Security Journal (2022) 35:600–627
https://doi.org/10.1057/s41284-021-00292-4

ORIGINAL ARTICLE

# Security as a key contributor to organisational resilience: a bibliometric analysis of enterprise security risk management

**Jose Marquez-Tejon**[1] · **Montserrat Jimenez-Partearroyo**[1] · **Diana Benito-Osorio**[1]

Accepted: 23 February 2021 / Published online: 20 March 2021


## Abstract

Globalisation and hyperconnectivity affect organisational resilience with threats such as the recent COVID-19 pandemic or large-scale cyberattacks. To strengthen organisational resilience capabilities, a framework such as enterprise risk management (ERM) is necessary so as to enable holistic risk management. Specifically, in this paper, we analyse the role of security, which has great potential in crisis management and makes it possible to follow up businesses integrated in enterprise security risk management (ESRM). This paper examines, for the first time in the literature, the output of scientists on ESRM. After analysing 463 articles from the period between 1986 and 2019, it is concluded that Security Risk Management is a subject area on its own and is closely linked to ERM.

**Keywords** Enterprise security risk management · Enterprise risk management · Organisational resilience · ERM · Security management · Crisis management

## Introduction

Traditionally, risk management in companies has been uncoordinated and siloed (Mcshane et al. 2011). However, over the past three decades, the new volatile, uncertain, complex and ambiguous (VUCA) environment in which organisations carry out their activities has given rise to the need to adapt and implement a new strategic

✉ Jose Marquez-Tejon
jose.marquez-tejon@outlook.com

Montserrat Jimenez-Partearroyo
montserrat.jimenez@urjc.es

Diana Benito-Osorio
diana.benito@urjc.es

[1] Universidad Rey Juan Carlos, Paseo de los Artilleros, s/n, 28032 Madrid, Spain

framework for risk management. In this scenario, the most widespread and accepted model is so-called enterprise risk management (ERM) model, which contributes to organisational resilience in a coordinated manner.

Some of the risks faced by organisations are those related to corporate security management (hereinafter security). Such management must be integrated with the organisation's overall risk strategy along with other corporate and business areas. Even senior management and other departments must be actively involved (Nalla and Morash 2002). From a strategic perspective, companies and their board leaders need to understand and make clear that different individuals and groups within the organisation are the owners of their risk and responsible for (Bromiley et al. 2015). Since its inception, the field of security in business organisations has focused on the role of directly managing and handling intentional antisocial risks that may affect a business, including providing cross-sectional support during crises to minimise impact (Ludbey et al. 2018).

In recent years, important associations of security professionals and managers worldwide have progressed beyond the simple convergence of security (physical security and cybersecurity) and have worked on a new holistic model aligned with ERM (Johnson and Spivey 2008) called enterprise security risk management (hereinafter ESRM).

Today, company CEOs have understood that corporations' goal achievement depends on how they strategically manage risks (Hoyt and Liebenberg 2011); hence, incorporating ESRM as part of the ERM framework has become vital, particularly in large organisations and multinational companies. Therefore, from an academic perspective, it is appropriate to empirically study the actual contribution of security through ESRM to the resilience capacity of business organisations. The first step in this article is to conduct a bibliometric study of ESRM as a research field and identify whether there are any gaps in the literature. The article is structured as follows: first, the most important concepts of the theoretical framework are defined; second, the methodology used is described by using contrasting bibliometric techniques; then, the results are analysed and discussed; and finally, in the conclusion, the academic and practical import of the findings and possible new research trends are outlined.

## ESRM: a conceptual approach

Below are the concepts identified in the academic literature on security within the ERM framework, according to Johnson and Spivey (2008). These authors posit that ESRM is designed to be an ERM element enabling cross-functional collaboration between multiple management disciplines. Both compliance and governance processes under board-level oversight are closely related to resilience (Dahms 2010) and involve the set of enterprise risk management (ERM) and security risk (ESRM) as part of the same. ESRM governance, a subtype of corporate governance, is modelled on organisational governance, and its implementation is based on establishing an enterprise security risk policy and strategy, allocating resources and ensuring compliance (ASIS International 2019). We designed this approach on the basis

of the notion of organisational resilience, starting from the internationally accepted ERM model and then going deeper into the part of that framework related to governance of security risks in organisations (ESRM).

### Organisational resilience

Security's direct relation with organisational resilience was observed by the International Organization for Standardization (ISO) when it created the ISO/TC 292 committee in 2015. Among the goals of this committee are capabilities standardisation, organisational security and resilience management. According to ISO 22316 (2017) 'Security and resilience—Organisational resilience—Principles and attributes', organisational resilience is defined as "the ability of an organisation to absorb and adapt in a changing environment" to achieve its goals, survive and prosper. According to this standard, the most resilient organisations can anticipate and respond to threats and opportunities that may result from sudden or gradual changes in their internal and external contexts. Improving resilience should be a strategic organisational objective and is the result of good business practices and effective risk management.

Business activity is intrinsically subject to risks in the attainment of goals, regardless of the nature of the activity, business turnover or the geographical area of operation. Exposure to and the handling of those risks condition the capacity to maximise value, and that is the reason that the results obtained vary depending on the management of such risks. Eastburn and Sharland (2017) established in their research how an effective risk management process can be a solution to help firms capitalise upon risk/reward opportunities.

Many companies currently operate in a VUCA environment, which makes it more difficult for leaders to make the reliable risk diagnoses that are necessary for making decisions, to allocate adequate resources to protect the company from negative risks and to identify opportunities (Bennett and Lemoine 2014). Business organisations perceive uncertainty as the greatest risk that threatens goal achievement. Therefore, they need a management framework that helps them mitigate all known and emerging risks before they occur (Gupta 2016). Among all possible risks, the extreme impact of unpredictable and unlikely events, called 'black swans' (Taleb 2007), is highlighted. Although there is no fool-proof risk management system to prevent the occurrence of black swan events, the system's implementation can help support decision-making processes regarding the measures that should be implemented to mitigate the impact on the organisation.

### Enterprise risk management (ERM)

Although in the late 1980s, there was already incipient work in the field, the risk management framework based on ERM appeared in the 1990s as a result of the need arising from a competitive and complex environment, seeking to link risk management with companies' activities (Arena et al. 2010). ERM became the main form adopted by the companies making growing efforts to address uncertainty, which

peaked in that decade (Shetty et al. 2018). According to Govender (2019), Australia and New Zealand were the first countries to develop a holistic risk management model in 1999 through the AZ/NZS 4360 standard. The financial scandals of later years and the collapse of large multinational companies such as Enron and Worldcom made it necessary to introduce regulatory standards, such as the Sarbanes-Oxley Act (2002), to avoid fraud and bankruptcy risk.

In 2004, the Committee of Sponsoring Organizations of the Treadway Commission (COSO) published the first comprehensive guide to ERM (COSO ERM—Enterprise Risk Management—Integrated Framework). This standard was updated in 2017 to guide ERM integration towards the establishment of strategies and performance (Prewett and Terry 2018). Bharathy and McShane (2014) propose an ERM implementation approach that allows the effective implementation of business and strategic complex risk management through ISO 31000 (2018).

Having a risk management framework in place does not mean that it can be trusted and that companies can become acculturated to it. If we go back in time and look at the negative effect on the world economy of the subprime mortgage crisis of 2008, we can see that companies with the most sophisticated risk management (e.g. Wall Street banks) were the ones that suffered the most. Therefore, companies need to understand and define which different individuals and groups within the organisation are responsible for different risks, the possible biases in risk assessments, and the challenges in the implementation of risk management initiatives (Bromiley et al. 2015).

Until recently, financial risks (such as credit and market risks) and reputational risks were the most concerning for business organisational leaders. However, operational risks are gaining in importance, particularly due to information technology development (Doo 2019).

Kalia and Müller (2015) explain in their book that the idea of operational risk management first appeared in the 1990s. Fig. 1 shows how approaches to risk management in companies, particularly operational risk management, have evolved over time since their appearance in Basel II documents in the 1990s.

Operational risk is defined as the risk of direct or indirect loss resulting from inadequacies or failures of internal processes (Basel II-BCBS 2001a, b), people or systems or from external events. Karam and Planchet (2012) showed that the importance of operational risks has increased to the point where they are no longer considered minor risks; they are an important factor in the possibility of businesses failure (especially in the financial sector). The seven operational risks identified in Basel II are internal fraud; external fraud; employment practices and job security; customers, products and business practices; damage to physical assets; business interruptions; and system failures or execution, delivery or process management issues.

Security is defined in the ESRM Guideline (ASIS International 2019) as the condition of being protected against hazards, threats, risks or loss. After analysing the academic literature and with the purpose of investigating the conceptual and scientific distinctions between security and safety, Jore (2019) proposed defining security as the perceived or actual ability to prepare for, adapt to, withstand and recover from dangers and crises caused by people's deliberate, intentional, malicious acts, such as terrorism, sabotage, organised crime or hacking. Among the seven operational risks

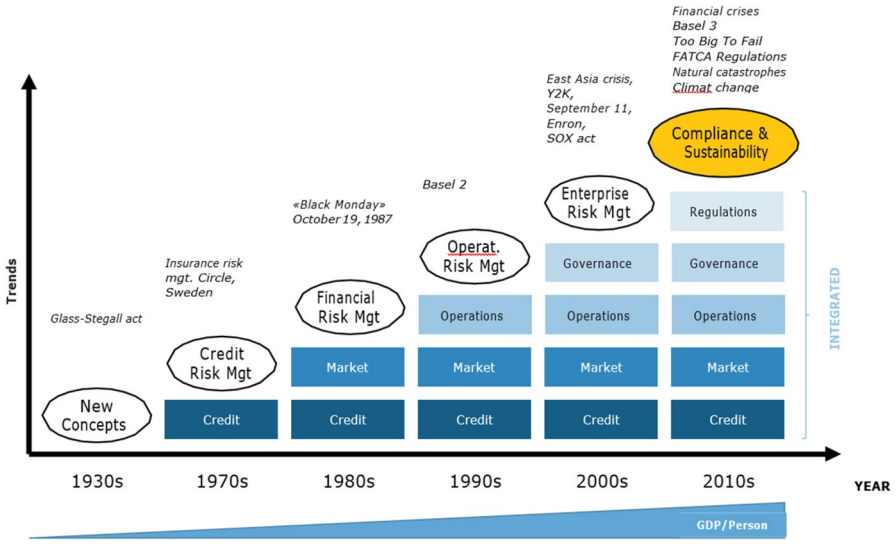



**Fig. 1** Evolution of risk management. *Source* Kalia and Müller (2015, p. 59)

identified in Basel II, we see that in either a direct or cross-sectional way, security must be an active component of managing some of these operational risks.

### Enterprise security risk management (ESRM)

Enterprise security risk management is defined as a strategic approach to security management that ties an organisation's security practices to its mission and goals using globally established and accepted risk management principles, where security risk is considered the potential of a given threat to exploit vulnerabilities to cause harm, loss or damage to an asset (ASIS International 2019). Regarding the management of security risk, Jore (2019) considers it to include assessing and reducing the likelihood and consequences of possible attacks with various types of risk-reducing measures—for example, the establishment of critical infrastructure protection and the building of organisational and societal resilience.

Arena et al. (2014) propose a conceptual model for research in ERM systems on the basis of the strategic management literature, and they also emphasise that most of the papers with models and approaches to implementing ERM have been developed by professionals or professional associations.

ASIS International has played an important role in the past few decades in improving a new security paradigm in the context of risk management, thus, paving the way for progression from a physical and cyber convergence of security (Tyson 2007) towards a holistic model linked to ERM (Johnson and Spivey 2008). The first major initiative was the joint creation by ASIS-ISACA in 2005 of the Alliance for Enterprise Security Risk Management (AESRM), which proposed that ESRM requires multifunctional collaboration in the ERM context across various management areas, including but not limited to physical and logical security, occupational

risk prevention, legal, risk management and crisis management and business continuity planning.

ASIS International has continued to work on ESRM development with that holistic approach, which was reflected in its paper 'Enterprise Security Risk Management: A Holistic Approach to Security' (CSO Roundtable 2015). Later, Petruzzi and Loyear (2016) explored the basic philosophy concepts and life cycle of ESRM. The authors highlighted that this philosophy encourages all company sectors to proactively recognise and deal with risk from a security perspective by presenting a model that substantially contributes to organisational resilience throughout the cycle represented in Fig. 2.

Allen and Loyear (2017) define enterprise security risk management as the application of fundamental risk principles to manage all security risks—whether related to information, cyber or physical security as well as asset management or business continuity—through a comprehensive, holistic approach. In this book, they provided concepts that allow a better understanding of the strategic approach to ESRM and its applicability in different fields, such as investigations, physical security, cybersecurity, information security, workplace violence, business continuity and crisis management. Another practical example applied to cybersecurity, and more specifically the dimension of information technology, is found in the work of Adekanye and Rahman (2019), who address how security risks related to emerging technologies present new challenges due to the rapid deployment of mobile devices and cloud use.

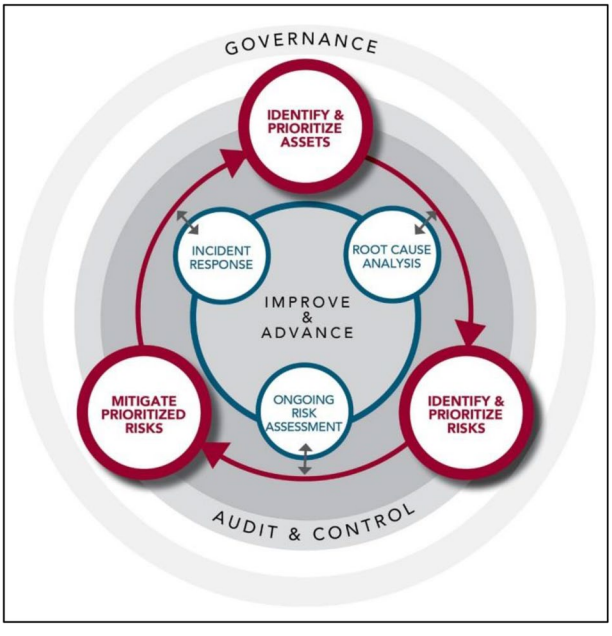



**Fig. 2** Enterprise security risk management cycle. *Source* Allen, B. Accessed March 15, 2020

Allen et al. (2018) analysed case studies on ERM business implementations related to corporate governance and risk management and described how fundamental risk management principles based on the philosophy of corporate governance and ERM can be used by business management in an organisation to manage security risks. They propose that the key to managing security risk in a governance model is understanding that security risk is simply one subset of all risks that must be comprehensively managed across the enterprise. Although security risk may require highly specialised risk response and mitigation actions, the fundamental risk principles of the risk management process are the same for security, financial, operational, or other risks. In corporate governance, the body in charge of overall ERM is the board of directors, and ESRM can also serve as a governance model for security risks. After analysing several case studies, the authors outlined three basic models that can be used as a framework to organise security risk governance in almost any enterprise: security councils (with or without subcommittees), security discipline councils or security networks/working groups.

The ASIS ESRM Guideline offers ASIS's current view of ESRM and is the first strategic security management tool of its kind: it elevates the security function by establishing a partnership between security professionals and business leaders to manage security risks (ASIS International 2019). According to this guideline, ESRM governance is carried out by the organisation's security governance body (e.g. committee, council or other governance group).

## Research methodology

According to Gutierrez-Salcedo et al. (2018), bibliometrics is an academic science with the objective of evaluating the research developed by a scientific community in any research field. Specifically, bibliometrics is a set of methods used to study or measure research through scientific papers stored or indexed in large bibliographic databases.

This study is based on the bibliometric procedures described by Keathley-Herring et al. (2016) and Gutierrez-Salcedo (2018) and supported by other articles (Palomo et al. 2017; Santisteban-Espejo et al. 2019; Castillo-Vergara et al. 2018). As shown in Fig. 3, we divide the process into five phases. The first phase is the identification of the research area, followed by a selection process and then by a subsequent data filter taken from scientific databases. Finally, a specific analysis of the treatment of the subject matter over time is conducted.

### Phase 1: identification of the research area, research scope and goals

This paper conducts a review of the literature on the relationship of ERM with security to analyse the evolution of business risk management over the past three decades and its maturity or development level. To this end, it is necessary to obtain activity indicators as well as identify the themes in and evolution of the literature (Keathley-Herring et al. 2016).

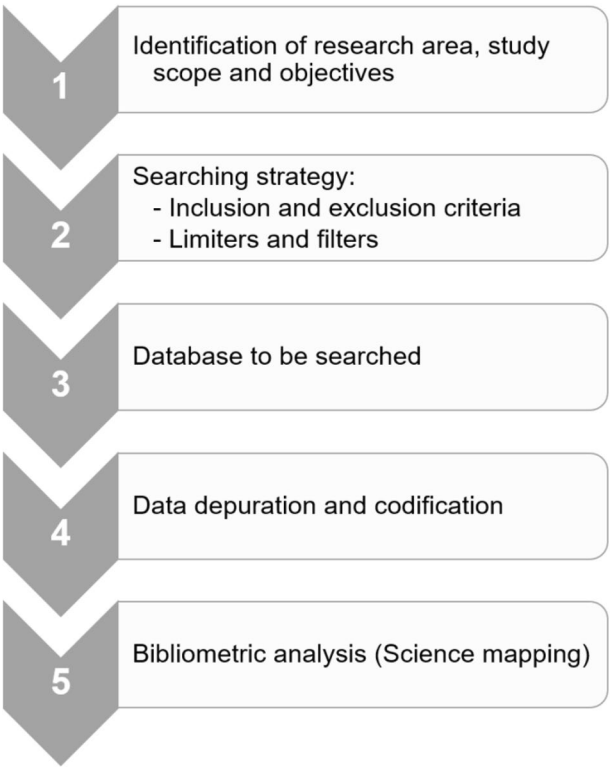



**Fig. 3** Bibliometric process. *Source* Own elaboration

There are currently two bibliometric procedures to explore a research field: performance analysis and scientific mapping analysis (Cobo et al. 2011). On the one hand, performance analysis aims at evaluating groups of scientific actors (countries, universities, departments and researchers) and the impact of their activity on the bibliographic database. On the other hand, knowledge extraction on the intellectual, social or conceptual structure of a research field can be done through scientific mapping analysis based on bibliographic networks (Gutierrez-Salcedo et al. 2018). The present study focuses on the analysis of a specific research field; therefore, the selected bibliometric procedure is scientific mapping analysis, specifically through the SciMAT tool, as it allows the researcher to perform a scientific mapping analysis in a longitudinal framework to analyse and observe the conceptual, intellectual or social evolution of a research field throughout consecutive periods.

Three consecutive periods were established based on relevant disruptive events that could be precursors of the evolution of organisations' risk management models:

(1) From the 1980s until 2001—On October 19, 1987, the Hong Kong stock exchange crashed, causing the rest of the world's stock markets to collapse rapidly in a single day, affecting Europe and causing the worst drop in the history of the stock market indices in the New York Stock Exchange, similar to that of 1914. This event was called Black Monday in the financial world (Kalia and Müller 2015).
(2) 2002–2008—The terrorist attack in New York on September 11, 2001 caused organisations to rethink their recovery capabilities and business continuity (Aleem et al 2013). Additionally, financial scandals and the collapse of large multinational companies, such as Enron and Worldcom, made it necessary to introduce regulatory standards, such as the Sarbanes-Oxley Act of 2002 or the comprehensive COSO ERM Guide, to prevent fraud and bankruptcy risk (Power 2009). In 2003, the SARS epidemic affected 26 countries and resulted in more than 8000 cases.
(3) 2009–2019—The beginning of this period was marked by the consequences of the subprime mortgage crisis, which had a negative effect on the world economy, after the largest drop in the Dow Jones stock index in history. In 2009, all continents were affected by the Influenza A (H1N1) pandemic. During this period, an update of the COSO ERM framework was published, and the first scientific papers on security were published within this framework. The papers studied the ESRM concept elaborated several years before by professional security associations. However, one of the security threats that increased significantly in this period and continues to concern organisations are cybersecurity breaches and hacks of both information technology (e.g. WannaCry and Petya/NotPetya) and operational technology (e.g. Stuxnet, Havex, BlackEnergy).

#### Phase 2: search criteria

To search academic databases, we selected as our inclusion criterion the appearance of the keywords 'enterprise risk management' or 'security' in the title, abstract or keywords. The search was limited to papers published in journals up to the end of 2019. Since there are studies on organisational resilience in a variety of fields, other subject areas, such as medicine and psychiatry, are excluded because they are not directly related to the topic analysed in this study.

#### Phase 3: database selection

The largest academic databases commonly used today are the Web of Science (WoS) by Clarivate Analytics and Scopus by Elsevier. When researchers use bibliometric methods for research evaluation, it is important that they understand what each tool offers and what its limitations are to choose the right tool for the task. The use of WoS was discarded because according to Mongeon and Paul-Hus (2016), its coverage of social sciences is limited, and we are also researching a relatively incipient topic. Indeed, with the selected search criteria, the WoS yielded less than 50 articles, an insufficient number for a bibliometric study.

As demonstrated by Harzing and Alakangas (2016), in a comparison of the average number of papers per author in all disciplines, Scopus presents a higher number of papers than the WoS. Using the search criteria established for this study, we obtained 463 articles. Therefore, the database selected was Scopus, and the results obtained were exported in RIS format, so they could then be used with the SciMAT scientific mapping analysis software tool.

### Phase 4: data depuration and coding

Before the data could be analysed through SciMAT, it was necessary to filter them and identify inconsistencies in the results obtained from Scopus.

First, we filtered by author name and references to avoid duplication, after which we executed a keyword standardisation of the documents to group them. If there was any doubt about classification within the specified groups, a further in-depth review of the document was carried out to ensure its relevance.

Groups not related to the research purpose, such as 'coronary risk', were dismissed.

### Phase 5: bibliometric analysis

In this fifth and final phases, theme identification, evolution and activity indicator analysis were be carried out. To that end, we used two tools:

- SciMAT: A programme used for scientific mapping analysis (science mapping analysis in the Anglo-Saxon literature) by means of the bibliometric analysis methodology defined by Cobo et al. (2012), which is based on word co-occurrence analysis and the h-index, which measures quality, impact, and performance.
- VOSviewer: A software developed by Van Eck and Waltman (2010) that is available free of charge to build and view bibliometric maps. VOSviewer is especially useful for displaying large two-dimensional bibliometric maps in a way that is easy to interpret (Castillo-Vergara et al. 2018).

Regarding SciMAT, Cobo et al. (2011) established a workflow in four stages to analyse the themes and thematic evolution in a field of research, as shown in Fig. 4.

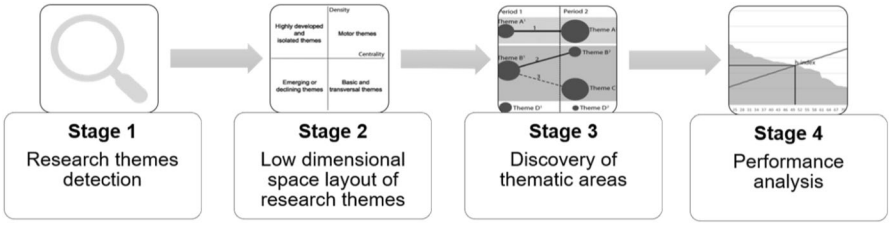



**Fig. 4** Bibliometric analysis workflow. *Source* Own elaboration, based on the paper by Cobo et al. (2011)

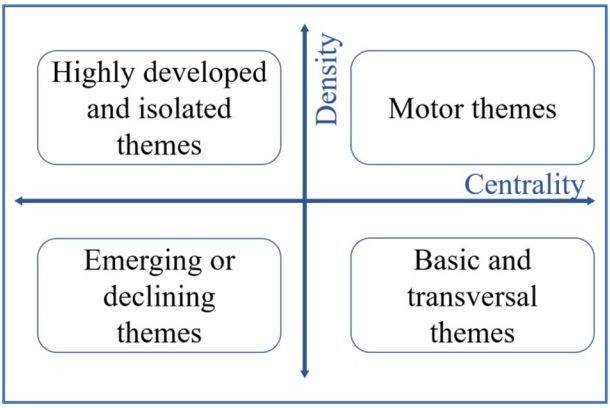



**Fig. 5** Meaning of a strategic diagram. *Source* Adaptation of a graph taken from the Cobo et al. (2012)

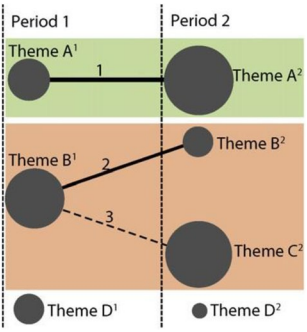
In stage 2, a graphic representation of the themes identified in the previous phase of research theme detection is drawn through a strategic diagram (as shown in Fig. 5) and a thematic network.

In the third stage, the diachronic changes in the main themes of the field are drawn, as shown in Fig. 6. Finally, the performance analysis is carried out based on bibliometric indicators consisting of both quantitative and qualitative or impact measures.

## Results of the analysis

We applied the scientific mapping approach described above to all 463 articles obtained, in line with previous research on thematic analysis (Moral-Muñoz et al. 2014; Martínez 2015; Montero-Díaz et al. 2018; Castillo-Vergara et al 2018). The aim is to carry out an exhaustive analysis of the research field in ESRM that provides the scope of the academic approach in this area and details what research prospects support its development.

**Fig. 6** Examples of evolution. *Source* Adaptation of a graphic taken from Cobo et al. (2011)



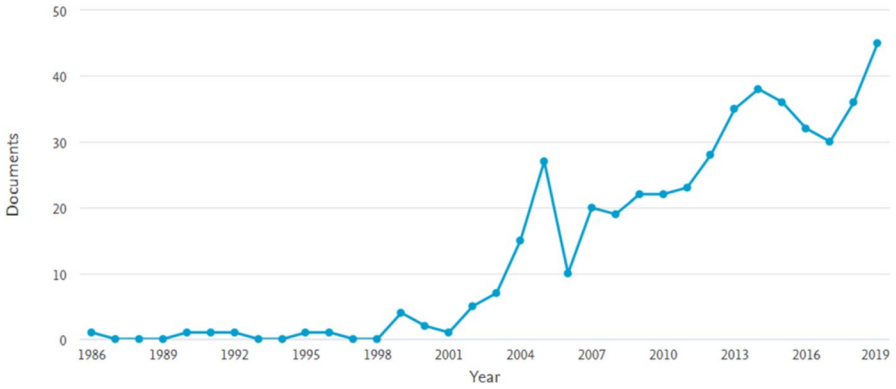



**Fig. 7** Documents by year created with scopus (Elsevier)

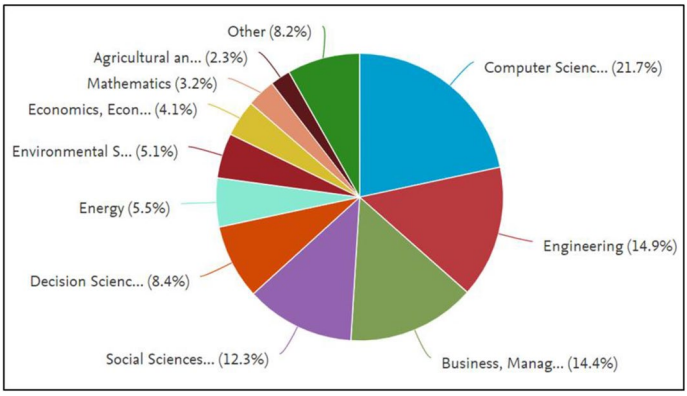



**Fig. 8** Documents by subject area created with scopus (Elsevier)

The SciMAT tool was used for coding, cleaning, analysis and representation of bibliometric data, and the VOSviewer tool was used to better interpret the large two-dimensional bibliometric map resulting from analysing 3340 keywords.

Also, the quantitative and qualitative measures that can be applied to different levels to help analyse topics, themes, thematic areas and different subperiods are shown. Specifically, we obtain quantitative data for the entire period, regarding the number of documents published per year (Fig. 7), subject area (Fig. 8), impact of the journals in which they were published (Table 1), countries of origin of publications (Fig. 9), the most frequently cited articles (Table 2), or the particulars from each period, both quantitative (number of associated documents belonging to each theme) and qualitative (citations and h-index) as seen in Table 3.

As for the publication trend, as shown in Fig. 7, there is an incipient phase from 1986 and an increasing quantitative leap since the early years of the 21st century.

**Table 1** Top 5 publication sources created with scopus (Elsevier)

| Source | SCImago journal rank by year | | | | |
|---|---|---|---|---|---|
| | 2014 | 2015 | 2016 | 2017 | 2018 |
| International journal of critical infrastructures | 0.333 | 0.277 | 0.302 | 0.173 | 0.192 |
| International journal of risk assessment and management | 0.209 | 0.178 | 0.143 | 0.142 | 0.279 |
| Computers and security | 0.641 | 0.819 | 0.815 | 0.684 | 0.667 |
| Computers fraud and security | 0.172 | 0.17 | 0.211 | 0.261 | 0.177 |
| Economic annals-XXI | 0.187 | 0.235 | 0.242 | 0.219 | 0.21 |

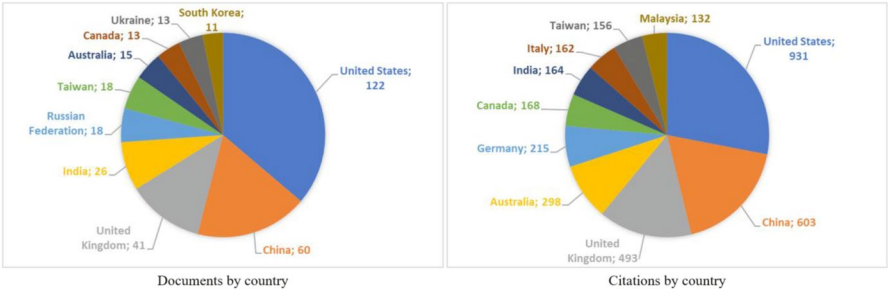



**Fig. 9** Documents and citations by top 10 countries—own elaboration

Table 1 summarises the five most common publication sources, along with the journal's impact in the year of publication, obtained through the SJR ranking. SJR is employed by Scopus and is considered prestigious by SCImago Journal Rank. The five identified journals focus on topics such as risk assessment, management, critical infrastructures, economics and security. Moreover, the publications are categorised by subject area (Fig. 8), showing great mainstreaming in terms of disciplines affected by the topic, including, among others, business, management, computer science, engineering and social sciences.

The country with the most publications in ESRM research field is the United States with 122 articles, followed by China with 60 articles and the United Kingdom with 41 articles. The highest number of citations is also found in the United States with 931 citations (Fig. 9).

The co-occurrence map based on keywords extracted from the 463 articles and prepared with VOSviewer (Fig. 10) allows the visualisation of the most relevant terms in different map views (network and density), after a coding and reduction process that finally allows working with 120 terms. In the density map, each dot has a colour, the temperature and size of which increases depending on the number of elements in the dot's proximity and the near elements weight. The greater the number of elements around it and the greater its weight, the darker

**Table 2** Top 10 most cited publications created by SciMAT

| Title | Authors | Year | Citations |
|---|---|---|---|
| 1. Risky business: expanding the discussion on risk and the extended enterprise | Spekman, R.E., Davis, E.W. | 2004 | 255 |
| 2. Entropia: architecture and performance of an enterprise desktop grid system | Chien, A., Calder, B., Elbert, S., Bhatia, K. | 2003 | 232 |
| 3. The risk management of nothing | Power, M. | 2009 | 203 |
| 4. A VIKOR technique based on DEMATEL and ANP for information security risk control assessment | Ou Yang, Y.-P., Shieh, H.-M., Tzeng, G.-H. | 2013 | 192 |
| 5. Enterprise risk management and firm performance: a contingency perspective | Gordon, L.A., Loeb, M.P., Tseng, C.-Y. | 2009 | 189 |
| 6. Enterprise social networking: opportunities, adoption, and risk mitigation | Turban, E., Bolloju, N., Liang, T.-P. | 2011 | 128 |
| 7. From new deal institutions to capital markets: commercial consumer risk scores and the making of subprime mortgage finance | Poon, M. | 2009 | 112 |
| 8. Exploring organisational culture for information security management | Chang, S.E., Lin, C.-S. | 2007 | 106 |
| 9. Challenging environments: danger, resilience and the aid industry | Duffield, M. | 2012 | 104 |
| 10. Risk perception and risk management in cloud computing: results from a case study of Swiss companies | Brender, N, Markov, I. | 2013 | 100 |

**Table 3** Performance of the themes by periods – Own elaboration.

| Name | Subperiod 1986–2001 | | | Subperiod 2002–2008 | | | Subperiod 2009–2019 | | |
|---|---|---|---|---|---|---|---|---|---|
| | Documents | h-index | Citations | Documents | h-index | Citations | Documents | h-index | Citations |
| Financial management | 1 | 1 | 2 | | | | | | |
| Cybersecurity | 5 | 1 | 44 | 46 | 13 | 696 | 132 | 17 | 1267 |
| Innovation | 6 | 2 | 80 | | | | | | |
| Security risks management | 3 | 2 | 67 | 56 | 17 | 936 | 154 | 17 | 1027 |
| Socioeconomic factors | 1 | 1 | 2 | | | | | | |
| Geography | 1 | 1 | 2 | | | | | | |
| Decision making | 2 | 1 | 31 | | | | 111 | 15 | 997 |
| Automated teller machine | 1 | 0 | 0 | | | | | | |
| Open systems | 1 | 0 | 0 | | | | | | |
| Information systems | | | | 39 | 15 | 677 | 102 | 15 | 885 |
| Risk management | | | | 70 | 18 | 1079 | 177 | 20 | 1568 |
| Investments | | | | 9 | 4 | 153 | | | |
| Enterprise risks management | | | | | | | 109 | 15 | 1129 |
| Internet | | | | | | | 38 | 9 | 391 |

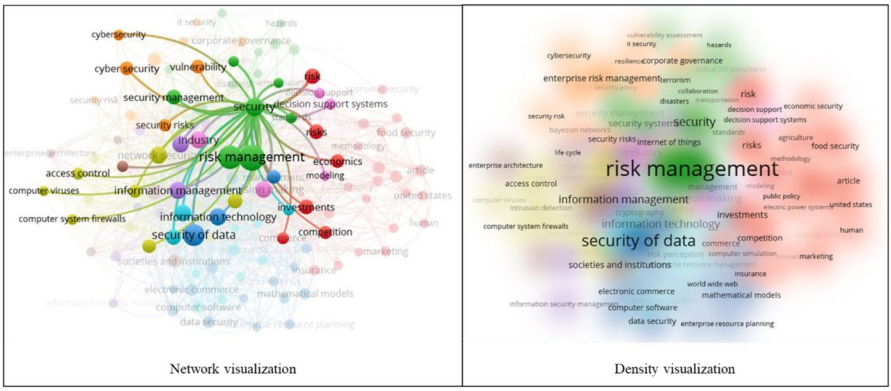



**Fig. 10** Term-based co-occurrence map created with VOSviewer

the colour. It should be noted that density is higher for the term 'risk management' and that the network map focusing on the term 'security' highlights interconnections with other clusters such as 'investments', 'decision-making', 'cybersecurity' or 'security of data'.

## Visualisation of ESRM research themes

With the SciMAT tool, two strategic diagrams are made for each of the three periods. In the first diagram, the proportion of each sphere is established by the number of documents associated with their respective topic, and the second diagram is proportional to the number of citations of documents associated with each theme. SciMAT allows the opening of each of the clusters reflected in the spheres of the diagram to visualise the topics that constitute the diagram, as shown in the example in Fig. 11.

Table 3 will complement the analysis in each period with production and impact measures.

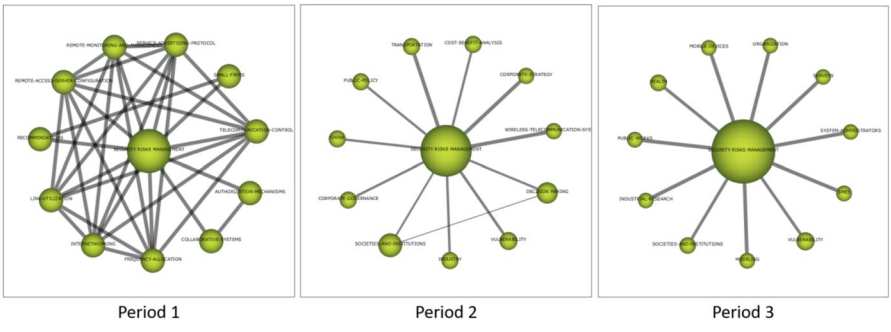



**Fig. 11** Network of the 'security risk management' theme created by SciMAT

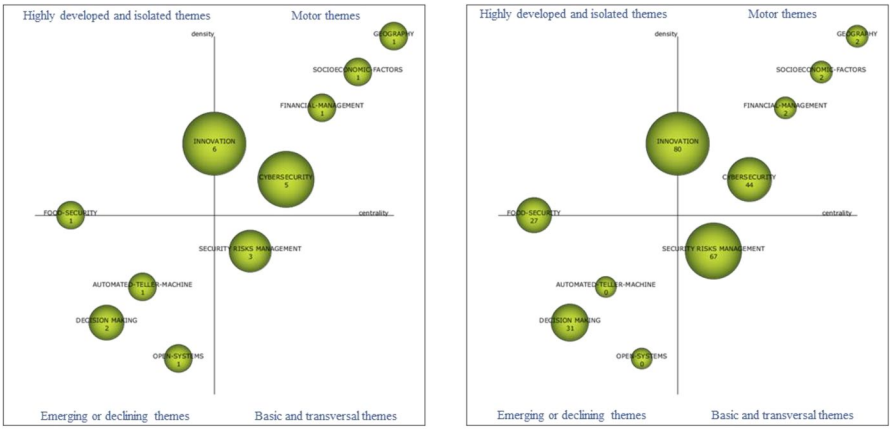



**Fig. 12** Strategic diagrams for the period 1986–2001 created by SciMAT

### First period (1986–2001)

During this period, ESRM research field revolved around ten research themes as shown in Fig. 12. If we analyse the performance measures established in Table 3, 'Cybersecurity' stands out as the motor theme, followed by 'Innovation' to a lesser extent. Both themes obtained the highest number of documents and were cited 124 times, although the centrality of 'Cybersecurity' is greater. 'Geography', 'Socio-economic Factors' and 'Financial Management' also appear as very central and dense themes, with research studying the birth rate decline in Asia and the possible socioeconomic causes, the consequences of which can be extrapolated to Western countries.

'Security risk management' stands out as a basic and cross-sectional theme; it presents a high citation and impact rate during this period. This theme is related to research on topics such as telecommunication control, remote monitoring and management, among others.

The theme 'Decision-Making' is identified as an emergent one as it presents the highest density and number of documents in this quadrant; while 'Automated Teller Machine' and 'Open Systems' are to be assumed as declining themes because of the scarcity of documents and the lack of citations. The theme 'Food Security' is also considered to be a declining theme because there is only one document, although it is denser and has some citations.

### Second period (2002–2008)

In the strategic diagram of Fig. 13, there are five research themes, which, although fewer than in the previous period, represent a quantitative leap in terms of the number of citations of the more-than-100 articles published in the aimed field of this research.

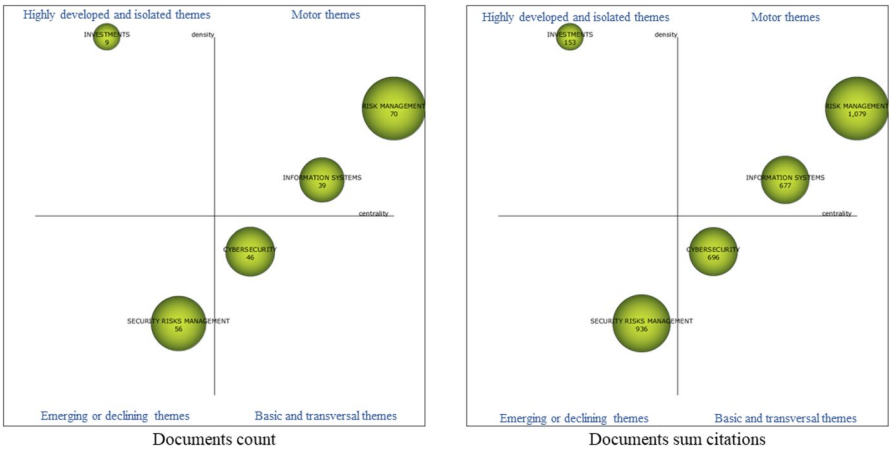



**Fig. 13** Strategic Diagrams for the Period 2002–2008 created by SciMAT

The research theme 'Risk Management' appears to be the most important one in this period as it appears in 70 documents and in more than 1000 citations, and it was not an emerging theme in the previous period. Another motor theme is 'Information Systems', which seems to depart from 'Cybersecurity', a theme directly related to it, and it becomes an entity on its own. These last two themes are closely related and evolve in parallel because as they delve into their topics, their relationship with regulatory aspects and computer and communication networks are similar. 'Cybersecurity' appears as a basic, cross-sectional theme with a number of documents and citations similar to that of 'Information Systems'.

'Security Risk Management' has grown remarkably as a theme regarding the number of documents (56) and citations (936), only second to 'Risk Management'. They both show similar high impact rates (Table 3). The 'Security Risk Management' theme includes topics related to corporate strategy and governance, public policy and industry focused on the protection of critical infrastructure from both a governmental and business point of view. An example is the article 'How much security is enough?' (Roberts-James 2002), which proposes the new paradigm of security in transport and supply chain.

In the highly developed and isolated themes quadrant, 'Investments' appears, and it is observed in the associated documents that they have a particularly productive approach towards research on the energy sector and more specifically in the electric one, along with other topics related to competitiveness, costs and supply chain.

### Third period (2009–2019)

During this period, the ESRM research field encompassed seven research themes according to the strategic diagram shown in Fig. 14. Most of them establish the consolidation of issues that rose in previous periods. This decade brings together more than half of the articles published in the field of research ESRM.

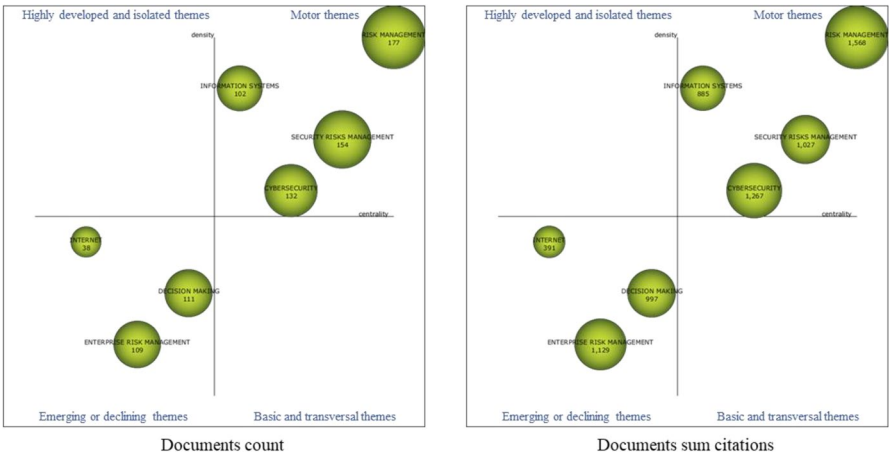



**Fig. 14** Strategic diagrams for the Period 2009–2019 created by SciMAT

This is the case of the motor theme 'Risk Management', which is consolidated as the most important of the last decade, increasing even more its centrality and density in this quadrant, according to Table 3, with 177 documents and over 1,500 citations and the highest impact of the three periods studied. With regard to the topics, it continues to address regulatory and compliance issues or e-commerce, but new topics related to civil defence or risk management also appear, not only in connection with strategic sectors and extended enterprises but also in connection with small- and medium-sized enterprises.

The theme 'Security Risk Management' barges in, surpassing the centrality of 'Information Systems' and 'Cybersecurity'. The latter doubled the number of citations to more than 1200 when compared with the numbers for the previous period.

Two emerging themes appear: 'Decision-Making' and 'ERM', and they have more importance than the 'Internet' theme. The first two show topics related to organisational resilience, such as business continuity, financial management, corporate governance and environmental management.

## Thematic evolution of ESRM research field

### Thematic composition

After discovering a total of 15 different themes in the three periods analysed (Table 3), an analysis of the thematic evolution is made. Fig. 15 shows each of the three periods separated in columns (1986–2001, 2002–2008 and 2009–2019). The volume of the spheres is determined by the number of documents associated with each theme. The continuous line means that there is a conceptual link—both topics have the same name—or the name of one of the topics is part of the other theme. The dotted line means that the link is not conceptual, i.e. elements are shared in the themes but not the name of the theme. The themes belonging to the same thematic

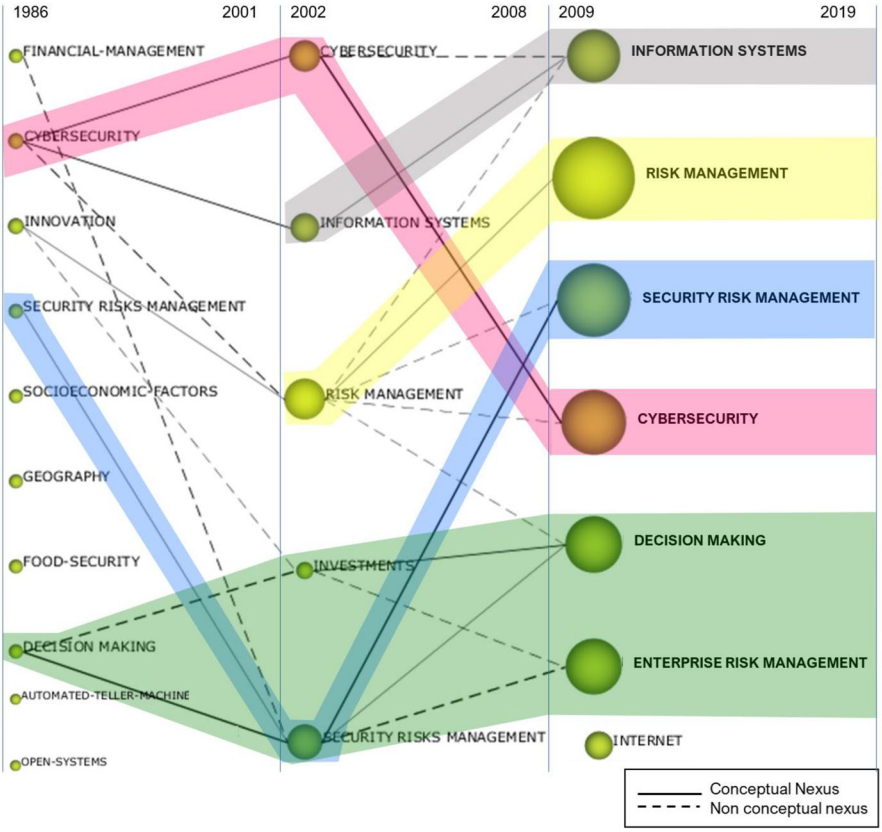



**Fig. 15** Thematic evolution of ESRM (1986–2019)—own elaboration

area are shaded with different colours to distinguish them easily. There are seven topics that are not shaded and therefore do not belong to any thematic area: the first period would have, 'Financial Management', 'Geography', 'Food Security', 'Automated Teller Machine' and 'Open Systems'; and in the last period, the same happens with the theme 'Internet'.

Figure 15 shows a strong cohesion of themes in five thematic areas in ESRM research field: Information Systems; Risk Management; Security Risk Management; Cybersecurity and ERM.

Most of these thematic areas have a conceptual link with previous periods. For example, the themes 'Cybersecurity' and 'Security Risk Management' are present through all the periods. The themes 'Information Systems' and 'Risk Management' appear later, in the second period. In the first period, the theme 'Decision-Making' appears, and in the second period, it is divided into 'Investments' and 'Security Risk Management', and in the third period, they converge

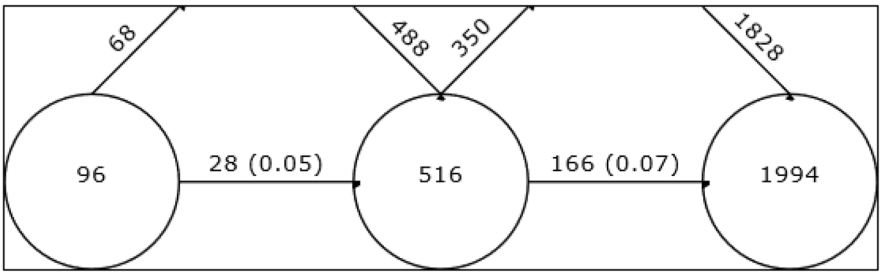



**Fig. 16** Overlapping map created by SciMAT

again in 'Decision-Making', and they encourage strong emergence of the theme 'ERM'.

When a theme is double shaded, it indicates that it belongs to two different thematic areas. This is the case of 'Security Risk Management', which is also shaded in the second period in the 'ERM' thematic area.

### Structural evolution of the thematic areas

Figure 16 shows the stability between the three periods, where the circles correspond to each of these periods and the number of keywords is reflected inside. The horizontal arrow shows the number of items shared by both periods, and the stability index is shown between brackets. The ascending arrow indicates the number of new items with respect to the next period, and the descending arrow indicates the items that disappear in the next period.

A consolidation of the terms used is observed because throughout time, there are exponential leaps in the number of keywords per period (from 96 in the first period to 1994 in the last one), in the number of keywords shared between periods (from 28 to 166) and in the stability factor that increases from 0.05 to 0.07.

### Performance and impact indicators of the ESRM scientific field

According to Table 4, the subject area with more citations is 'Risk Management' (2647 citations), followed by 'ERM' (2310 citations) and then by 'Security Risks Management' (2030 citations). As for the average citations, 'Information Systems' stands out with 11.08. Almost all of the themes in Table 3 increase their impact (h-index) as they progress through the periods, with 'Cybersecurity' being the theme with higher differential between the second and third period (h-index from 13 to 17), although, in absolute terms, 'Risk Management' is higher (h-index = 20).

## Discussion

To study the themes and thematic evolution of the ESRM research field, a bibliometric analysis was carried out on the basis of 463 publications taken from Scopus till the end of 2019.

Through science mapping analysis and co-word networks, we have been able to detect the themes and present them in a graphic and visually interpretable way within the framework of longitudinal evolution, which resulted in five main thematic areas (Fig. 15): 'information systems', 'risk management', 'security risk management', 'cybersecurity' and 'ERM'.

The ten most cited documents were generated as those from 2003, the two more cited ones in the second period and the most recent one was in 2013, in the third period. It is in these two periods that the highest h-index indicators are found.

Of the publications shown in Table 2, the most cited one (255 citations) has been Risky business: 'Expanding the Discussion on Risk and the Extended Enterprise' by Spekman and Davis (2004), whose research focuses on ERM associated with security. Also, in the second period, we find the second-most-cited publication, 'Entropy: Architecture and Performance of an Enterprise Desktop Grid System' by Chien et al. (2003), which was cited 232 times and is about solutions for ERM and information systems improvement of efficiency and performance. No publication from the first period is in the top 10, and to find the most cited article, we must go to the 24$^{th}$ position with 44 citations, 'High-performance Computing in Finance: The Last 10 Years and the Next' (Zenios 1999), on high-performance development of financial information systems including enterprise-wide risk management.

70% of the top 10 most cited publications are in the third period (Table 2), and the most prominent publication is 'The Risk Management of Nothing' (Power 2009), which had 203 citations. It delves into the causes of the financial crises, highlighting the lack of understanding of risk and the actual security offered by the ERM model and is based on an audit approach. This research proposes business continuity management (BCM) as a means to redirect business risks management.

The most developed motor theme in the ESRM research field has been 'Risk Management', particularly in the second and third periods, presenting high density and centrality. In addition, its h-index is the highest of the topics throughout the periods, with a maximum indicator of 20 (Table 3). The co-occurrence map based

**Table 4** Performance of the themes by thematic area—own elaboration

| Name | Documents | Citations | Citations average |
|---|---|---|---|
| Risk management | 247 | 2647 | 1072 |
| Enterprise risk management | 231 | 2310 | 10 |
| Security risks management | 213 | 2030 | 953 |
| Cybersecurity | 183 | 2007 | 1097 |
| Information systems | 141 | 1562 | 1108 |

on keywords (Fig. 10) shows up both in the visualisation of the network map as well as in the density map as the most relevant term.

'Information Systems' presents the highest average citations of all the thematic areas, emerges as a motor theme in the second period and remains so over the third period. 'Information Systems' has the same thematic origin and conceptual link strength as 'Cybersecurity'. Thus, both thematic areas have a close relationship.

'Cybersecurity' and 'Security Risk Management' have been present from the first period. The h-index of 'Cybersecurity' is one of the highest; thus, it is consolidated as a motor theme in the third period. It can be seen that 'Security Risk Management' is a basic or emerging theme in the early periods and that it is in the latter period that it becomes a motor theme, surpassing 'Cybersecurity' in respect of both centrality and density.

'ERM' stands out as an emerging theme in the third period (Fig. 15), which emerges as an evolution of 'Decision-Making' and 'Investments', and although it has its own thematic line, it also has a link with 'Security Risk Management'.

Three time intervals were established in the scope of this research. The first of them (1986–2001) is not very detailed either quantitatively or qualitatively. There is incipient research on information systems that provide effective, safe and even remote control and facilitate financial decision making to help predict adverse situations. This period coincides with the fall of the Hong Kong stock exchange on October 19, 1987 (the so-called 'Black Monday').

In the second period (2002–2008), security-related issues evolved, specifically in terms of the security risk management of infrastructures and critical processes for governments and industries. The terrorist attack in New York on 11 September 2001 led to a rethink of the strategies of both the states and their intelligence systems (Fischbacher-Smith 2016) in the business world and in the industry. Concerning the latter, it was not only companies based in the WTC that were affected but also financial markets, which were closed for 6 days following the fall in stock indices. In addition, sectors such as air transport and tourism were impacted. Fortunately, some of these companies located in the WTC were able to minimise the impact and resume operations as they had evacuation and contingency plans after the attack on the same site in February 1993 (Johnson 2005).

The last period (2009–2019) is the most organised one regarding the ESRM research field. The difference with previous periods is that in the face of a globalised and changing world, security and ERM are extended to medium- and small-sized enterprises. Braes and Brooks (2010) argued that as that the exchange rate in the market accelerates, companies require adaptive risk management that responds to and anticipates business changes. Moreover, the interdependence of countries with different regulatory systems influencing the spread of the crisis is to be considered (Sabkha et al. 2019).

In this last period, we can see that there are also relevant topics such as 'mobile-devices' and 'health' (Fig. 11). The first one entails an advantage for organisations because it has revolutionised the manner in which people interact, particularly in the work environment, but at the same time—from a security perspective—it increases exposure to the risk of theft of corporate resources and confidential information (Achtaich et al. 2019) and can result in a serious impact on the continuity

of organisational operations, such as from the threat of ransomware (Al-rimy et al. 2018), both on IT (e.g. WannaCry and Petya/NotPetya) and Operational Technology (e.g. Stuxnet, Havex, BlackEnergy). (Mihaela 2020). The health risk is high because terrorist groups may use chemical, biological or nuclear materials as was the case in 1995 when sarin gas was dispersed in a Tokyo subway (Hyams et al. 2002), or those not intentional related health risks as the recent global pandemics. However, regarding homeland security, some authors (Enemark 2009) argue that there is also a risk that addressing a health issue in security terms will lead to emergency responses which are ineffective, counterproductive or unfair.

## Conclusions

A first bibliometric and scientific production-mapping analysis was carried out in the field of ESRM research, which allowed the visualisation of how the different thematic areas detected have evolved. In the specific case of the thematic area 'Security Risk Management', during the first period, scientific production focused on the protection of information systems supporting financial aspects in an environment that has become increasingly globalised and interconnected thanks to the Internet. For the second period, possibly in view of the emergence of global threats, it was observed that security was implemented in critical infrastructures and in supply chains from a convergent physical and cyber perspective. In the third period, 'Security Risk Management' consolidated as a thematic area in its own right and as a field closely linked to ERM.

As mentioned by Gill (2007), there is a need to understand how security research, as a body of knowledge, helps add value to organisations. Security, in addition to managing the human-induced operational risks of organisations, actively collaborates in obtaining and analysing intelligence information received by senior management for strategic decision making (Crump 2015) as well as in comprehensively managing crises in the face of serious disruptive events (global pandemics, natural disasters, large-scale cyberattacks, etc.). According to Petruzzi and Loyear (2016), ESRM involves all parts of businesses recognising and proactively dealing with risk without overlooking that business continuity alignment and crisis management within the ESRM philosophy are key requirements in any resilience programme. Security is currently understood as both a state and a process of reducing risk and protecting or building resilience against possible threat scenarios (Jore 2019).

In the development of this study, the main limitation that we found is that in reputable academic databases, the literature is scarce mainly due to the novelty of the topic. However, the results of this comprehensive analysis of the field of ESRM show the scope of the area's academic approach and the research perspectives supporting its development as a scientific discipline, as it has been observed that scientific outcomes in this field are still in their early stages and that new research areas are promising.

Therefore, this study serves as a base for future research on the actual contribution to organisational resilience of an ESRM-based security management system. Previous ESRM studies have been carried out on governance models that propose

managing security risks through the composition of councils or working groups and at the same corporate level and with the same focus that characterises the management of financial, regulatory, operational and other risks (Allen et al. 2018). Therefore, academic work could explore in greater depth how the security management system is currently embedded into organisations' integrated management system with other corporate areas involved in risk governance. It also seems relevant to identify and analyse the managerial implications of corporate security leadership and its ability to promote organisational resilience through ESRM.

#### Declarations

**Conflict of interest** The authors declare that they have no conflict of interest.

## References

Adekanye, Michael O., and Shawon S. M. Rahman. 2019. The Effect of Information Technology Using Enterprise Security Risk Management. *International Journal of Network Security & Its Applications* 10 (5): 13–23.

Achtaich, A., R. Mazo, N. Souissi, C. Salinesi, and O. Roudies. 2019. Management Capabilities for Mobile and IoT Devices: An Evaluation Framework. *International Journal of Engineering and Advanced Technology* 8 (6): 420–430. https://doi.org/10.35940/ijeat.E7822.088619.

Aleem, Azeem, Alison Wakefield, and Mark Button. 2013. Addressing the Weakest Link: Implementing Converged Security. *Security Journal* 26 (3): 236–248. https://doi.org/10.1057/sj.2013.14.

Allen, B., and R. Loyear. 2017. *Enterprise Security Risk Management: Concepts and Applications*, 4. Brooksfield: Rothstein Publishing.

Allen, B., T. Kelly, R. Loyear, A. Poole, A. Awojulu, A. Kmetetz, M. Rakotomavo, Z. Wang, H. Xu, M. Xu, and H. Yuan. 2018. Security Risk Governance: A Critical Component to Managing Security Risk. *The Journal of Applied Business and Economics* 20 (1): 132–146.

Allen, B. 2020. *Enterprise Security Risk Management*. Accessed January 15, 2020. https://esrm.info/esrm/.

Al-rimy, B., M.A. Maarof, and S.Z.M. Shaid. 2018. Ransomware Threat Success Factors, Taxonomy, and Countermeasures: A Survey and Research Directions. *Computers and Security* 74: 144–166. https://doi.org/10.1016/j.cose.2018.01.001.

Arena, M., G. Azzone, E. Cagno, A. Silvestri, and P. Trucco. 2014. A Model for Operationalizing ERM in Project-Based Operations through Dynamic Capabilities. *International Journal of Energy Sector Management* 8 (2): 178–197.

Arena, Marika, Michela Arnaboldi, and Giovanni Azzone. 2010. The Organizational Dynamics of Enterprise Risk Management. *Accounting Organizations and Society* 35 (7): 659–675.

ASIS International. 2019. "Enterprise Security Risk Management (ESRM) Guideline" Enterprise Security Risk Management.. Accessed December 19, 2020. https://www.asisonline.org/publications--resources/news/press-releases/asis-releases-new-enterprise-security-risk-management-esrm-guideline/.

BCBS. 2001. Consultative Document. Operational Risk-Supporting Document to the New Basel Capital Accord. Retrieved from https://www.bis.org/publ/bcbsca07.pdf (accessed 09 Jan 2019).

BCBS. 2001. Quantitative impact study 2 - Operational Risk Loss Data, 2001, https://www.bis.org/bcbs/qisoprisknote.pdf. (accessed 09 Jan 2019).

Bennett, N., and G.J. Lemoine. 2014. What a Difference a Word Makes: Understanding Threats to Performance in a VUCA World. *Business Horizons* 57 (3): 311–317.

Bharathy, Gnana K., and Michael K. McShane. 2014. Applying a Systems Model to Enterprise Risk Management. *Engineering Management Journal* 26 (4): 38–46.

Braes, B. and D. Brooks. 2010. In: *Proceedings 3rd* Australian Security *and* Intelligence *Conference* November: 14–22.

Bromiley, P., M. McShane, A. Nair, and E. Rustambekov. 2015. Enterprise Risk Management: Review, Critique, and Research Directions. *Long Range Planning* 48 (4): 265–276.

Castillo-Vergara, M., A. Alvarez-Marin, and D. Placencio-Hidalgo. 2018. A Bibliometric Analysis of Creativity in the Field of Business Economics. *Journal of Business Research* 85: 1–9. https://doi.org/10.1016/j.jbusres.2017.12.011.

Chien, A., B. Calder, S. Elbert, and K. Bhatia. 2003. Entropia: Architecture and Performance of an Enterprise Desktop Grid System. *Journal of Parallel and Distributed Computing* 63 (5): 597–610. https://doi.org/10.1016/S0743-7315(03)00006-6.

Cobo, M.J., A.G. López-Herrera, E. Herrera-Viedma, and F. Herrera. 2011. An Approach for Detecting, Quantifying, and Visualizing the Evolution of a Research Field: A Practical Application to the Fuzzy Sets Theory Field. *Journal of Informetrics* 5 (1): 146–166.

Cobo, Mj., A.G. López-Herrera, E. Herrera-Viedma, and F. Herrera. 2012. SciMAT: A New Science Mapping Analysis Software Tool. *Journal of the American Society for Information Science and Technology* 63 (8): 1609.

CSO Roundtable of ASIS International. 2015. *Enterprise Security Risk Management: Overview and Case Studies*. Retrieved from https://cso.asisonline.org/esrm/Documents/Enterprise%20Security%20Risk%20Management--Overview%20and%20Case%20Studies%20pt%202.pdf (accessed 9 Jan 2020).

Crump, J. 2015. *Corporate Security Intelligence and Strategic Decision Making*. Abington: Taylor and Francis. https://doi.org/10.1201/b18399.

Dahms, T. 2010. Resilience and Risk Management: Dahms Argues that Compliance Against a Universal Set of Rules Reduces Resilience. *Australian Journal of Emergency Management* 25 (2): 23–28.

Doo, Song Il. 2019. A Study on Legal Risk Under Enterprise Risk Management & Management System Centered on the Board of Directors. *Journal of Hongik Law Review* 20 (1): 651–684.

Eastburn, Ronald William, and Alex Sharland. 2017. Risk Management and Managerial Mindset. *The Journal of Risk Finance* 18 (1): 21–47. https://doi.org/10.1108/JRF-09-2016-0114.

Enemark, C. 2009. Is Pandemic Flu a Security Threat? *Survival* 51 (1): 191–214. https://doi.org/10.1080/00396330902749798.

Fischbacher-Smith, Denis. 2016. Breaking Bad? In Search of a (Softer) Systems View of Security Ergonomics. *Security Journal* 29 (1): 5–22. https://doi.org/10.1057/sj.2015.41.

Gill, Martin. 2007. The Challenges for the Security Sector: Thinking about Security Research. *Security Journal* 20 (1): 27–29. https://doi.org/10.1057/palgrave.sj.8350041.

Govender, D. 2019. The use of the Risk Management Model ISO 31000 by Private Security Companies in South Africa. *Security Journal* 32 (3): 218–235. https://doi.org/10.1057/s41284-018-0158-x.

Gupta, Neeraj. 2016. Developing a Decision Support Enabled Enterprise Risk Control Framework for Sector Focused Indian Companies Transforming into Global Energy Enterprises. *Gurukul Business Review-Gbr* 12: 46–53.

Gutierrez-Salcedo, M., M. Angeles Martinez, J.A. Moral-Munoz, E. Herrera-Viedma, and M.J. Cobo. 2018. Some Bibliometric Procedures for Analyzing and Evaluating Research Fields. *Applied Intelligence* 48 (5): 1275–1287.

Harzing, A.-W., and S. Alakangas. 2016. Google Scholar, Scopus and the Web of Science: A Longitudinal and Cross-Disciplinary Comparison. *Scientometrics* 106 (2): 787–804.

Hoyt, Robert, and Andre Liebenberg. 2011. The Value of Enterprise Risk Management. *Journal of Risk and Insurance* 78 (4): 795–822. https://doi.org/10.1111/j.1539-6975.2011.01413.x.

Hyams, K.C., F.M. Murphy, and S. Wessely. 2002. Responding to Chemical, Biological, Or Nuclear Terrorism: The Indirect and Long-Term Health Effects may Present the Greatest Challenge; 12043900. *Journal of Health Politics, Policy and Law* 27 (2): 273–291.

International Organization for Standardization. 2017. ISO 22316:2017 Security and resilience—Organizational resilience—Principles and attributes, Geneva.

International Organization for Standardization. 2018. ISO 31000:2019 Risk management—Principles and guidelines, Geneva.

Johnson, C.W. 2005. Applying the Lessons of the Attack on the World Trade Center, 11 Th September 2001, to the Design and Use of Interactive Evacuation Simulations. *CHI 2005: Technology, Safety, Community: Conference Proceedings—Conference on Human Factors in Computing Systems*, 651–60.

Johnson, Michael, and Jeff Spivey. 2008. Erm and the Security Profession. *Risk Management* 55 (1): 30–35.

Jore, S.H. 2019. The Conceptual and Scientific Demarcation of Security in Contrast to Safety. *European Journal for Security Research* 4: 157–174. https://doi.org/10.1007/s41125-017-0021-9.

Kalia, Vinay, and Roland Müller. 2015. *Risk Management at Board Level—A Practical Guide for Board Members*, 2nd ed. Austria: Haupt Bern.

Karam, E. and F. Planchet. 2012. Operational Risks in Financial Sectors. *Advances in Decision Sciences*.

Keathley-Herring, Heather, Eileen Van Aken, Fernando Gonzalez-Aleu, Fernando Deschamps, Geert Letens, and Pablo Orlandini. 2016. Assessing the Maturity of a Research Area: Bibliometric Review and Proposed Framework. *Scientometrics* 109 (2): 927–951.

Ludbey, C.R., D.J. Brooks, and M.P. Coole. 2018. Corporate Security: Identifying and Understanding the Levels of Security Work in an Organisation. *Asian Journal of Criminology* 13 (2): 109–128. https://doi.org/10.1007/s11417-017-9261-x.

Martínez, M.A. 2015. *Analyzing the Scientific Evolution of Social Work using Science Mapping*. 25: 257–277.

Mcshane, M., Anil Nair, and E. Rustambekov. 2011. Does Enterprise Risk Management Increase Firm Value? *Journal of Accounting, Auditing & Finance* 26 (4): 641–658.

Mihaela, C. 2020. Current Security Threats in the National and International Context. *Accounting and Management Information Systems* 19 (2): 351–379.

Mongeon, P., and A. Paul-Hus. 2016. The Journal Coverage of Web of Science and Scopus: A Comparative Analysis. *Scientometrics* 106 (1): 213–228.

Montero-Díaz, J., M.-J. Cobo, M. Gutiérrez-Salcedo, F. Segado-Boj, and E. Herrera-Viedma. 2018. A Science Mapping Analysis of "Communication'' WoS Subject Category (1980–2013)." *Comunicar* 26 (55): 81–91. https://doi.org/10.3916/C55-2018-08.

Moral-Muñoz, J. A., M. J. Cobo, E. Peis, M. Arroyo-Morales, and E. Herrera-Viedma. 2014. Analyzing the Research in Integrative & Complementary Medicine by Means of Science Mapping. *Complementary Therapies in Medicine* 22 (2): 409-418. https://doi.org/10.1016/j.ctim.2014.02.003. https://www.scopus.com/inward/record.uri?eid=2-s2.0-84898829811&doi=10.1016%2fj.ctim.2014.02.003&partnerID=40&md5=ed061f7cc56eccf329d803b4a3673155.

Nalla, Mahesh, and Merry Morash. 2002. Assessing the Scope of Corporate Security: Common Practices and Relationships with Other Business Functions. *Security Journal* 15 (3): 7–19. https://doi.org/10.1057/palgrave.sj.8340119.

Palomo, J., C. Figueroa-Domecq, and P. Laguna. 2017. Women, Peace and Security State-of-Art: A Bibliometric Analysis in Social Sciences Based on SCOPUS Database. *Scientometrics* 113 (1): 123–148.

Petruzzi, J., and R. Loyear. 2016. Improving Organisational Resilience through Enterprise Security Risk Management. *Journal of Business Continuity & Emergency Planning* 10 (1): 44–56.

Power, M. 2009. The Risk Management of Nothing. *Accounting, Organizations and Society* 34 (6–7): 849–855. https://doi.org/10.1016/j.aos.2009.06.001.

Prewett, Kyleen, and Andy Terry. 2018. COSO's Updated Enterprise Risk Management Framework: A Quest for Depth and Clarity. *Journal of Corporate Accounting and Finance* 29 (3): 16–23.

Roberts-James, C. 2002. How Much Security is enough? *Highways and Transportation* 49 (3): 16-17+19.

Sabkha, S., C. de Peretti, and D. Mezzez Hmaied. 2019. International Risk Spillover in Sovereign Credit Markets: An Empirical Analysis. *Managerial Finance* 45 (8): 1020–1040.

Santisteban-Espejo, Antonio, Fernando Campos, Jesus Chato-Astrain, Daniel Durand-Herrera, Oscar Garcia-Garcia, Antonio Campos, Miguel Angel Martin-Piedra, and Jose Antonio Moral-Muñoz. 2019. Identification of Cognitive and Social Framework of Tissue Engineering by Science Mapping Analysis. *Tissue Engineering Part C-Methods* 25 (1): 37–48. https://doi.org/10.1089/ten.tec.2018.0213.

Shetty, S., M. McShane, L. Zhang, J.P. Kesan, C.A. Kamhoua, K. Kwiat, and L.L. Njilla. 2018. Reducing Informational Disadvantages to Improve Cyber Risk Management†. *Geneva Papers on Risk and Insurance: Issues and Practice* 43 (2): 224–238.

Sarbanes Oxley Act of 2002 Retrieved from https://www.govinfo.gov/app/details/PLAW-107publ204 (accessed 15 Jan 2020).

Spekman, R.E., and E.W. Davis. 2004. Risky Business: Expanding the Discussion on Risk and the Extended Enterprise. *International Journal of Physical Distribution and Logistics Management* 34 (5): 414–433.

Taleb, Nassim Nicholas. 2007. The "Black Swan' (the "Black Swan—the Impact of the Highly Improbable', Gregg Easterbrook's Review). *New York Times Book Review*: 4.

Tyson, D. 2007. Security Convergence: Managing Enterprise Security Risk. In: *Butterworth-Heinemann*, pp. 3–5.

Van Eck, N.J., and L. Waltman. 2010. Software Survey: VOSviewer, a Computer Program for Bibliometric Mapping. *Scientometrics* 84 (2): 523–538.

Zenios, S.A. 1999. High-Performance Computing in Finance: The Last 10 Years and the Next. *Parallel Computing* 25 (13): 2149–2175. https://doi.org/10.1016/S0167-8191(99)00083-6.