Computer Standards & Interfaces 92 (2025) 103935

Contents lists available at ScienceDirect

Computer Standards & Interfaces

journal homepage: www.elsevier.com/locate/csi

MARISMA: A modern and context-aware framework for assessing and managing information cybersecurity risks

Luis E. Sánchez [a,d,*], Antonio Santos-Olmo [a,d], David G. Rosado [a,d], Carlos Blanco [b], Manuel A. Serrano [c], Haralambos Mouratidis [d], Eduardo Fernández-Medina [a]

[a] GSyA Research Group, University of Castilla-La Mancha, Ciudad Real, Spain
[b] ISTR research group, Department of Computer Science and Electronics, University of Cantabria, Spain
[c] Alarcos Research Group, University of Castilla-La Mancha, Ciudad Real, Spain
[d] Institute for Analytics and Data Science, University of Essex, UK

ARTICLE INFO

Keywords:
Security management system
Security risk analysis and management
Reuse of knowledge
Hierarchical risks
Dynamic security risk management

ABSTRACT

In a globalised world dependent on information technology, ensuring adequate protection of an organisation's information assets has become a decisive factor for the longevity of the organisation's operation. This is especially important when these organisations are critical infrastructures that provide essential services to nations and their citizens. However, to protect these assets, we must first be able to understand the risks to which they are subject and how to manage them properly. To understand and manage such the risks, we need first to acknowledge that organisations have changed, and they now have an increasing reliance on information assets, which in many cases are shared with other organisations. Such reliance and interconnectivity means that risks are constantly changing, they are dynamic, and potential mitigation does not just rely on the organisation's own controls, but also on the controls put in place by the organisations with which it shares those assets. Taking the above requirements as essential, we have reviewed the state of the art, and we have concluded that current risk analysis and management systems are unable to meet all the needs inherent in this dynamic and evolving risk environment. This gap in the state of the art requires novel approaches that draw on the foundations of risk management, but they are adapted to the new challenges.

This article fulfils this gap in the literature with the introduction of MARISMA, a novel security risk analysis and management framework. MARISMA is oriented towards dynamic and adaptive risk management, considering external factors such as associative risks between organisations. MARISMA also contributes to the state of the art through newly developed mechanisms for knowledge reuse and dynamic learning. An important advantage of MARISMA is the connections between its elements that make it possible to reduce the subjectivity inherent in classical risk analysis systems, thereby generating suggestions that allow the translation of perceived security risks into real security risks. The framework comprises a reusable meta-pattern comprising different elements and their interdependencies, a supporting method that guides the entire process, and a cloud-based tool that automates data management and risk methods. MARISMA has been applied to many companies from different countries and sectors (government, maritime, energy, and pharmaceutical). In this paper, we demonstrate its applicability through its application to a real world case study involving a company in the technology sector.

1. Introduction

Cybersecurity has become a decisive requirement in a digitalised society, in which the number and impact of threats are constantly growing [1,2], thus requiring adequately protected information systems [3]. Therefore, security management and threat mitigation within information systems have become fundamental concerns for citizens (to preserve their privacy), businesses (to protect digital assets and transactions), and states to protect their critical infrastructures and ensure the continuity of governments and public services [4,5].

* Corresponding author at: GSyA Research Group, University of Castilla-La Mancha, Ciudad Real, Spain.
E-mail addresses: luise.sanchez@uclm.es (L.E. Sánchez), antonio.santosolmo@uclm.es (A. Santos-Olmo), david.grosado@uclm.es (D.G. Rosado), Carlos.Blanco@unican.es (C. Blanco), manuel.serrano@uclm.es (M.A. Serrano), h.mouratidis@essex.ac.uk (H. Mouratidis), eduardo.fdezmedina@uclm.es (E. Fernández-Medina).

https://doi.org/10.1016/j.csi.2024.103935
Received 7 August 2024; Received in revised form 1 October 2024; Accepted 9 October 2024
Available online 10 October 2024

The evolving landscape of cybersecurity demands a comprehensive analysis of emerging risks, particularly as digital threats like deepfakes increasingly challenge information integrity. Advanced detection technologies, such as those leveraging deep learning, are crucial for effectively identifying and mitigating these risks [6]. In the context of managing risks in distributed systems, especially within the Industrial Internet of Things (IoT), the aggregation and optimisation of data using hybrid algorithms are crucial. These methods enhance the accuracy and efficiency of risk management processes in increasingly interconnected environments [7]. Ensuring the security of advanced IoT systems requires robust intrusion detection mechanisms. Utilising blockchain in combination with neural networks offers a promising approach to enhance the resilience and reliability of these systems against emerging threats [8]. A systematic approach to deploying these technologies helps address open issues and enhances the overall security framework [9].

Furthermore, in today's globalised and competitive business environment, companies rely heavily on information systems, which are key to boosting their competitiveness [10]. Therefore, they are aware that information, support systems, and network processes are their paramount assets [11], and are subject to a wide variety of risks that can seriously affect the company [12,13]. Thus, it is important for companies to implement security controls in order to identify and control the risks to which they may be exposed [14,15]. However, the implementation of these controls is insufficient, as systems are needed to manage security over time that are capable of reacting rapidly to issues such as new risks, vulnerabilities, and threats are needed to manage security over time [16]. Thus, security management [17] is required to provide solutions to these problems. However, most companies have chaotic security management systems that lack adequate guidelines, documentation, sufficient resources and a high security culture. On the other hand, understanding the associated risks and their severities for ICPS assets is crucial to protecting them from cyber-attacks; risk analysis is a main step in threat modelling, and the evaluation of risk levels is vital for business decisions [18]. This problem is particularly acute in the case of small and medium-sized enterprises (SMEs), which have limited human and financial resources for providing adequate security management systems.

Therefore, it is necessary to establish mechanisms that are sufficiently simple so that they can be adapted to all types of companies [19], which allows companies to understand their cybersecurity, and in particular the risks associated with it [20], because risk management is an essential process in any business management model, and all the activities of a company involve risks [21]. Thus, an effective risk assessment helps an organisation's top management make optimal decisions and avoid losses [22], which requires the selection and implementation of safeguards to understand, prevent, deter, reduce, or control identified risks.

In response to these needs, the scientific community and international standardisation organisations have proposed a set of techniques and methods that have made it possible to implement risk management mechanisms effectively, with wide acceptance by companies in multiple sectors, especially large enterprises. However, the rapid evolution of information technology, particularly the proliferation of new and more sophisticated cybersecurity risks, has led to new needs that have not been adequately met by previous solutions. One example is the need to consider risk not only at an individual level in the organisation but also derived from the company's relationship with its environment, its circumstances (variants at all times), and with other companies (associative risks), either as technological partners, as third parties in some services provided by the company, or as co-participants in multi-company projects, as well as considering the relationships that can occur between different companies in the same group (hierarchical risks). In this sense, a fundamental aspect is to consider the concept of collaborative risk; that is, several companies can align their risk systems to better manage them, especially when collaboration is vital in the current market situation.

The management of hierarchical and associative risks has also acquired particular importance with the appearance of new developments such as cloud computing [23], fog computing [24], critical cyber infrastructures [25,26], the Internet of Things (IoT) [27,28], Big Data [29], and cyber–physical systems [30] associated with Industry 5.0 [31,32]. These developments have sensibly altered the perception of information system infrastructure and architecture; thus, traditional risk catalogues, which define basic elements such as assets, threats, and controls, as well as their static interrelationships, are not fully capable of adapting to the different specific characteristics of these new emerging technologies. Thus, there is a need for approaches that can adapt risk catalogues and interrelationships to different sectors and technologies [33,34]. Furthermore, when constructing these risk catalogues, a large number of subjective aspects must be defined to perform a risk analysis, which is of particular importance. These subjective factors frequently lead to haphazard and nonanalytical results, resulting in highly subjective risk assessments. This highlights the need to develop new methods to improve risk assessment by making it as objective as possible [35], which is an approach to risk calculation anchored by probability theory [36].

Another key issue for organisations is the cost of performing and maintaining risk analyses and management over time. Current solutions are generally not designed to repeat the process every time changes occur in an asset and risk structure. This leads to high maintenance costs or, in the worst-case scenario, to the necessary updating of risks not taking place and to a lack of awareness of real risks at all times. This maintains a static image of the risks that have occurred months or even years previously, which detracts from the value of the analysis and compromises correct decision-making [37]. Therefore, it is important to develop strategies that make it possible to dynamically maintain the results of risk analysis without increasing costs [38,39] and adapt to any type of organisation, regardless of its size or sector.

Finally, another important issue is the possibility of reusing the knowledge acquired during the execution of previous risk analyses. This gives rise to a system that improves and learns over time and aims to introduce measures to detect, mitigate, predict, and deter attacks using lessons learned over time, both within and among organisations. To this end, it is vital to use support tools that automate tasks and facilitate compliance with the applied methodologies, as the strategic potential of IT security remains mostly untapped because of the lack of appropriate decision-making and communication tools that would enable project managers to address IT security in a purposeful manner [40].

Consequently, considering the preceding analysis, the principal research question this study seeks to address is as follows: Is it feasible to devise a risk analysis approach that aligns with these identified requirements? Specifically, this involves (i) developing the ability to adapt to emerging risks associated with technological advancements such as big data, CPS, and blockchain; (ii) establishing associative and hierarchical relationships among risk components; (iii) facilitating the reuse of knowledge; (iv) managing the dynamic and evolving nature of risks; (v) integrating capabilities that support collaborative risk management among organisations; and (vi) enhancing the objectivity and explainability of decision-making processes.

In response to our research question and building on the foundational contributions of the research and standards community, we developed MARISMA, a comprehensive cybersecurity risk analysis and management framework. MARISMA offers key innovations, including its adaptive catalogues for flexible risk identification, dynamic criteria for real-time risk adjustment, and an emphasis on collaboration between organisations sharing similar technological environments. It maximises automation in risk assessment processes, reducing manual intervention and enhancing efficiency. Additionally, it promotes a holistic approach, covering all organisational assets to ensure no critical element is overlooked, and provides tools for knowledge reuse and learning to continually improve risk management practices. This

framework was designed to adapt to these evolving needs and was conceived predominantly in a real-life context by employing the action–research method throughout the research process. We progressively refined and validated MARISMA for numerous SMEs across Spain, Brazil, and Colombia operating under diverse regulatory frameworks. Moreover, it has been implemented by several large Spanish companies within the critical infrastructure sectors of chemicals and hydrocarbons. MARISMA has been utilised as a benchmark framework in cybersecurity risk analysis within the maritime sectors of Spain and Colombia.

The remainder of this article is structured as follows. Section 2 describes the results of a systematic review of the literature carried out to identify the principal risk analysis and management tools currently available and to analyse their suitability to meet the requirements identified. Section 3 presents the MARISMA framework, together with its three main components: a meta-pattern that enables reusable risk catalogues for sectors and organisations to be built; a method that provides detailed guidance for risk experts and customers regarding the steps to be taken for risk analysis and management; and a cloud-based tool that fully automates meta-pattern creation and instantiation, together with risk analysis and management tasks. In Section 4, we describe a detailed case of a company which uses our risk analysis and management framework. In Section 5, the limitations of the framework and the main lessons learned are discussed. Finally, in the final section, we present our main conclusions and outline possible future developments in the MARISMA framework.

2. Related work

To identify and consider the primary approaches of the scientific and standards communities relevant to our research question, we conducted two systematic literature reviews, the findings of which are summarised in this section. These reviews adhered to the protocol developed by Kitchenham [41,42], which was appropriately adapted for research in the field of information systems. This approach not only facilitated the identification of compelling risk analysis methodologies but also helped to more accurately define the desired criteria. This enabled us to categorise various proposals based on whether they fully, partially, or did not meet these criteria.

Throughout the course of these systematic reviews, additional valuable references emerged, such as proposals for creating risk models based on MBCA [43] and some tools have been identified that automate aspects of the risk analysis processes, focusing on developing cloud-based knowledge bases. Examples include ALL4TEC[1] and EGERIE-SOFTWARE.[2] However, despite their importance, these proposals and tools were not included in the table, as in some cases their orientation was different from the one proposed in the paper (e.g. oriented to address risks related to the definition of requirements and the software life cycle), and in others, as in the case of the tools, their commercial character prevented them from being analysed from a scientific point of view.

The first systematic review focused on the identification and analysis of the major risk assessment methodologies and standards currently in use, provided that they continue to be actively referenced in the scientific literature and have been updated with reasonable frequency in recent years. We identified MAGERIT [44], OCTAVE [45], MONARC [46], CORAS [47], EBIOS [48] and MEHARI [49] as the main methodologies currently available, along with the ISO/IEC 27005 [50], COBIT [51], and NIST standards [52]. Following detailed analysis, these useful approaches were judged to have created a solid foundation in the field of international risk analysis and management. However, these methodologies have not been fully adapted to the main challenges identified in the scientific literature. In fact, we observed some important weaknesses, such as excessively rigid element catalogues, which make their application in technologically changing contexts difficult. Moreover, there is a lack of processes that facilitate knowledge reuse and learning from experience, which negatively affects the efficient application of these tools. Furthermore, despite increasing inter-organisational dependence, certain tools to determine risks in an associative and hierarchical manner between different organisations are still lacking.

The second systematic review was conducted to identify and analyse the principal scientific research that explicitly focused on challenges in the context of security risk assessment and management identified above. A detailed description of this systematic review and an analysis of the results obtained can be found in [53], whose principal conclusions are presented below, leading to the construction of the MARISMA framework. In this second systematic literature review, we identified existing risk analysis models and methodologies, focusing on issues such as associative and hierarchical risks, dynamic and low-cost risk assessment, and identification of the most important approaches, followed by analysis and a comparative study. Thus, after obtaining an initial list of 6635 studies for the period 2011–2022, we selected 30 approaches that precisely matched our inclusion and exclusion criteria as defined in the systematic review protocol. These approaches were classified into the following five groups: (i) processes, involving a set of actions planned in successive phases for the development of risk assessment and risk management; (ii) frameworks, consisting of structured components with defined interrelationships, focusing on risk assessment and risk management; (iii) models, based on artefacts or specific techniques that provide a representation of complex systems in the context of risk assessment and management in order to better understand their rationale; (iv) methodologies, composed of sets of procedures and techniques that are applied in an orderly and systematic manner to resolve specific problems, which, in our case, involve risk assessment and management, bringing together both processes and models; (v) Other, consisting of approaches that do not fit neatly into the categories listed above, but which constitute interesting strategies in the context of our research.

To conduct a detailed analysis of these approaches, we define a specific set of criteria or properties that have been identified as desirable in the scientific literature in the context of risk assessment and management proposals. These criteria (Table 1) were then evaluated in relation to each of the 30 proposals identified, distinguishing between full compliance (yes), partial compliance (part), and noncompliance (no) (Table 2). Specifically, we identify several criteria that closely align with the aspects delineated in our research question. They are classified into two main categories: scientific and technological. Table 1 presents the details of these categories.

Admittedly, while the identified scientific objectives may be more prominently featured in the current proposal, fulfilling the technological objectives is equally important from a practical standpoint.

The analysis of compliance with these criteria is summarised in Table 2, which shows that many of the tools studied did not comply with the criteria used in the review. In fact, virtually none of the approaches involved catalogues of risk elements (SO1) that could change over time without altering the risk assessment and management processes. However, none fully complied with the risk hierarchy and associativity criteria (SO2) used to determine the risk dependencies and interrelationships, although many began to show partial compliance. Regarding knowledge reuse (SO3), few approaches have implemented processes that facilitate learning from previous experiences, although many recognise the need for this. Most strategies cannot be considered dynamic because they do not provide mechanisms to react quickly to security incidents (SO4). Unfortunately, none of the tools studied had a collaborative capacity (SO5) to provide a global threat assessment to improve incident responses. We also observed that different tools

[1] https://www.all4tec.com/en/cyber-architect-en/
[2] https://egerie.eu/en/egerie-risk-manager/

Table 1
Detailed description of scientific and technological objectives.

Type	Code	Objective	Description
Scientific	SO1	Adaptative Catalogues	It refers to the flexibility of risk catalogues to adapt to changing contexts, risks, and technologies. Adaptive catalogues allow continuous updating of risk elements and dynamic relationships between assets, threats, vulnerabilities, and controls, providing a comprehensive and evolving view of risk. Example: If a new threat like ransomware appears, the catalogue should be able to add it and link it to relevant assets (like databases) and security controls (like backups and encryption).
	SO2	Hierarchies and Associativity	It refers to managing interconnected risks across departments or organisations that share assets or services. This collective approach ensures that actions in one area are understood in relation to their impact on overall risk, as risks in one entity can affect others. Example: In a company outsourcing its cloud infrastructure, both the company and provider share responsibility for data security. If the provider is breached, all relying entities are affected.
	SO3	Knowledge Reuse and Learning	It refers to a risk management system's ability to reuse knowledge from previous analyses to improve decision-making and optimise future assessments. This reduces subjectivity and reliance on individual interpretations by leveraging data and past experiences, preventing mistakes and applying best practices. Example: A security team can use an analysed risk catalogue to make objective decisions about controls, instead of relying only on intuition or personal experience.
	SO4	Dynamic and Evolutive Criteria	It refers to a system's ability to quickly adjust risk values in response to significant security incidents or emerging threats. This dynamic adaptation ensures accurate and up-to-date risk management in rapidly evolving threat environments. Risk values, like likelihood or impact, are continuously updated based on new events or incidents. Example: If an organisation assessed DDoS attack risk as low but the system detects an increase in such attacks, it automatically updates the threat's likelihood and impact.
	SO5	Collaborative Capacity	It refers to organisations' ability to collaborate by using shared global risk frameworks, allowing entities in similar sectors or with similar technologies to work together in managing risks and responding to external threats. This approach emphasises cooperation and information sharing to strengthen collective defences against evolving risks. Example: Financial companies can create a shared risk framework to address industry threats like electronic fraud or data theft, enabling a coordinated response.
	SO6	Low Level of Subjectivity	It refers to the ability of a system to minimise the influence of the personal interpretation of evaluators in risk analyses. The goal is to ensure that risk assessments are objective, consistent, and repeatable, regardless of the person conducting the assessment. This is crucial to ensuring that risks are managed uniformly and that decisions are not biased by the perspective of an individual evaluator. Example: Instead of guessing the likelihood of a cyberattack, the system uses data, vulnerability analyses, and current threats to calculate the probability objectively.
Technological	TO1	Simplicity and Low Cost	The need to develop risk management solutions that are easy to implement and use, as well as being economically viable for all types of organisations, especially small and medium-sized enterprises (SMEs). A simple and low-cost system should be designed in such a way that it can be adopted quickly and without complications by all types of organisations. Example: A risk assessment system based on a simple graphical interface that allows users to quickly select relevant risks and associated controls, without the need for advanced knowledge in cybersecurity or risk management.
	TO2	Tool Support	There is a need for a tool that automates risk assessment and management, reducing manual work, improving efficiency, and providing faster, more accurate evaluations. This makes risk management more effective, cost-efficient, and allows organisations to focus on strategic decisions. Example: A dashboard that visually displays the organisation's key risks, the controls in place, and the current security status, enabling executives to quickly assess the situation and prioritise actions.
	TO3	Global Scope	It refers to using a risk management tool across all assets of an organisation, not just specific departments. This ensures a comprehensive view of risks for more efficient management. Example: In a manufacturing company, the system analyzes risks for hardware, software, production lines, suppliers, and HR policies.
	TO4	Practical Cases	It emphasises the importance of evaluating tools used in real-life scenarios to ensure their practical effectiveness. This approach ensures that technological solutions perform well in real-world contexts, not just in theory or controlled tests. Example: A risk assessment tool that has been used in hospitals to manage cybersecurity risks can offer insights into how the same tool can be adjusted and applied in other sectors, such as banking or manufacturing.

often lack specific strategies to ensure objective and repeatable risk assessment (SO6), although some provide conceptual solutions for this purpose. Most of the strategies reviewed, which were found to be complicated, were more oriented towards large corporations that require multiple resources (TO1), whereas some provided software tools to support risk assessment and analysis (TO2) fully or partially. Moreover, not all the tools can be applied to the full range of an organisation's assets (TO3). Finally, we found it problematic that most of the tools studied do not demonstrate proven applicability in a large number of real-life cases (TO4).

Despite the undeniable value of existing proposals and the progress achieved in risk assessment and management, there remains a pressing need for comprehensive, integrated solutions that are adapted to the new challenges posed by advancements in information technology, as stated in the research question. In developing our approach, some contributions from these methodologies were utilised, particularly the

Table 2
Analysis of the selected proposals.

Proposal	SO1	SO2	SO3	SO4	SO5	SO6	TO1	TO2	TO3	TO4
Alhawari, S. et al. [54]	No	No	Yes	No	No	No	No	No	No	No
Feng, Nan et al. [55]	No	Part	No	Part	No	Part	No	No	Yes	Yes
Lo, Chi-Chun et al. [56]	No	Part	No	No	No	No	No	No	No	No
Yu-Ping Ou Yang et al. [57]	No	No	Part	No	No	No	No	No	Yes	Yes
Shamala, P et al. [58]	No	Part	Yes	No	No	No	No	No	Yes	No
Wulan, M. et al. [59]	No	Part	No	No	No	No	No	Yes	No	Yes
Saleh, M et al [60]	No	Part	No	No	No	No	No	No	No	No
Sato, H. [61]	No	No	Yes	No	No	No	No	No	Yes	No
Feng, Nan et al. [62]Wang Lijian et al. [63]	No	Part	No	No	No	Part	No	No	Yes	No
Webb, J. et al. [64]	No	Part	Part	No	No	No	No	No	Yes	Yes
Armenia, S. et al. [65]	No	No.	No	Yes	No	No	Yes	Yes	No	Yes
Raktim, D. et al. [66]	No	Part	No	No	No	Part	No	No	No	Part
Vicente, E. et al. [67]	No	Part	No	Part	No	Part	No	No	Yes	No
Saptarshi, M. et al. [68]	No	Part	No	No	No	Part	No	No	Yes	No
Shameli-Sendi, A. [69]	Part	Part	No	No	No	No	No	No	No	Part
Sicari, S. et al. [70]	No	No	No	No	No	No	No	No	No	Yes
Staalduinen, M.A. et al. [71]Abdo, H et al. [72]	No	No	No	No	No	No	No	No	No	Yes
Khan, F. et al. [73]	No	No	Part	No	No	Part	No	No	Yes	No
Munodawafa, F. et al [74]	No	Part	No	Part	No	No	No	No	No	Part
Panchal, D. et al [75]	No	No	No	No	No	Part	No	No	Yes	No
Sangaiah, A.K. et al [76]	No	No	No	No	No	Part	No	No	No	No
Wangen, G. et al [77]	No	Part	Yes	Part	No	No	No	No	Yes	No
Zhang, H. et al [78]	No	Part	No	No	No	Part	No	No	No	No
Schmitz, C. et al. [79]	No	Part	Yes	No	No	No	Yes	Yes	Yes	No
Lamine, E. et al. [80]	Part	No	No	No	No	No	No	Part	Yes	Part
Schmidt, A [81]	No	No	No	Part	No	No	No	No	No	No
Tubío, P. et al. [82]	No	No	No	Part	No	Part	Part	No	Yes	Yes
Cherdantseva, Y., et al. [83]	Part	Yes	No	Yes	No	No	No	No	No	Yes
Bozku, E., et al. [84]	No	Part	No	No	No	Yes	No	No	No	No

use of their taxonomic catalogues, which form an invaluable part of the initial knowledge base of the system, to build the new solution.

Therefore, we present a proposal aimed at contributing, especially in the scientific aspect, but also technically, by offering various techniques, processes, tools, and knowledge bases to address the problems outlined in Table 1.

3. MARISMA framework

This section introduces the MARISMA framework used for risk assessment and management. Fig. 1 provides an overview of this framework, consisting of two main components, described in the subsections below, together with the objectives achieved (defined in the previous section) and the roles involved (which will be described as the components in the following subsections). The first component is the ”MARISMA Method” described in Section 3.1, with the risk analysis and management process as well as the information model or risk meta-pattern (reusable and applicable in different contexts) and the specific patterns which are created for specific sectors using the elements of the risk meta-pattern. Finally, the second component is ”Automatic Support” described in Section 3.2, where the eMARISMA software tool is used to support the risk meta-pattern and the process mentioned above and to implement the specific patterns.

3.1. MARISMA method

As indicated above, the proposed method comprises a risk analysis and management process, a risk meta-pattern, and specific risk patterns.

3.1.1. Meta-pattern and patterns

The risk meta-pattern structure defines the elements and relationships that support the data modelling necessary to conduct risk assessment and management in any type of organisation. It mainly defines the necessary structure of Controls, Assets, and Threats (CAT) together with the relationships that define the semantic details of each pattern (intra-pattern relationships) and the mechanisms that enable pattern hierarchies (inter-pattern relationships) to be established by reusing and inheriting control, asset, and threat components. New patterns to extend the meta-pattern structure can be generated to create target patterns adapted to specific contexts, such as a certain sector, company size, system type (e.g. critical systems), and specific technology (e.g. Big Data). This enables the knowledge acquired in previous implementations to be used as a starting point for improving and accelerating the development of new risk assessment and management in new contexts. In addition, it is possible to apply a global pattern to an organisation and more specific patterns to different parts of the organisation, such as divisions, departments, and technologies. This enables relationships and dependencies between elements of different risk patterns to be established so that hierarchical risk structures can be represented and inherited, as well as the associativity between different implementations.

Fig. 2 shows how, in our method, the MARISMA meta-pattern, specific patterns, and intra-pattern relationships are positioned. For its representation, it uses the meta-object facility (MOF) standard from the Object Management Group [85], which provides a framework for defining metamodels organised into four levels of abstraction (from M3 to M0). M3 represents the highest level, the meta-metamodel, where MOF defines itself and describes how metamodels should be

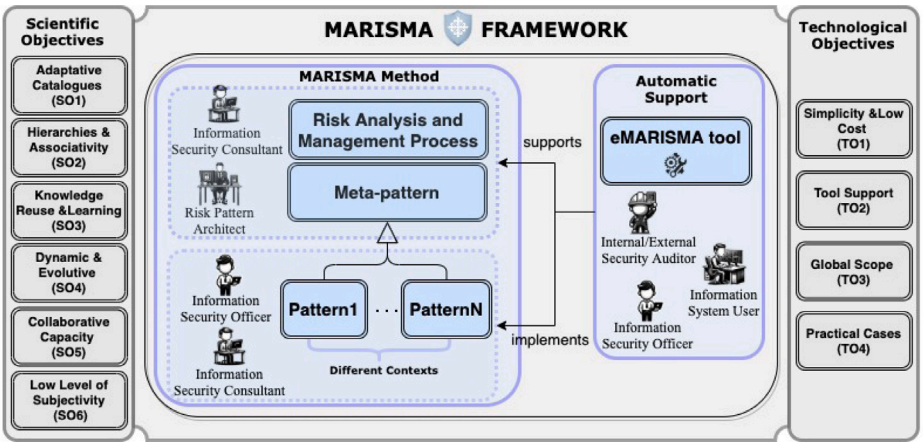

Fig. 1. Architecture of our MARISMA framework.

constructed. At the M2 level, the metamodels that describe the structure and rules that must be followed by the models based on them are defined. The MARISMA meta-pattern was placed at this level. At the M1 level, models are defined according to a specific metamodel, and this is where we place the specific patterns (CPS, ISO 27001, Big Data, etc.) defined according to the MARISMA meta-pattern. Finally, at the M0 level, we identified concrete instances of the models when they were applied to specific analyses.

A more detailed view of risk metapattern is presented in Fig. 3. This shows a UML model which includes meta-classes that define the main elements, as well as their interrelationships and interdependencies. The set of components outlined below can be clearly identified in this model.

- **Controls**: Using this structure, a security pattern architect can define the safeguards and security measures to be implemented in a specific risk analysis to control the impact of threats that may affect an organisation's assets. This structure is composed of an aggregation hierarchy that groups security controls upward into targets to be controlled, which are then grouped into normative domains to be managed. MARISMA considers vulnerabilities as a lack of appropriate security controls. Finally, security controls are associated with key risk indicators (KRIs), which are fed by metrics that facilitate knowledge and improvements in successive implementations.
- **Assets**: This structure enables an organisation's assets to be defined and categorised. Assets, which can be grouped according to type, are also associated with different dimensions according to possible threats to elements such as confidentiality, integrity, and availability. Thus, assets can be examined from various perspectives (dimensions).
- **Threats**: This structure enables the identified threats to be defined and organised into groups, thus making improved reuse and threat management possible. These threats are related to assets and controls defined by certain components in the form of matrices.
- **Intra-pattern relations:**
  (i) Type of Asset x Threat x Dimension (TAxTxD) relations: Using this matrix, the relationships between different types of assets, potential threats, and possible dimensions affected can be specified. These are considered intra-pattern relationships, whose definition enables risk analysis to be optimised, thus avoiding incorrect tuples that might unnecessarily complicate the risk analysis process because not all assets are affected by all threats or related to all possible security dimensions.
  (ii) Control x Threat (CxT) relations: This matrix enables control-threat interdependency to be specified. Controls are defined to prevent or reduce the effects of threats, whereas a lack of security controls related to a threat implies an incomplete protection scenario. The lack of threats related to control may indicate that control can be ignored in the context of this risk analysis. This matrix, which represents an intra-pattern relationship, is connected to the TAxTxD relationship to understand the controls applicable to specific types of assets.
- **Inter-pattern relations**: Our approach not only enables specific risk patterns to be defined but also enables the development of new risk patterns by inheriting components from other previously defined patterns, which is an important feature of MARISMA. This feature, which is not shown in Fig. 3, can be exploited to provide a highly dynamic and intelligent risk analysis and management ecosystem.

Recently, several risk patterns have been successfully defined and applied. In fact, we used the inheritance and instantiation mechanisms of our meta-patterns to develop several risk-pattern structures (see Fig. 2), which are currently used by dozens of clients in several countries to conduct risk assessment and management. The first pattern, which we defined by inheriting our meta-pattern based on ISO/IEC 27001:2013 [86] and MAGERIT V3 [44], has been used by many SMEs. In addition, this risk pattern acted as the basis for developing a new pattern focused on critical infrastructures involving the inheritance of components such as controls, assets, and asset types, as well as security dimensions and the definition of new patterns. However, this critical infrastructure pattern has been used to define more specific patterns in specific contexts, particularly for critical infrastructure in the chemical sector. In addition to the above, we also defined other independent risk patterns inherited directly from the meta-pattern and defined them for specific technological contexts, such as cyber–physical systems [87], big data-based systems [88] (see Fig. 2), and even for business process models [89].

Thus, the evolution of risk patterns, which is one of the most versatile features of the MARISMA framework, enables the implementation of adaptability mechanisms. This principle of evolution is based on the notion that each pattern is a species. Therefore, the risk analysis subsequently performed by each organisation is an instantiation of that species. In other words, we believe that patterns have evolutionary characteristics which allow them to: (i) reproduce and generate new individuals adapted to the pattern, as well as to generate new patterns through evolution; (ii) learn through dynamic learning techniques, so that each instantiation of a pattern helps it improve through new applications; (iii) evolve under new circumstances, giving rise to more modern and complete patterns, through the cloning or fusion of previous patterns; and (iv) die when patterns become obsolete, giving rise to others that are better adapted and therefore more effective.

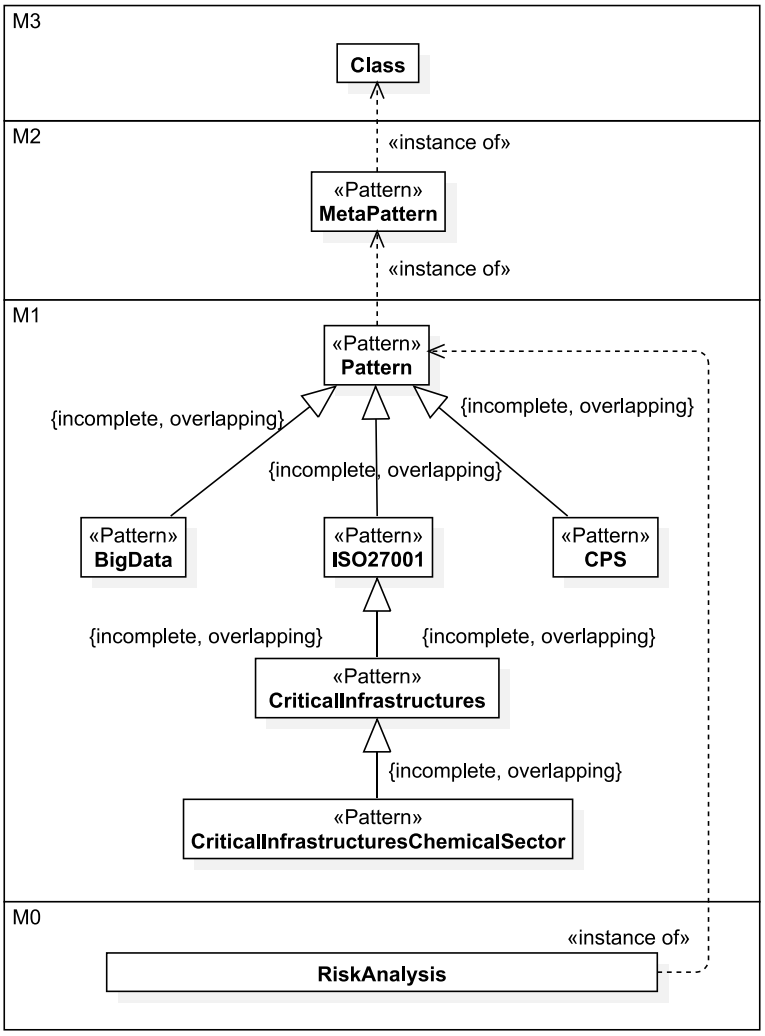

Fig. 2. Pattern inheritance and instantiation.

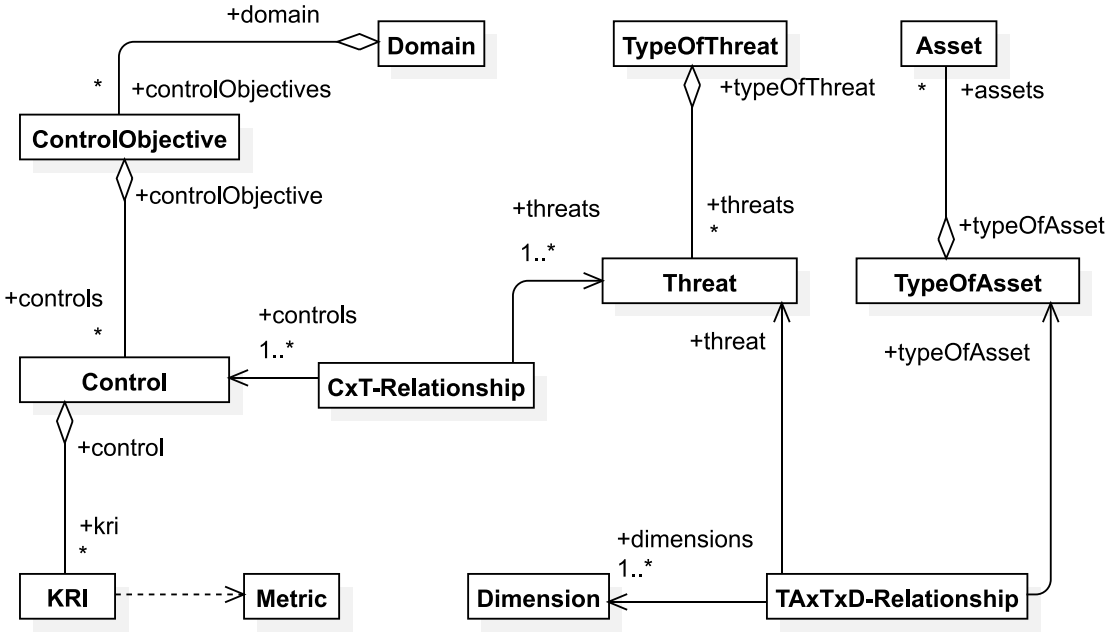

Fig. 3. Meta-pattern CAT (detailed view).

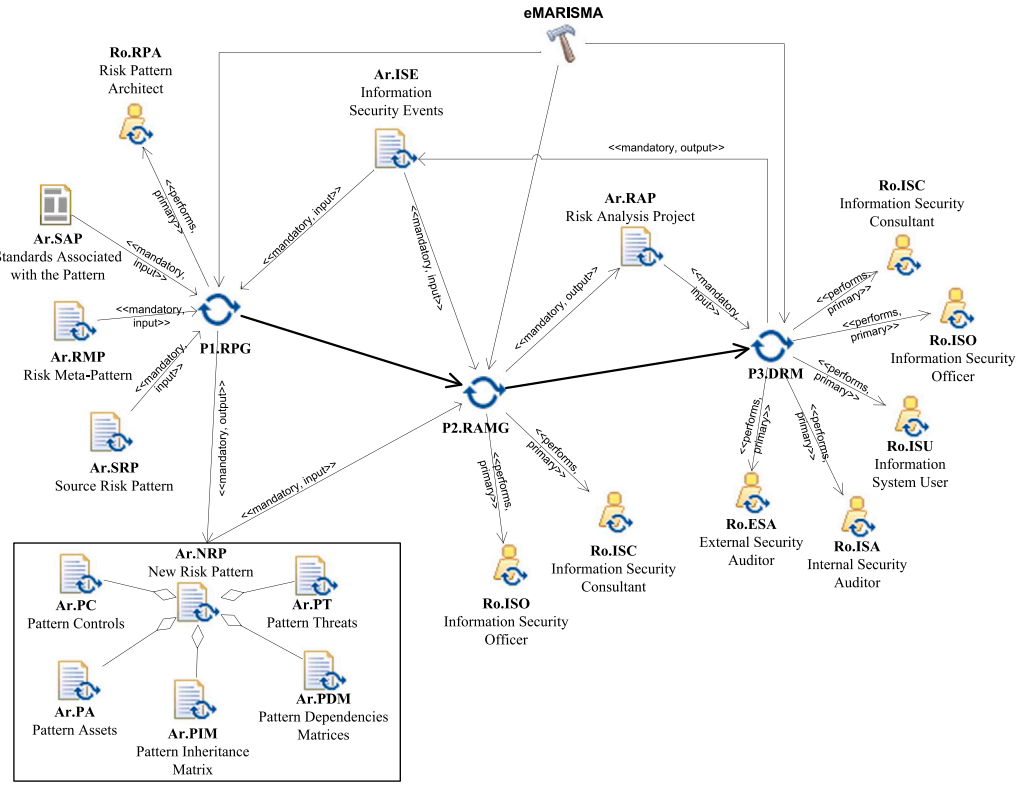

Fig. 4. MARISMA processes overview.

3.1.2. MARISMA processes

In this section, we provide details of the MARISMA method, which we designed to perform risk analysis and management procedures. We also describe the principal functions, three main processes, actions, and input and output artefacts. A SPEM 2.0 representation of the overall structure of MARISMA is shown in Fig. 4. The three aforementioned processes are as follows.

Risk-Pattern Generator (RPG) process. This process is responsible for defining all the components of a specific risk pattern, which consists of types of assets, controls, threats, security dimensions, and their interrelationships, that is, the creation of a new pattern for a specific context (Ar.NRP output artefact in Fig. 4). The risk pattern is developed by analysing the most appropriate standards and reference documents (Ar.SAP input artefact) related to the application area, and through direct inheritance from our meta-pattern (Ar.RMP input artefact) or from another previously developed risk pattern (Ar.SRP input artefact), taking advantage of the knowledge and experience accumulated during previous implementations. In addition, when MARISMA is fully operational, inputs in the form of security events (Ar.ISE input artefact) that update different parameters of the risk pattern are received.

The Risk Analysis and Management Generator (RAMG), which applies the developed (or reused) risk pattern in the RPG process (Ar.NRP input artefact), and reifies this pattern to the specific details of the organisation in which risk analysis and management are carried out. Through this process, we finally obtained a risk map or analysis of the current situation, as well as a risk treatment or management plan (Ar.RAP output artefact in Fig. 4). Once the risk analysis is generated, and the risks are managed through the dynamic risk management (DRM) process, the identification of security events (Ar.ISE input artefact) can lead to improvements in the parameters of risk analysis and management.

The Dynamic Risk Management (DRM) process, is responsible for dynamically updating the risk indicators (Ar.RAP input artefact), such as the value of assets and threat probabilities, in the corresponding risk matrices that connect the different components when security events occur (Ar.ISE output artefact in Fig. 4) or non-conformities are detected by security auditors.

It is important to note that the eMARISMA tool (eMARISMA input artefact in Fig. 4) provides automatic support for all the processes described in this method, as described in Section 3.2.

As implied by the above definition of MARISMA's three processes, MARISMA, its workflow implements a cyclical process of continuous improvement. First, the risk pattern needed (the RPG process) is generated, and the schema to be reified by risk analysis and risk management is defined based on this pattern. If necessary, this process is executed when there is no existing pattern to meet the requirements. Subsequently, specific risk details were generated using the RAMG process in specific cases. After implementing the risk treatment plan, even though risks are controlled using the DRM process, security events occur, whose detailed analysis produces feedback to improve risk analysis and management as well as the corresponding risk pattern. Certain parameters of risk analysis and management, such as the threat probability and degradation rate, can then be updated to improve a particular case. Moreover, security events such as threats to previously unidentified assets may even be identified, possibly leading to further modifications at the risk-pattern level, which, once incorporated into the pattern, improves all risk analyses and management generated from this pattern.

Several specialists, with different skills and backgrounds, may be involved in the different processes of the MARISMA method. Although all these functions must be carried out when the risk analysis and management methodology is used, some could be carried out by the same person, especially in SMEs (not the case for external security auditors). The following participants are needed to carry out these procedures:

Risk Pattern Architect: who is an expert, in the field of cybersecurity risk and is in charge of designing, implementing and managing one or more of MARISMA's risk patterns.

Information Security Consultant: who needs to be an expert in security management standards, such as ISO, NIST, and Cobit, and

related reference documents. This person is responsible for one or more risk analysis and management projects and also for guiding their implementation.

Information Security Officer: who is the organisation's security manager. This person works closely with the information security consultant, who is more familiar with the organisation's context, security needs, security domain prioritisation, among other things, in order to implement the risk analysis and management project.

Internal Security Auditor: who is in charge of verifying the achievement of the proposed objectives and provides both an internal and external perspective with regard to the implementation process.

External Security Auditor: who is responsible for verifying the fulfilment of the objectives proposed and also provides an external perspective with regard to the implementation process and the organisation, thus reinforcing the objectivity of the evaluation carried out.

Information System User: who is an employee, customer or supplier who has access to an organisation's information system.

The content and details of each MARISMA process are described in the subsections below.

3.1.2.1. RPG process - Risk pattern generator. A Software Process Engineering Metamodel (SPEM 2.0) [90] was used to specify the components of MARISMA. Specifically, the processes, activities, steps (not included in this study owing to space constraints), artefacts, and tools were defined. A role and product diagram was drawn for each process, focusing on the roles involved as well as the input and output artefacts. An activity diagram was created to show how the process was broken down into different activities.

The objective of the RPG process is to design the details of the risk pattern to be used in the development of a risk analysis and management project for all or part of a specific organisation, which is one of its specific technological components. This process can be performed through direct inheritance from our meta-pattern or from an existing risk pattern that shares similar characteristics with the new pattern. In the former, the risk-pattern architect defines and configures the risk pattern components from scratch, considering the most relevant standards and reference documents, depending on the context in which the risk framework is applied. However, in the latter case, an existing pattern is reused, which requires only a reconfiguration of its components, leading to a highly efficient process for risk-pattern definition.

Fig. 4 shows the role and product diagram corresponding to the RPG process in which the risk-pattern architect was primarily involved. The principal input artefacts are those necessary for the definition of a new pattern from scratch using the risk meta-pattern, as well as the relevant security standards and reference documents, or those inherited from another existing pattern, together with the corresponding security standards and reference documentation, to develop and improve the risk pattern already created relating to information security events. However, the main output artefact is the risk pattern (Ar.NRP output artefact in Fig. 4), which includes all its components. In the figure below, the artefact corresponding to the risk pattern is broken down into the following components: (i) assets, composed of base asset types and assets specific to the context, as well as the security dimensions that affect these asset types; (ii) threats, consisting of base threat types and threats specific to the context; (iii) controls, covering a hierarchy of domains, control objectives and controls identified in the relevant security standards and reference documents, as well as KRIs and metrics that enable the level of compliance of controls to be measured; (iv) the dependency matrix, an artefact containing the matrices that establish relationships between the previous components, which are crucial for risk assessment and for defining the risk treatment plan, and (v) the inheritance matrix, which determines the element inheritance relationships between source and new patterns in the case of inheritance from an existing pattern.

The RPG process comprises the following five activities (see Fig. 5) that are responsible for defining and configuring parts of the risk pattern:

Asset Definition (AD) activity (P1.A1 - Ac.AD), which defines the data corresponding to an asset hierarchy and the security dimensions of the pattern. Different approaches can be used, depending on whether a risk pattern is created from scratch or whether a previous pattern is reused. For example, when defining a risk pattern for cyber–physical systems from scratch, the ENISA report defines a set of asset families and types as the basis for defining assets [52]. However, when developing a new risk pattern for critical infrastructure in the chemical sector, for which a risk pattern for critical infrastructure was previously created, we reuse most of its asset types and define those specific to this sector.

The Threat Definition (TD) activity (P1.A2 - Ac.TD) defines the data corresponding to the threat hierarchy (specific threats and threat types). As in the case of assets, threats are defined only according to standards and reference documents, such as the ENISA threat taxonomy in the context of cyber–physical systems [91], or the threat hierarchy could be inherited and adapted from an existing risk pattern. This activity is also responsible for updating the threat hierarchy based on the occurrence of security events which may modify it, usually by incorporating new types of threats that were not initially considered.

Control Definition (CD) activity (P1.A3 - Ac.CD), through which the risk pattern architect specifies a complete control hierarchy (domains, control objectives, controls, KRIs, and metrics). Similar to previous activities, CD activities can be defined from scratch or inherited from a previous risk pattern. The structure of the data gathered from security events identified during the risk-management process can also be improved.

Intra-Pattern Relationships Definition (intraPRD) activity (P1.A4 - Ac. IntraPRD): Once the previous activities to define the asset, threat, and control hierarchies have been executed, it is time to define their interrelationships. Specifically, the risk-pattern architect fills in a matrix of relationships between types of assets, threats, and dimensions to specify which assets can be affected by the defined threats and in which security dimensions they are interrelated. In addition, a matrix linking controls and threats must be filled in to determine which controls are appropriate for mitigating the defined threats. Both matrices are crucial for the automatic generation of risk analysis and defining the risk treatment plan.

Inter-Pattern Relationships Definition (InterPRD) activity (P1.A5 - Ac. InterPRD), is executed only when a new pattern inherited from another existing risk pattern is defined. In this case, the risk-pattern architect establishes the inheritance relationships between the components of both patterns. In this manner, a family or hierarchy of risk patterns can be built and used to propagate changes and improvements (and thus to any of their instances) both efficiently and quickly.

In order to maintain the clarity of Fig. 5, the relevant information has been shown in the image, and the remaining elements are explained below. The meta-pattern, source risk pattern (when inheriting an existing pattern), security standards, and reference documents, which are mandatory RPG inputs, were used in its five activities. Furthermore, the asynchronous flows between activities are not shown. Obviously, assets, threats, and controls should be defined before defining intra-pattern relationships, whereas inter-pattern relationships should only be defined in the case of inheritance from an existing pattern and at the end of the process

Owing to the definition of the meta-pattern structure, we obtained the capacity to support hybrid catalogues, which can be composed of taxonomies extracted from different international standards and form unique patterns (SO1). These patterns can be specialised at a business sector and technological level, which allows them to be adapted to all required casuistry. On the other hand, through inheritance mechanisms, patterns that are created from the composition of several

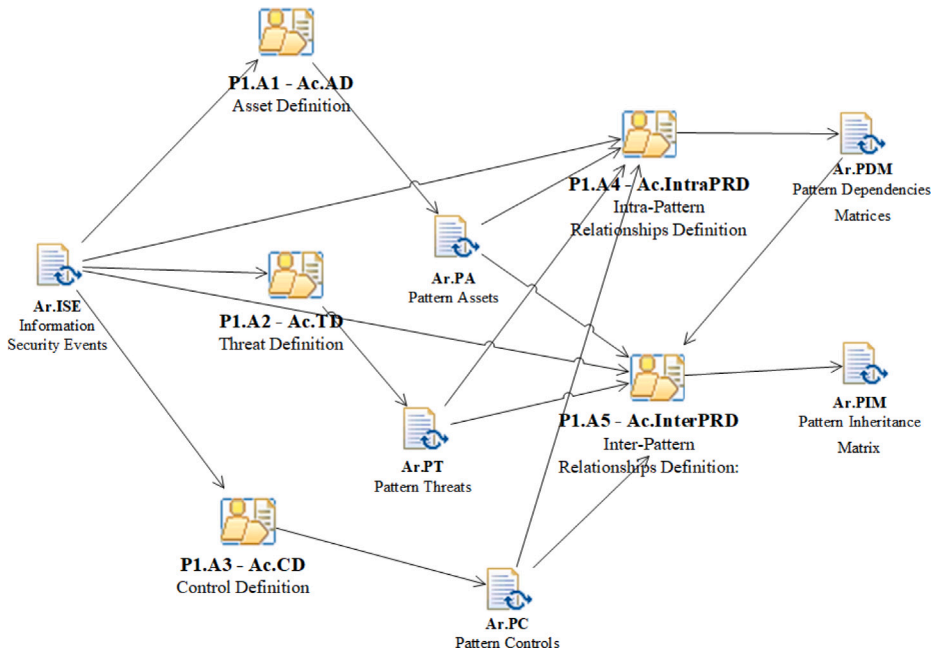

Fig. 5. Diagram of activities, inputs and outputs. RPG process.

patterns, or through their specialisation, maintain their relationships to conserve the properties of associativity (SO2, SO5). The meta-pattern establishes connections between all elements that constitute risk analysis (CAT). These connections are not static, but are fed by the knowledge they receive through the use of these patterns. Similarly, this new knowledge is transmitted to all existing connections through other related patterns. In this manner, all patterns dynamically adjust to reality as they learn from their use, which allows us to have a dynamic knowledge base (SO3, SO4, and SO5). Finally, the ability to obtain information from different sources helps to adjust the interrelationships and values of each pattern so that it offers the most reliable information at all times (SO6).

3.1.2.2. RAMG process - Risk analysis and management generator. The main function of this process is to create risk analysis and management projects by instantiating the risk pattern specified through the RPG process, or by reusing another existing risk pattern. A risk analysis and management project consists of a detailed analysis of assets and threats, as well as the coverage of controls, together with a risk treatment plan or a selection of controls to be implemented to mitigate risks in accordance with the established security objectives. This process was performed through an agile and iterative process using the eMARISMA tool.

Fig. 4 shows the role and product diagrams of the RAMG process. As it can be seen, the main persons involved in this process are the information security consultant, who provides expert knowledge in the technological and regulatory field of security and risk in the context of a risk analysis and management project, and the security officer, who provides contextual knowledge and experience related to the specific organisation and information system to be analysed to define the scope of the risk management project. The main input artefacts are those necessary to instantiate the chosen risk pattern under consideration to adapt and improve the already created risk analysis of information security events. In contrast, the key output artefact is the risk analysis and management project configured for a specific organisation the main output artefact is the risk pattern (Ar.RAP output artefact in Fig. 4).

The RAMG process comprises four activities (Fig. 6), each of which is responsible for defining and configuring a specific part of the risk analysis and management project.

Preliminary Risk Analysis (PRA) activity (P2.A1 - Ac.PRA) enables a simplified and rapid risk analysis to be carried out to obtain an initial view of information system security. This PRA provides high-level information owing to the execution of a simplified checklist, which enables the security officer to define the specific security objectives for the risk analysis and management project. This activity also enables information security consultants to select the most appropriate risk patterns for a project.

Company Profile Configuration (CPC) activity (P2.A2 - Ac.CPC), through which a complete profile of an organisation is created to determine contextual information regarding elements such as economic, geographical, and business data, organisational charts, principal roles, and project scope, which facilitates more objective and detailed risk analyses. This contextual information also facilitates the customisation of the alerts generated by eMARISMA; for example, the known increase in the probability of a threat event in a specific business sector will propagate the alarm to all organisations catalogued in that business sector.

The **Asset Information Management (AIM) activity (P2.A3 - Ac.AIM)** is responsible for defining the set of assets that make up information systems whose risks need to be analysed. The assets considered, which are clearly the cornerstone of an analysis that provides value to the organisation, must be protected. This activity is conducted semi-automatically owing to the metadata defined (types of assets) in the chosen risk pattern, which will be customised and reified by the security officer.

The **Risk Project Configuration (RPC) activity (P2.A4 - Ac.RPC)** is the foremost activity in this process because it provides the main output artefact for risk analysis and management projects. It is important to acknowledge that one of MARISMA's main objectives is to provide rapid, low-cost risk analysis and management with the necessary quality properties. Therefore, the details of the risk analysis and management project were incorporated using the metadata defined in the selected risk pattern. Specifically, based on the information gathered in the previous activity, information regarding the security dimensions corresponding to the assets is input, the identified threats that may affect the assets are specified, and an exhaustive control checklist generated from the KRI defined in the risk pattern is carried out, which facilitates the establishment of the initial coverage level of each security control identified. Using this information, a detailed map of the current risks (risk analysis) and a recommendation plan are created, which is composed of selected security controls that best protect the assets in

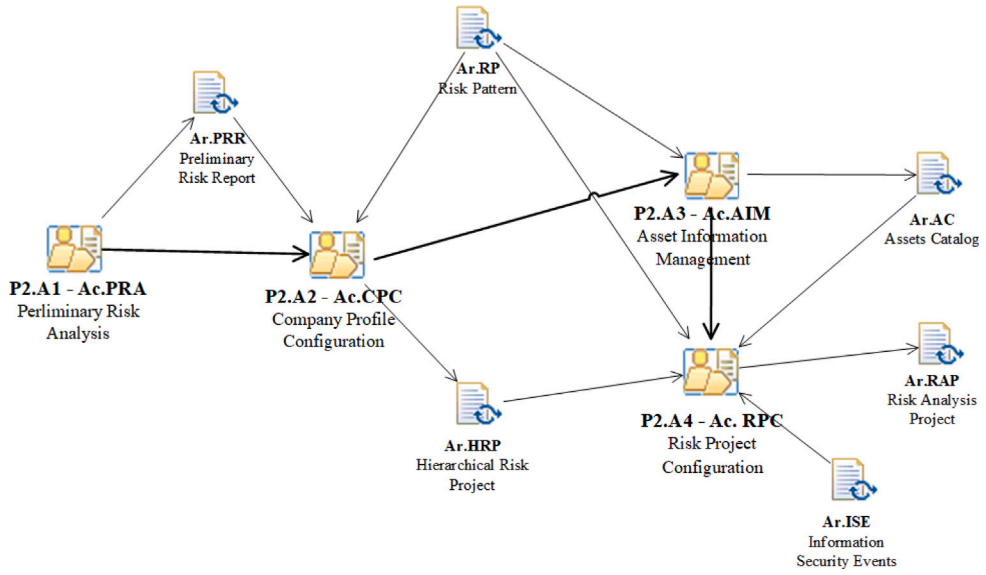

Fig. 6. Diagram of activities, inputs and outputs. RAMG process.

accordance with the security objectives and budget. In addition, this activity involves checking and, if necessary, implementing suggestions for the development of a security event risk analysis.

This process also considers the need to include the risk derived from assets shared between different companies, an aspect that is increasingly seen in companies through the use of cloud assets (SO2). This process also receives feedback on the patterns as they evolve because of the knowledge acquired from their instantiations, which can be of two types: (i) an adjustment of a long-term pattern or (ii) a recommendation of an external and temporary risk change, which allows us to increase the coverage of certain controls that are under a particular attack at a specific moment in time (SO3, SO4). This process allows us to define the associativity that exists between different instances of a pattern, which sends information to their pattern of origin, which in turn sends it to the remaining instances, creating the concept of a hive mind (SO5). Finally, this process reduces the level of subjectivity inherent in the security assessment of an IS. On the one hand, by receiving more precise information from the evolution of the patterns, and on the other hand, by allowing controls to be subdivided into sub-controls, the initial level of compliance of each control in the organisation can be more accurately set (SO6).

3.1.2.3. DRM process - Dynamic risk management. The objective of this process is to manage security incidents as they are detected, which provides the actions necessary to dynamically control risks and learning mechanisms for the risk analysis and management project and for the risk pattern used. This process is optimised for low management costs, to be fully dynamic, and to provide the necessary information regarding identified security events throughout the procedure. Fig. 4 shows the roles and product diagrams of DRM. All persons, except the risk-pattern architect, selected for this process are involved in some type of risk management, with some involved in more general aspects of security, together with the information security consultant and the information security officer, who deal with security problems that require deep knowledge of information system domains. Internal and external security auditors conduct audits to detect and improve security, whereas information system users clearly identify and report security events. The input artefact was the risk analysis and management project developed in the previous process, whereas the output artefact was the set of information security events used by other processes to provide dynamic learning and overall improvements. This latter artefact integrates the suggestions generated to improve the risk analysis and management project as well as the risk pattern. The DRM process consists of four activities (Fig. 7).

Security Event Controller (SEC) activity (P3.A1 - Ac.SEC), which is responsible for the centralised catalogue of possible security events that directly affect the evolution of the risk levels of the information system. These security events may have different origins, such as security incidents, non-conformities following an external or internal audit, or adjustments made to the level of coverage of security controls. However, all security events affect the recorded level of coverage of the controls, and therefore cause dynamic changes in the current risk scenario, which was initially created through the RAMG process.

The **Security Event Manager (SEM) activity (P3.A2 - Ac.SEM)**, which is automatically executed each time a new security event is registered in the system. Because each security event is related to the threat that has occurred, the level of compliance of the related controls is automatically penalised because of the CxT relationship specified for the pattern. Additionally, these security controls must be revised to obtain an appropriate level of risk for the information system. This results in an automatic update of the security dashboard, which shows the impact on the risk level of such a security event and provides a permanent view of the organisation's current security status.

Dynamic Risk Analysis Evolution (DRAE) activity (P3.A3 - Ac.DRAE) manages the dynamic evolution of risk analysis and management projects in response to the effects of security events. This activity processes the security events managed through the previous activity and automatically generates a set of suggestions regarding the risk analysis and management project map, with, for example, a change in the recorded probability of a specific threat, thus lowering the coverage level of security control. The information security officer receives and processes these alerts and suggestions to evaluate whether they lead to changes in the corresponding risk analysis and management projects.

Pattern Dynamic Evolution (PDE) activity (P3.A4 - Ac.PDE), which manages the dynamic evolution of the related risk patterns in response to the effects of security events. A great advantage of a global knowledge base, thanks to sets and hierarchies of risk patterns and their instances, is that automatic alerts can be generated and propagated to other risk analysis and management projects. Therefore, a dynamic ecosystem is provided in which the occurrence of a security event in a specific risk project produces suggestions that refer to the risk pattern itself and, for example, creates a new relationship between a control and a threat. These suggestions are propagated to the hierarchy of risk patterns and risk projects defined by these risk patterns. The

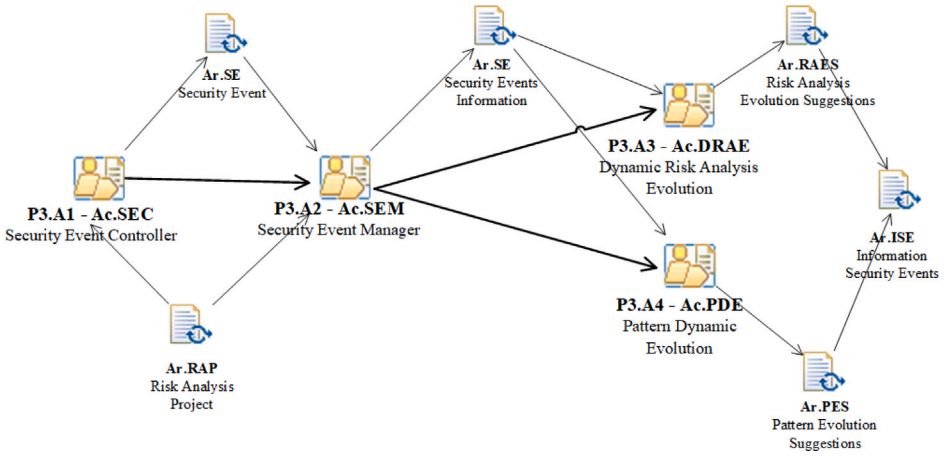

Fig. 7. Diagram of activities, inputs and outputs. DRM process.

risk-pattern architect receives and processes these suggestions to assess whether a risk pattern has evolved.

This process makes it possible to integrate events derived from the impact of an asset associated with other risk analyses, which differs from the current analysis. In other words, we can transfer the impact of inter-related assets (SO2 and SO4). This process allows the capture of security events, both manually and automatically, which are categorised into a specific taxonomy and can be converted into useful knowledge to be used by the risk analysis, which will also allow the evolution of the pattern on which it is based (SO3, SO4). The collaborative capabilities of this process are achieved through the events themselves, which transfer internal knowledge to other instances through the pattern, thereby allowing them to gain full knowledge of the existing risk at any given moment (SO5). Finally, this process helps reduce the level of subjectivity inherent in the risk assessment of information systems through suggestions, automatically generated from security events. This mechanism allows for a more effective refinement of control and risk levels, dynamically adapting to reality (SO6).

3.2. Automatic support

The eMARISMA tool, which was developed to provide automated support for the MARISMA framework, facilitates the management of MARISMA's knowledge base, including the risk meta-pattern, hierarchy of risk patterns, and their implementation in risk projects, and simplifies the risk analysis and management process.

This tool was developed using J2EE technology and can be accessed by customers on an Internet browser from any device. This model is based on the deployment of an application on an Apache server with a servlet container called Tomcat that separates a module to manage risk patterns from a module that manages risk analysis projects for greater security, thereby protecting the analytical data of clients and guaranteeing data confidentiality in the cloud. As this platform operates in disconnection mode, it requires only a connection when requesting a risk pattern update.

Although the eMARISMA tool automates the three processes of the MARISMA framework, it is designed to be extensible to support new functionalities in the future.

3.2.1. RPG - Risk pattern generator

The implementation of this process in eMARISMA facilitates the creation of new patterns adapted to the specific needs of organisations. The Fig. 8 shows the process of creating a new pattern, and how the eMARISMA tool supports each of the tasks of the process to easily and intuitively add all the information that is generated in each of the tasks of the process. For instance, when establishing the pattern for CPS [87], we must first identify the existing taxonomies, recommendations, and standards for this type of environment. Once these are identified, it is necessary to define the types of assets typically present in these environments (such as devices, communications, infrastructure, etc.) and the relevant security dimensions to consider (e.g., privacy, reliability, confidentiality). Additionally, the most common types of threats within these environments must be identified (such as abuse, eavesdropping, natural disasters, etc.). It is also crucial to select an appropriate set of security controls to safeguard these systems, drawing from international standards and recommendations like those provided by NIST or ENISA. Once all these elements are identified, the relationships between them must be established. This involves defining relationship matrices between different elements, which will help determine the likelihood of occurrence and the potential degradation should a threat materialise and target an asset within the system. With all this information in place, the pattern is then defined for application in a specific real-world environment.

Using this tool, new risk patterns can be easily created and configured using two possible strategies. For a base risk pattern from which a new pattern is generated, eMARISMA enables the selection of specific elements of the inherited base pattern, followed by the addition and parameterisation of the specific distinctive elements of the new risk pattern. On the other hand, the tool also facilitates the creation of new patterns from scratch and guides the user through the process in order to register and properly configure each of the elements in the pattern structure according to the definition of the MARISMA meta-pattern, as is shown in Fig. 9. The eMARISMA tool implements a guide to create the different components of the risk pattern, assisting and supporting the incorporation of all necessary information (i.e. addition of assets, controls, dimensions, threats, different relationships, probabilities, etc.) to make it as easy and straightforward as possible.

Thus, eMARISMA facilitates the construction of a centralised repository of security patterns with high growth potential that stores the knowledge of groups of experts from different technical and regulatory domains. Thus, eMARISMA provides all the necessary functionalities to manage and extend, if necessary, these patterns, which can be applied to multiple risk analyses and management projects as required and are adapted to specific sectors and environments.

3.2.2. RAMG – Risk analysis and management generator

The implementation of this process in eMARISMA facilitates the creation of new risk analyses and management projects adapted to the context and specific needs of each implementation. Thus, with a repository of patterns to cover specific needs, the information security consultant in charge of the risk analysis and management project has a wide range of options from which to choose the base pattern that is best suited to the requirements. Once the pattern has been selected, the tool generates the base structure to carry out the initial risk analysis

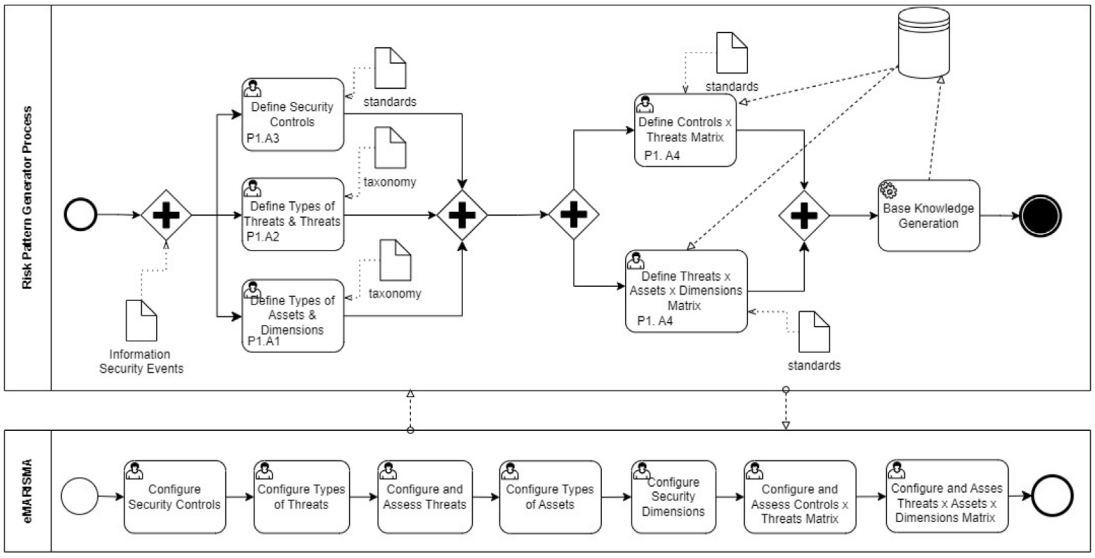

Fig. 8. Risk pattern generator process.

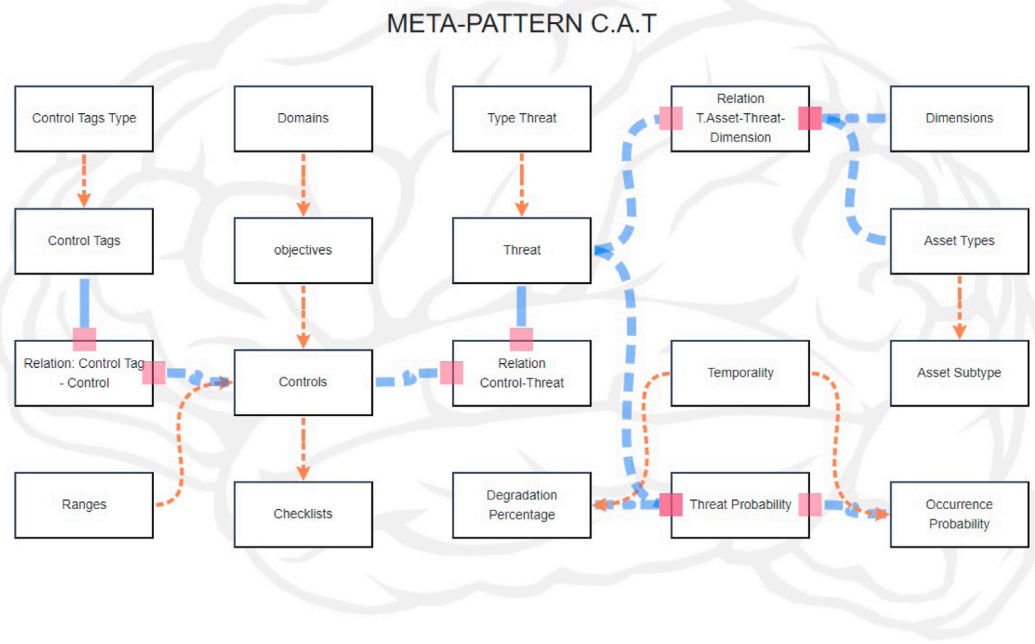

Fig. 9. Meta-Pattern structure guide in eMARISMA.

as well as its subsequent management and maintenance in a simple and efficient way in terms of the effort, cost, and expert knowledge required. The Fig. 10 shows the process that is carried out to generate the risk analysis together with the risk treatment plan, and how the tool supports you in each of the tasks. Once we have created or identified the pattern, it can be used by instantiating all the elements defined within it for a specific environment. For a CPS environment, after creating the pattern in the previous process, the next step is to map its elements to the specific components of the environment being analysed. For example, identifying an RFID system as a type of 'Device,' or an IoT Gateway as 'Infrastructure,' to name a few. Once the assets of the system to be analysed are defined, a preliminary analysis must be conducted by completing a security checklist to assess the current state of the system. Information related to the company should be added, and the most important and valuable assets should be identified so that MARISMA can link and assign all values and establish the relationships within the pattern, enabling a detailed risk analysis. Based on the results of this risk analysis, MARISMA will provide a set of necessary recommendations to appropriately protect the assets with the most suitable security controls, with the aim of mitigating risk.

Additionally, eMARISMA is designed to adapt precisely to organisational structures by offering a hierarchical tree model that organises analysis and management projects by area and department. Fig. 11 illustrates an example of a hierarchical tree generated for a company operating at two sites. At the organisational level, risk analyses were conducted and managed at the departmental level for each site, with three departments per site in this example. The percentages displayed indicate the control-coverage level for each node. To calculate these values, each department (leaf node) completed a checklist to determine its level of control, as explained in the following section. In

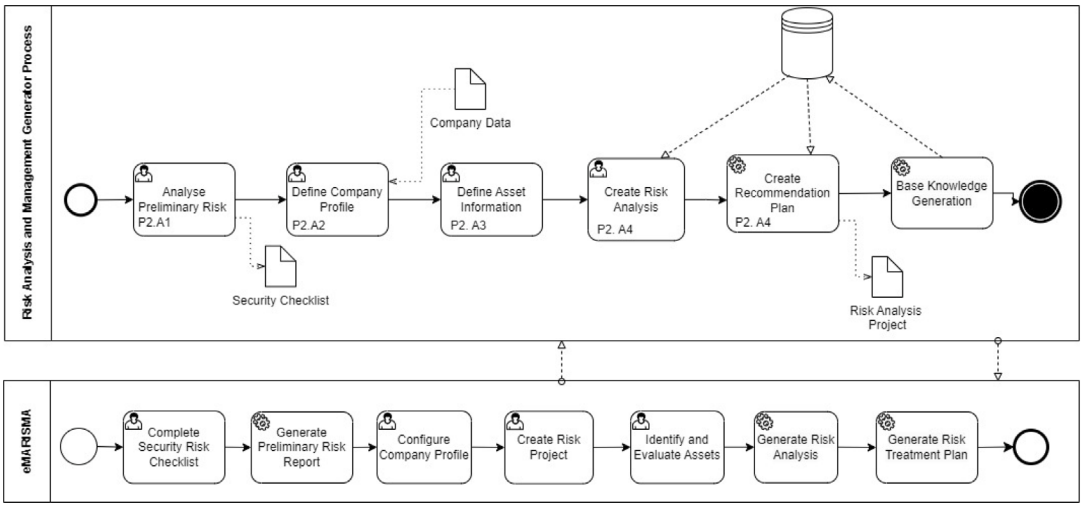

Fig. 10. Risk analysis and management generator process.

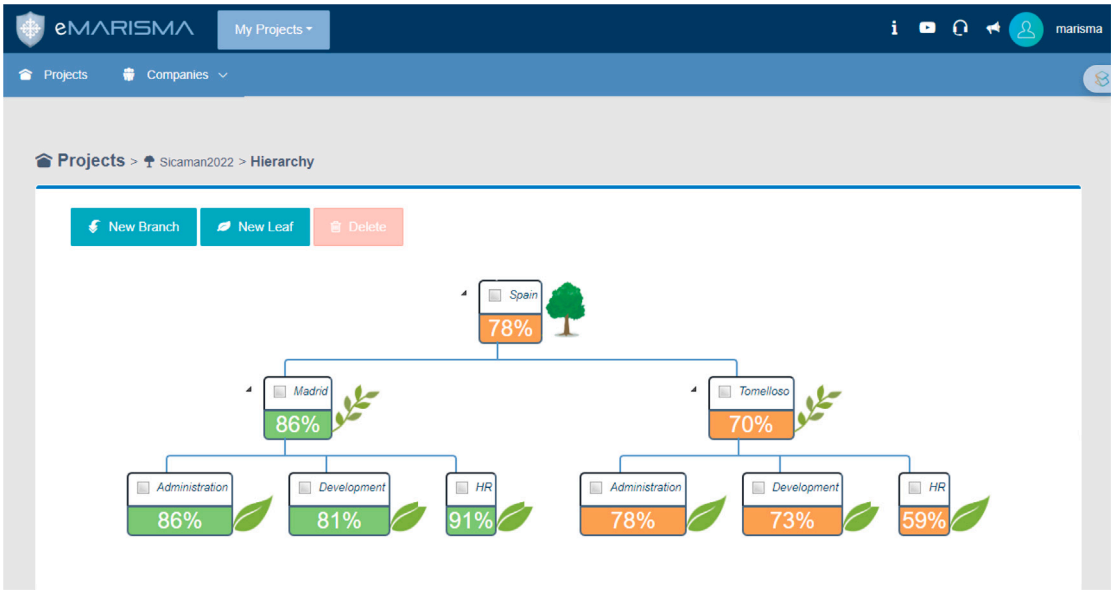

Fig. 11. Hierarchy tree in eMARISMA.

practise, these values are derived using weighted formulas, where the importance and weight of each division are considered in the final control-coverage percentage. However, in the example shown, we have opted for a simplified representation to enhance clarity. Based on this approach, the control level for each node in the tree is automatically computed as the average of the control levels of its child nodes, which are propagated back to the root. This process provides a comprehensive indicator of the overall control level of the organisation. As the control levels change throughout the lifecycle of the information system, the values are automatically recalculated to keep the overview up-to-date.

eMARISMA offers the possibility of customising the hierarchy tree for any organisational casuistry required, allowing branches and leaves to be created and managed in a flexible and personalised manner. In this way, the tool provides a visual overview of the level of coverage both at the leaf level (department in the example) and, by propagating down to the root, the percentage of control of each branch and sub-branch of the company's organisational chart.

The eMARISMA tool also provides information security officers in organisations with a set of support tools for risk analysis and management, such as dashboards and Kiviat diagrams (see Fig. 12), which facilitate a simple, visual, and real-time evaluation of control and risk values as well as dynamic changes as organisational risks evolve. This tool, which enables the constant monitoring of risk levels, is important for security decision-making. Thus, in Fig. 12, Kiviat diagrams for the compliance and coverage of controls organised by domains, control objectives, and controls are shown as defined in the meta-pattern. Fig. 12 (left) shows the complete Kiviat diagram with all defined domains of a company's risk analysis. In particular, the "Deming Cycle" is highlighted, showing the name of the system and the coverage of this domain to be 67.74% (indicating the sum of the coverage of all the control objectives that are part of it). On the right, at the top of Fig. 12, the diagram by domain is shown, showing the one previously selected, and the coverage of each control objective that forms part of the "Deming Cycle" domain is displayed. The coverage of the "[0.07] - Support" target is 70%, obtained by adding the coverage of each control to that domain. Finally, on the right at the bottom of Fig. 12, the Kiviat diagram at the level of the control objectives can be seen, showing all controls that belong to that objective with their level of coverage. Any change in the coverage of controls automatically updates all values at all levels (objectives, domains, and projects), and the entire risk analysis is fed back with that change, showing the changes in real time.

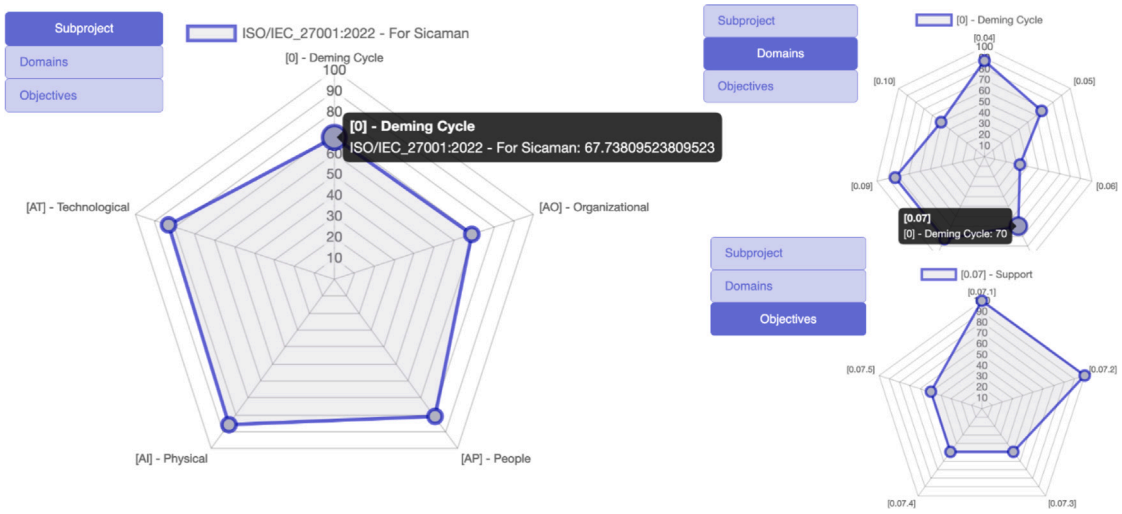

Fig. 12. Compliance Kiviat diagram in eMARISMA tool.

3.2.3. DRM - Dynamic risk management

As mentioned above, one of the classic problems with risk analysis is that it provides a static picture of the current state of organisational risk. However, as risk scenarios change daily, with security events occurring during the normal operation of an information system, this static picture quickly becomes obsolete. The dynamic risk management process of the MARISMA framework is illustrated in Fig. 13. This process makes it possible to create and manage the security events that are identified, configuring all the elements that form part of the risk analysis and controlling the possible evolution and possible changes in all the parameters, both of the risk analysis and of the pattern used, in order to enrich and improve it for the future. For example, if the system detects a DDoS attack, this event needs to be logged in MARISMA to update the risk analysis for future assessments. To do so, it is crucial to analyse this type of attack, its impact on the system and assets, and the affected security dimensions to gradually incorporate this information into the pattern being used. In this way, the threat is identified as a service disruption, which could target, for instance, the 'Web-Based Services' asset defined in the pattern instance. Consequently, MARISMA must adjust both the probability and occurrence rates, as well as the affected dimensions, to reflect the actual damage caused and assess whether the frequency is higher than initially indicated. This dynamic management allows for continuous updating of the risk evolution within the system, and these values must also be updated in the pattern itself, so that the next time it is instantiated, the pattern includes values that are more appropriate for the current type of system and environment. With this information, the potential security controls to recommend or implement are also updated, such as suggesting the use of Intrusion Detection and Prevention Systems (IDS/IPS) or enhancing protection against malicious code, among others.

eMARISMA fully implements this procedure and provides a structured approach for managing security incidents. First, it allows the input of incident details, such as description, cause, responsible person, and resolution deadline. Second, it uses predefined risk patterns to identify and categorise the relevant elements (such as threats, assets, and controls) associated with the incident, determine aspects such as severity, and temporarily reduce the effectiveness of the affected controls until the issue is resolved. Finally, once the incident has been resolved, it supports knowledge management by documenting the lessons learned, cost of resolution, and final observations. Notably, when a security incident is logged, automatic changes are triggered in the risk components based on the existing meta-information. This is because the level of compliance with security controls is downgraded when a threat breaches control, thereby affecting the risk associated with many other assets and requiring a review and strengthening of these controls. Thus, to adapt to these changes, eMARISMA automatically manages and updates both the control level and risk status based on recorded security events.

The relationship matrices between the elements that are part of the pattern structure allow valuable information, such as controls associated with threats, to be obtained from each security event. Thus, when a security event is registered, the tool recalculates possible real-time variations in the level of coverage of the controls affected and updates the dashboards to constantly maintain the most accurate view of the global levels of control. It also informs the information security officer that the risk status has changed and automatically generates suggestions to enable both risk analysis projects and their associated patterns to evolve.

Using this tool, it was possible to fulfil some of the technological objectives pursued in this research. eMARISMA allows us to automate part of the proposed processes and provides the necessary support to comprehensively manage the operations related to risk analysis and risk management. This helps simplify the overall risk analysis process and reduce the associated costs, minimising the resources needed to create and maintain the risk analysis (TO1–TO2). However, owing to the flexibility of the pattern structure and its ability to deal with hierarchical risks, this tool allows the risk assessment process to be managed globally within the context of the company, regardless of its size (TO3). Thus, eMARISMA allows us to support a knowledge base of all types of patterns that can be used globally by all types of companies, allowing other research groups to create new patterns oriented towards new visions of risk (TO3–TO4). In addition, the MARISMA framework was refined through its application to different case studies in different sectors and contexts (TO4), as detailed in the following section, based on the generated knowledge base and different patterns defined throughout our research. Therefore, the tool provides a solution for the four technological objectives set out in this study.

4. Case of application

This section presents an application in which MARISMA was used to create a risk analysis and management project for a real-world company. The application serves two main purposes: to test the adaptability and effectiveness of MARISMA in a company with specific requirements, and to use the knowledge generated from this initial implementation to refine and improve the meta-pattern, MARISMA method, and eMARISMA tool.

The company chosen for the case study is Sicaman Nuevas Tecnologías (SNT), a Spanish SME focused on the ICT sector. Despite its

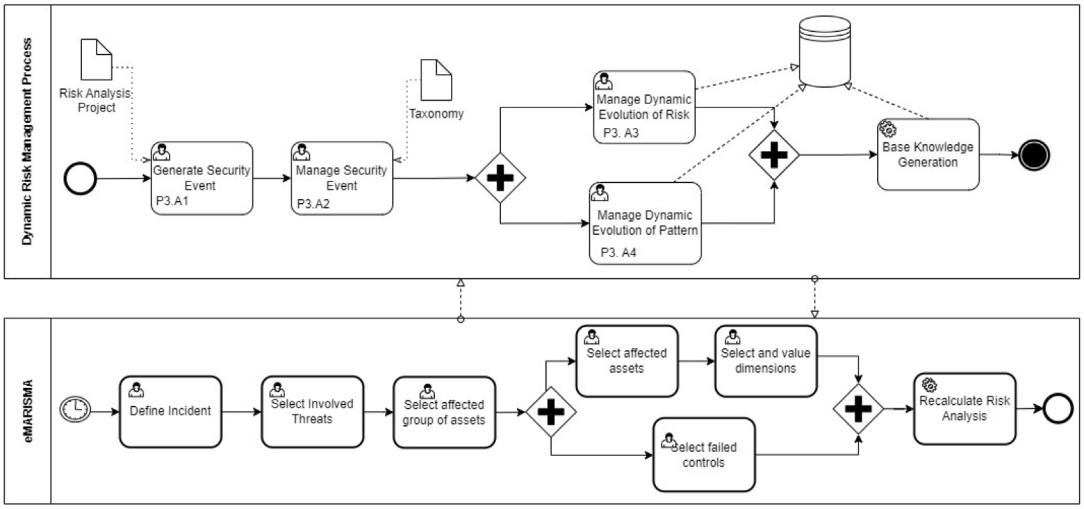

Fig. 13. Dynamic risk management process.

relatively small size, SNT has a complex business structure, with offices in Ciudad Real, Madrid (Spain), and Bogota (Colombia), and a departmental structure divided between central services, human resources, and information technology. Similar to most SMEs, despite their limited resources for management and quality projects, risk analysis and management systems must be implemented in accordance with the ISO/IEC 27001 standard. In particular, the company must implement this standard within a period of no more than one year, considering the implementation of the required risk analysis and subsequent risk-management processes. The main objective is to ensure the security of information systems, an issue of vital importance for companies in the technological field, with a view towards cementing the growth and stability of their business models. It should be noted that previous attempts to implement the ISO/IEC 27001 standard in the company failed owing to the cost in terms of the time and resources required to implement and maintain all its processes, especially those related to risk management, as well as the difficulty of gathering the extensive expert knowledge needed for updating and continuous improvement.

The first step was to design and construct a pattern adapted to the ISO/IEC 27001 standard, drawing on the experience and knowledge of experts from the Security and Audit (GSyA) research group at the UCLM, who were responsible for developing the catalogues of elements required for the pattern and defining and categorising the matrices of relationships between the elements. The pattern is created using the controls proposed by the ISO/IEC 27001:2022 standard and the taxonomies of asset types, dimensions, and threats proposed by Magerit V3. The relationships between the matrices were formed from the information available in the standards and supplemented by an expert group. Fig. 14 shows the fragments of different elements configured within the pattern. To the left of Fig. 14, we can see the added information related to the TAxTxD matrix, where it is established which dimensions will be affected by each asset in the face of each threat. To the right of the figure, the configuration of the values of the occurrence probabilities and the degradation percentage of the threats can be updated.

Once the relationship matrices between the elements were configured, a final complete risk pattern was made available for use as a basis for new risk analyses and management projects adapted to the ISO/IEC 27001 standard. Thus, the information security consultant in charge of the risk analysis and management project only needed to select the pattern in eMARISMA to create the new project. All the elements (the asset types, threats, controls, and the configured and categorised interrelated matrices) defined in the risk pattern were automatically loaded, thus reusing the knowledge of the domain experts to create the basis of the project both quickly and effectively.

To conduct the risk analysis, a sub-project (instance) was created for each of the leaves (see Fig. 11) on the project tree (departments in this case), each of which had an independent structure in the company with its own assets (shared or not) and its own defined responsible parties. The risk level of each leaf of the tree propagates upward, such that any change in the risk level of a leaf automatically recalculates the risk levels of the higher nodes until the root is reached. In this case, one of the leaf nodes, the development department of the Ciudad Real Office, was selected as the scope for the initial risk analysis.

The next step involved customising the base elements in the generated risk analysis and management project to adapt their values to the context of SNT. First, the asset inventory is generated from the asset types defined in the risk pattern. The system automatically loads a taxonomy of asset types associated with the selected pattern. While this may seem simple at first, it becomes very important for highly specialised patterns such as sector-specific critical infrastructure, helping consultants to more accurately define the types of assets present.

Next, the occurrence probabilities and degradation rates of both of the threats and threat-asset type-dimension relationships were reviewed and customised based on the values defined in the pattern (see Fig. 14). eMARISMA loads the threat taxonomy associated with the selected pattern and pre-loads the most likely values, based on its experience, for the probabilities of occurrence and degradation rates, thereby reducing the time required to customise these values. Experience with the tool has shown that consultants typically spend an average of 1–2 h completing this part of the process, as observed in this application case. From the configuration of the parameters associated with the threats, the tool generates a matrix of all the viable pairs between the threats, the assets, and the security dimensions to be considered, also importing their most probable values from the pattern. The tool allows these values and feasible pairs to be modified, but our experience based on this and many other application cases, shows that less than 10% of the values are adjusted compared to those automatically generated by the system. This task typically takes consultants between 0.5 and 1 working day, which represents an average saving of around 90% compared to traditional mechanisms.

Finally, the initial level of each control defined in the pattern was established. The information security consultant, together with the information security officer, completed a checklist to define the initial values of the controls. eMARISMA defines two mechanisms for completing this checklist, depending on the level of accuracy required and the time available to complete the process. Firstly, it supports the classic model, which asks only for basic coverage of a control (assuming an average time of 1–2 working days). Secondly, for a more precise result, it offers a much more detailed questionnaire that calculates the

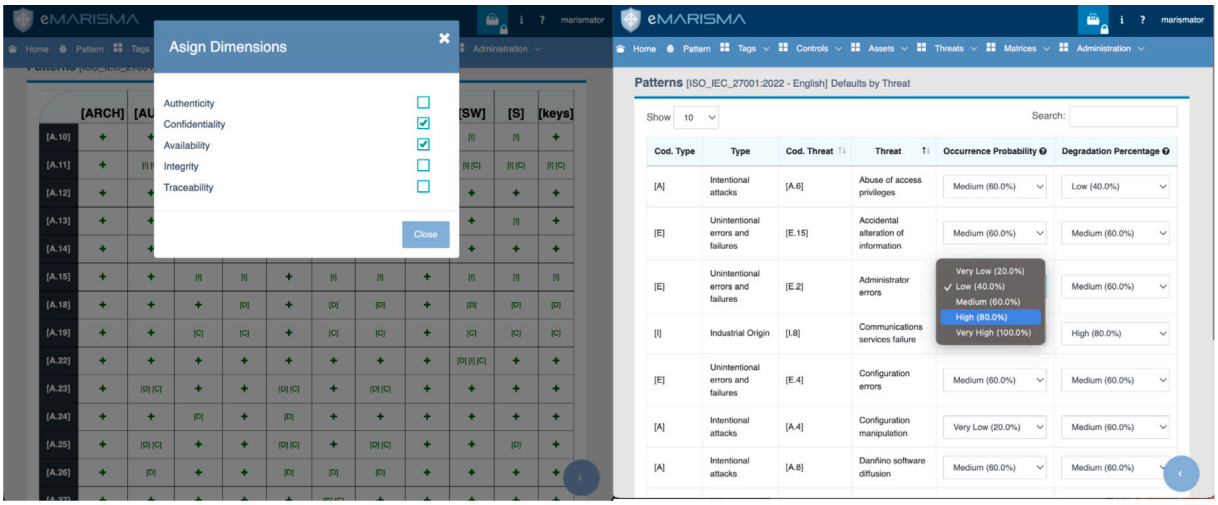

Fig. 14. Fragment of the configuration of "TAxTxD matrix" for the ISO27001 pattern (left), configuration of probabilities and degradation of Threats (right).

coverage of each control through various sub-controls. Although this second option requires more effort (approximately 3–5 days), we have found that the results are about 30% more accurate in reflecting the actual initial state of the control.

It is important to mention that both of the aforementioned experts must be involved in this process. The information security officer must be familiar with the information system, and it is important that the information security consultant is a norm and standard expert, particularly regarding ISO/IEC 27001. The joint involvement of both experts facilitated the creation of a highly precise initial control-coverage scenario. In addition, the eMARISMA-implemented checklist enables an SNT's information security officer to quickly and easily obtain a precise control-level scenario without the need for additional experts. Thus, thanks to eMARISMA, the company can establish a basis for risk analysis in a virtually autonomous manner.

The information obtained from the checklist is organised in a three-level structure: domains, control objectives, and controls. Thus, the final results were broken down into each of these levels to provide an overview of the security status of the instance worked on by identifying the main strengths and weaknesses, which can then be easily monitored, thus aiding security-related decision-making. Fig. 15 displays a dashboard that presents the real-time coverage levels of controls across all grouping levels (domains, objectives, and controls), facilitating their graphical and visual tracking. This enables a straightforward and intuitive interpretation (via percentages and visual colour coding) of the most robust aspects and identifies the controls requiring the most reinforcement at various levels.

For example, in the case study carried out, it was possible to take preventive decisions to strengthen certain aspects related to the level of security. In this way, as can be seen in Fig. 15, it was possible to see graphically how the area related to organisational security [AO] presented a 'medium' level of control, clearly identifying the controls ([A.05.02], [A.05.03]) that could increase the level of compliance in order to strengthen the security of this particular area. This enabled the company to proactively drive the necessary decisions to strengthen the implementation of these controls for the next improvement cycle.

Upon establishing and calculating the specific values for threats, risks, and controls, it became possible to conduct the initial risk analysis. The system, utilising the information inputted and customised in preceding steps, autonomously generates a risk analysis and a prioritised risk treatment plan. This represents a significant advancement for consultants, as it obviates the need for their direct involvement, beyond reviewing the results. Instead, the system executes millions of calculations to ascertain individual risk levels and offers an initial strategy for prioritising the most urgent tasks, thereby aiming to diminish the residual risk within the system.

The various application cases implemented have demonstrated how the MARISMA framework, supported by the eMARISMA tool, can substantially reduce the time and effort needed for a complete risk analysis process. In traditional systems, this process might span weeks or even months in more complex scenarios. However, our framework enables the initial step to be completed within a matter of days. In this particular application, for instance, an initial risk analysis was achievable in under two weeks. Following the completion of the risk analysis, the application provides various perspectives on the risks. One such view is illustrated in Fig. 16, which displays the risk associated with each asset, identifying 'Source code' as the asset with the highest risk.

Being a technology company focused on software development, knowing in a visual and easy to understand way for the management that one of its main assets was the one most at risk allowed the company to dedicate a significant budget item to the protection of this asset. In this way, measures were planned to strengthen controls over the source code, such as replication of the code repositories, access to the repositories via certificates and the drafting of new code management and access policies.

To provide a comprehensive risk overview, the tool incorporates additional utilities. Notably, Fig. 17 displays a heat map illustrating both pure and residual risks. This map is categorised into five colour levels, where red signifies maximum risk and green indicates acceptable risk levels. Each cell within the map reveals the frequency of asset-threat pair occurrences identified in the risk analysis, reflecting the risk level associated with the impact of the threat on the specific asset. The left-hand map delineates the risk analysis outcomes without any control measures (pure risk), whereas the right-hand map shows the residual risks after implementing the current control levels within the organisation (residual risk).

The residual risk value obtained from the risk analysis made it possible to enable the eMARISMA tool of a base treatment plan adapted to the level of risk, defined as a target to be achieved for the next improvement cycle. Thus, SNT expected that, given the current risk level of 6, the objective for the next iteration should be a risk level of 5. The eMARISMA tool makes it possible to generate a treatment plan aimed at reaching a specific risk level within a few minutes.

Upon implementing the process within a company's operational framework, we noted a marked decrease in both costs and time consumption, exceeding 50% in comparison to traditional models facilitated by tools. This efficiency gain is attributable to the semi-automation and enhanced support of the various tasks comprising the process.

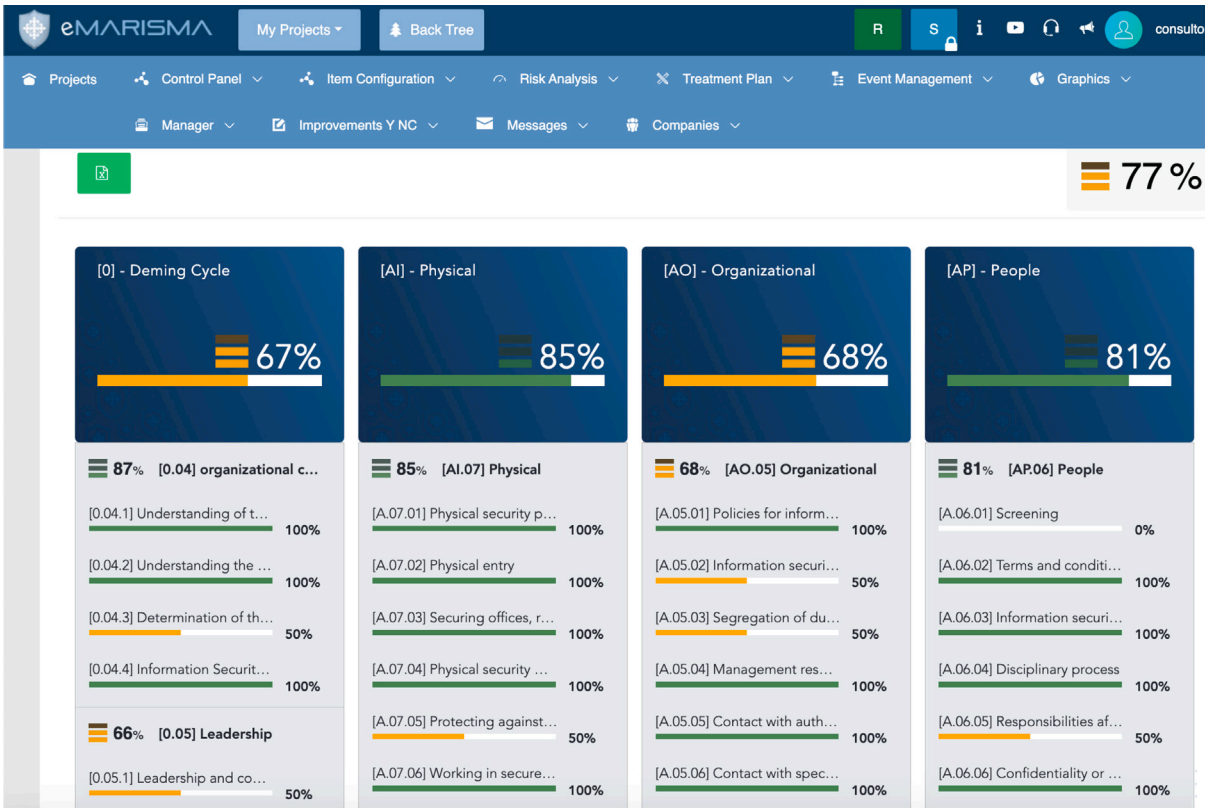

Fig. 15. Dashboard in eMARISMA tool.

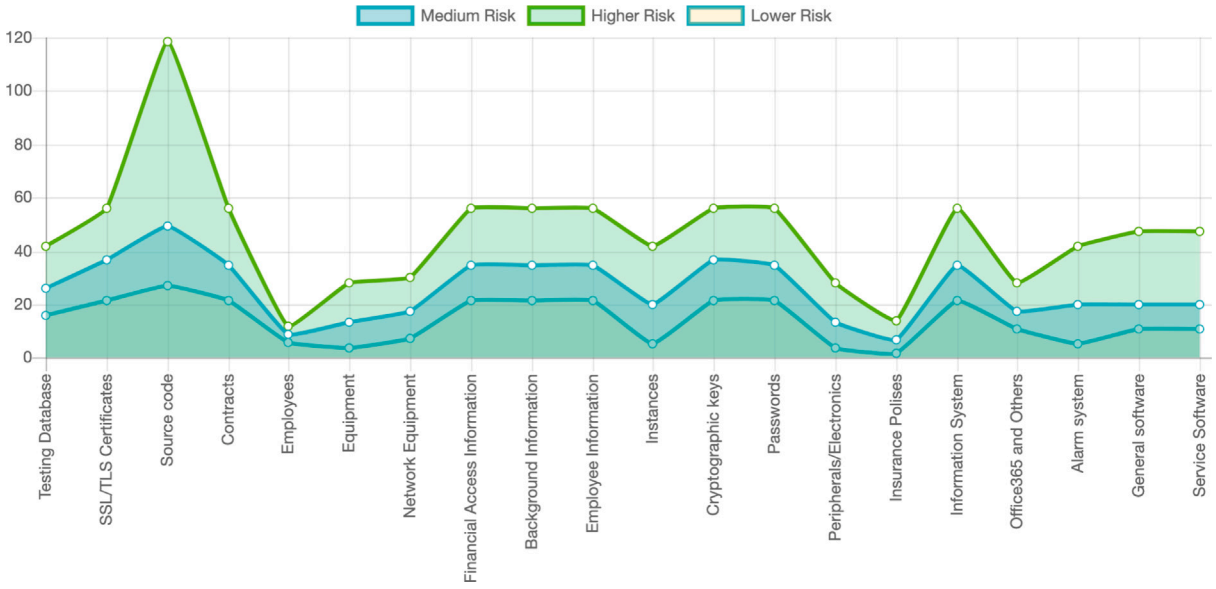

Fig. 16. Risk calculated per asset type using the eMARISMA tool for the case of application.

Once the initial risk analysis was conducted and a treatment plan for the evolution of the security of the information system was developed, eMARISMA was used to manage the risks of the system through the management of security events. This allows information system users to enter the tool and manage the detected security events. By cataloguing the data for each security event (threats, assets, and controls), we verified that the risk analysis and management project values were automatically recalculated satisfactorily, with the level of coverage of the affected controls being automatically updated. In parallel, eMARISMA checks whether the changes made following the incident alter any of the elements of the pattern. For example, following a variation in the probability of the occurrence of a threat, suggestions were automatically sent to all risk analysis projects created from the pattern used or those hierarchically related to this pattern.

Fig. 18 illustrates the methodology employed for recording security events. Initially, the event is categorised according to the pattern's taxonomies, delineating elements such as the initiating threat and its severity, the affected assets and their impacted dimensions, and any controls that were compromised. Following this, the system analyses

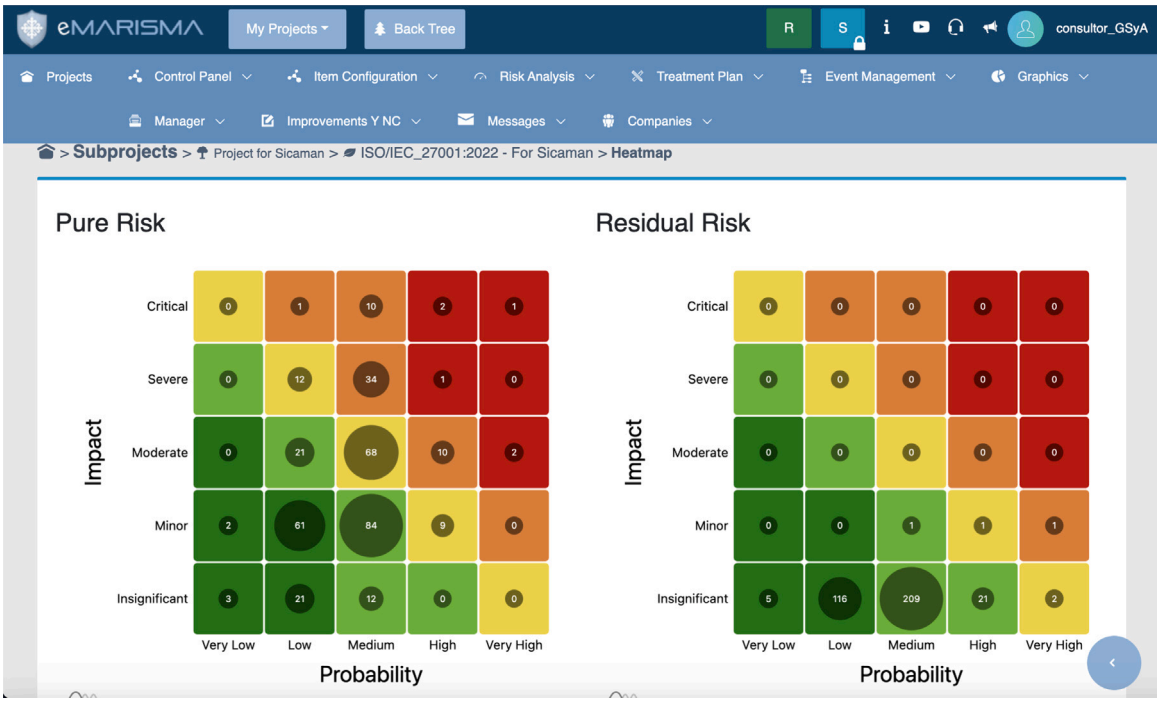

Fig. 17. Heat Map with the probabilities and impacts for Pure and Residual Risk shown in eMARISMA.

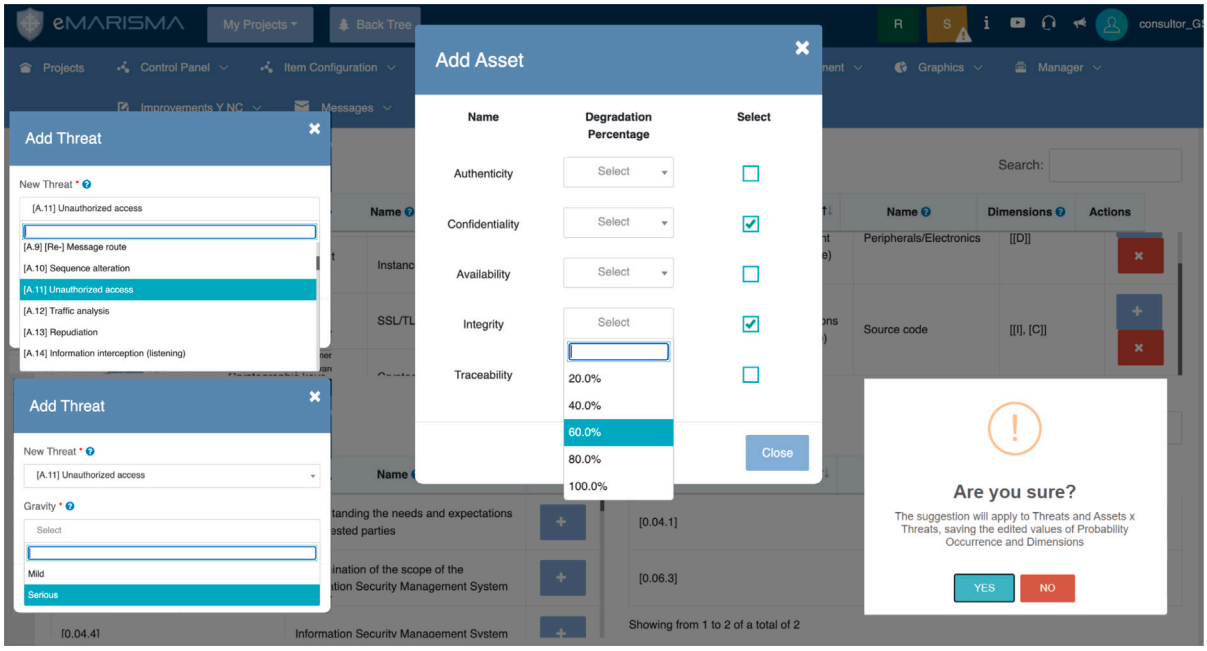

Fig. 18. Security event management in eMARISMA.

the data inputted for the event. Should it identify a potential enhancement, the system will present this as a suggestion, offering the option for acceptance or rejection.

With regard to suggestions for project improvements, the information security officer is responsible for accepting or rejecting the application of the suggested change; if the suggestion is related to the risk pattern, the risk-pattern architect modifies the suggested values when considered appropriate. For example, during the course of the case study, one of the suggestions generated by eMARISMA was to increase the probability of occurrence of the 'Unauthorised Access' threat, which was initially set to 'Medium'. After receiving the suggestion, the security manager reviewed the security incidents and found that several unauthorised access attempts had been made to the system in the previous week. He then accepted the proposal, which automatically increased the probability of occurrence of this threat in the system to 'High'.

Among the lessons learned in this process, the most important is that it avoids having to redo risk analysis from scratch every year, as is currently done by many organisations. The system requires an initial effort to create an initial version of the risk analysis; however, the management of events (both manual and automated), as well as the information entering the system via the template, generates a sustainable and updatable ecosystem with a very low level of effort. Based on our experience, the average time to categorise a manual security event

is less than 1 h, and automated events require no time at all. Another lesson learned is that even if the initial values of some elements are wrong when generating the risk analysis, the mechanisms incorporated in the system (security events and suggestions) allow the system to evolve towards real risk, as opposed to the initially perceived risk. This evolution is a slow process, in which the system continuously adjusts the values of the risk analysis. In our experience, it takes between three months and one year to reach a point of stability, and this depends on the number of events the system receives (the greater the number of events, the faster the system adapts to reality).

In conclusion, the application case shows that the MARISMA framework can be used in a real-life environment, in which MARISMA makes it possible to generate a risk pattern fully adapted to a specific security standard, in this case ISO/IEC 27001, covering all the necessary aspects to conduct a risk analysis within the framework of this standard in a comprehensive, efficient, and objective manner, at a low cost in terms of both time and resources. The application case also shows that dynamic management and real-time monitoring of risk values can be carried out throughout the life cycle of a project. Finally, based on the information gathered from the security events recorded in the system, the application case demonstrates how the risk analysis and management project, as well as the base pattern itself, evolves and adapts dynamically to the real-life context following implementation.

This application case made it possible to improve and refine the activities and tasks of MARISMA by refining or reformulating certain steps and processes, as well as improving the risk-pattern structure. In addition, tool support has proven to be crucial for the practical application of MARISMA because of the large number of artefacts used, the tasks to be performed, the complexity of both calculating risk values and generating a base treatment plan adapted to the maturity status of an organisation, and DRM in real time.

5. Discussion

This section analyses the extent to which this framework improves both the scientific and technological objectives defined in the introduction section.

The main problems associated with the scientific objectives are:

SO1 — Adaptive Catalogues (AC): The risk meta-pattern, together with pattern inheritance mechanisms, facilitates the total or partial selection of a base pattern and even several patterns, if necessary, in addition to the generation of new patterns adapted to specific requirements. Moreover, this structuring of patterns allows numerous instances to be created, which are adapted to the element catalogues in specific contexts, such as technology, sector, and standard.

SO2 — Hierarchies and Associativity (HA): MARISMA enables hierarchical risk patterns to be created by applying the inheritance mechanisms described above. Furthermore, associations can be established between different risk analyses and management projects, while assets can be shared between different organisations. The hierarchical structure supported by eMARISMA not only facilitates inheritance and associativity between different projects but also provides features such as Kiviat diagrams and dashboards to visualise global risk.

SO3 — Knowledge Reuse and Learning (KRL): The MARISMA framework introduces reusable patterns for risk analysis, allowing organisations to leverage knowledge from previous assessments. These patterns can be used to create new risk models and generate analysis instances, automating much of the risk configuration and leading to significant cost reductions. The pattern structure also enables the creation of a continuously updated knowledge base, which evolves when security incidents occur. This allows risk patterns to learn from experience and pass that knowledge to new, updated, or related instances. As a result, MARISMA fosters continuous learning and knowledge reuse, enhancing the organisation's ability to respond effectively to future threats.

SO4 — Dynamic and Evolutive (DE): The pattern's structure allows new elements to be added to a given instance, making it able to adapt and evolve; for example, new threats or controls can be added to a pattern to adapt it to changing needs. In addition, both patterns and risk analyses can evolve dynamically from security events, thereby facilitating agile adaptation to changing conditions.

SO5 — Collaborative Capacity (CC): Given its capacity to generate multiple instances of risk analysis from a pattern, the MARISMA framework enables the generation of early warnings. Thus, when a risk analysis and management project notifies others of a security event related to the appearance of a specific threat, a security suggestion is generated that allows other projects related to the source risk pattern to react preventively. This facilitates the construction of a global security shield between organisations that share the same hierarchy of risk patterns.

SO6 — Low Level of Subjectivity (LLS): MARISMA provides several means of reducing uncertainty. First, each control has fine-grained KRIs that enable the accurate evaluation of an organisation's situation. In addition, through the generated recommendations, the DRM process facilitates the adaptation of the values of the catalogue of elements, such as the threat probability, to the real-life context of each risk analysis project. Finally, MARISMA implements automated mechanisms to guide information security consultants at all times and generate risk analysis as accurately as possible.

The Table 3 provides a detailed comparison of the advancements proposed by the MARISMA framework concerning classical models, specifically focusing on scientific objectives.

On the other hand, with regard to the technological objectives, the main problems associated with this feature, and how they have been solved, are outlined below:

TO1 — Simplicity and Low Cost (SLC): risk analysis carried out by the RAMG process, together with the eMARISMA tool, is agile and straightforward, as it is based on predefined patterns; has automatic mechanisms that facilitate its generation, maintenance, and evolution; and its implementation is affordable for any type of organisation, regardless of size.

TO2 — Tool Support (TS): As part of the MARISMA framework, the multiplatform, scalable, and flexible tool eMARISMA was developed. This tool is designed to adapt to the needs of organisations of various sizes and sectors, providing the flexibility to manage different types of assets and risk scenarios. Its scalable architecture allows it to grow alongside the organisation, ensuring that it can handle increased volumes of data and complexity without compromising performance. Additionally, eMARISMA has been certified under the international product quality standard ISO25000:2014 in its functional adequacy dimension, further validating its reliability and effectiveness in diverse environments.

TO3 — Global Scope (GS): The diversity of catalogues that can be implemented in MARISMA makes it possible to adapt to any need by selecting the most suitable pattern for the objective set by an organisation, and even using several catalogues if necessary, thus generating several risk analyses that can be combined through the tree structure of eMARISMA to obtain a unified global result.

TO4 — Practical Cases (PC): In addition, the MARISMA framework was developed through the application of the Action–Research method to real-life cases, which has facilitated a cycle of continuous improvement. The action–research method was already successfully applied to obtain significant cost reductions in the management and maintenance of information security management systems prior to the development of MARISMA [92]. We use a specific case study to demonstrate the applicability of the MARISMA tool.

Table 4 provides a detailed comparison of the advancements proposed by the MARISMA framework concerning classical models, specifically focusing on technological objectives.

Drawing on our experience, the GSyA research group has actively participated in the creation of ten patterns (security management under

Table 3
Detailed description of Scientific Objectives solved in the MARISMA framework.

ID	Scientific objective	Classic models	Proposed advances - MARISMA
SO1	Adaptative Catalogues	They are based on fixed taxonomic catalogues	Ability to contain multiple taxonomic catalogues and the relationships between their elements.
SO2	Hierarchies and Associativity	They are intended for independent risk analysis	Ability to establish hierarchy trees and dependencies between different patterns. Ability to establish a risk analysis hierarchy. Ability to establish associativity relationships between shared assets.
SO3	Knowledge Reuse and Learning	Lack knowledge reuse capacity	Ability to learn based on information received from multiple sources: (i) Other associated patterns; (ii) Employer installations; (iii) The pattern of origin; (iv) Categorised security events.
SO4	Dynamic and Evolutive Criteria	It is designed for static risk analysis	Once the initial creation effort has been made, the system will be dynamic and will evolve into its reality over time, thanks to the feedback of its patterns and events it receives.
SO5	Collaborative Capacity	Lack the ability to collaborate	Ability to function as a hive mind. The security impacts received by the systems and categorised by means of events can be transferred to other systems of the network, to warn them of the increase in temporary attacks that affect certain controls. This makes it possible to introduce the concept of ”temporary external risk”.
SO6	Low Level of Subjectivity	They lack mechanisms that reduce subjectivity	Ability to make suggestions over time, to adjust the values of the different elements of the RA, to the existing reality and not to the perceived reality.

Table 4
Detailed description of Technological Objectives solved in the MARISMA framework.

ID	Scientific objective	Classic models	Proposed advances - MARISMA
TO1	Simplicity and Low Cost	They are not focused on reducing the cost or complexity of it. Completion time: From several weeks to months.	Focused on minimising generation and maintenance efforts through process automation. Completion time: From 1 day to 1 week.
TO2	Tool Support	Only some of them are supported by tools, but these act as mere content management systems.	It has a tool with two parts: (i) A global knowledge base of patterns hosted in the cloud; (ii) Support for instances that can be hosted in local clouds, with the option of sharing or not sharing information between the nodes that make up the cloud.
TO3	Global Scope	They are usually focused on a specific objective, or even a specific sector.	Ability to contain taxonomies focused on any objective (safety management, critical infrastructures, naval security, ...) and sectorised. All of a company’s risk views can be supported on the same basis.
TO4	Practical Cases	Many of them do not have real application cases.	Currently, the methodology has been applied in hundreds of cases around the world with multiple standards, sectors, and countries, which allows you to have an ever-increasing knowledge base.

the ISO/IEC 27001:2013 standard, security management under the ISO/IEC 27001:2022 standard, cyber–physical systems, security in big-data environments, security for business processes, generic critical infrastructures, critical infrastructures in the chemical sector, critical infrastructures in the energy sector, critical infrastructures in the port sector, ship security, etc.) that have been subsequently refined in real-world applications. Experience has shown that creating a pattern requires between 1000 and 1500 h of research, including the refinement phase. The lifetime of a pattern is currently estimated to be between 5 and 10 years. However, eMARISMA enables quick and easy maintenance of patterns, allowing them to evolve and adapt.

During the implementation of MARISMA across different sectors, several challenges arose, extending beyond technical aspects. Organisational challenges were particularly evident in companies with rigid structures or defined hierarchies, where the adoption of new tools and processes was slower due to resistance to change and a lack of specialised cybersecurity training. These obstacles were addressed by providing specific training for staff and adapting the framework to the unique needs of each organisation, enabling a more gradual and natural adoption of the system.

At a technical level, integrating MARISMA with legacy infrastructures and pre-existing systems proved challenging, especially in organisations with outdated technology. These barriers were overcome through the flexibility and scalability of eMARISMA, which allowed for a phased integration without disrupting daily operations.

Furthermore, cultural challenges related to risk management in sectors less familiar with cybersecurity required an emphasis on raising awareness of the importance of proactive risk management.

Among the lessons learned, it became clear that a gradual, collaborative implementation approach is essential. Ensuring participation from all levels of the organisation and providing ongoing support were key to facilitating the transition and maximising the success of MARISMA’s deployment.

In summary, we believe that the proposed method has demonstrated its capacity to provide a solution to the proposed scientific and technological objectives, obtaining a new method that allows for much more advanced and complete risk analyses than classic methods. Moreover, the management and maintenance processes of these systems have become simpler and less costly, thereby increasing the accuracy of the results. However, opportunities for further improvement and new advances in the proposed method exist, which will allow increasingly accurate and valuable results to be obtained for companies that use it.

6. Conclusions and future work

Traditional methods of risk analysis and risk management, although developed over a long period, still have important limitations that are further accentuated in today’s changing environment, as they were not created to take advantage of the technological changes and opportunities that have arisen from this technological evolution. As we have seen throughout the article, the emergence of new technologies gives us the

opportunity to create a new generation of risk analysis that is more powerful, with greater capacity for adaptation, associativity, learning, and reuse of knowledge, dynamic, collaborative, and more accurate. All this, while making them simpler to generate and maintain, allows them to be used by all types of organisations, regardless of their size.

Thus, the purpose of this study is to present the development of a new framework called MARISMA to analyse and manage technological risks, which is supported by a cloud-based tool called eMARISMA. This framework, which provides solutions to the main problems encountered in classic risk analysis and management systems, is the result of years of validation in organisations of different sizes (from SMEs to large corporations and state bodies), in different sectors (mainly technological, chemical, energy, insurance, port, and public sector), in different countries (mainly in Spain, Argentina, Colombia and Ecuador), and with different security standards (mainly based on Magerit, ISO/IEC 27001, IEC 62443 taxonomies) and applied to different contexts (mainly Security Management, Critical Infrastructure, Naval Cybersecurity).

In addition, the ability to evolve dynamically through the reuse of knowledge introduces the high-potential concept of collaborative security (hive-mind). This mechanism allows companies to protect each other and make their risk analysis an element that evolves not only with internal information but also draws on a global knowledge network.

Lessons learned from our work include the construction and validation of the framework through a large number of real cases with great diversity (size, geographic, and business sector) that have led to improvements and the possibility of defining patterns with a higher level of specialisation. MARISMA's inheritance capabilities, as well as its knowledge acquisition and reuse mechanisms, are being used to define new, more precise patterns with new approaches (e.g. applied to measure risk levels associated with security systems in shipbuilding, to measure cybersecurity risks in business processes, patterns to analyse security risks associated with individuals or households, and patterns for cybersecurity models associated with Agriculture 4.0).

In the future, in addition to ongoing research to develop new patterns such as those mentioned in the previous paragraph, other challenges that have been identified in the current application phase will be addressed. One of them is the creation of multidimensional patterns, derived from the increasing need in organisations for an asset to be analysed from different risk dimensions (e.g. a software asset can be analysed from the dimensions of confidentiality, integrity, availability, authenticity, and trustworthiness in a security management-oriented approach, while its dimensions will be cybersecurity, privacy, reliability, resilience, and safety in a cyber–physical systems security oriented approach). In other words, an asset of value for a company can be analysed from multiple dimensions and therefore requires the application of different patterns, but at the same time, these patterns can have partial or total coincidences in their elements (threats and controls); therefore, it is necessary to create a process to support this multidimensional vision of the assets. This will provide systems with a greater risk-management capacity to enhance the mechanisms of evolution and learning patterns. In addition, new algorithms based on deep learning techniques will be developed, which should provide MARISMA's DRM process with a greater risk prediction capacity, enriching the current results of temporary external risk by introducing predictions derived from artificial intelligence (e.g. the probability of the occurrence of a natural disaster in a certain geographical location or of a potential denial of service attack). Finally, we intend to extend this knowledge to a new generation of individuals with more accurate risk patterns.

Other future lines of research, which are planned, include exploring the application of MARISMA in new sectors, such as healthcare, finance, or transportation, where the framework's adaptability and comprehensive risk analysis could address sector-specific challenges. Additionally, research should focus on integrating MARISMA with emerging technologies like blockchain, the Internet of Things (IoT), and artificial intelligence (AI). These technologies introduce new risks that MARISMA's tools could help mitigate, but further refinement of its components is required to ensure optimal effectiveness. Finally, continued research into improving MARISMA's automation and predictive capabilities, such as the use of machine learning algorithms, will enhance its ability to anticipate and respond to evolving threats, making it even more powerful in proactive risk management.

CRediT authorship contribution statement

Luis E. Sánchez: Software, Methodology, Investigation. **Antonio Santos-Olmo:** Software, Methodology, Investigation. **David G. Rosado:** Investigation, Formal analysis, Conceptualization. **Carlos Blanco:** Software, Resources, Formal analysis. **Manuel A. Serrano:** Supervision, Resources, Methodology. **Haralambos Mouratidis:** Validation, Methodology, Investigation. **Eduardo Fernández-Medina:** Supervision, Methodology, Investigation.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgements

This work has been developed thanks to the financing provided by the following projects: Di4SPDS projects (CHIST-ERA grant - PCI2023145980-2) funded by MCIN/AEI and co-funded by the European Union, AETHER-UCLM (PID2020-112540RB-C42) financed by MCIN/AEI/10.13039/501100011033; ALBA-UCLM (TED2021-130355B-C31), ALBA-UC (TED2021-130355A-C33) financed by CIN/AEI/10.13039/501100011033/Unión Europea NextGenerationEU/PRTR, and MESIAS (2022-GRIN-34202) financed by FEDER.

Data availability

No data was used for the research described in the article.

References

[1] R. Villalón-Fonseca, The nature of security: A conceptual framework for integral-comprehensive modeling of IT security and cybersecurity, Comput. Secur. 120 (2022) 102805, http://dx.doi.org/10.1016/j.cose.2022.102805.

[2] A. Mishra, Y.I. Alzoubi, M.J. Anwar, A.Q. Gill, Attributes impacting cybersecurity policy development: An evidence from seven nations, Comput. Secur. 120 (2022) 102820, http://dx.doi.org/10.1016/j.cose.2022.102820.

[3] W. Yeoh, S. Wang, A. Popovič, N.H. Chowdhury, A systematic synthesis of critical success factors for cybersecurity, Comput. Secur. 118 (2022) 102724, http://dx.doi.org/10.1016/j.cose.2022.102724.

[4] S. Durst, C. Hinteregger, M. Zieba, The effect of environmental turbulence on cyber security risk management and organizational resilience, Comput. Secur. 137 (2024) 103591, http://dx.doi.org/10.1016/j.cose.2023.103591, URL https://www.sciencedirect.com/science/article/pii/S0167404823005011.

[5] M. Mirtsch, K. Blind, C. Koch, G. Dudek, Information security management in ICT and non-ICT sector companies: A preventive innovation perspective, Comput. Secur. 109 (2021) 102383, http://dx.doi.org/10.1016/j.cose.2021.102383.

[6] A. Heidari, N. Navimipour, H. Dag, M. Unal, Deepfake detection using deep learning methods: A systematic and comprehensive review, Wiley Interdiscip. Rev. Data Min. Knowl. Discov. 14 (2023) http://dx.doi.org/10.1002/widm.1520.

[7] A. Heidari, H. Shishehlou, M. Darbandi, N. Navimipour, S. Yalcin, A reliable method for data aggregation on the industrial internet of things using a hybrid optimization algorithm and density correlation degree, Cluster Comput. 27 (2024) http://dx.doi.org/10.1007/s10586-024-04351-4.

[8] A. Heidari, N. Navimipour, M. Unal, A secure intrusion detection platform using blockchain and radial basis function neural networks for internet of drones, IEEE Internet Things J. PP (2023) http://dx.doi.org/10.1109/JIOT.2023.3237661.

[9] A. Heidari, N. Navimipour, M. Unal, G. Zhang, Machine learning applications in internet-of-drones: Systematic review, recent deployments, and open issues, ACM Comput. Surv. 55 (2022) http://dx.doi.org/10.1145/3571728.

[10] L. Feng, C. Tao, W. Bin, Z. Jianye, Q. Song, Research on information security technology of mobile application in electric power industry, in: 2020 Asia-Pacific Conference on Image Processing, Electronics and Computers, IPEC, 2020, pp. 51–54, http://dx.doi.org/10.1109/IPEC49694.2020.9115191.

[11] K. Khando, S. Gao, S.M. Islam, A. Salman, Enhancing employees information security awareness in private and public organisations: A systematic literature review, Comput. Secur. 106 (2021) 102267, http://dx.doi.org/10.1016/j.cose.2021.102267.

[12] A.A. Ganin, P. Quach, M. Panwar, Z.A. Collier, J.M. Keisler, D. Marchese, I. Linkov, Multicriteria decision framework for cybersecurity risk assessment and management, Risk Anal. 40 (1) (2020) 183–199, http://dx.doi.org/10.1111/risa.12891.

[13] K. van der Schyff, S. Flowerday, Mediating effects of information security awareness, Comput. Secur. 106 (2021) 102313, http://dx.doi.org/10.1016/j.cose.2021.102313.

[14] A. Chopra, M. Chaudhary, The need for information security, in: Implementing an Information Security Management System: Security Management Based on ISO 27001 Guidelines, A Press, Berkeley, CA, 2020, pp. 1–20, http://dx.doi.org/10.1007/978-1-4842-5413-4_1.

[15] S.A. Grishaeva, V.I. Borzov, Information security risk management, in: 2020 International Conference Quality Management, Transport and Information Security, Information Technologies, IT&QM&IS, 2020, pp. 96–98, http://dx.doi.org/10.1109/ITQMIS51053.2020.9322901.

[16] M.K. Zaini, M.N. Masrek, M.K.J. Abdullah Sani, The impact of information security management practices on organisational agility, Inf. Comput. Secur. 28 (5) (2020) 681–700, http://dx.doi.org/10.1108/ICS-02-2020-0020.

[17] A. Shameli-Sendi, An efficient security data-driven approach for implementing risk assessment, J. Inf. Secur. Appl. 54 (2020) 102593, http://dx.doi.org/10.1016/j.jisa.2020.102593.

[18] M. Jbair, B. Ahmad, C. Maple, R. Harrison, Threat modelling for industrial cyber physical systems in the era of smart manufacturing, Comput. Ind. 137 (2022) 103611, http://dx.doi.org/10.1016/j.compind.2022.103611, URL https://www.sciencedirect.com/science/article/pii/S0166361522000069.

[19] B. Uchendu, J.R. Nurse, M. Bada, S. Furnell, Developing a cyber security culture: Current practices and future needs, Comput. Secur. 109 (2021) 102387, http://dx.doi.org/10.1016/j.cose.2021.102387.

[20] I.M.M. Putra, K. Mutijarsa, Designing information security risk management on bali regional police command center based on ISO 27005, in: 2021 3rd East Indonesia Conference on Computer and Information Technology, EIConCIT, 2021, pp. 14–19, http://dx.doi.org/10.1109/EIConCIT50028.2021.9431865.

[21] L.E. Sánchez, A. Santos-Olmo, H. Mouratidis, E. Fernández-Medina, New frontiers in security risk management, IT Prof. 25 (3) (2023) 61–67, http://dx.doi.org/10.1109/MITP.2023.3251720.

[22] F.O. Sönmez, B.G. Kilic, A decision support system for optimal selection of enterprise information security preventative actions, IEEE Trans. Netw. Serv. Manag. 18 (3) (2021) 3260–3279, http://dx.doi.org/10.1109/TNSM.2020.3044865.

[23] A. Sen, S. Madria, Application design phase risk assessment framework using cloud security domains, J. Inf. Secur. Appl. 55 (2020) 102617, http://dx.doi.org/10.1016/j.jisa.2020.102617.

[24] S. Tanimoto, M. Matsumoto, T. Endo, H. Sato, A. Kanai, Risk management of fog computing for improving IoT security, in: 2021 10th International Congress on Advanced Applied Informatics, IIAI-AAI, 2021, pp. 703–709, http://dx.doi.org/10.1109/IIAI-AAI53430.2021.00125.

[25] I. Šarūnienė, L. Martišauskas, R. Krikštolaitis, J. Augutis, R. Setola, Risk assessment of critical infrastructures: A methodology based on criticality of infrastructure elements, Reliab. Eng. Syst. Saf. 243 (2024) 109797, http://dx.doi.org/10.1016/j.ress.2023.109797, URL https://www.sciencedirect.com/science/article/pii/S0951832023007111.

[26] A. Salvi, P. Spagnoletti, N.S. Noori, Cyber-resilience of Critical Cyber Infrastructures: Integrating digital twins in the electric power ecosystem, Comput. Secur. 112 (2022) 102507, http://dx.doi.org/10.1016/j.cose.2021.102507.

[27] T.S. AlSalem, M.A. Almaiah, A. Lutfi, Cybersecurity risk analysis in the IoT: A systematic review, Electronics 12 (18) (2023) http://dx.doi.org/10.3390/electronics12183958, URL https://www.mdpi.com/2079-9292/12/18/3958.

[28] H. Nozari, S.A. Edalatpanah, Smart systems risk management in IoT-based supply chain, in: Advances in Reliability, Failure and Risk Analysis, Springer Nature Singapore, Singapore, 2023, pp. 251–268, http://dx.doi.org/10.1007/978-981-19-9909-3_11.

[29] Z. Zhang, A new method for information security risk management in big data environment, in: 2020 2nd International Conference on Information Technology and Computer Application, ITCA, 2020, pp. 1–4, http://dx.doi.org/10.1109/ITCA52113.2020.00100.

[30] A.E. Ibor, O.B. Okunoye, F.A. Oladeji, K.A. Abdulsalam, Novel hybrid model for intrusion prediction on cyber physical systems' communication networks based on bio-inspired deep neural network structure, J. Inf. Secur. Appl. 65 (2022) 103107, http://dx.doi.org/10.1016/j.jisa.2021.103107.

[31] J.V. Barraza de la Paz, L.A. Rodríguez-Picón, V. Morales-Rocha, S.V. Torres-Argüelles, A systematic review of risk management methodologies for complex organizations in industry 4.0 and 5.0, Systems 11 (5) (2023) http://dx.doi.org/10.3390/systems11050218, URL https://www.mdpi.com/2079-8954/11/5/218.

[32] P.K.R. Maddikunta, Q.-V. Pham, P. B, N. Deepa, K. Dev, T.R. Gadekallu, R. Ruby, M. Liyanage, Industry 5.0: A survey on enabling technologies and potential applications, J. Ind. Inf. Integr. 26 (2022) 100257, http://dx.doi.org/10.1016/j.jii.2021.100257.

[33] D.J. Ferreira, N. Mateus-Coelho, H.S. Mamede, Methodology for predictive cyber security risk assessment (PCSRA), Procedia Comput. Sci. 219 (2023) 1555–1563, http://dx.doi.org/10.1016/j.procs.2023.01.447, URL https://www.sciencedirect.com/science/article/pii/S1877050923004581 CENTERIS – International Conference on ENTERprise Information Systems / ProjMAN – International Conference on Project MANagement / HCist – International Conference on Health and Social Care Information Systems and Technologies 2022.

[34] A. Capodieci, L. Mainetti, F. Dipietrangelo, Model-driven approach to cyber risk analysis in industry 4.0, in: Proceedings of the 10th International Conference on Information Systems and Technologies, ICIST '20, Association for Computing Machinery, New York, NY, USA, 2020, pp. 1–7, http://dx.doi.org/10.1145/3447568.3448541.

[35] D.J. Ferreira, H.S. Mamede, N. Mateus-Coelho, Risk management in the current digital reality of organizations, in: Contemporary Challenges for Cyber Security and Data Privacy, IGI Global, 2023, pp. 31–50.

[36] R.L. Baskerville, J. Kim, C. Stucke, The cybersecurity risk estimation engine: A tool for possibility based risk analysis, Comput. Secur. 120 (2022) 102752, http://dx.doi.org/10.1016/j.cose.2022.102752.

[37] P.G. Genchev, Analysis of changes in the probability of an incident with information security, in: 2021 56th International Scientific Conference on Information, Communication and Energy Systems and Technologies, ICEST, 2021, pp. 119–122, http://dx.doi.org/10.1109/ICEST52640.2021.9483532.

[38] S.G. Govender, E. Kritzinger, M. Loock, A framework and tool for the assessment of information security risk, the reduction of information security cost and the sustainability of information security culture, Pers. Ubiquitous Comput. (2021) http://dx.doi.org/10.1007/s00779-021-01549-w.

[39] P. Cheimonidis, K. Rantos, Dynamic risk assessment in cybersecurity: A systematic literature review, Future Internet 15 (10) (2023) http://dx.doi.org/10.3390/fi15100324, URL https://www.mdpi.com/1999-5903/15/10/324.

[40] F. Guggenmos, B. Häckel, P. Ollig, B. Stahl, Security first, security by design, or security pragmatism – Strategic roles of IT security in digitalization projects, Comput. Secur. 118 (2022) 102747, http://dx.doi.org/10.1016/j.cose.2022.102747.

[41] S. Barat, T. Clark, B. Barn, V. Kulkarni, A model-based approach to systematic review of research literature, in: Proceedings of the 10th Innovations in Software Engineering Conference, ISEC '17, Association for Computing Machinery, New York, NY, USA, 2017, pp. 15–25, http://dx.doi.org/10.1145/3021460.3021462.

[42] B. Barn, S. Barat, T. Clark, Conducting systematic literature reviews and systematic mapping studies, in: Proceedings of the 10th Innovations in Software Engineering Conference, ISEC '17, Association for Computing Machinery, New York, NY, USA, 2017, pp. 212–213, http://dx.doi.org/10.1145/3021460.3021489.

[43] D. Naouar, J.E. Hachem, J.-L. Voirin, J. Foisil, Y. Kermarrec, Towards the integration of cybersecurity risk assessment into model-based requirements engineering, in: 2021 IEEE 29th International Requirements Engineering Conference, RE, 2021, pp. 334–344, http://dx.doi.org/10.1109/RE51729.2021.00037.

[44] Magerit, Magerit_v3: Methodology for information systems risk analysis and management. The method, in: Magerit_V3, Ministry of Public Administration, 2012, URL http://administracionelectronica.gob.es/.

[45] R. Caralli, J. Stevens, L. Young, W. Wilson, Introducing OCTAVE allegro: Improving the information security risk assessment process, Tech. Rep. CMU/SEI-2007-TR-012, Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA, 2007, URL http://resources.sei.cmu.edu/library/asset-view.cfm?AssetID=8419.

[46] NC3 Luxembourg, MONARC Technical Guide, 2023, URL https://www.monarc.lu/documentation/technical-guide/.

[47] M.S. Lund, B. Solhaug, K. Stølen, Model-Driven Risk Analysis, Springer Berlin Heidelberg, 2011, http://dx.doi.org/10.1007/978-3-642-12323-8.

[48] Agence nationale de la sécurité des systèmes d'information, EBIOS risk manager, in: EBIOS Risk Manager - The Method, Agence nationale de la sécurité des systèmes d'information, 2019, EBIOS RM URL https://cyber.gouv.fr/publications/ebios-risk-manager-method.

[49] M. CLUSIF, Processing guide for risk analysis and management, in: Club de la Securite de LInformation Francias, second ed., 2010, April 2011.

[50] ISO/IEC 27005:2022, Information Technology – Security Techniques – Information Security Risk Management, Tech. Rep., 2022, Iso/Iec, Vol. 3.

[51] S. De Haes, W. Van Grembergen, A. Joshi, T. Huygh, COBIT as a framework for enterprise governance of IT, in: Enterprise Governance of Information Technology: Achieving Alignment and Value in Digital Organizations, Springer International Publishing, Cham, 2020, pp. 125–162, http://dx.doi.org/10.1007/978-3-030-25918-1_5.

[52] M. Ross, A.J. Jara, A. Cosenza, Baseline Security Recommendations for IoT in the Context of Critical Information Infrastructures, (November) European Union Agency For Network And Information Security, 2017, http://dx.doi.org/10.2824/03228.

[53] A. Santos-Olmo, L.E. Sánchez, D.G. Rosado, B. Serrano, H. Mouratidis, F.-M. Eduardo, Towards an integrated risk analysis security framework according to a systematic analysis of existing proposals, Front. Comput. Sci. 18 (3) (2024) 1–18, http://dx.doi.org/10.1007/s11704-023-1582-6.
[54] S. Alhawari, L. Karadsheh, A. Nehari Talet, E. Mansour, Knowledge-based risk management framework for information technology project, Int. J. Inf. Manage. 32 (1) (2012) 50–65, http://dx.doi.org/10.1016/j.ijinfomgt.2011.07.002.
[55] N. Feng, M. Li, An information systems security risk assessment model under uncertain environment, Appl. Soft Comput. 11 (7) (2011) 4332–4340, http://dx.doi.org/10.1016/j.asoc.2010.06.005.
[56] C.C. Lo, W.J. Chen, A hybrid information security risk assessment procedure considering interdependences between controls, Expert Syst. Appl. 39 (1) (2012) 247–257, http://dx.doi.org/10.1016/j.eswa.2011.07.015.
[57] Y.P. Ou Yang, H.M. Shieh, G.H. Tzeng, A VIKOR technique based on DEMATEL and ANP for information security risk control assessment, Inform. Sci. 232 (2013) 482–500, http://dx.doi.org/10.1016/j.ins.2011.09.012.
[58] P. Shamala, R. Ahmad, M. Yusoff, A conceptual framework of info structure for information security risk assessment (ISRA), J. Inf. Secur. Appl. 18 (1) (2013) 45–52, http://dx.doi.org/10.1016/j.jisa.2013.07.002.
[59] M. Wulan, D. Petrovic, A fuzzy logic based system for risk analysis and evaluation within enterprise collaborations, Comput. Ind. 63 (8) (2012) 739–748, http://dx.doi.org/10.1016/j.compind.2012.08.012.
[60] M.S. Saleh, A. Alfantookh, A new comprehensive framework for enterprise information security risk management, Appl. Comput. Inform. 9 (2) (2011) 107–118, http://dx.doi.org/10.1016/j.aci.2011.05.002.
[61] S. Hiroyuki, A new formula of security risk analysis that takes risk improvement factor into account, in: Privacy, Security, Risk and Trust (PASSAT) and 2011 IEEE Third Inernational Conference on Social Computing (SocialCom), 2011 IEEE Third International Conference on, 2011, pp. 1243–1248, http://dx.doi.org/10.1109/PASSAT/SocialCom.2011.44.
[62] N. Feng, H.J. Wang, M. Li, A security risk analysis model for information systems: Causal relationships of risk factors and vulnerability propagation analysis, Inform. Sci. 256 (2014) 57–73, http://dx.doi.org/10.1016/j.ins.2013.02.036.
[63] L. Wang, B. Wang, Y. Peng, Research the information security risk assessment technique based on Bayesian network, in: Advanced Computer Theory and Engineering (ICACTE), 2010 3rd International Conference on, Vol. 3, 2010, pp. V3–600–V3–604, http://dx.doi.org/10.1109/icacte.2010.5579740.
[64] J. Webb, A. Ahmad, S.B. Maynard, G. Shanks, A situation awareness model for information security risk management, Comput. Secur. 44 (2014) 1–15, http://dx.doi.org/10.1016/j.cose.2014.04.005.
[65] S. Armenia, M. Angelini, F. Nonino, G. Palombi, M.F. Schlitzer, A dynamic simulation approach to support the evaluation of cyber risks and security investments in SMEs, Decis. Support Syst. 147 (2021) 113580, http://dx.doi.org/10.1016/j.dss.2021.113580.
[66] R. Deb, S. Roy, A software defined network information security risk assessment based on Pythagorean fuzzy sets, Expert Syst. Appl. 183 (2021) 115383, http://dx.doi.org/10.1016/j.eswa.2021.115383.
[67] E. Vicente, A. Mateos, A. Jiménez-Martín, Risk analysis in information systems: A fuzzification of the MAGERIT methodology, Knowl.-Based Syst. 66 (2014) 1–12, http://dx.doi.org/10.1016/j.knosys.2014.02.018.
[68] S. Mandal, J. Maiti, Risk analysis using FMEA: Fuzzy similarity value and possibility theory based approach, Expert Syst. Appl. 41 (7) (2014) 3527–3537, http://dx.doi.org/10.1016/j.eswa.2013.10.058.
[69] A. Shameli-Sendi, An efficient security data-driven approach for implementing risk assessment, J. Inf. Secur. Appl. 54 (2020) 102593, http://dx.doi.org/10.1016/j.jisa.2020.102593.
[70] S. Sicari, A. Rizzardi, D. Miorandi, A. Coen-Porisini, A risk assessment methodology for the Internet of Things, Comput. Commun. 129 (2018) 67–79, http://dx.doi.org/10.1016/j.comcom.2018.07.024.
[71] M.A. van Staalduinen, F. Khan, V. Gadag, G. Reniers, Functional quantitative security risk analysis (QSRA) to assist in protecting critical process infrastructure, Reliab. Eng. Syst. Saf. 157 (2017) 23–34, http://dx.doi.org/10.1016/j.ress.2016.08.014.
[72] H. Abdo, M. Kaouk, J.M. Flaus, F. Masse, A safety/security risk analysis approach of Industrial Control Systems: A cyber bowtie – combining new version of attack tree with bowtie analysis, Comput. Secur. 72 (2018) 175–195, http://dx.doi.org/10.1016/j.cose.2017.09.004.
[73] F. Khan, S.J. Hashemi, N. Paltrinieri, P. Amyotte, V. Cozzani, G. Reniers, Dynamic risk management: a contemporary approach to process safety management, Curr. Opin. Chem. Eng. 14 (2016) 9–17, http://dx.doi.org/10.1016/j.coche.2016.07.006.
[74] F. Munodawafa, A.I. Awad, Security risk assessment within hybrid data centers: A case study of delay sensitive applications, J. Inf. Secur. Appl. 43 (2018) 61–72, http://dx.doi.org/10.1016/j.jisa.2018.10.008.
[75] D. Panchal, A.K. Singh, P. Chatterjee, E.K. Zavadskas, M. Keshavarz-Ghorabaee, A new fuzzy methodology-based structured framework for RAM and risk analysis, Appl. Soft Comput. 74 (2019) 242–254, http://dx.doi.org/10.1016/j.asoc.2018.10.033.
[76] A.K. Sangaiah, O.W. Samuel, X. Li, M. Abdel-Basset, H. Wang, Towards an efficient risk assessment in software projects–fuzzy reinforcement paradigm, Comput. Electr. Eng. 71 (2018) 833–846, http://dx.doi.org/10.1016/j.compeleceng.2017.07.022.
[77] G. Wangen, C. Hallstensen, E. Snekkenes, A framework for estimating information security risk assessment method completeness, Int. J. Inf. Secur. 17 (6) (2018) 681–699, http://dx.doi.org/10.1007/s10207-017-0382-0.
[78] H. Zhang, Q. Sun, An integrated approach to risk assessment for special line shunting via fuzzy theory, Symmetry 10 (11) (2018) http://dx.doi.org/10.3390/sym10110599.
[79] C. Schmitz, S. Pape, LiSRA: Lightweight security risk assessment for decision support in information security, Comput. Secur. 90 (2020) 101656, http://dx.doi.org/10.1016/j.cose.2019.101656.
[80] E. Lamine, R. Thabet, A. Sienou, D. Bork, F. Fontanili, H. Pingaud, BPRIM: An integrated framework for business process management and risk management, Comput. Ind. 117 (2020) 103199, http://dx.doi.org/10.1016/j.compind.2020.103199.
[81] A. Schmidt, L.A. Albert, K. Zheng, Risk management for cyber-infrastructure protection: A bi-objective integer programming approach, Reliab. Eng. Syst. Saf. 205 (2021) 107093, http://dx.doi.org/10.1016/j.ress.2020.107093.
[82] P. Tubío Figueira, C. López Bravo, J.L. Rivas López, Improving information security risk analysis by including threat-occurrence predictive models, Comput. Secur. 88 (2020) 101609, http://dx.doi.org/10.1016/j.cose.2019.101609.
[83] Y. Cherdantseva, P. Burnap, S. Nadjm-Tehrani, K. Jones, A configurable dependency model of a SCADA system for goal-oriented risk assessment, Appl. Sci. 12 (10) (2022) http://dx.doi.org/10.3390/app12104880.
[84] E. Bozku, x015F, x, Kaya, M. Yakut, A fuzzy based model proposal on risk analysis for human-robot interactive systems, in: 2022 International Congress on Human-Computer Interaction, Optimization and Robotic Applications, HORA, 2022, pp. 1–6, http://dx.doi.org/10.1109/HORA55278.2022.9799820.
[85] J. Overbeek, Meta Object Facility (MOF): Investigation of the State of the Art, University of Twente, 2006.
[86] ISO/IEC 27001:2013, SO/IEC 27001:2013 - Information Technology — Security Techniques — Information Security Management Systems — Requirements, Standard, International Organization for Standardization, Geneva, CH, 2013, Iso/Iec 2013.
[87] D.G. Rosado, A. Santos-Olmo, L.E. Sánchez, M.A. Serrano, C. Blanco, H. Mouratidis, E. Fernández-Medina, Managing cybersecurity risks of cyber-physical systems: The MARISMA-CPS pattern, Comput. Ind. 142 (2022) 103715, http://dx.doi.org/10.1016/j.compind.2022.103715.
[88] D.G. Rosado, J. Moreno, L.E. Sánchez, A. Santos-Olmo, M.A. Serrano, E. Fernández-Medina, MARISMA-BiDa pattern: Integrated risk analysis for big data, Comput. Secur. 102 (2021) 102155, http://dx.doi.org/10.1016/j.cose.2020.102155.
[89] D.G. Rosado, L.E. Sánchez, Á.J. Varela-Vaca, A. Santos-Olmo, M.T. Gómez-López, R.M. Gasca, E. Fernández-Medina, Enabling security risk assessment and management for business process models, J. Inf. Secur. Appl. 84 (2024) 103829, http://dx.doi.org/10.1016/j.jisa.2024.103829.
[90] R. Bendraou, B. Combemale, X. Cregut, M.-P. Gervais, Definition of an executable SPEM 2.0, in: 14th Asia-Pacific Software Engineering Conference, APSEC'07, 2007, pp. 390–397, http://dx.doi.org/10.1109/ASPEC.2007.60.
[91] L. Marinos, ENISA Threat Taxonomy: A Tool for Structuring Threat Information. Initial Report, Tech. Rep. January, European Union Agency For Network And Information Security, 2016, pp. 1–24, URL https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/enisa-threat-landscape/threat-taxonomy/view.
[92] A. Santos-Olmo, L. Sánchez, D. Rosado, E. Fernández-Medina, M. Piattini, Applying the action-research method to develop a methodology to reduce the installation and maintenance times of information security management systems, Future Internet 8 (3) (2016) 36, http://dx.doi.org/10.3390/fi8030036.