Security Journal
https://doi.org/10.1057/s41284-023-00389-y

ORIGINAL ARTICLE

How do professionals assess security risks in practice? An exploratory study

William Harris[1] · **Moufida Sadok**[1]

Accepted: 23 June 2023

Abstract

There are a number of standards and frameworks for security risk assessment; however, it appears that their application and adaptation to real organisational practices are rather limited. This paper reports some results from inquiries into risk assessment practices of security professionals in Ireland. The key findings show a lack of consensus on basic terminology when it comes to defining risk and risk assessment. The interviewed security professionals have developed varied approaches in practice and rather refer to their intuition and previous experiences. While the paper focuses on Ireland, the lack of consensus regarding the definition, and use of security terminology and practices, especially in the area of security risk management, is not necessarily limited to Ireland.

Keywords Security risk assessment · International risk standards · Security professional · Operational risk · Professional practices · ISO 31000

Introduction

Risk assessment is a key activity that should be performed by all organisations (Munodawafa 2018). Managing risk exposure is critical to organisational security, resilience, and business continuity to address evolving threats in a complex global landscape; Covid19 has merely reinforced the necessity to identify, understand, and implement an adaptive approach to undertaking risk assessments (Khunti et al. 2021). Organisations that fail to conduct a rigorous risk assessment process may experience significant negative impacts, in terms of reputational damage, legal issues, and financial losses (Sendi et al. 2016).

✉ Moufida Sadok
moufida.sadok@port.ac.uk

William Harris
WILLIAM.Harris3@myport.ac.uk

[1] School of Criminology and Criminal Justice, University of Portsmouth, St George's Building, 141 High Street, Portsmouth PO1 2HY, UK

Published online: 10 July 2023

In practice, there is no absolute rule on how a risk assessment should be performed (Ostrom et al. 2019), and organisations can choose between several published methodologies and frameworks in the field of security risk management. These methodologies include those specified by Roper (1999), where he outlines a process incorporating the identification of assets, threats, and vulnerabilities as inputs into the assessment of security risks. Biringer et al. (2007) suggest a more quantitative approach based on the following equation: [likelihood] × [system effectiveness] – [adversary success rate] × [consequences of loss]. This approach based on probabilistic reasoning requires a significant amount of data that are not always readily available to security professionals when undertaking a security risk assessment. Further, Allen (1987) highlights the limited effectiveness of quantitative algorithms such as the product of probabilities and consequences to understand risk due to its multidimensional nature. Talbot and Jakeman (2009) outline in a diagrammatic format an expansion of AS/NZS 4360:2004 Risk management process for undertaking security risk assessments with some additional inputs into the overall process. Within this format, the most widely adopted security risk assessment process is that outlined in HB 167:2006, Security Risk Management (2006).

Consideration needs to be given to the contention by Brooks (2011) that security risk management is somehow different from other forms of risk management and those generic risk standards such as ISO 31000:2018 Risk Management – Guidelines (referred to as ISO 31000) and COSO 2017, Enterprise Risk Management, Integrating with Strategy and Performance (referred to as COSO 2017) do not specify the key concepts necessary for the management of security risks. The standards only outline a general process and approach and not the specific variables associated with undertaking a security risk assessment; this could create a practical difficulty for security professionals, in particular, as to how to facilitate the integration of security as a field of risk management into the overall risk management approach specified in relevant international standards. Although set out as generic guidelines, security professionals still consider these standards to lack pragmatism for effective design application and mitigation of security risks (Brooks 2011).

It is worth mentioning here that a key differentiator in managing security risks is based on the contention that security risk management is focused on deliberate, malicious, and unwanted actions of people directed towards organisational assets (Harding, 2016; Koien. 2020). This study focuses on operational risk and explores current practices employed by security professionals while undertaking security risk assessments in Ireland.

The remainder of the paper is organised as follows. The next section identifies past research related to security risk assessment. Section three summarises the research method and design and provides details about data collection process and data analysis method. Section four presents the key findings of the empirical study. Those findings illustrate important patterns in security risk assessment practices and will be discussed in section five. The final section draws some conclusions and suggests future areas of research.

Background research

The literature review is organised around three main themes: theories on the nature of risk, theories on the nature of security risk, and approach(es) to the practice of assessing security risk. Overall, this literature review shows that there is no single definition of risk or approach to conducting a security risk assessment. However, very little of the literature provides an explanation of how to address the lack of adoption and applicability of security risk assessment standards in practice.

Defining risk

This paper focuses on risk perception which is the process of collecting, selecting, and interpreting the signals about uncertain impacts of events, activities, or technologies (Slovic 1987; Wachinger et al. 2010). Although risk perception is central to the human experience, risks are perceived differently depending on social, political, and cultural factors (Renn and Rohrmann 2000). Wachinger et al. (2013) suggest that factors such as knowledge, experience, values, attitudes, and emotions influence the thinking and judgement of individuals about the seriousness and acceptability of risks. Further, Slovic et al. (2004) argue that the "experiential system" based on intuition remains the most natural and most common way to comprehend risk. Renn and Rohrmann (2000) state that social sciences are still struggling with risk perception which could explain the difficulty in developing an agreed-upon definition of the concept of risk (Aven and Renn 2009; Aven 2012; Andretta 2014; Haimes 2009).

At an organisational level, the categorisation of risks varies from organisation to organisation but there are some commonalities when it comes to strategic, operational, and financial risks (Ward 2005). Sadgrove (2015) adds to this list by including compliance, people, and technology risks. Each risk category comprises a number of fields of risk; these might include liquidity, credit, currency, treasury, and interest risk under financial risk. Operational risk—the focus of this paper—is primarily concerned with the uncertainty inherent in the execution of organisational activities (Raz and Hillson 2005) based on people, processes, and procedures (Hutchins 2018). Operational risk comprises the fields of risk such as insurance, health and safety, business continuity, and security (Tattam 2011). Operational risks are generally managed within the control of the organisation through risk assessment and risk management practices (Matthews 2008).

The lack of clarity around the definition of the concept of risk permeates through the disciplines of risk management including the field of security. For example, Wangen et al. (2018) raise the issue of an ambiguous use of language for describing threats while undertaking security risk assessments. Manunta (1999) suggests a consistent use of terminology to convey a common meaning and Spring et al. (2017) recommend having a set of basic concepts through which the security community can develop a shared understanding.

Security risk assessment

Prior to exploring the concept of security risk assessment, an overall analysis of the term risk assessment would bring about a clear delineation between pre- and post-1995 definitions. This contention is based on the publication in 1995 by Standards Australia, of AS/NZ 4360: 1995 'Risk Management Standard' which outlined in diagrammatic form a risk management overview which included the identification, analysis, evaluation, and treatment of risk. However, it only included *risk analysis* and *evaluation* in the risk assessment process and was further developed to include *risk identification* in later Australia-published standards AS/NZ 4360: 1999 and again by AS/NZ 4360: 2004 Risk management standard. Publication of HB: 167:2006 'Security Risk Management' Handbook was based on the specific requirements of AS/NZ 4360:2004 but concentrated on the application of the standard to the field of security risk management. The security handbook also identified some fundamentally important components of an effective security risk assessment: identification of critical assets; identification of threats to those assets based on the capabilities and intent of adversaries; and finally the vulnerabilities of the assets to the threats posed. Adoption and integration of the components of an effective security risk assessment process by HB: 167:2006 into a generic risk management standard are a significant step in identifying security as a subset of risk, and clarifying how and where security variables are inputted into the overall risk assessment process. Since the publication of HB: 167:2006, the overall discipline of risk management has evolved leading to a requirement for the approach to undertaking security risk assessments in accordance with the international standards to be adopted further.

An evaluation of the two internationally recognised risk management standards shows that the adoption of ISO 3000:2018 advocates for the management of risk, based on the principles, framework, and processes outlined in the document. It notes that these components may already exist in full or in part within the organisation and irrespective of the current situation they can be implemented in any industry or sector and applied to any activity including undertaking security risk assessments (ISO 31000:2018). The undertaking of security risk assessments within the current ISO 31000 standard takes place during the 'process' stage and involves identification and explanation of the security risk context simultaneously while establishing the internal and external context evaluation. Similarly, within the COSO 2017 standard, the adoption of the 'process' component of the standard is critical as it deals with the identification and assessment of risks that may affect the ability of the organisation to achieve its stated objectives.

Situating security as a subdomain of the overall risk management discipline (Smith and Brooks 2013) and as an essential part of any individual's, organisation's or community's wider risk management activity (Talbot and Jakeman 2009) begins to develop an understanding of the interconnectivity of the field of risk management and the multiple contextually dependant activities where risk assessments are carried out. The field of security risk can be further developed where a number of specialist areas or security model elements such as physical security, information security, personnel security, logistics, and cyber security are included (ASIS International 2009).

With the publication of risk standards, there is still little evidence that the prescribed risk assessment process as outlined in the standards has been widely adopted by the security sector. This can be evidenced through the publication of books such as 'The Security Risk Assessment Handbook' (Landoll 2006) where it is noted that security risk assessment is 'an objective analysis of the effectiveness of the current security controls that protect an organisations asset'. At the same time, Sadgrove (2015) notes that the risk assessment should 'examine the project's sensitivity to various factors', while Vellani (2020) identifies a risk assessment as 'the process of identifying and prioritising risks' in the same paragraph it is noted that a 'risk assessment is the foundation for prioritising risks in order to effectively implement countermeasures'. These publications all differ in their use of terminology to define the term 'risk' and all advocate for differing risk assessment methodologies.

Security risk assessment in practice

Adoption of risk management standards and guidelines is expected to support security professionals in identifying risks in a structured and systematic manner ensuring identified risks facing the organisation are handled. Research suggests that the adoption of a defined risk assessment process provides a consistent and systematic approach to the assessment and treatment of risks (Govender 2018) while ensuring a consistent language is achieved (Brooks 2011).

However, the diversification of approaches has contributed significantly to variations in tools and techniques applied by professionals while undertaking security risk assessments in practice. This confirms the findings of Brooks and Cotton (2011) who identified that 'no specific frameworks or standards are implemented by many working professionals within the security risk management field'.

Research method and design

Participants in the empirical study were selected from lists of registered and approved security professionals in Ireland. Of the security professionals listed, 38 participated in the study with extensive experience in the security industry ranging from 10 to 40 years. The security professionals come from varied backgrounds with a wide range of industry clients, and all have undertaken security risk assessments as part of their service provision to the industry. The research assumption is that security professionals with experience in undertaking security risk assessment would have knowledge of the phenomena under investigation. The basic criteria for participant sampling and selection are as follows: the professional works full time in the field of security, they undertake security risk assessments as part of their role, and for all those except independent security professionals, hold a current Private Security Authority (PSA) Licence. Security consultants in Ireland are currently not licenced by the PSA. The final sample of participants included the following cohorts:

- Eighteen (18) independent security consultants operating in Ireland. Selection of this cohort was achieved through consultation with the Security Institute of Ireland (SII), the Irish Security Industry Association (ISIA), and the Private Security Authority (PSA).
- Ten (10) in-house security managers of corporate companies operating in Ireland. Selection of this cohort was through consultation with the SII, ISIA, and the PSA.
- Ten (10) service providers to industry (Contract Security Professionals). Selection of this cohort was also through consultation with the SII, ISIA, and the PSA.

In order to meet the specific aims of the research project and to explore the security professionals' experience and personal perspectives on undertaking security risk assessments, a qualitative approach was adopted. This approach coupled with the lack of current research on the topic allowed for an explorative study of the actions, experiences, and subjective meanings attributed to the activity by the research participants and how they then interpret these meanings and associations from their own personal experiences. Each participant brought their personal views and opinions, which formed a relevant and informative description of their experience while undertaking a risk assessment. An inductive approach was adopted, which moved from specific patterns and themes to a more general holistic overview (Patton 2015). Gaining a perspective on the initial specific patterns which emerged from the research would bring into focus the participants' understanding, adoption, and awareness of the complex structures of organisational risk management and the tight coupling these activities create through their close interdependencies with other management functions.

The data collection method used semi-structured or guided interviews and these were undertaken with consideration given to the ethical issues associated with conducting interviews with both academic and legislative requirements met.

A total of seven main questions were used throughout the interview process to guide the discussion with a number of subquestions or prompts being presented to the participants as required. As each interview commenced, the researcher asked questions relating to the professional background and history of the participant in order to create context and establish a level of comfort between the participant and the researcher. Each participant was asked two introductory questions. The first question sought to establish a brief outline of the participant's experience within the field of security management. The second question reviewed the sectors the participants operated in and the type of services they provide. Once satisfied that the participants were relaxed and ready to narrate their professional experience, the researcher introduced the participant into the area of risk assessments through a series of pre-defined questions.

Data analysis was conducted using reflective thematic analysis approach which entailed an initial reading followed by a total immersion in the transcribed interview notes prior to identifying irrelevant data to the aims and objectives of the research project, so these data were removed from the analysis stage or winnowed (Guest et al 2012). Irrelevant data in the context of this research refer to very personal details about previous experiences of the participants. Then, the coding process was

conducted to identify the units of analysis or themes within the data which became sub- or overarching themes (Braun and Clarke 2006).

Key findings

The reflective thematic analysis revealed three main themes (i) lack of consistent terminology describing the process of undertaking security risk assessments, (ii) lack of a defined and structured approach to undertaking security risk assessments, and (iii) neither of the two key internationally recognised risk management standards, i.e. ISO 31000 or COSO 2017 was considered by most of the interviewed participants.

Lack of consistent terminology

While all participants are engaging in the provision of security risk assessment services, six participants indicated that they differentiate and perceive a significant difference between the provision of security audits, security reviews, and security risk assessments. Of those that saw no significant difference; one participant noted that "I would be less fussed about the title rather than the way it is done" while another noted that there was a bit of "semantics in there" and a third participant said they believed "that it was just wording". Another participant suggested that "from a consultant's point of view you will be asked to pull them together as one".

Overall, there was an inconsistent definition of security audits, security reviews, and security risk assessment or what they entail. Failure to identify a clear definition of terms is supported in the literature review where it has been shown that both academics (e.g. Chicken and Posner 1998; Haimes 2009; Aven 2012) and preeminent societies, such as Society of risk analysis and Britain's royal society, all failed to define the term risk. However, cognisance must be paid to the development and adoption of international risk management standards where a clear definition of the term 'risk' was presented in 1995 in the risk standard AS/NZ 4360:1995 and developed over the years to be included in the latest updated standard ISO 31000:2018.

A lack of consistent definition of risk and risk assessment could lead to confusing practices among security professionals when it comes to: (1) what activity they are required to undertake, (2) what service they are required to provide, (3) what definable outcomes they are to deliver, and (4) how they will report their findings to the client on completion of the assessment.

Further, the analysis of the responses to the question about, if the participants believed their clients made a distinction between security audit, security review, and security risk assessment supports this argument. Most of the participants stated that their clients would not make any distinction between these activities, with one participant indicating he believed that the client would have some understanding of the difference, but this was dependent on their experience and professional background. This appears to support the proposition that in practice both security professionals and clients have a shared understanding of the activities associated with undertaking

a security audit, security review, or security risk assessment. While this proposition is rather subjective as it is based on the participants' belief of their client's knowledge but it could be a relevant indication of the lack of shared understanding of what these activities entail. This is a surprising finding as ISO Guide 73:2009 provides a clear proxy definition of risk audit 'systematic, independent, and document process of obtaining evidence and evaluating it objectively in order to determine the extent to which the risk framework or any selected part of it is adequate and effective'; risk review 'activity undertaken to determine the suitability, adequacy, and effectiveness of the subject matter to achieve established objectives' and risk assessment 'overall process of risk identification, analysis, and evaluation'. These definitions have been in the risk management domain since 2009 and are available to security professionals and end users alike.

Lack of use of a structured and consistent risk assessment approach

Our results show a shared understanding of the main phases of risk assessment; however, when it comes to practice, there are an array of approaches to conducting risk assessment process. Only three of the interviewed security professionals follow pre-defined criteria for or a structured approach to undertaking security risk assessments.

When asked about the component parts of the security risk assessment again, only three of the participants gave a list of internationally recognised inputs into a risk assessment process, which may have included the identification, analysis, and evaluation of risk. The remainder of the participants rather moved across a wide range of topics which they perceived to form part of the assessment process; two participants referenced the "use of a pre-defined template" although no specifics were presented by the participants as to its contents or applicability. One participant referenced the use of CPTED (crime prevention through environmental design) as the means through which a security risk assessment is undertaken. Another noted that it was "not an exact science" and finally one participant indicated that the basis of the assessment was contained in the client's documentation, including policies, procedures, and operating manuals available at the time of performing the security risk assessment.

Focusing on the clients' needs, some of the participants (10) align their offering to suit clients' requirements as one of the participants noted 'it depends on the person in the client's business that engages us, if it is a security manager, they will have a different requirement to that of a compliance or health and safety manager'.

This shows that the interviewed security professionals rather rely on their own personal knowledge and experience to develop an ad hoc approach. This finding is consistent with previous research in particular Govender (2018) when they note that security practitioners operating within the security industry use no specific principles, framework, or process to undertake security risk assessments. Talbot and Jakeman (2009) advocate that ideally security professionals undertake a pre-defined process and apply their own personal dedication, experience, aptitude, and capabilities.

Use of internationally recognised risk management standards

The third theme that emerged from data analysis was the lack of engagement with and use of international risk management standards which are COSO 2017 and ISO 31000. Only three participants state that they refer to and follow the standard guidelines ISO 31000.

In addition, the security professionals have not referenced a number of alternative published risk management standards within the UK and Irish context which include 'A risk management standard' (2002) by AIRMIC/ALARM/ IRM, The Orange Book, 'Management of risk, principles and concepts' HM Treasury (2004), and BS 31100 'risk management code of practice' (2008). All of the noted risk management standards outline a process to be adopted by organisations to support the management of risk. The Chartered Institute of Internal Auditors, however, note that managers must select a standard that suites the size, nature, and culture of the organisation while also meeting the demands of their stakeholders and business.

Although no definitive process was identified by any of the research participants, three participants did mention or refer to the Security Institute of Ireland (SII), 'Asset Risk Management Manual', a document produced by the SII in 2015 which deals with the protection of assets and includes a large amount of text on undertaking security risk assessments. None of the three participants presented a defined approach advocated by the SII publication nor did they reference any methods outlined in the publication.

This finding seems to be in contradiction with the proposition supported by Smith and Brooks (2013) that a security risk management system should comply with the requirements of ISO 31000 as its overarching structure.

Discussions

The research identified a number of areas where language and the use of language created confusion. The findings presented in this paper show that professionals are not using the same definitions or terminology and therefore could struggle to understand each other. This issue may have its foundation in the application of different meanings to the same word by security professionals or different words to mean the same concept. The other finding suggests that they do not refer to or apply any particular standard which is likely a contributing factor to the identified inconsistency in their use of terminology. The core argument of the paper is that referring to security standards would limit the confusing use of terminology. The consistent use of terminology could be used as a vehicle to increase the quality of communication and facilitate the dialogue between professionals.

Although there is supporting literature to develop a defined and shared body of knowledge (e.g. Brooks 2010; Talbot and Jakeman 2009), the outcome of this research shows that the development of an agreed-upon body of knowledge is a work in progress and that the composition of such a body of knowledge is still subject to debate within the security field.

This paper suggests that ISO 31000 could be used to achieve consistent use of terminology, therefore facilitating communication between security professionals and between security professionals and their clients. Figure 1 presents ISO 31000:2018 and ISO 31010:2019 'Risk Management–Risk assessment' including Principles, Framework, and Process contained for managing risk.

Security risk professionals could approach the integration of the security risk assessment process into the generic risk management standard as follows:

(i) Risk management principles consists of eight foundational propositions on which the remainder of the framework and processes are supported. When considering the specified principles, it should be noted that the purpose of risk management is the creation and protection of value. The principles link the framework and process to the organisation's goals and objectives. The principles should be adopted to suit the individual circumstances of the organisation including its ethos, culture, and operational activities.

(ii) The framework consists of five component parts, when taken together they contribute towards the integration of risk management into significant activities undertaken by the organisation. The achievement of integration is dependent on the leadership and commitment of the board of management and oversight bodies. The connection between the framework and the process is achieved at the implementation phase where all significant activities are subject to a formal risk assessment process including security.

(iii) The process consists of six component parts which should be applied in a systematic way across all significant activities. The output from the risk process

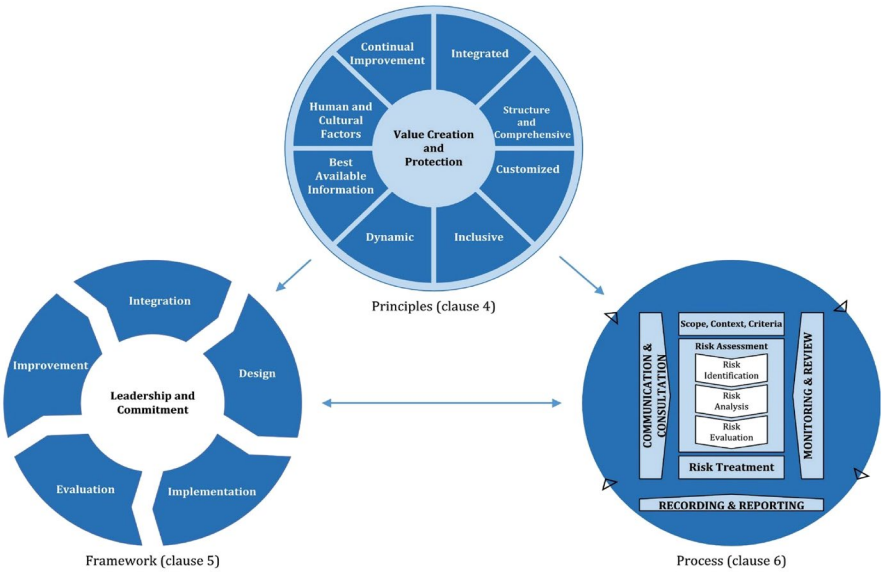

Fig. 1 Risk management principles, framework, and process as outlined in ISO 31000:2018 risk management—guidelines. Reproduced with permission of ISO

should form an input into management decision-making across the organisation.

The implementation phase of a risk management framework is where the interconnectivity between the framework and the risk management process takes place. An overview of the risk process shows a component part dealing with the scope, context, and criteria prior to undertaking the risk assessment. It is within this context that a security professional needs to gather information on the organisation's internal and external security infrastructure in order to set up the scope and criteria for the project. Setting the boundaries assists the security professional to identify and prioritise those areas that are explicitly included in the assessment and those that are outside the assessment remit. For example, IT or finance may be outside the scope while operations and manufacturing may be included.

Communication and consultation with the client are very important to identify the focus of risk analysis and decide whether the security professional is going to undertake a security audit, a security review, or a security risk assessment. This will also allow specifying the amount and type of security risks the organisation is willing to accept in order to achieve its objectives (risk appetite). Classifying and recording the criteria allows the security risk professional to evaluate the inherent risks (risks before additional controls are implemented) and identify which risks are for treatment. Some risks may fall within an acceptable level and will be tolerated while others may fall outside the criteria and require treatment. Once established, the risks that are analysed will be evaluated against the set criteria prior to the selection of treatment options. Figure 2 presents an adapted diagram based on the content of ISO 31000 risk process.

The first two activities—security audit and security review—can be undertaken independently of each other and of a security risk assessment. Where there is a requirement to undertake a security risk assessment then both the audit and review will be undertaken first and the output from these activities will form part of the input into the risk assessment process. The security audit consists of a systematic, independent, and documented process of obtaining evidence and evaluating it to determine the extent to which the security documentation, policies, and procedures are adequate and effective to manage the security risks faced by an organisation (ISO Guide:73 2018). This activity will form part of establishing the internal context of the organisation and will require the security professional to be cognisant of the security compliance and regulatory requirements within both the organisation and the national security authority. A security risk review is conducted of the organisational activities to determine the suitability, adequacy, and effectiveness of control measures currently in place to manage the exposure of critical assets to identified threats and vulnerabilities (ISO Guide:73 2018). The outputs from the security review will form the inputs into the security risk assessment where criticality of the assets will contribute towards assessing the potential consequences of an adverse security event occurring. Identification of the threats and evaluation of the capabilities and intent of an adversary will contribute towards establishing the likelihood of an event occurring, while identification and

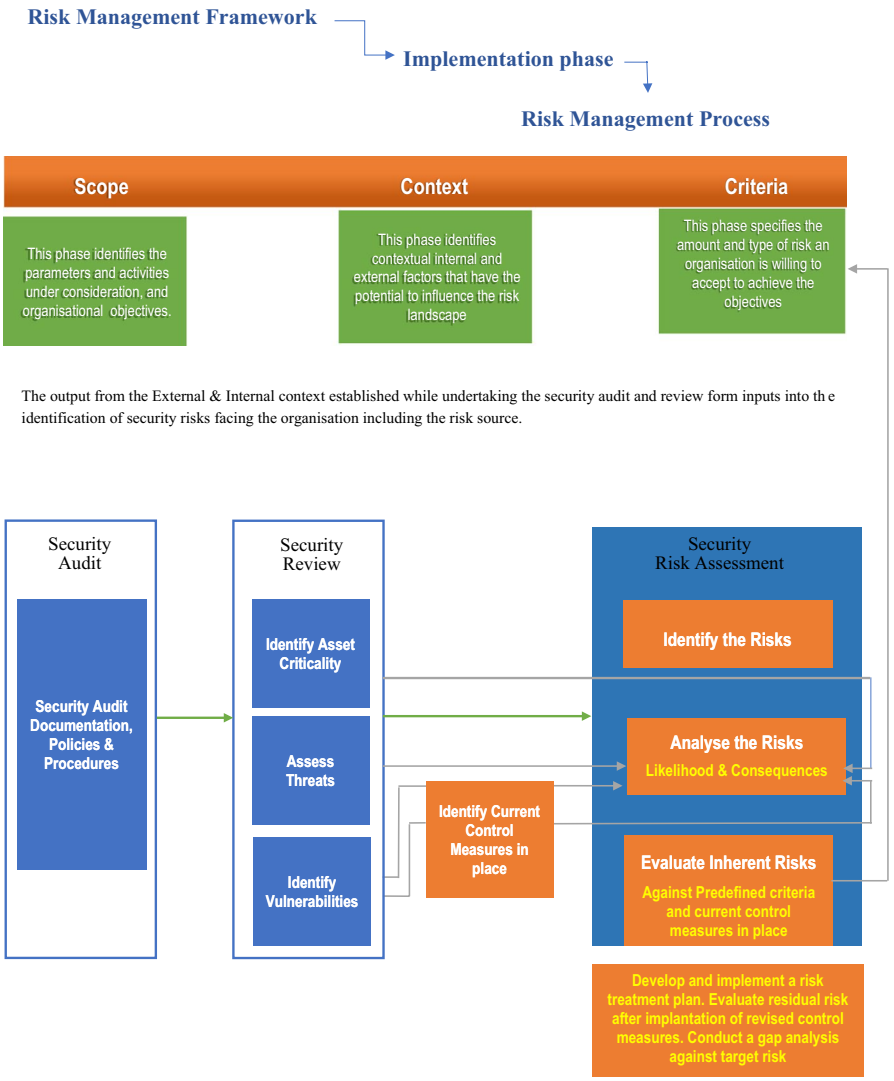

Fig. 2 An adapted diagram based on the contents of ISO 31000 risk management process.

evaluation of the vulnerabilities will contribute towards both the likelihood and potential consequences of an adverse event occurring (HB 167: 2006).

Finally, the security risk assessment which involves the first two stages (audit and review) is undertaken. The risk assessment process is an iterative process which must be carried out systematically and involve input from multiple stakeholders of every business unit affected (Peltier 2009, p. 266); the process consists of the identification, analysis, and evaluation of risks. When undertaking a security risk assessment, it is critical for the security professional to be aware that it is the security review that differentiates the activity from other fields of risk such as health

and safety, environment, business continuity, and compliance. The differentiator between the fields of operational risk forms the variables that are assessed and, in this instance, the variables are the assets, threats, and vulnerabilities (Roper 1999) and the outcomes from these initial reviews will contribute towards the analysis of the identified risks. The final part of the risk assessment process is an evaluation of the risks against pre-defined criteria which must be established and defined prior to undertaking the risk assessment.

Conclusion

This study explored the practices employed by security professionals in Ireland while undertaking security risk assessments. It sought to ascertain whether there was a shared understanding of the process of security risk assessment, and as a result whether there were shared 'so-called best practices' and consistent approaches to risk assessment. The main findings show that the definitions of risk and security risk assessment depend on who is doing the definitions. This can lead to many challenges when it comes to the interpretation and application of security risk standards.

While this research acknowledges that security risk assessment is contextually dependent and that the expertise and judgement of security professionals are valuable input to the risk assessment process, it is relevant to achieve some consistency in terms of terminology and approach. This paper suggests a revised version of ISO 31000 that could potentially meet these requirements while recognising the crucial input of security professionals in terms of contextual analysis of the client's needs and objectives. Further research will be needed to explore the factors that have the potential to influence the adoption of risk management standards by security professionals.

Data availability Not applicable.

Declarations

Conflict of interest On behalf of all authors, the corresponding author states that there is no conflict of interest.

References

AIRMIC, ALARM, IRM. 2002. Risk Management Standard. AIRMIC, ALARM, IRM.

Andretta, Massimo. 2014. Some considerations on the definition of risk based on concepts of systems theory and probability. *Risk Analysis* 34 (7): 1184–1195.

American Society of Industrial Security International. 2015. Risk assessment. American Society of Industrial Security International.

Allen, F.W. 1987. Towards a holistic appreciation of risk: the challenge for communicators and policy-makers. *Science, Technology, and Human Values* 12: 138–143.

ASIS International. 2009. Academic, practitioner symposium. Paper presented at the 2009 Academic, practitioner symposium, university of Maryland, College Park, 1.

Aven, Terje. 2012. The risk concept-historical and recent development trends. *Reliability Engineering and System Safety* 99: 33–44.

Aven, Terje, and Ortwin Renn. 2009. On risk defined as an event where the outcome is uncertain. *Journal of Risk Research* 12 (1): 1–11.

Biringer, E Betty, V Rudolph Matalucci, O. Connor, and L. Sharon. 2007. *Security risk assessment and management, a professional guide for protecting buildings and infrastructure*, 6. New Jersey: Wiley.

Braun, Virginia, and Victoria Clarke. 2006. Using thematic analysis in psychology. *Qualitative Research in Psychology* 3 (2): 77–101.

Brook, David. 2010. What is security: Definition through knowledge categorisation. *Security Journal* 23 (30): 225–239.

Brooks, David. 2011. Security risk management: A psychometric map of expert knowledge structure. *Risk Management* 13 (1/2): 17–41.

Brooks, David, and Hamish Cotton. 2011. Security risk management in the Asia Pacific region, what are security professionals using?. https://doi.org/10.4225/75/57a00f0dac5c1

British Standards, 31100. 2008. Risk management-code of practice. British Standards Institute.

Chartered Institute of Internal Auditors. 2020. Standards for managing risk. Chartered Institute of Internal Auditors.

Chicken, C John, and Tamar Posner. 1998. *The philosophy of risk*, 7. London: Thomas Telford Publishing.

Committee of Sponsoring Organisations of the Treadway Commission. 2017. Enterprise risk management—Integrating with strategy and performance. Committee of Sponsoring Organisations of the Treadway Commission.

Govender, D. 2018. The use of risk management model ISO 31000 by private security companies in South Africa. *Security Journal* 32 (3): 218–235.

Guest, Greg, Kathleen MacQueen, and Emily Namey. 2012. *Applied thematic analysis*, 22. Thousand Oaks: Sage Publications.

Haimes, Yacov. 2009. On the complex definition of risk; a systems approach. *Risk Analysis* 29 (12): 1647–1654.

Harding A. (2016). A risk culture comparison between risk practitioners and business managers. Available at https://repository.nwu.ac.za/bitstream/handle/10394/24939/Harding_A.pdf?sequence=1

HM Treasury. 2004. Orange Book, Management of risk, principles and concepts. HM Treasury.

Hutchins, Greg. 2018. ISO 31000:2018 enterprise risk management, 115. Portland: Quality and Engineering/CERM Academy.

International Standard Organisation, Guide 73. 2009. Risk management-vocabulary, 12. Geneva. International Standard Organisation.

International Standard Organisation, 31000. 2018. Risk management-guidelines, 1. Geneva: International Standard Organisation.

International Standard Organisation, 31010. 2019. Risk management-risk assessment, 1. Geneva: International Standard Organisation.

Khunti, K., Stefano Del Prato, Chantal Mathieu, Steven E. Kahn, Robert A. Gabbay, and John B. Buse. 2021. COVID-19, Hyperglycemia, and New-Onset Diabetes. *Diabetes Care* 44: 2645–2655. https://doi.org/10.2337/dc21-1318.

Koien, Geir M. 2020. A Philosophy of Security Architecture Design. *Wireless Personal Communications.* 113: 1615–1639. https://doi.org/10.1007/s11277-020-07310-5.

Landoll, Douglas J. 2006. *The security risk assessment handbook*, 9. Boca Raton: Auerbach Publications.

Manunta, Giovani. 1999. What is security. *Security Journal* 12 (3): 57–66.

Matthews, Helen. 2008. Operational risk topic, gateway series No 51, 4. Chartered institute of management accountants. https://www.cimaglobal.com/Documents/ImportedDocuments/51_Operational_Risk.pdf.

Munodawafa, Fortune, and Ali Ismail Awad. 2018. Securty risk assessment within hybrid data centres, a case study of delay sensitive applications. *Journal of Information Security Application* 43 (7): 61–72.

Ostrom, Lee T., and Cheryl A. Wilhelmsen. 2019. *Risk assessment, tools techniques and their application*, 2nd ed., 5. New York: Wiley.

Patton, Michael Patton. 2015. *Qualitative research and evaluation methods*, 4th ed., 47. New York: Sage Publications.

Peltier, Thomas R. 2009. *How to complete a risk assessment in 5 days or less*. Boca Raton: CRC Press Taylor & Francis Group.

Raz, Tzvi, and David Hillson. 2005. A comprehensive review of risk management standards. *Risk Management: an International Journal* 7 (4): 53–66.

Renn O. and Rohrmann B. (2000). Cross-Cultural Risk Perception: State and Challenges. In O. Renn et al. (eds.), Cross-Cultural Risk Perception, © SpringerScience+Business Media Dordrecht

Roper, Carl A. 1999. *Risk management for security professionals*, 6. Burlington: Butterworth-Heinemann.

Sadgrove, Kit. 2015. *The complete guide to business risk management*, 3rd ed., 331, 327. Aldershot: Gower.

Security Institute of Ireland. 2015. *Asset risk management manual*. Security Institute of Ireland (SII).

Sendi, Shameli A., and Aghababaei R. Barzegar. 2016. Taxonomy of information security risk assessment (ISRA). *Computer and Science* 57 (2): 14–30.

Security Risk Management (2006). Standards Australia & Standards New Zealand. (2006). Security risk management (AS/NZ 167:2006). Standards Australia & Standards New Zealand.

Slovic, P. 1987. Perception of risk. *Science* 236: 280–285.

Slovic P., Melissa L. Finucane, Ellen Peters and Donald G. MacGregor (2004). Risk as Analysis and Risk as Feelings: Some Thoughts about Affect, Reason, Risk, and Rationality. Risk Analysis, Vol. 24, No. 2

Smith, Clifton A., and David J. Brooks. 2013. *Security science, the theory and practice of security*, 52, 58. Amsterdam: Elsevier.

Spring, Jonathan M., Tyler Moore and Pym David. 2017. Practicing a science of security, a philosophy of science perspective. In *NSPW*, 47, October 1–4, 2017, Santa Cruz, CA, USA.

Standards Australia. 1995. AS/NZ 4360:1995 Risk management. Australia, Standards Australia/Standards New Zealand.

Standards Australia. 1999. AS/NZ 4360:1999 Risk management. Australia, Standards Australia/Standards New Zealand.

Standards Australia. 2004. AS/NZ 4360:2004 Risk management. Australia, Standards Australia/Standards New Zealand.

Standards Australia. 2006. HB 167:2006 Security risk management, 14. Australia, Standards Australia/Standards New Zealand.

Talbot, Julian and Jakeman, Miles. 2009. *Security risk management, SRMBOK, body of knowledge*, 5, 43, 271. New York: Wiley.

Tattam, David. 2011. *A short guide to operational risk*, 37. New York: Routledge.

Vellani, Karim H. 2020. *Strategic security management, a risk assessment guide for decision makers*, 2nd ed., 14. Boca Raton: CRC Press.

Wangen, Gaute, Christoffer Hallstensen, and Einar Snekkenes. 2018. A framework for estimating information security risk assessment method completeness. *Journal of Information Security* 17 (6): 681–699.

Wachinger G, and Renn O. (2010). Risk perception and natural hazards. WP-3-Review of the EU-Project CAPHAZNET, Available at: http://caphaznet.org/outcomes-results/CapHaz-NetWP3Risk-Perception2.pdf.

Wachinger, G., O. Renn, C. Begg, and Ch. Kuhlicke. 2013. The Risk Perception Paradox—Implications for Governance and Communication of Natural Hazards. Risk Analysis, Vol. 33, No. 6. https://doi.org/10.1111/j.1539-6924.2012.01942.x.

Ward, Stephen. 2005. *Risk management organisation and context*, 51. UK: Witherby Publishing.