the University of Castilla-La Mancha, Spain. He is an Associate Professor at the Escuela Superior de Informática of Castilla-La Mancha University in Ciudad Real, Spain. His research interests are cybersecurity (especially in Big Data and IoT), data quality, software quality and measurement and business intelligence. He is member of the Alarcos Research Group at the University of Castilla-La Mancha. His e-mail address is manuel.serrano@uclm.es.

Carlos Blanco holds a PhD in Computer Science from the University of Castilla-La Mancha, Spain. He is an Associate Professor at the University of Cantabria, Spain and is a member of several research groups: GSyA (University of Castilla-La Mancha) and ISTR (University of Cantabria), Spain. His research lines are Security for Information Systems but focused on Big Data, Data Warehouses and OLAP systems by using MDE approaches.

Haralambos Mouratidis is Director of the Institute for Analytics and Data Science (IADS) and a Professor at the School of Computer Science and Electronic Engineering, University of Essex, UK. He holds a BEng (Hons) from the University of Wales, Swansea, UK, and an MSc and a PhD from the University of Sheffield, UK. He is also a Fellow of the Higher Education Academy (HEA) and a Professional Member of the British Computer Society (BCS). His research interests lie in the area of secure software systems engineering, requirements engineering, and information systems development.

Eduardo Fernández-Medina holds a PhD in Computer Science from the University of Castilla-La Mancha, Spain. He is a Full Professor at the Escuela Superior de Informática of the University of Castilla-La Mancha in Ciudad Real, Spain. His research activity deals with security in information systems, and particularly in security in big data, Cloud Computing and CPS. He leads the GSyA research group at the University of Castilla-La Mancha.