Exiting the Risk Assessment Maze: A Meta-Survey

DIMITRIS GRITZALIS, Athens University of Economics & Business, Greece
GIULIA ISEPPI and ALEXIOS MYLONAS, Bournemouth University, United Kingdom
VASILIS STAVROU, Athens University of Economics & Business, Greece

Organizations are exposed to threats that increase the risk factor of their ICT systems. The assurance of their protection is crucial, as their reliance on information technology is a continuing challenge for both security experts and chief executives. As risk assessment could be a necessary process in an organization, one of its deliverables could be utilized in addressing threats and thus facilitate the development of a security strategy. Given the large number of heterogeneous methods and risk assessment tools that exist, comparison criteria can provide better understanding of their options and characteristics and facilitate the selection of a method that best fits an organization's needs. This article aims to address the problem of selecting an appropriate risk assessment method to assess and manage information security risks, by proposing a set of comparison criteria, grouped into four categories. Based upon them, it provides a comparison of the 10 popular risk assessment methods that could be utilized by organizations to determine the method that is more suitable for their needs. Finally, a case study is presented to demonstrate the selection of a method based on the proposed criteria.

Categories and Subject Descriptors: A.1 [**Introductory and Survey**]

General Terms: Security, Risk Assessment

Additional Key Words and Phrases: Risk assessment methods, comparison, criteria, overview

ACM Reference format:
Dimitris Gritzalis, Giulia Iseppi, Alexios Mylonas, and Vasilis Stavrou. 2018. Exiting the Risk Assessment Maze: A Meta-Survey. *ACM Comput. Surv.* 51, 1, Article 11 (January 2018), 30 pages.
https://doi.org/10.1145/3145905

1 INTRODUCTION

Information and Communication Technology (ICT) has been adopted widely by modern organization's procedures and activities. Organizations' reliance on ICT has become a continuous challenge for security experts and researchers, as its protection is an important issue, due to the numerous threats they are exposed to. When it comes to information security, the purpose of the organizations is to maintain the confidentiality, availability, integrity, non-repudiation, accountability, authenticity, and reliability of the IT systems and their data (Schumacher et al. 2013). In addition, every organization faces threats that could hinder its activities, growth, and profitability (Moeller 2004). These threats increase the risk factor of the ICT system and lead to the emergence of several security demands, which need to be met appropriately and systematically to assure the protection of the system.

Authors' addresses: D. Gritzalis and V. Stavrou, Athens University of Economics & Business, 76 Patission Ave., GR-10434, Athens, Greece; G. Iseppi and A. Mylonas, Bournemouth University, Talbot Campus, Fern Barrow, Poole, BH12 5BB United Kingdom.

https://doi.org/10.1145/3145905

The means of developing a security strategy and roadmap is risk assessment (RA), which facilitates the estimation and calculation of the risk faced by the organization. Risk is mostly represented as a function of the degree of harm and the possibility of harm occurrence (NIST 2012). Risk management aims to identify, control and mitigate the risks to information systems (Stoneburner et al. 2002). Thus, risk assessment is a cornerstone of risk management, which includes steps that can be grouped into the following four phases, namely: (i) determination of risk faced, (ii) risk assessment, (iii) responsive actions to mitigate the risk, and (iv) risk monitoring (Halliday et al. 1996; Bandyopadhyay et al. 1999; ASIS 2003; NIST 2012).

Currently, a plethora of heterogeneous RA methods is available, having a different focus (e.g., government agency, small and medium-sized enterprises (SME)). Moreover, as a "silver bullet" RA methodology does not exist, analysts have to choose from this number of different methods one that fits best the organization that will be assessed. However, apart from the heterogeneity of the methods, currently there is no consensus with regards to this selection process.

As such, the goal of this work is to limit the ambiguity of selecting the appropriate RA method by an organization. To this end, this work provides a meta-analysis of the RA methods that have been studied in the literature, enabling organizations to decide their appropriateness according to their demands. A set of comparison criteria has been extracted from the literature and grouped into four categories, namely validity, compliance, cost, and usefulness. The use of the comparison criteria is demonstrated with a case study, in which an organization determines the method that is more suitable for its needs based on the technical, operational, and procedural specifications of the methods.

The rest of the article is organized as follows: Section 2 discusses related work that compares risk assessment methods and proposes comparison criteria for the choice of a RA method. Section 3 describes our methodology, and Section 4 briefly describes the RA methods that are included in our analysis. Section 5 provides a generic comparison of the RA methods followed by a case study demonstrating the selection of an RA method by an SME. Section 6 concludes our work and discusses future work.

2 RELATED WORK

One of the most crucial challenges faced by organizations is the estimation of the effectiveness and the cost of the actions deployed to ensure the security robustness of their activities (ENISA 2012). To ensure the determination of the appropriate measures, with regard to cost effectiveness, to protect the Information System (IS), Risk Assessment is performed. Consequently, RA is one of the processes that are considered as the most essential to take into account nowadays (Mellado et al. 2007) and provides a more thorough view of the operations of the information system. It is the most common security management methodology and has become almost mandatory for all the big organizations. Calder et al. (2010) stress that RA is *"the core competence of information security."*

Nowadays many RA methods exist, each having its strengths and weaknesses. Each of them can thus be more or less suitable, according to the case or the specific needs of the organization. This section presents relevant literature and the comparison criteria that have been proposed for the comparison of RA methods. Even though there are many academic publications that present the most common RA methods, only a few of them provide their comparison as in our work. We also note that, contrary to our work, often academic publications propose comparison criteria without using them, or using them to compare only a few risk assessment methods (two or three methods). Ionita (2013) and ENISA (2006) examined previous versions of some of the RA methods that are examined in this work. We extend and/or revisit their results by using a different grouping of some common criteria and by examining newer versions of the RA methods.

Garrabrants et al. (1990) proposed the CERTS method to effectively and objectively evaluate tools for managing the risk that an information system is exposed to and to create comparison criteria for the tools. CERTS consists of seven criteria, namely: consistency, usability, adaptability, feasibility, completeness, validity, credibility. Each criterion includes two to four attributes that describe and define the specific criterion (Garrabrants et al. 1990). This work has been used by the academia and specialists; e.g., ENISA (2006) used CERTS to create a sub-list of comparison criteria for RA methods.

Lichtenstein (1996) proposed 17 criteria for the selection of an appropriate risk analysis method. This work mainly focuses on systems under development rather than existing ones and is based on CERTS (Garrabrants et al. 1990). It uses five of seven CERTS criteria. The proposed criteria were grouped into (a) method characteristics (including cost, agreement of analysts and management, flexibility, complexity, completeness, consistency, ease of use, usefulness, validity, reliability, and software support) and (b) organization characteristics (including risk level, size, security awareness, external requirements, and organizational structure) (Lichtenstein 1996). Lichtenstein's (1996) and Garrabrants et al.'s (1990) work is the springboard for several proposed criteria frameworks (Smojver 2011; Nair 2013).

In a different approach, Van Niekerk and Labuschagne (2006) compare the steps of RA methods. The structural dimensions of the framework include scope and assessment criteria that support its context depth and breadth. The procedural dimensions of the framework include: "process" and "assessment tools" that are used to enhance its functionality.

ENISA has developed a *"Log of risk assessment and risk management methods"* (ENISA 2006) by using the various stages of evaluation and risk management, EU directives, and ISO definitions, producing an updated inventory and comparison of Risk Assessment methods now available at the ENISA website (ENISA 2006). The methods' comparison used: (a) a list of products (methods and standards) that are related to risk analysis and (b) the definition of specific properties of "products." The ENISA criteria are summarized to general information that comprises the "identity" of the method or tool (e.g., life cycle, price, supported languages, etc.), field area (licenses, certifications, appropriateness for organizations, etc.), and user opinion (skills, support, method maturity, etc.).

NATO compared the steps of CRAMM, EBIOS, HTRA, NIST, and MAGERIT to perform the analysis and evaluation of risk (NATO 2008).

Syalim et al. (2009) presented a comparison framework focusing on MAGERIT, MEHARI, NIST, and Microsoft's Security Guide. The framework is based on the steps of each method and its documentation (Syalim et al. 2009). Syalim's work suggests that the methods include three general steps of risk analysis, namely "identification of threats," "identification of vulnerabilities," and "risk determination." All methods recommend countermeasures as part of the risk management process.

Dong and Yadav (2014) created a framework for the comparison and analysis of methods of risk assessment. The framework relies on the phases of the analysis, such as ascertainment, measurement, evaluation and their results, and on key performance indicators related to the completeness and effectiveness of each method (Dong et al. 2010). The objective of the framework was to provide an easy way for organizations to compare and select the appropriate method. However, as the author also admits, the framework has not been used in practice, yet.

Sajko et al. (2010) used Analytic Hierarchy Process (AHP) to develop a framework of criteria for the evaluation of risk analysis methods and tools (Saaty 1988). In particular, one of the proposed criteria is the support of the method or process. The support can either be methodical (metrics, objectivity, accuracy, flexibility, integrity) or software (user interface, appropriate equipment, etc.). Other criteria are the required resources (information, people, money, time) and the motives and objectives of the method (Sajko et al. 2010).

Derakhshandeh et al. (2011) proposed a framework for methods' comparison based on six criteria ranging from 0 to 3, namely: required resources, data collection for assets, threats and vulnerabilities, cost, time, accuracy, and simplicity (Derakhshandeh et al. 2011).

Smojver used the Analytic Hierarchy Process (AHP) and the criteria proposed by ENISA (2006) to propose a model that allows the transparent and objective comparison of the different RA methods. The model aims to aid the selection of the method that is more appropriate for the needs of an organization (Smojver 2011). It includes five key criteria (namely method scope, the ease of use, the maturity of the method and the target audience) analysed in 17 further sub-criteria. The analysis of the 17 criteria is particularly extensive and helps to create an integrated assessment framework and to identify the characteristics of each method.

Sunyaev (2011) proposed a comparison table for RA methods focusing on the health sector. The work used the ENISA criteria, which were enhanced with the level of detail and the ability to integrate in an organization. The table includes values in a scale from 0 to 5 to indicate the extent a criterion is met by each method (Sunyaev 2011).

Macedo et al. (2012) proposed five comparison criteria for RA methods, namely: complexity, methodological approach, support tool, geographical coverage, and the origin. The aim was to provide assistance in the selection of methods through a foreclosure process based on a series of simple criteria (Macedo et al. 2012).

Padney et al. (2012) proposed seven comparison criteria, namely: quantification, integration of security features, integration of threats and vulnerabilities, requirements phase perspective, accuracy level/validation, compliance with standards, and the supporting tools (Pandey et al. 2012). As in Macedo's work (Macedo et al. 2012), a comparison table is used with binary (YES/NO) values for each criterion.

Kiran et al. (2013) propose a framework comprising of a 10 comparison criteria for RA methods. Some of the criteria and the approach followed resemble the work of Macedo (2012), but more details and criteria were added.

Ionita complements the criteria proposed by ENISA, NATO, and Kiran et al. (2013) to compare RA methods using a table with binary (YES/NO) values (Ionita 2013). During the same period, Al-Ahmad et al. (2013) conduct a survey on the various risk management frameworks, creating a framework for the selection of the method that best fits an organization. The framework utilizes a set of seven comparison criteria for RA methods, i.e., implementation costs, necessary skills, implementation of the method by other organizations, availability of detailed guidelines and instructions from the provider, implementation and application complexity, flexibility, and adaptability (Al-Ahmad et al. 2013). The authors demonstrate their framework with a case study.

Pan and Tomlinson (2016) provide a review of the RA literature from 2004 to 2014. They classify academic articles according into seven categories related to risk assessment, namely those: (a) that identify risk, (b) compare risk analysis, (c) improve risk analysis, (d) compare frameworks, (e) improve frameworks, (f) provide case studies, and (g) perform risk evaluation by comparing the results of risk analysis. Finally, Shameli-Send et al. (2016) proposed a risk assessment taxonomy, which focuses only on risk analysis, using the following criteria: appraisement, perspective, resource valuation, and risk measurement.

Wangen (2017) compares 11 Risk Assessment methods according to the identified tasks, application, and results of the analysis using the Core Unified Risk Framework (CURF) (Wangen et al. 2016). His perspective is that previous frameworks for methods' comparison are restrictive as predetermined parameters limit the analysis when elements of the analysed methods do not fit into their definitions. Using his bottom up method that first identifies the tasks of the methods and them defines them, the Author identifies numerous elements of risk identification, estimation and evaluation, ranking them according to completion scores (not addressed, partially addressed, fully addressed). After applying the method to case studies, the Author can illustrate advantages and disadvantages of a set of three methods (OCTAVE A, ISO 27005, and NSMROS) demonstrating their level of completeness (Wangen 2017).

In conclusion, one may notice the ambiguity among the criteria definitions, as they change over time and also the lack of consensus on the set of comparison criteria.

3 METHODOLOGY

This section describes our methodology with regards to (a) initial collection of the available RA methods and their filtering and (b) the comparison of the RA that are in scope of our analysis.

3.1 Method Selection Criteria

As discussed earlier, organizations have a lot of options when it comes to the selection of a RA method. This work considered the popularity of RA methods to compile a list that was subsequently filtered into a list of ten popular RA methods. To assess the popularity of the methods, we considered: (a) if the method is provided by an agency (e.g., NIST) or standardization body (e.g., ISO), (b) if the method is recognized by the relevant scientific community (with academic citations) or industry, and (c) ranking in the relevant search engines (Google Scholar, Google search). To narrow the number of RA methods the following selection criteria were used, which are commonly used in the literature (Houmb 2007; Kouns et al. 2010; Macedo 2012; NATO 2008; ENISA 2006):

- Is the proposed approach a method or a guideline? If it is a guideline, then does it contain a proposed method to use? If not, then exclude.
- Price and available documentation? Exclude if unavailable or hard to find in English.
- Does the approach identify Information Security Risks? If not, then exclude.

3.2 Comparison Criteria

As discussed in Section 2, there is no consensus in the relevant academic literature regarding the comparison and evaluation of RA methods in the form of a framework or set of criteria. In addition, the definition of criteria changes over time; therefore, we created working definitions grounded on the reviewed literature. More specifically, this work uses a set of criteria have been compiled via: (a) surveying the relevant literature, (b) discussions with RA experts who work in the industry, and (c) the experience of a subset of the authors of this work, who have experience in delivering RA projects. Table 1 summarizes the comparison criteria that are used in this work.

Validity. This criterion refers to the extent in which the results of the analysis resembles reality (i.e., real circumstances and the real phenomenon) in multiple independent applications of the method in each configuration of the system (Garrabrants et al. 1990). Under this criterion, the following sub-criteria are grouped: (a) proof of *completeness*, i.e., if the RA method includes all the phases of the risk assessment (Merkhofer 1985; Garrabrants et al. 1990; Lichtenstein 1996), which typically includes the following four phases: (i) preparation/scoping, (ii) risk identification, (iii) risk analysis, and (iv) risk evaluation; (b) *type of analysis* (qualitative, quantitative) (Fischhoff et al. 1981; Vorster and Labuschagne 2005; Van Niekerk and Labuschagne 2006; Katzke 1988); and (c) *risk calculation class*, which is based on the properties and factors of risk calculation (Zambon et al. 2011). In this criterion, likelihood is considered, according to ISO 31000, as the possibility of an event to happen, whether defined, measured or determined (probability/frequency). This is used for flexibility reasons, since an event can occur multiple times within a specified period of time. The operator ⊗ states a combination between two factors. This work uses the five classes of risk calculation as defined in Zambon et al. (2011):

Table 1. Evaluation and Comparison Criteria

Validity	Compliance	Cost	Usefulness
Completeness Preparation (1) Risk Identification (2) Risk Analysis (3) Risk Evaluation (4)	Compliance with Standards	Support cost Software cost	**Ease of Use** Usability (Interface, handle errors Documentation)
Type of Analysis Qualitative Quantitative			**Scope** Target Organization (Type, Size), Focus
Risk calculation Class Class A Class B Class C Class D Class E			**Life Cycle** Release Last Update
			Adaptability
			Software Support
			Training

- *Class A*. Methods in which risk calculation is based on the relationship between assets and threats, namely the combination of threat likelihood, the vulnerability of the asset to that specific threat, and the impact on the asset:

  $$\text{Risk (Threat, Asset)} = \text{Likelihood (Threat)} \otimes \text{Vulnerability (Threat, Asset)} \otimes \text{Impact (Threat, Asset)}$$

- *Class B*. Methods in which risk calculation is based on the outcome of the realization of a threat and on the defined security requirements for a specific asset. This approach is helpful when risk assessment is performed for organizations that want to be certified and compliant to standards:

  $$\text{Risk (Threat, Asset, Requirements)} = \text{Vulnerability (Threat, Asset)} \otimes \text{Impact (Threat, Requirements)}$$

- *Class C*. Methods that present the financial loss that the incident would cause:

  $$\text{Risk (Threat, Asset)} = \text{Annual Loss Expectancy (Threat, Asset)} = \text{Likelihood (Threat, Asset)} \otimes \text{Average Loss (Threat, Asset)}$$

- *Class D*. Methods in which risk calculation considers critical assets (e.g. assets of a critical infrastructure), based on the vulnerability level of the critical asset and the impact of the threat on this critical asset:

  $$\text{Risk (Threat, Critical Asset)} = \text{Vulnerability (Critical Asset)} \otimes \text{Impact (Threat, Critical Asset)}$$

- *Class E*. Contrary to Class A methods, Class E methods calculate risk based on security incidents (i.e. combining a threat with a vulnerability that is necessary for the occurrence of the threat), instead of threats thus are less generic. Risk is calculated with the combinations of the likelihood of the security incident and its impact to a critical asset:

  $$\text{Risk (Incident, Asset)} = \text{Likelihood (Incident)} \otimes \text{Consequences (Incident, Asset)}$$

Finally, a qualitative risk assessment is based on evaluations made by an expert, so that risks can be classified in natural language according to nominal and ordinal scales (Refsdal et al. 2015). This approach does not use any numeric value and is usually based on opinion-based and subjective estimations. The output is summed up in classes, using scales such as "low," "medium," and "high." On the other hand, quantitative risk assessment uses ratio, difference absolute scales to represent money units, risk percentages, or the quantification of the asset's value that has been lost. In general, qualitative methods are faster to extract results and require less resources and data. Furthermore, proficiency in mathematics and economics is not required (Rosenquist 2009). At the same time, the use of quantitative methods is suggested in cases of finer granularity or evaluations at technical level while a qualitative approach is recommended when information to be qualified is not homogeneous (Refsdal et al. 2015).

Compliance. This criterion refers to compliance with standards related to information security, regulations, and other methods (ENISA 2006; Merkhofer 1985; Lichtenstein 1996; Sajko et al. 2010).

Cost. This criterion refers to the risk assessment related expenditures (Olle et al. 1988). This includes the sub-criteria *support cost* and *software cost* (Browne 1989; Lichtenstein 1996; ENISA 2006). The former refers to the expenditure that is necessary to access documentation and other sources related to the method (e.g., training, books, and user manual). The latter refers to the cost of the license of the software/tool.

Usefulness. This criterion refers to the quality of having utility and especially practical worth or applicability of the method. It includes the following sub-criteria: (a) *ease of use*, which consists of interface's usability and documentation (Syalim et al. 2009); (b) *life cycle*, namely the method's release date and latest update (Olle et al. 1988; Craft et al. 1998; Syalim et al. 2009; ENISA 2006); (c) *scope*, namely the method's adaptability to meet an organization's demands (Lichtenstein 1996; Kitchenham et al. 1997; Craft et al. 1998; Smojver 2011) and the *focus* of the risk assessment method (Olle et al. 1988; Garrabrants et al. 1990); (d) *software support*, namely if the method is accompanied by a tool that facilitates the RA process; (e) required *training* for implementation, usage, and maintenance of the RA method (Kitchenham et al. 1997), and adaptability, i.e., the ability to adapt the method to the needs of a specific industry (Garrabrants et al. 1990; Lichtenstein 1996; Sajko et al. 2010).

In this work, *usability* is defined by Lichtenstein (1996) and uses three criteria for its assessment, namely: (1) user friendly, (2) capable to handle errors, and (3) simple and comprehensive. If a method satisfies the above-mentioned criteria, then the usability rate is evaluated as *sufficient*. If it satisfies two of them, then it is considered *relatively sufficient* and if it satisfies only one, then it is considered as *insufficient*.

Finally, this work considers life cycle details as an indication of usefulness, as an outdated method does not include all the recent vulnerabilities, threats, and safeguards, and this hinders the process of the risk assessment.

4 RISK ASSESSMENT/RISK MANAGEMENT METHODS

We now provide a brief description of the RA methods that are in scope of our analysis.

4.1 EBIOS

As described by Agencenationale de la sécurité des systems d' information the "EBIOS method was initially developed by the French Central Information Systems Security Division. The method is now maintained by private club experts from different fields (e.g., Club EBIOS)" (ANSSI 2010). EBIOS aims to support management in decision making by creating a common ground for security debates between different stakeholders. To assess and manage the risks associated with Information Systems the method uses the five phases that are descripted in Table 2.

Table 2. EBIOS Phases (ANSSI 2010)

	Phase	Description
1	Context Establishment	The correlation between the business context and the Information System is determined. Additionally, the system under consideration is defined and the dependencies between the assets are determined
2	Determination of Security Requirements	The dreaded security events are assessed to determine security requirements
3	Risk Study	A risk study is contacted for the identification and analysis of risk scenarios
4	Risk and Security Goals Identification	The identification of risks and the description of the necessary security goals are derived by information from the above mentioned phases
5	Safeguards Selection	Determination of the necessary safeguards and residual risk

Unlike other methods that are scenarios-based, EBIOS uses a modular approach that allows a more in-depth analysis via the identification of the various individual components or risk causes, such as vulnerabilities, entities, and attack methods (Kouns et al. 2010). This modular design is one of the strongest aspects of EBIOS.

4.2 MEHARI

MEHARI was designed by security specialists of the French institute CLUSSIF ("Club de la Sécurité de l' Information Français"). The method replaced MARION and MELISA methods. It was announced in 1996 and provides a model for risk assessment, modular components and procedures to support it. MEHARI aims to help upper management/executives implement the security standard ISO/IEC 27005. The method is compliant with current security standards such as ISO 13335, 27001 and 27005. The purpose was to enable a validated procedure for analyzing risk scenarios and provide tools for security management both long and short term (CLUSIF 2010). The method describes a complicated process that contains circular risk management steps and the formation of a knowledge base. Following the formation of the knowledge base, a separate RA process is developed and implemented. For each risk scenario the steps that are presented in Table 3 are followed:

4.3 OCTAVE

OCTAVE was created by the Software Engineering Institute of the Carnegie Mellon University (CERT 2008). The U.S. Ministry of Defense initially funded the project to deal with the challenge of compliance with the HIPAA security standard. OCTAVE can be adapted to the needs of each organization and takes into account the resources, threats and vulnerabilities of organizational and technical nature. Several variations of the method and supporting tools exist, each serving a specific purpose (CERT 2008).

The most recent supported method is OCTAVE Allegro and is based on the previous methods OCTAVE Original and OCTAVE-S (Caralli et al. 2007). The current framework consists of three variants of the OCTAVE method and its main OCTAVE method for risk assessment is designed

Table 3. MEHARI Phases (CLUSIF 2010)

	Phase	Description
1	Risk Situation Identification	By using knowledge base or by manually identifying possible faults the risk is identified
2	Physical Threats Evaluation	Threats coming from nature are identified and evaluated. Exposure to such risks is classified using four levels (Very Low exposure. Low exposure, Medium exposure and High exposure)
3	Evaluation of Dissuasive and Preventive Factors	The dissuasive and preventing factors of risk areassessed
4	Evaluation of Protective, Palliative and Recuperative Factors	This step includes the assessment of the following risk factors: (a) protective, (b) palliative and (c) recuperative
5	Evaluation of Potentiality	The potential of any threat leading to a security incident is evaluated. A scale of four levels is used (Level O-not considered. Level 1-very unlikely. Level 2-unlikely, Level 3- likely, Level 4-very likely)
6	Evaluation of Intrinsic Impact	A table is used for the evaluation of the intrinsic impact. The evaluation is done using an intrinsic impact table. The knowledgebase also gives the mentioned table
7	Evaluation of Impact and Impact Reduction	An automated computation evaluates impact and impact reduction. The evaluation is done in two steps. First, an evaluation of an impact reduction indicator takes place and then the impact is evaluated. The impact reduction factor measures the debilitation of the risk's effects, compared to the intrinsic impact that has been earlier evaluated
8	Global risk assessment, taking into account the previous factors	*Residual Likelihood*: Intrinsic Likelihood (from the analysis of the threats parameters). Resulting likelihood reduction (from the analysis of the dissuasion and prevention capabilities *Residual Impact*. Intrinsic impact (from the analysis of the consequences of each type of damage to the assets). Resulting impact reduction (from the analysis of the confinement and palliation capabilities of the existing safeguards)
9	Decision on whether risk is acceptable or not	In the case that the risk is not acceptable, development of a control mechanism that will be able to prevent the occurring risk is necessary

for organizations employing three hundred or more employees and consists of the phases that are summarized in Table 4 (Alberts et al. 2003).

OCTAVE is based on employee participation in the analysis team. Employees from different levels of the organization are involved to satisfy the organizational, operational and technical requirements of the method. The focus of the method is on critical assets, for which the analysis is taking place.

Table 4. OCTAVE Phases (Alberts et al. 2003)

Phase		Description
Preparation		Involves the selection of the team members and secondary participants, determination of the scope, and getting senior management sponsorship
1	Creation of threat profiles based onassets	(a) The analysis team evaluates and identifies the important assets. (b) Current safeguards are identified. (c) The security requirements are determined. (d) Processes: • Process 1: "Identification of senior management knowledge regarding critical assets, threats, vulnerabilities, security requirements and existing security practices." • Process 2: "Identification of operational area knowledge regarding important assets, threats, vulnerabilities, security requirements and existing security practices." • Process 3: "Identification of staff knowledge about important assets, threats, vulnerabilities, security requirements and existing security practices." • Process 4: "Use of gathered information to create threat profiles."
2	Vulnerabilities Identification	(a) Infrastructure assessment is carried out. (b) The analysis team examines important assets and areas for technical vulnerabilities. (c) Processes • Process 5: "Identification of key components for each critical asset and selection of the ones that must be further evaluated." • Process 6: "Evaluation of the selected components and identification of vulnerabilities and weaknesses, while cross referencing them with the respective threat profiles."
3	Develop Security Strategy and Plan	(a) Identify threats for important assets. (b) Develop strategies and plans based on previous phases' findings. (c) Processes: • Process?: "Perform risk analysis. Following, Identification of threats' impacts on critical assets and development of criteria for evaluation of these impacts. Use of the previous for the overall evaluation. The outcome is summarized to a risk profile for each critical asset." • Process 8: "Development and establishment of a protection strategy based on the extracted findings. This step includes the creation of management reviews and the approval of the security strategy and plans."

Table 5. IT-Grundschutz Phases (German BSI 2014)

	Phase	Description
1	Initialization Process	A list of relative threats is prepared for each asset
2	Identification of Additional Threats	Potential additional threats that are related to the applied scenario are identified via a brainstorming session
3	Threat Evaluation	The threats are systemically analyzed and assessed in order to determine the effectiveness of existing safeguards
4	Safeguards Selection	The management decides on the way risk mitigation is to be handled
5	Consolidating Results	Verification and monitoring of the new security policies and mechanisms for consistency and adequacy in the target environment

4.4 IT-Grundschutz

IT-Grundschutz was proposed in 1994 alongside a series of standards from the German Federal Security Service (BSI). It aims to achieve the appropriate organizational security level, by offering general recommendations and actions to create an effective security procedure along with detailed technical guidelines (German BSI 2014). IT-Grundschutz provides a qualitative method for identifying, analysing, and assessing security incidents that can cause damage to the business. IT-Grundschutz consists of the steps that are summarized in Table 5.

The main body of IT-Grundschutz does not outline a specific method and provides “recommendations and suggestions for safeguards and security controls that are appropriate for standard and typical business processes, applications and IT systems with common security requirements” (Nidd et al. 2015). Therefore, common assets are outlined along with aspects regarding the organization, the infrastructure and the personnel involved. The standard enumerates potential threats and suggests the appropriate safeguards. To identify the major inadequacies of the system and to comply with IT-Grundschutz standard, “relevant modules are chosen and implemented to each aspect of the information system. This approach enables a quick and financially sustainable way to a reasonable security level” (Kouns et al. 2010). Last, the method complies with the security standard ISO/IEC 27001.

4.5 MAGERIT

MAGERIT is a method for risk analysis and risk management developed by the Spanish Higher Council for Electronic Government (CSAE) (Amutio et al. 2014). MAGERIT is a response to the increasing dependence of public services and private organizations to information technology. The method is designed to serve anyone who works with digital information management systems.

MAGERIT consists of the steps that are summarized in Table 6. To better organize the results, step 3 is perform upon the execution of all the other steps and the development of the scenario. As a result, a realistic estimation of the impacts, threats and risks is provided. MAGERIT is, also, supported by EAR/Pilar tool.

4.6 CRAMM

CRAMM is a RA method that was created by the British Central Communication and Telecommunication Agency (CCTA) in 1985 (ENISA 2006). It was created with the aim to provide security

Table 6. MAGERIT Phases (Amutio et al. 2014)

	Phase	Description
1	Identification of assets	Determination of the organizations assets, their relationships and their value, for example the damage (cost) caused by their degradation. The vital asset is the information handled by the system (i.e., its data). All other relevant assets are identified by using these data, such as services that manage data, software that handles data, hardware that hosts the data, storage devices, and so on.
2	Identification of Threats	Determination of the threats. There are threats from natural disasters, industrial accidents, or threats caused by the human factor
3	Definition of safeguards	Determination of available safeguards and how effective they are against the risk
4	Assessment of Impact	Assessment of the impact, defined as the damage that can happen to an asset as a result of a threat
5	Risk calculation & Assessment	Assessment of risk, defined as the aggregate effect on incidence (or the expectation of appearance) of the threat. Having available the information regarding the impact of the threats on the assets facilitates the risk derivation by considering the frequency of occurrence. Risk increases with the frequency and the impact

evaluation of Information Systems in government departments. CRAMM provides a tool, which was later made commercially available to the public through Insight Consulting. The method and tool were developed mainly for application in large-scale organizations, but can be also applied to SMEs (Yazar 2002; Spinellis et al. 1999). CRAMM can also be used to (a) Justify investment decisions in the security of information systems and networks, based on measurable results and (b) demonstrate the compatibility of the organizations information systems with the British standard during an auditing process. CRAMM consists of three phases (Table 7).

4.7 HTRA

"The Harmonized Threat and Risk Assessment (HTRA) method was published under the auspices of the Chief of Communications Security Establishment and the Commissioner of the Royal Canadian Mounted Police (RCMP)" (CSE 2007). The method aims at providing (Shallal 2013):

(1) Flexibility—The method must be flexible so that it can manage all assets, either in physical or informational form, both within large organizations and small.
(2) Scalability—To allow for the separation of larger and more complex HTRA's into smaller modules that are easier to handle, the method should support analysis, and provides the appropriate interfaces between the relevant data.
(3) Simplicity—The method should be satisfactory and described in simple steps to allow easy implementation by management programs and projects, as well as security professionals.
(4) Generality—The method must be adequately applied to all assets.

Table 7. CRAMM Phases (ENISA 2006)

	Phase	Description
1	Identification and valuation of goods	Step 1: Description of information systems and facilities Step 2: Valuation of assets and infrastructure Step 3: Verification and validation of the assay
2	Risk Analysis	At this stage, an assessment of risk is undertaken. Identifying risks and their degree is done with the following steps. • Step 1: Identification of threats relating to each asset • Step 2: Assessment of threats and risks (threats and vulnerability assessment) • Step 3: Calculation of combinations of risk "Asset - Threat - Vulnerability" • Step 4: Verify and validate the level of risk
3	Bisk Management	Step 1: Identify recommended countermeasures Step 2: Create security Plan

Table 8. HTRA Phases (Shallal 2013)

	Phase	Description
1	Preparation Phase	Preparation and creation of project plan takes place
2	Identification and Valuation of Assets	In this phase the following two steps take place: (a) Identify critical assets (b) Use valuation tables
3	Identification and Valuation of Threats	(a) Identify threat sources (b) Enumerate threats and relative metrics (c) Use evaluation table
4	Assess Vulnerabilities	(a) Identify vulnerabilities and their sources (b) Enumerate vulnerabilities and corresponding metrics (c) Use valuation table
5	Risk Assessment	Asset risks and use tables for residual risks
6	Recommendations Phase	(a) Identify sources of data protection measures (b) Enumerate protection measures (c) Selection of possible protection measures (d) Cost-benefit calculation for each safeguard (e) Recommendations table (f) Analysis report

(5) Consistency—To achieve greater coherence between different HTRA used by different organizations, the method needs to establish common and simple vocabulary and terminology for all aspects of risk management.

(6) Automation—It has been developed in order to allow automation to facilitate and support the HTRA process.

The method consists of the six phases that are summarized in Table 8:

Table 9. NIST SP800 Phases (NIST 2012)

	Phase	Description
1	Risk Assessment	During this phase the following processes take place: (a) System Characterization: The scope and the purpose of the analysis are specified, and the system is analyzed to identify critical assets. (b) Threat Identification: Threats are identified and classified in three categories (Natural, Human, or Environmental). (c) Vulnerability Identification: Drafts a list with vulnerable system points (d) Control (safeguard) Analysis: Analyzes existing controls or the ones planned to be added in the future. (e) Determination of Likelihood: Any potential vulnerability is assessed to determine the likelihood of exploitation and the realization of an unwanted security incident. The likelihood is measured on a scale of High, Medium, or Low. (f) Impact Analysis: The severity of the impact of each vulnerability and threat is measured, in a scale of High, Medium, and Low. (g) Risk Identification: Evaluates the risk level of the information system. Risk is defined as a function of the likelihood of a specific threat realization and the impact on the information system. (h) Control Recommendations: Identifies the safeguards that reduce or eliminate the risks. Mechanisms and safeguards are examined for their effectiveness, compliance with the law, reliability and organizational policy and the consequences that they bring to the organization. (i) Results Documenting: The results are documented in a formal report, which helps senior managers in decision making.
2	Risk Mitigation	During this phase, a decision is made on which safeguards will be implemented.
3	Evaluation & Assessment	As most Information Systems must be updated periodically, which creates a need for security reassessment. As such, a review of the security plan after each update of the information system or after three years is required.

4.8 NIST SP800

The NIST SP800 complements other standards of the SP800 framework, "providing a general method for overall risk management in Information Systems" (Kouns et al. 2010; Stoneburner et al. 2002; NIST 2012). The method consists of the three phases that are summarized in Table 9 (NATO

Table 10. RiskSafe Phases (Platinum Squared 2014)

	Phase	Description
1	Asset Identification and Valuation	The critical assets are identified and evaluated. Dependencies between assets are also recognized. The valuation is made in terms of the impact of the loss an asset. The impact is derived after performing interviews to selected representatives of users of the assets and data.
2	Identification and Valuation of Threats	Cover the full range of deliberate and accidental threats that may affect information systems such as (Platinum Squared 2014): (a) Hacking (from insiders and outsiders). (b) Viruses or other forms of malware. (c) Damage to equipment or software. (d) Theft., intentional damage or terrorism. (e) Errors by humans. Threat levels are measured on a scale of five points, from Very Low to Very High, whilst the vulnerability levels are measured in a Low, Medium, High scale. The phase ends with the calculation of risk level, combining the threat and vulnerability levels with the incidence levels that were established during the identification phase. The result is a risk rating on a scale from 1 to 7.
3	Safeguard Selection	The measurements calculated in previous phases are taken into consideration and are compared with the accepted levels of risk of each safeguard. The aim is to find the areas that need further attention and to assess whether the existence of vulnerabilities justifies the implementation of a particular safeguard.

2008). The method described in NIST SP800-30 is mainly qualitative. NIST 800-30 is primarily a model rather than a specialized method. Still, it contains a complete guide for defining all aspects of an effective risk management program. It also incorporates the guidelines and the processes required to assess and mitigate risks. It suits better large organizations such as government agencies and large enterprises. NIST SP800 supports the management of organizations, CIO's (Chief Information Officers), security officers, IT consultants, and generally any person who has to do with risk management in an organization (Kouns et al. 2010).

4.9 RiskSafe Assessment

RiskSafe method was proposed and released in 2012 as a Software-as-a-Service (SaaS) solution. It has been developed by consultants with extensive experience in conducting risk assessments on a wide range of business sectors, including Central Government, Local Government, and Financial Services (Platinum Squared 2014). RiskSafe aims at making risk assessment a much more transparent process and help transform the assessment and management of risks in a collaborative approach. This allows all interested parties to see how risks have been identified and then to record, maintain, and comment on how these risks are treated (Platinum Squared 2014).

Table 10 summarizes the phases of RiskSafe.

4.10 CORAS

CORAS basically consists of three artefacts, namely a method for risk assessment, a language, and a computerized tool. The CORAS language is a customized language for risk modeling. The language is diagrammatic. It uses simple graphical symbols and relations between these to facilitate diagrams that are easy to read and that are suitable as a medium for communication between stakeholders of diverse backgrounds. In particular, CORAS diagrams are meant to be used during brainstorming sessions where the discussion is documented along the way (Lund et al. 2011).

The first version of CORAS was developed within a European Union project (IST-2000-25031), which was completed in 2003. Since then CORAS has undergone several major updates. The CORAS book (Lund et al. 2011) provides a comprehensive overview of the current version. The CORAS language was originally defined as a UML profile. The language has since then evolved into a domain specific language independent of UML through several iterations with feedback from industrial case studies, teaching and empirical investigations. The language has a formal semantics and is supported by a specialized calculus for risk reasoning.

CORAS project aimed to develop a practical framework based on models and also being supported by a tool for effective risk assessment of critical systems (Aagedal et al. 2002). It uses a UML-based modeling language, which is used together with risk assessment for three purposes (Raptis et al. 2002): (a) an abstract description of the RA's target, (b) facilitate communication between stakeholders, who can be management, experts, departments, and so on, (c) document the results and underlying assumptions. The CORAS language offers five kinds of basic diagrams: asset diagrams, threat diagrams, risk diagrams, treatment diagrams, and treatment overview diagrams (Lund et al. 2011). Table 11 summarizes the phases of CORAS.

5 COMPARISON OF RA METHODS

This section utilizes the comparison criteria that were discussed in Section 3.2, to compare the RA methods that were selected for the analysis. The evaluation is based on the perceptions and experience of a subset of the authors—some of whom have experience in delivering RA projects—and the survey of the relevant literature (see Section 2). The results of the analysis are presented in the following subsections and are summarized in Tables 13 to 16.

5.1 Type of Analysis, Risk Assessment Phases, and Class

Table 12 summarizes the comparison of the RA methods under the validity criterion.

Regarding the *risk calculation class* sub criterion, our results suggest that the majority of the RA methods, which were studied in this work, fall under the Class A category, when risk calculation is considered. CORAS and IT-Grundschutz are classified as Class E, namely risks are assessed in relation to a security incident regarding an asset, and can be defined only in relation to a vulnerability. Even though these methods differ in the way risk is calculated, this does not necessarily mean they are inferior to others. It seems, however, that other methods have a slight advantage as they contain a broader concept of risk. Class A, methods consider that threats can affect an asset even without a vulnerability and this gives them the advantage over methods of Class E.

Considering the *completeness* in RA phases, most perform similar risk analysis steps (Analysis, Management and Risk Mitigation). Some of the methods have refined these into smaller, separate analysis steps, covering most aspects, while others have grouped them in phases. More specifically, The HTRA divides the steps into six phases. The lack of technical depth and the fact that existing safeguards are not taken into consideration is considered as a disadvantage. The documentation of the method describes mostly general guidelines without deepening in technical details. In each step predefined tables are provided. These tables are used to summarize the important data and evaluate it on the scale of values High, Medium, and Low. The restrictive limit of characters allowed

Table 11. CORAS Phases (Lund et al. 2011)

	Phase	Description
1	Preparation	Preparation includes the identification of the target and the depth of the analysis
2	Meeting with the client	Meeting with the client to reach a common agreement on the broad goals and planning as well as the focus and scope of the evaluation
3	Further definitions of the evaluations target and goal	Further definition of the evaluations target and goal, as well as identification of the critical assets is taken place. Following a few high level threat cases, vulnerabilities and risks that should be examined are chosen. Afterwards, the CORAS language is used to document the goals and the description of the system analysis
4	Elicitation of the risk assessment criteria	The fourth step focuses on elicitation of the risk assessment criteria that are to be used in the next steps. In this step, it is also verified that the system and context description is approved by the client, including any assumptions and conditions drafted up by the previous steps
5	Multi-disciplinary brainstorming workshop	In the fifth step a multi-disciplinary brainstorming workshop is performed to exchange ideas and point of views. The workshop uses as a base the CORAS language, and aims at identifying the majority of all possible risks and threats
6	Risk Analysis Brainstorming Session	The sixth step focuses on assessing the level of risk, which can be achieved via risk analysis or via an interdisciplinary brainstorming session. During this step, the likelihoods and the consequences for each risk, which was identified in the previous steps, are determined
7	Risk Mitigation	In the seventh step, the criteria regarding risk evaluation are used to determine each risk as accepted or as it requires mitigation
8	Identification of Safeguards	The eighth step involves the identification, evaluation, and comparison of the possible safeguards

on each table is deemed as a disadvantage, since useful data can be lost. Also the division into six phases introduces a certain level of complexity into the method, even though each step is relatively easy to understand.

CORAS supports all steps equally, which makes it a time-consuming process if the company is interested in a superficial evaluation of its security posture. It consists of eight steps, with the first 4 aiming to achieve an agreement with management (Lund et al. 2011). Valuable time is spent in trying to achieve convergence with the administration that gives to this method the depth required for an analysis that involves from 150 to 300 man hours. For each asset the degree of significance is defined in relation to its type (direct/indirect asset). Evaluation scales are defined by the user in these first four steps and can be eventually adjusted in later phases (Lund at al. 2011). For the identification and evaluation of risks a workshop is carried out in which threats, vulnerabilities, and incident scenarios are identified. The method is based on the creation of threats diagrams, which depict how a combination of different vulnerabilities can lead to loss of one or

Table 12. Comparison of the RA Methods Based on the Validity Criterion

Category: Validity	**Completeness**				**Risk Calculation**	**Type of analysis**
	Risk assessment phase					
Method/Criteria	1	2	3	4	Class	Qualitative or Quantitative
EBIOS	✓	✓	✓	✓	B	Qualitative
MEHARI	✓	✓	✓	✓	A	Qualitative
OCTAVE	✓	✓	✓	✓	D	Qualitative
IT-Grundschutz	✗	✓	✓	✓	E	Quantitative
MAGERIT	✓	✓	✓	✓	A	Both
CRAMM	✓	✓	✓	✓	A	Qualitative
HTRA	✓	✓	✓	✓	A	Qualitative
NIST SP800	✗	✓	✓	✓	A	Qualitative
RiskSafe Assessment	✓	✓	✓	✓	A	Qualitative
CORAS	✓	✓	✓	✓	E	Both

Note: The RA phases is using the following notation: 1 = preparation/scoping, 2 = risk identification, 3 = risk analysis, and 4 = risk evaluation.

more safety parameters. The data that is required to carry out the analysis is collected through meetings with a representative of the organization, during which a brainstorming session is held and is followed by a collection of any relevant documentation and other materials (like statistics on risks for targets) (Lund et al. 2011). A meeting must be scheduled for each threat diagram and this characterises the usefulness of the method in respect of checklist approaches, which are not recommended by practitioners nowadays considering the nature of crime-as-a-service and legal and regulatory requirements business have to comply with. Risk level is defined with a table that shows the correlation of the likelihood of an incident and the severity of the impact and the security parameters that are affected.

CRAMM follows rigorous standardization in the preparation phase, which reduces its flexibility when compared to other methods. Strict standardization is utilized in all phases, which makes the method complex and time consuming. The data that are required by CRAMM, is mainly collected through interviews. CRAMM also separates assets into four categories: physical, applications/software, information/data and locations. Prior to asset valuation, CRAMM requires the construction of a model for each asset. A model is a relational schema, showing the relationships between the assets. The level of threat is identified in a scale of five qualitative values (from "very low" to "very high") and the vulnerability is determined on the Low, Medium, or High scale. CRAMM takes into account any existing safeguards in the assessment of risk. The calculation of an asset's implied value is also deemed as advantage, as it is something that seems to be missing from some of the other methods. CRAMM calculates the risk of each asset group using predefined tables and comparing the value of assets, the impact and levels of threats and vulnerabilities.

EBIOS is divided into five phases. The documentation though is available only in French, which is deemed as disadvantage as it prevents non-native speakers to understand the method. The method considers the existing safeguards, which is considered as an advantage. The method defines threat as the combination of a threat agent, an exploitation method and a set of vulnerabilities and entities that suffer from them. For each threat, the method uses an opportunity value, calculated from the number of vulnerabilities associated with it. The EBIOS method does not make use

Table 13. Acceptance and Cost Criteria

	Acceptance	**Cost**	
Method/Criteria	Compliance with standards	Support cost	Software cost
EBIOS	ISO/IEC 27001, 15408-1:2009, 21827:2008	Free	Free
MEHARI	ISO/IEC ISO/IEC 27005:2011, 27001	Free + Open source	Free
OCTAVE	N/A	Free	€1300
IT-Grundschutz	ISO/IEC 27001	Free	€860
MAGERIT	ISO/IEC, 27002, 15408-1:2009, 27001	Free + Trial Version	€1500
CRAMM	ISO/IEC 27001	€1800-€3500	€1900-€3730
HTRA	N/A	Free	N/A
NIST SP800-30	ISO/IEC 27001	Free	N/A
RiskSafe	ISO/IEC 27001, HMG Security Policy Framework, The Baseline Control Set defined by HMG, PCI DSS, PSN Code of Connection, SANS Institute Top 20, Cloud Security Alliance's Cloud Controls Matrix	Pay per User	After contact
CORAS	ISO/IEC 27001, ISO31000	€95	Free

of scenarios, but follows a structured approach to identify and evaluate risk components. This gives it the advantage of a relatively flexible and exhaustive risk analysis, compared with other methods such as MEHARI, which are less flexible and use scenarios.

IT-Grundschutz contains detailed technical guidelines and general recommendations. Its steps are similar to those of CRAMM and MAGERIT. However, IT-Grundschutz does not focus on defining the project's context. It divides risk analysis into two levels, which allows faster execution of the whole process. Due to the time saving achieved, this characteristic is considered an advantage.

MAGERIT has the advantage that it can use either qualitative or quantitative calculations of risk. The method conducts risk calculation via predefined tables or algorithmic analysis. It separates the steps into more sub phases, which enhances the method with more flexibility compared to methods that strictly follow the standardization of four phases, such as CRAMM and IT-Grundschutz. MAGERIT does not make use of the concept of vulnerability, which can be regarded as disadvantage when compared to other methods. MAGERIT separates assets into nine categories and uses a scale with values from Minimum to Very High for the likelihood of realization of a threat. Threats valuation follows a different approach from most methods. To assess threats, MAGERIT defines a 5 metric table (potential, likelihood, easy, frequency), each with its own value range. This is considered as an advantage as it gives more granularity to the threat valuation. Also, the method calculates different types of risks, such as accumulated and deflected risk. This gives an advantage over methods such as CRAMM, IT-Grundschutz, and MEHARI, which calculate only one type of risk.

MEHARI is divided into eight steps, which adds complexity to the execution of the method. Its dependence on a knowledge base is not something that can be deemed as advantage or disadvantage, due to the fact that its creation can be either helpful or time consuming. This holds true as the steps of the method are closely dependent upon the use of the knowledge base, but on the other hand, the use of such database may help to accelerate the whole RA process. MEHARI uses scenarios to identify and assess risk, which are stored and modeled within its knowledge base. The analysts must choose the scenario that best fits in each situation. The scenarios are chosen based on the impact level, the type of the asset and the type and nature of the stake-holders. To calculate the severity of a given scenario, the residual impact and likely-hood are taken into account. These are calculated from the difference of the intrinsic impact and likelihood of an incident with the existing safeguards. The method utilizes questionnaires to calculate risk. Additionally, tables with untimely values for assessing risk and reducing agents are used. One could claim that the overall process of creating the knowledge base can be complicated and time consuming.

NIST SP800 is primarily a general standard and not a specific method. This can be considered as disadvantage as each organization may implement its guidelines in a different way. Nevertheless, NIST SP800 describes the risk management process based on three phases, which incorporate all the steps of the risk management process. The method focuses mainly on risk assessment and uses a scale with values Low, Medium, and High to evaluate risk. The fact that NIST SP800 considers the existing countermeasures is deemed as an advantage. However, the first phase involves nine steps, therefore increasing the complexity and the time that is needed.

OCTAVE uses all 4 RA phases. Each phase consists of workshops, in which all the necessary data is gathered, through the use of questionnaires. A relatively large number of employees is involved in each phase, which may increase the overall completion time. Another disadvantage is the fact that the existing safeguards are not taken into consideration. Contrary to other methods such as CRAMM, MAGERIT, MEHARI, and EBIOS, OCTAVE does not analyse and does not make recommendations of safeguards to mitigate risk. OCTAVE forms a threat profile for each asset, which matches the asset with security requirements, possible threats, vulnerabilities and impacts. These profiles are then extended into risk profiles with the addition of the impact of each threat. For the impact classification, a scale with Low, Medium, High values is used. Technical vulnerabilities are divided into nine classes (servers-hosts, wireless components, networking components, desktop workstations, storage devices, security components, other devices). The fact that the method is dependent on external tools to identify vulnerabilities of the system components for which no documentation is included, is considered as a limitation of the method.

RiskSafe turns risk assessment into a collaborative process, which is considered as an advantage over other methods. As a process, RiskSafe includes three phases, which is deemed as an advantage due to its simplicity. One of the method's advantages is the fact that the existing security countermeasures are included in the RA process. However, its collaborative approach requires good team management skills, which might increase the time needed for the completion of a project, if a good level of cooperation and coordination among the analysis team does not exist.

5.2 Compliance with Standards, Costs

With regards to the compliance criterion, this subsection summarises the methods' compliance with standards from ENISA (2006), omitting those that have been withdrawn and replaced by subsequent standards (e.g., BS7799 replaced by ISO/IEC 27001). More specifically, our analysis suggest that MAGERIT is the method that is compliant with the most standards (four international ISO/IEC standards in total). MAGERIT is followed by CRAMM, RiskSafe as well as IT-Grundschutz (see Table 13). CORAS is compliant with ISO/IEC 27001 and ISO31000 (Beckers et al. 2014). For OCTAVE and HTRA no sufficient information was found regarding their compliance with standards, either in their documentation or the relevant literature. As summarized in Table 13, most analysed methods comply with the international standard ISO/IEC 27001.

Table 14. Usefulness Criteria: Ease of Use, Life Cycle, and Scope

Category: Usefulness	**Ease of Use**	**Life Cycle**		**Scope**	
Method/Criteria	Overall Usability Level	Release	Last update	Target Organization	Focus
EBIOS	Unsatisfactory	1995	2004 (v2.0)	Small & Big	RA
MEHARI	Unsatisfactory	1998	2010 (MEHARI 2010)	Small & Big	RM
OCTAVE	Quite Satisfactory	1999	2005 (v2.0)	Small & Big	RA/RM
IT-Grundschutz	Quite Satisfactory	1997	2005 (v2.0)	Small & Big	RM
MAGERIT	Quite Satisfactory	1997	2013 (v3.0)	Small & Big	RA
CRAMM	Quite Satisfactory	1985	2011 (v5.1)	Small & Big (mostly big & governmental)	RA
HTRA	Unsatisfactory	2007	2007 (TRA-1)	Small & Big	RM
NIST SP800	Quite Satisfactory	2002	2002 (rev. 2012)	Small & Big	RM
RiskSafe Assessment	Quite Satisfactory	2012	2012 (v1.0)	Small & Big	RA
CORAS	Quite Satisfactory	2003	2010	Small & Big	RA

Considering the expenditures, at the time of writing this article, most methods are available for free with the exception of CRAMM and RiskSafe. CORAS is available free of charge and a book, which explains in detail the method, exists that costs €96. CRAMM requires an annual usage license with varying cost (from €312 for the basic version up to €1.000 for the full edition). The CRAMM Express software also requires an annual license that begins from €1.800 and can reach €3.500 for the full version. RiskSafe also provides software and access to documentation on a monthly charge.

MAGERIT's advantage against CRAMM and RiskSafe is the free access to its documentation, along with the 30 days free use of all supporting tools. Pilar, the commercial tool that supports MAGERIT, is provided in three different versions, each one with improved functionality. Its basic version costs €250 and each additional profile costs extra €150. The full version of Pilar costs €1500. Purchase of the supporting database and technical support is optional. Finally, the basic cost of €500 includes only qualitative analysis. EBIOS, MEHARI, and CORAS are provided for free along with their corresponding supporting tool. MEHARI is supported by the RISICARE tool, which is distributed by BUG SA. For the rest of the methods, a variety of supporting tools exist, with a price range between 250–700 euros, while the HTRA and NIST SP800 are not supported by such software.

The above mentioned are summarized in Table 13.

Table 15. Usefulness Criteria: Software Support, Training, Adaptability

Category: Usefulness	**Software Support**	**Training**			**Adaptability**
		Users*			
Method/Criteria	Software	M	O	T	Flexibility
EBIOS	EBIOS tool	✓	✓	✓	Relatively Flexible
MEHARI	MEHARI 2010 basic Tool (Free), RISCCARE	✓	✓	✓	Relatively Flexible
OCTAVE	Resolver Ballot	✓	✓	✓	Relatively Flexible
IT-Grundschutz	BSI - GSTOOl, HiScout SME, SAVe, IGSDoku, Secu-Max, Baseline-Tool, PCCheckheft	✗	✗	✓	Relatively Flexible
MAGERIT	μPilar, Pilar Basic, Pilar	✓	✓	✓	Relatively Flexible
CRAMM	CRAMM expert, CRAMM express	✓	✓	✓	No Flexibility
HTRA	N/A	✗	✗	✓	Relatively Flexible
NIST SP800	N/A	✗	✓	✓	Relatively Flexible
RiskSafe Assessment	SaaSRiskSafe Tool	✓	✓	✓	Relatively Flexible
CORAS	CORAS Tool	✓	✓	✓	No Flexibility

Note: M refers to Management, O to Operational, T to Technical. Management means that guidelines are given at a very generic level, Operational that guidelines contain details about the implementation suitable for most users and Technical means that guidelines contain mostly technical details.

5.3 Ease of Use, Life Cycle, Scope, Focus

The HTRA method is described with simple steps. However, its user guide is complicated and hard to comprehend by non-experts. In addition, the lack of technical depth and guidelines adds more difficulty in understanding the use of the method. As a result, the usability level is considered as unsatisfactory. CORAS is simple to use. Through the continuous board of directors' meetings the method attempts to reduce and handle any possible errors. However, it adds complexity, since it demands from analysts to use skills that have no relation to the information systems, such as communication skills. In general, this method is considered simple to understand and use. The disadvantage, though, is the need of continuous communication and cooperation between related parties, as it increases the time complexity of the process. Therefore, the usability level is considered relevantly satisfactory.

CRAMM suffers from the strict standardization of each step. The method can be used by non-qualified people, only after being trained. Additionally, the method is limited by its strict standardization. The method facilitates error detection, since at the end of each phase analysts can review the results. Therefore, the usability level is considered as relevantly satisfactory.

EBIOS is relatively simple and easy to understand. The fact that the available documentation is provided only in the French language is deemed as a disadvantage, as it makes the method difficult to learn and use, hence the usability level is considered as unsatisfactory.

IT-Grundschutz requires both technical and theoretical background. This is due to the fact that it was part of a standard, addressed to people with specialized knowledge in the field of security. It divides risk analysis and risk assessment in two levels, which makes it easier to use and can be adjusted to systems with different complexity levels. Also, it is supported by thorough guidelines and documentation and this levels the required specialized background. Usability level is considered relatively satisfactory.

MAGERIT provides technical documents that facilitate the method's understanding, both to experts and those who only have basic security background. The steps are considered to be simple and easily understood and supported by detailed documentation. However, certain sections of the documentation have not been translated from Spanish, referencing Spanish version of the documentation is a considerable limitation. Thus, its usability is considered as relatively satisfactory.

MEHARI is highly dependent in the creation of the knowledge base, which quite complicated and time consuming. The use of the knowledge base increases the difficulty of the method's use and introduces difficulties in understanding the whole process. Also, MEHARI can only be used with specialized calculation sheets or applications, which is a limitation. Hence, its usability level is considered as non-satisfactory.

NIST SP800 is a standard, within which a simple and flexible procedure of risk assessment is provided. It provides thorough documentation, which assists the understanding of the risk assessment. During the first assessment phase, the steps 2, 3, 4, and 6 can take place simultaneously, providing the option of data validation and ease error handling. Therefore, the usability level is considered relatively satisfactory.

OCTAVE is based upon the knowledge and the participation of the organization's employees. It provides sufficient documentation that facilitates the method's understanding. OCTAVE is considered simple that can be implemented even by non-security experts. Therefore, the usability level is considered as relevantly satisfactory.

RiskSafe is similar to CRAMM. Its documentation is not easily found, which is characterized as a limitation. However, the method is relatively simple and can be comprehended even by non-security savvy users. It can easily comply with and support security standards and governmental directives. In addition, the facilitation of collaboration between analysts provides an ad hoc confrontation of any errors and data supply feedback. Thus, the usability level is regarded as relevantly satisfactory.

HTRA was released in 2007 however no further updates were found ever since and the method is not providing any software/tool. On the contrary, CORAS was created in 2003, but in 2011 it was updated, adding up-to date-safeguards, threats, and vulnerabilities. CRAMM is considered outdated as it was last updated in 2011. It is considered, though, more up to date than HTRA. EBIOS was created in 1995 and the last update was in 2010, thus it is considered outdated.

IT-Grundschutz was created in 1997 and last updated in 2005. It is considered obsolete especially compared to CRAMM and EBIOS, which were last updated in 2011 along with their relevant tools. There is a plethora of tools supporting IT-Grundschutz, but most have not been updated since 2004. MAGERIT was created in 1997 and was recently updated (2013), therefore, it is the most updated method. At the same time, its supporting tools are often being updated to comply with modern security requirements and demands.

Similarly to EBIOS, MEHARI was created in 1998 and was last updated in 2010. NIST SP800-30 is considered outdated as it was last updated in 2012 (it was released in 2001). However, it is the second most updated method after MAGERIT. OCTAVE was created in 1999 and last updated in 2005. RiskSafe method was created in 2012 and since then, has not been updated.

In summary, MAGERIT, NIST SP800, CRAMM, and RiskSafe are the methods that have been more recently updated. Among them, CRAMM is considered as the most obsolete, as the method and its supporting tools do not seem to receive the same amount of updates or attention from the organization that maintains it, compared to the other three abovementioned methods. MAGERIT is considered as the most updated method. Furthermore, EBIOS and MEHARI, even though they have not been updated since 2010, are still actively supported by large organizations such as CLUSIF and ANSSI.

5.4 Software Support, Training, Adaptability

Most of the RA methods that have been examined provide software/tools that facilitate their use. The HTRA and NIST SP800 are the only methods that did not provide such a tool. MEHARI only provides a purposely built, Microsoft Office Excel spreadsheet, which is both restrictive and disadvantageous. This holds true, as the spreadsheet provide limited functionality compared to software/tool. As discussed earlier, various tools exists that support IT-Grundschutz. However, this does not imply that the method has an advantage over other methods, such as CRAMM, MAGERIT, MEHARI, and RiskSafe. Regardless of the number of supporting tools, a method may have sufficient level of support with fewer or only one dedicated and updated tool.

These methods that have been examined require different experience and skills from their users. More specifically, MAGERIT, CORAS, MEHARI, and OCTAVE require their users to have experience in risk assessment and have at least practical experience in the field of security. CRAMM and RiskSafe require more specialized knowledge and experience. EBIOS and NIST SP800-30 are tailored to administrators, but they can also be used by most users, since they contain enough detail for the risk analysis and RA process. However, they do not include technical or organizational and human aspects of security of information systems. All the above mentioned methods require users to have expertise in risk assessment.

The HTRA method focuses on people who will perform the analysis and assessment process. It contains enough implementation details, but provides only limited technical depth when compared to other methods. The method only requires basic IT skills for its use. In contrast, IT-Grundschutz requires expert skill level for its use, specifically experience and expertise in security and is suitable primarily for use by individuals with specialized backgrounds, both technical and theoretical.

Regarding the flexibility and adaptability of the methods, HTRA has been designed to be flexible. Each phase contains clearly defined steps, which are supported by the use of tables. It can be adjusted to the needs of different organizations and their systems, regardless of their size and complexity. On the other hand, the procedure of completing all the assessment tables is a double-edged sword, as experienced analysts regard this as a time consuming and cumbersome process. Although not supported by a tool, the method provides automation. Therefore, the method is considered as relatively flexible.

CORAS uses its own modelling language and supporting diagrams. This helps the iterative collaboration and communication; however, the small set of symbols may be quite restrictive on its flexibility. The fact that it is supported by an open source tool is considered as an advantage as each organization can adjust it to its needs. The dependence on its diagrams, though, decreases the method's flexibility. This holds true as an analyst has to use a restrictive set of diagrams and must have expertise in the use of UML. Thus, the method is considered as non-flexible.

CRAMM is considered non-flexible due to its strict standardization in each step, which restricts analysts. In addition, the dependence to a single tool, the CRAMM tool, which is not free decreases the flexibility of the method.

The modular design of EBIOS, enable the method to be easily adapted to conform to national security standards. The method can be used in both the design of a system and on existing information systems. Also, it is supported by a free tool, which is relatively simple to use. Therefore, the method is relatively flexible and an analyst can easily adapt it to the needs of each use case.

The two-tier approach of IT-Grundschutz allows scaling the method in different size and complexity systems. The fact that specialized background is required for the use of the method is judged to be disadvantageous. Therefore, the methodology is considered as relatively flexible.

MAGERIT covers all aspects of a complete risk analysis process. The method presents a flexible RA procedure that can be applied both qualitatively and quantitatively. The method also provides the calculation of three types of risks while others such as CRAMM, the EBIOS or MEHARI calculate only one. Also, threats can be estimated either by the use of tables or algorithmic. The fact that the method can be applied only by using the EAR/Pilar tool is considered disadvantageous, but nevertheless it is considered as relatively flexible.

MEHARI describes a complex process that it is highly dependent on the creation of a knowledge base. It is designed to utilize the knowledge base, which means that it can only be used in conjunction with a special tool or a dedicated spreadsheet designed for this reason. The method devotes enough time in the creation of a knowledge base. The over-reliance on it is considered as disadvantage. The method provides relatively flexible steps for the RA phase, since it allows the analyst make the necessary changes so that they suit the needs of the organization. Despite the dependence on the creation and use of knowledge base the RA process is considered as being relatively flexible.

NIST SP800 provides a generic risk management method, which is based on the expertise and knowledge the analysts possess and their cooperation with the management and system operators. Therefore, it allows a relatively large flexibility to the analyst. Also, it provides generic guidelines that can be adapted to the needs of an organization. For these reasons, the method described in NIST SP800 is considered as relatively flexible.

OCTAVE can be adapted to the needs of each organization, while providing different versions that take into consideration the organization's size and the complexity. The method's steps are considered relatively flexible, allowing the adaptation to the project, based solely on the available resources of the organization. OCTAVE also allows the participation of external experts while relying on the skills of employees in the organization. Unlike other methods, such as CRAMM, MAGERIT, or MEHARI, it does not include the step of risk mitigation and the recommendation of safeguards. Overall it is a relatively flexible method, able to adapt to any specific situation.

The RiskSafe resembles CRAMM. However, the method supports collaborative processing of risk analysis via the Cloud and can easily support different standards beyond ISO/IEC 27001. The company that maintains the method provides guidance for compliance with other security standards and how can risk analysis easily be carried out with 10 steps. The tool that supports the method allows adding options and editing existing parameters, such as adding or editing threats. The method is relatively flexible.

Overall, as the results suggest most of the methods that have been analysed provide a sufficient level of flexibility. Nonetheless, it is worth noting that MAGERIT and RiskSafe suggest a fairly flexible valuation of risk, while providing the right tools to support it. RiskSafe is unique as it provides cooperative risk assessment via the Cloud. MAGERIT is the only method that supports both qualitative and quantitative risk analysis and is also supported by a fairly versatile tool.

5.5 Case Study

This subsection demonstrates the selection of a RA method based on the proposed comparison criteria. The case study refers to the SME sector in the UK, where based on literature (Henson

$$\begin{array}{r|cccc|} & \text{Cost} & \text{Validity} & \text{Usefulness} & \text{Compliance} \\ \text{Cost} & 1/1 & 2/1 & 3/1 & 4/1 \\ \text{Validity} & 1/2 & 1/1 & 2/1 & 3/1 \\ \text{Usefulness} & 1/3 & 1/2 & 1/1 & 2/1 \\ \text{Compliance} & 1/4 & 1/3 & 1/2 & 1/1 \end{array}$$

Fig. 1. Relative importance matrix.

and Garfield 2016), we need to turn estimations of the sector regarding the criteria, into ranking among them.

To this end, the Analytical Hierarchy Process (AHP) (Smojver 2011) is utilised, an approach that can be used to address problems involving selections based on multiple criteria. It is assumed that an SME uses AHP to select the appropriate method for Risk Assessment, considering the proposed criteria: validity, compliance, cost and usefulness. For readability reasons, we assume that the SME is considering only CRAMM, CORAS, MEHARI, and OCTAVE as alternatives available for the method selection.

Initially, AHP is applied to rank the four aforementioned criteria. Then, the same process is applied to rank the methods for each criterion. To rank the criteria, AHP requires that the relative importance among the criteria is defined. Based on Henson's and Garfield's (2016) work, we define the following relative importance among the criteria: (a) "Cost" is two times more important than "Validity," as SMEs attempt to limit expenses, (b) "Validity" is two times more important than "Usefulness," (c) "Cost" is four times more important than "Compliance," as they consider that standards are important only for large businesses, (d) "Usefulness" is two times more important than "Compliance," (e) "Validity" is three times more important than "Compliance," and (f) "Cost" is three times more important than "Usefulness." The following matrix (Figure 1) is formed based on the aforementioned.

By multiplying the matrix with itself, we get the eigenvector that contains the ranking of the criteria.

$$\begin{bmatrix} 1{,}000 & 2{,}000 & 3{,}000 & 4{,}000 \\ 0{,}500 & 1{,}000 & 2{,}000 & 3{,}000 \\ 0{,}333 & 0{,}500 & 1{,}000 & 2{,}000 \\ 0{,}250 & 0{,}333 & 0{,}500 & 1{,}000 \end{bmatrix} * \begin{bmatrix} 1{,}00 & 2{,}000 & 3{,}000 & 4{,}000 \\ 0{,}500 & 1{,}000 & 2{,}000 & 3{,}000 \\ 0{,}333 & 0{,}500 & 1{,}000 & 2{,}000 \\ 0{,}250 & 0{,}333 & 0{,}500 & 1{,}000 \end{bmatrix} = \begin{bmatrix} 4{,}000 & 6{,}833 & 12{,}000 & 20{,}000 \\ 2{,}416 & 4{,}000 & 7{,}000 & 12{,}000 \\ 1{,}416 & 2{,}333 & 4{,}000 & 6{,}833 \\ 0{,}833 & 1{,}416 & 2{,}416 & 4{,}000 \end{bmatrix}$$

Then, we add each row's sum and normalize the values by diving each sum with the total one.

$$\begin{bmatrix} 42{,}833 \\ 25{,}416 \\ 14{,}583 \\ 8{,}666 \end{bmatrix} \xrightarrow[\text{normalization}]{} \begin{bmatrix} 0{,}284 \\ 0{,}094 \\ 0{,}449 \\ 0{,}171 \end{bmatrix}$$

The result ranks the criteria with the following order: (a) Cost, (b) Validity, (c) Usefulness, and (d) Compliance.

Following, we apply the same procedure for each criterion for the available alternatives (i.e., the RA methods) to rank them appropriately. We demonstrate the process for Usefulness criterion.

$$\begin{array}{c|cccc|} & \text{CORAS} & \text{Octave} & \text{CRAMM} & \text{Mehari} \\ \text{CORAS} & 1/1 & 1/2 & 2/1 & 2/1 \\ \text{Octave} & 2/1 & 1/1 & 2/1 & 2/1 \\ \text{CRAMM} & 1/2 & 1/2 & 1/1 & 2/1 \\ \text{Mehari} & 1/2 & 1/2 & 1/2 & 1/1 \end{array}$$

Fig. 2. Usefulness relative importance matrix.

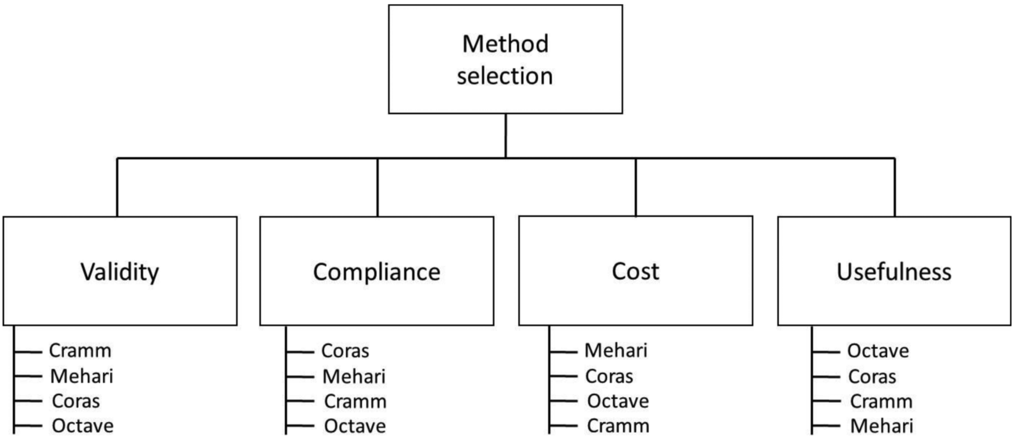

Fig. 3. Criteria ranking.

We, again, define the following relative importance among the alternatives: (a) OCTAVE is two times more useful than CORAS, (b) OCTAVE is two times more useful than CRAMM, (c) CRAMM is two times more useful than MEHARI, (d) CORAS and CRAMM are considered to have the same usefulness level between them, (e) CORAS is two times more useful than MEHARI, and (f) OCTAVE is two times more important than MEHARI. The following matrix (Figure 2) is formed based on the aforementioned.

By multiplying the matrix occurred with itself, we get the eigenvector that contains the ranking of the alternative methods. For Usefulness, the alternatives are ranked with the following order: (a) OCTAVE, (b) CORAS, (c) CRAMM, and (d) MEHARI.

Applying the same approach for each criterion, we get the final outcome of the ranking process, which is presented in Figure 3. This allows an SME to choose the desired RA method based on the criteria that the company considers as most important. In this case study, MEHARI would be a desirable selection, with CORAS being second in ranking, based on the requirements set by such a company, as they rank highly in the “Cost” criterion.

6 CONCLUSIONS

This work examined and presented a set of criteria for the comparison of RA/RM methods, which was identified as a need by the state of the art review. The criteria allow analysts and organizations to determine which method is best for their needs. The proposed criteria are grouped into four categories: validity, acceptance, cost, and usefulness. Each category includes more sub-criteria that are used to compare ten widely used RA methods. The selection of the methods was made in relation to specific factors, such as their popularity, e.g., their use from organizations and governments, agencies, such as NIST, or standardization bodies, such as ISO and recognition by the relevant scientific community.

Implicit guidelines on how organizations should select the most appropriate RA method based on comparison criteria is missing from the literature. Consequently, this work demonstrates a ranking method using the proposed comparison criteria. The ranking adjusts in accordance to each organization's needs. This holds true as organizations' security needs vary according to factors, such as their type, size or the environment they operate in, which affects the importance of each criterion. The comparison results of the RA methods, which are summarised in Tables 13 to 16, can be used by an organization as input in a ranking method (e.g., AHP) to select the most appropriate method tailored to its needs. In our work, this ranking is demonstrated in a case study for SMEs in the UK using the Analytical Hierarchical Process.

For future work, we plan to evaluate the criteria that have been presented in this work in conjunction with AHP using organizations of the public and private sector to examine the importance of each criterion with regards to its type and also verify that the indicated method would suit their needs.

ACKNOWLEDGMENTS

The authors thank Christina Saravanou and George Antoniou for their help during the early stages of drafting this article.

REFERENCES

Jan Øyvind Aagedal, Folker den Braber, Theo Dimitrakos, Bjørn Axel Gran, Dimitris Raptis, and Ketil Stolen. 2002. Model-based risk assessment to improve enterprise security. In *Proceedings of the 6th Enterprise Distributed Object Computing Conference*, 2002, 51–62.

Walid Al-ahmad and Bassil Mohammad. 2013. Addressing information security risks by adopting standards. *Int. J. Info. Secur. Sci.* 2, 2.

Christopher Alberts and Audrey Dorofee. 2003. Introduction to the OCTAVE approach. Carnegie Mellon University, Pittsburgh, PA.

M. A. Amutio, J. Candau, and J. Mañas. 2014. MAGERIT—Version 3, methodology for information systems risk analysis and management. *Book I—The Method, Ministerio de Administraciones Publicas.*

ANSSI: Agencenationale de la sécurité des systems d' information. 2010. Ebios 2010 - expression of needs and identification of security objectives. Retrieved from http://www.ssi.gouv.fr/en/the-anssi/publications-109/methods-to-achieve-iss/.

ASIS International Guidelines Commission. 2003. General security risk assessment: An ASIS International Guideline. ASIS International, Alexandria, VA.

Kakoli Bandyopadhyay, Peter P. Mykytyn, and Kathleen Mykytyn. 1999. A framework for integrated risk management in information technology. *Manage. Decis.* 37, 5, 437–445.

Kristian Beckers, Heisel Maritta, Solhaug Bjornar, and Stolen Ketil. A structured method for establishing an ISO 27001 compliant information security management system. In *Engineering Secure Future Internet Services and Systems*, Springer International Publishing, 315–344.

R. M. Blank and P. D. Gallagher. 2012. NIST special publication 800-30 revision 1 guide for conducting risk assessments.

Alan Calder and Steve G. Watkins. 2010. Information security risk management for ISO27001/ISO27002. It Governance Ltd.

P. L. Campbell and J. E. Stamp. 2004. A classification scheme for risk assessment methods. United States. Department of Energy.

R. A. Caralli, J. F. Stevens, L. R. Young, and W. R. Wilson. 2007. The OCTAVE allegro guidebook, v1.0, Software Engineering Institute.

CERT (Computer Emergency Response Team). 2008. Octave (operationally critical threat, asset, and vulnerability evaluation). Retrieved from http://www.cert.org/octave.

CLUSIF: Club de la Sécurité de l'Information Français. 2010. Mehari: Information risk analysis and management methodology. Retrieved from http://www.clusif.asso.fr/en/production/mehari/index.asp.

CORAS Tool, The Coras Tool. 2012. Retrieved from http://coras.sourceforge.net/coras_tool.htm.

CRAMM: UK Government, Security Service. 2010. CRAMM User Guide, Issue 5.2.

CSE: Communications Security Establishment. 2007. Harmonized threat and risk assessment (TRA) methodology, TRA-1.

Sadegh Derakhshandeh and Nasser Mikaeilvand. 2011. New framework for comparing information security risk assessment methodologies. *Aus. J. Basic Appl. Sci.* 5, 9, 160–166.

Tianxi Dong and Surya Yadav. 2014. A comprehensive framework for comparing system security assessment methods. In *Proceedings of the 20th Americas Conference on Information Systems*.

ENISA. 2006. Risk management: Implementation principles and inventories for risk management/risk assessment methods and tools. Retrieved from https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-methods.

ENISA ad hoc working group on risk assessment and risk management. 2006. Risk assessment and risk management methods: Information packages for small- and medium-sized enterprises (SMEs), 12–20.

ENISA. 2012. Introduction to return on security investment. Retrieved from http://www.enisa.europa.eu/activities/cert/otherwork/introduction-to-return-on-security-investment.

Baruch Fischhoff, Sara Lichtenstein, Paul Slovic, Stephen L. Derby, and Ralph L. Keeney. 1984. *Acceptable Risk*. Cambridge University Press.

W. M. Garrabrants, A. W. Ellis, L. J. Hoffman, M. Kamel, and D. C. Washington. 1990. Certs : A comparative evaluation method for risk management methodologies and tools. In *Proceedings of the 6th Annual Computer Security Applications Conference*. IEEE, 251–257.

German BSI. 2014. BSI standards 100-1, 100-2, 100-3, 100-4. Retrieved from https:// www.bsi.bund.de/EN/Publications/BSIStandards/standards.html.

Yacov Y. Haimes, Nicholas C. Matalas, James H. Lambert, Bronwyn A. Jackson, and James F. R. Fellows. 1998. Reducing vulnerability of water supply systems to attack. *J. Infrastruct. Syst.* 4, 4, 164–177.

Sharon Halliday, Karin Badenhorst, and Rossouw Von Solms. 1996. A business approach to effective information technology risk analysis and management. In *Info. Manage. Comput. Secur.* 4, 1, 19–31.

Richard Henson and Joy Garfield. 2016. What attitude changes are needed to cause SMEs to take a strategic approach to information security ? In *Athens J. Bus. Econ.* 2, 3303–318.

Siv Hilde Houmb. 2007. Decision support for choice of security solution: The aspect-oriented risk driven development (AORDD) framework. PhD thesis, Norwegian University of Science and Technology, Trondheim, Norway.

Information Security Management. 2013. Report ISMS-CORAS : A Structured Method for.

Dan Ionita. 2013. Current established risk assessment methodologies and tools. Master Thesis, University of Twente, Enschede, Netherlands.

Stuart W. Katzke. 1988. A government perspective on risk management of automated information systems. In *Proceedings of 1988 Computer Security Risk Management Model Builders Workshop*. 3–20.

K. V. D. Kiran, L. S. S. Reddy, and N. Lakshmi Haritha. 2013. A comparative analysis on risk assessment information security models. *Info. J. Comput. Appl.* 82, 9, 41–47.

Barbara Kitchenham, Stephen Linkman, and David Law. 1997. DESMET: A methodology for evaluating software engineering methods and tools. *Comput. Control Eng. J.* 8, 3, 120–126.

Matus Korman, Teodor Sommestad, Jonas Hallberg, Johan Bengtsson, and Mathias Ekstedt. 2014. Overview of enterprise information needs in information security risk assessment. In *Proceedings of the IEEE 18th International Enterprise Distributed Object Computing Conference (EDOC'14)*. IEEE, 42–51.

Jake Kouns and Daniel Minoli. 2010. *Information Technology Risk Management in Enterprise Environments: A Review of Industry Practices and a Practical Guide to Risk Management Teams*. John Wiley & Sons.

Sharman Lichtenstein. 1996. Factors in the selection of a risk assessment method. In *Info. Manage. Comput. Secur.* 4, 20–25.

David López, Oscar Pastor, Luis Javier, and García Villalba. 2013. Dynamic risk assessment in information systems: State-of-the-art. In *Proceedings of the 6th International Conference on Information Technology*.

Mass Soldal Lund, Bjørnar Solhaug, and Ketil Stølen. 2011. Model-driven risk analysis: The CORAS approach. Springer Science & Business Media.

Filipe Macedo and Miguel Mira Da Silva. 2012. Comparative study of information security risk assessment models, Instituto Superior Técnico, UniversidadeTécnica de Lisboa, Lisboa, Portugal.

Daniel Mellado, Eduardo Fernández-Medina, and Mario Piattini. 2007. A common criteria-based security requirements engineering process for the development of secure information systems. *Comput. Stand. Interfaces* 29, 2, 244–253.

Miley W. Merkhofer. 1985. An approach for assessing health risks associated with alternative ambient air quality standards. In *Environmental Impact Assessment, Technology Assessment, and Risk Analysis*. Springer, 691–722.

Robert R. Moeller. 2004. Sarbanes-oxley and the new internal auditing rules. John Wiley & Sons.

Girish Karunakaran Nair. 2013. Influence of risk assessment factors on the tourism performance in qatar: An empirical study. *Amer. J. Tourism Res.* 2, 2, 141–153.

NATO: North Atlantic Treaty Organization. 2008. Review of existing methodologies. In *Improving Security Risk Analysis*, TR-IST-049.

Michael Nidd, Marieta Georgieva Ivanova, Christian W. Probst, Axel Tanner, Ryan Ko, and Raymond Choo. 2015. Tool-based risk assessment of cloud infrastructures as socio-technical systems. *Cloud Security Ecosystem Syngress.*

NIST S 800-30. 2012. Guide for conducting risk assessments. 800–830. Revision 1.

T. William Olle, A. A. Verrijn Stuart, and Love Bhabuta. 1988. Computerized assistance during the information systems life cycle. In *Proceedings of the IFIP WG 8.1 Working Conference on Computerized Assistance During the Information Systems Life Cycle (CRIS 88).* North Holland.

Liuxuan Pan and Allan Tomlinsont. 2016. A systematic review of information security risk assessment. *Int. J. Safety Security Eng.* 6, 2, 270–281.

Santosh K. Pandey. 2012. A comparative study of risk assessment methodologies for information systems. *Bull. Electric. Eng. Info.* 1, 2, 111–122.

Platinum Squared. 2014. Risksafe assessment-cloud based risk assessment. Retrieved from http://risksafe.co.uk/Usage/Operation.

Dimitris Raptis, Theo Dimitrakos, Bjørn Axel Gran, and Ketil Stølen. 2002. The CORAS approach for model-based risk management applied to e-commerce domain. In *Advanced Communications and Multimedia Security.* Springer, 169–181.

Atle Refsdal, Bjørnar Solhaug, and Ketil Stølen. 2015. Cyber-risk management. In *Cyber-Risk Management.* Springer, 33–47.

Matthew Rosenquist. 2009. Prioritizing information security risks with threat agent risk assessment. Intel Corp. White Paper.

Thomas L. Saaty. 1988. What is the analytic hierarchy process? In *Mathematical Models for Decision Support.* Springer, 109–121.

Mario Sajko, Nikola Hadjina, and Darija Pešut. 2010. Multi-criteria model for evaluation of information security risk assessment methods and tools. In *Proceedings of the 33rd International MIPRO Convention*, 1215–1220.

Markus Schumacher, Eduardo Fernandez-Buglioni, Duane Hybertson, Frank Buschmann, and Peter Sommerlad. 2013. Security patterns: Integrating security and systems engineering. John Wiley & Sons.

Louis Shallal. 2013. A generalized approach to threat risk assessment (TRA). White Paper.

Alireza Shameli-Sendi, Rouzbeh Aghababaei-Barzegar, and Mohamed Cheriet. 2016. Taxonomy of information security risk assessment (ISRA). *Comput. Secur.* 57, 14–30.

Slaven Smojver. 2011. Selection of information security risk management method using analytic hierarchy process (AHP). In *Proceedings of the Central European Conference on Information and Intelligent Systems (CECIIS'11).*

Diomidis Spinellis, Spyros Kokolakis, and Stefanos Gritzalis. 1999. Security requirements, risks and recommendations for small enterprise and home-office environments. *Info. Manage. Comput. Secur.* 7, 3, 121–128.

Gary Stoneburner, Alice Y. Goguen, and Alexis Feringa. 2002. Risk management guide for information technology systems. *Nist Special Publication*, 800(30).

Ali Sunyaev. 2011. Analysis of IS security analysis approaches. In *Health-Care Telematics in Germany: Design and Application of a Security Analysis Method.* GABLER, 83–117.

Amril Syalim, Yoshiaki Hori, and Kouichi Sakurai. 2009. Comparison of risk analysis methods: Mehari, magerit, NIST800-30 and microsoft's security management guide. In *Proceedings of the International Conference on Availability, Reliability and Security (ARES'09).* 726–731.

Liesl Van Niekerk and Les Labuschagne. 2006. The peculium model: Information security risk management for the South African SMME. Retrieved from http://icsa.cs.up.ac.za/issa/2006/Proceedings/Full/12-Paper.pdf.

Anita Vorster and L. E. S. Labuschagne. 2005. A framework for comparing different information security risk analysis methodologies. In *Proceedings of the 2005 Annual Research Conference of the South African Institute of Computer Scientists and Information Technologists on IT Research in Developing Countries.* 95–103.

Gaute Wangen. 2017. Information security risk assessment: A method comparison. *Computer* 50, 4, 52–61.

Gaute Wangen, Christoffer Hallstensen, and Einar Snekkenes. 2016. A framework for estimating information security risk assessment method completeness. *Int. J. Info. Secur.* 1–19.

Zeki Yazar. 2002. A qualitative risk analysis and management tool—CRAMM, GSEC, Version 1.3, as part of the Information Security Reading Room.

Emmanuele Zambon, Sandro Etalle, Roel J. Wieringa, and Pieter Hartel. 2011. Model-based qualitative risk assessment for availability of IT infrastructures. *Softw. Syst. Model* 10, 4, 553–580

Received January 2016; revised June 2017; accepted September 2017