Schmidt, Michael

Information security risk management terminology and key concepts

Risk Management

Provided in Cooperation with:
Springer Nature

Suggested Citation: Schmidt, Michael (2022) : Information security risk management terminology and key concepts, Risk Management, ISSN 1743-4637, Palgrave Macmillan, London, Vol. 25, Iss. 1, https://doi.org/10.1057/s41283-022-00108-8

This Version is available at:
https://hdl.handle.net/10419/308847

Risk Management (2023) 25:2
https://doi.org/10.1057/s41283-022-00108-8

ORIGINAL ARTICLE

Information security risk management terminology and key concepts

Michael Schmidt[1]

Accepted: 17 November 2022 / Published online: 16 December 2022

Abstract

Language is the foundation for any communication and the vocabulary used has a decisive influence on the ability of the communication partners to clearly understand each other. In Information Security Risk Management (ISRM), the terminology used is often dictated by industry standards and frameworks. However, there is no universally accepted terminology, which makes collaboration difficult for professionals and researchers alike. This publication compares the terminology defined by frequently used frameworks, such as ISO and NIST, in the field of ISRM. It examines the terms and inherent concepts of each terminology, compares the notion of risk and derives a concept diagram based on the most important key concepts. The result facilitates a common understanding of ISRM across frameworks and organisational boundaries, thus enables further research, discussion, intra- and inter-firm communication.

Keywords Risk management · Information security · Terminology · Terms · Concepts · Frameworks

Introduction

Risk management (RM) in the context of information security (IS) is an important topic for organisations across all industries. Information Security Risk Management (ISRM) is in part different from generic RM, due to other concepts in design, risk assessment and mitigation (Brooks 2011). Besides practitioners who establish and apply ISRM processes, there are also many scientific publications dealing with the improvement of ISRM or its implementation in a wide variety of use cases. People from different organisations use different ISRM frameworks or methods, so they

✉ Michael Schmidt
Michael.Schmidt@lrz.de

[1] Leibniz Supercomputing Centre of the Bavarian Academy of Sciences and Humanities, Boltzmannstr. 1, Garching n., 85748 Munich, Germany

struggle to communicate and thus cooperate. This is why a standardised terminology needs to be introduced to facilitate these activities.

As in many management disciplines, the terms used in ISRM are mostly derived directly from a practical application rather than from science. Through their adoption by international frameworks, many terms have become common and de-facto standardised. Shameli-Sendi et al. (2016) show in their comprehensive meta-study on risk assessment that these frameworks are essential for organisations worldwide and thus consider academic references and industry frameworks alike. However, there are a lot of different ISRM frameworks, some of which with a different focus, so the used terms are not always consistent between them. Some frameworks define their terminology in great detail and use numerous terms, others only use a few terms to outline the ISRM process. Thus, there is no universal terminology, terms used are not always unambiguous and even concepts may vary. In practice as well as in academic publications, the vocabulary used can differ based on many factors as the industry, technical knowledge or background of the author. All these make inter-organisational communication and framework-independent discussion about ISRM difficult and ultimately hinders the cooperation and further development of the field.

Furthermore, concept relations are rarely or only incompletely presented in the literature. For example, it is often assumed in ISRM that risk results from a vulnerability combined with a threat, but this relation is not often explicitly defined and is merely inferred by experts. The proper use of ISRM terms is both desirable in the scientific field and necessary in practice to be able to express risk concepts comprehensibly. A uniform terminology forms the basis of communication and cooperation beyond organisational boundaries, up to and including legal relevance when aspects of IS or RM become legally binding. Thus, it becomes particularly important that not only uniform terms are used, but that their concepts are equally understood. (Brooks 2011; Aven 2011; Luko and Johnson 2012)

This paper investigates terms and concepts commonly used in ISRM to outline current ISRM terminology. For this purpose, well-known ISRM frameworks are examined and their terminology compared. The analysis refers to international frameworks, as these are essential in all industrial sectors worldwide and thus form the basis of applied RM in organisations (Shameli-Sendi et al. 2016). In order to clarify the difference between a terminology, a term and a concept they are briefly discussed (Section "Terminology, terms and concepts") and existing publications in this area are investigated (Section "Related work"). The investigated frameworks include the *ISO/IEC 27000* series, the *NIST SP 800* publication, the *Risk IT* framework, the *Open FAIR* standard and the *Management of Risk* framework. Their terminology is analysed to identify core terms and key concepts (Section "Investigation of existing terminology"). Core terms are terms used in multiple frameworks, which is an indicator that they are stable and widely accepted. Key concepts are concepts shared across frameworks, which may be referenced with or without using the same term. Both are important for a generic ISRM terminology, thus the terms were listed, assessed and key concepts highlighted (Section "Comparison of framework terminology"). In particular, it is examined whether the central concept of risk is equal in these frameworks or whether they use the risk term to denote different concepts (Section "Composition of risk"). Concept relations defined by these frameworks are

modelled and presented as a concept diagram (Section "Key concepts & relations"). This provides a quick and easy overview of common ISRM terminology to understand core terms, key concepts and concept relations.

Terminology, terms and concepts

In order to examine ISRM terminology, it is a prerequisite to clarify what a terminology, terms and concepts actually are. These definitions originate from other academic fields like the sciences of language and terminology, which are presented without going into too much depth. One would need to understand related concepts like lexical units, signs, words, language, knowledge and naming as well as the linguistic and etymological differences between them to really define terminology entirely correct, but this is not necessary for the further understanding of this work. To put it simply, a terminology defines a group of distinguishable words, which are called terms. In contrast to systems of names to label objects (nomenclatures), we are familiar with in daily life, terminologies are systems of terms. What makes a term unique and therefore distinguishable is its definition, which explains the conceptual meaning. Following some traditional interpretations, a concept basically translates to the knowledge about using a designated word. The concept may exist even without a term. (Rey 1995; Kockaert and Steurs 2015)

In order to make the theoretical principles from terminology science easier to use, national and international organisations have put effort into creating a simplified vocabulary. The international standard Terminology work and terminology science (ISO 2019) defines the most important terms and their interrelationships, which will be used in this publication. According to the standard, a *terminology* is a 'set of designations (3.4.1 [term identifier]) and concepts (3.2.7) belonging to one domain (3.1.4) or subject (3.1.5)'. The latter two define the scope, where a *domain* is a 'field of special knowledge' and a subject an 'area of interest or expertise', which is ISRM in the context of this publication. A *concept* is a 'unit of knowledge created by a unique combination of characteristics (3.2.1)'. These *characteristics* are an 'abstraction of a property (3.1.3)', which is a 'feature of an object (3.1.1)', i.e. 'anything perceivable or conceivable'. An important feature of a *concept* is that it forms a *concept relation*, i.e. there is a 'relation between concepts (3.2.7)'. In contrast to that, a *designation* is just a 'representation of a concept (3.2.7) by a sign which denotes it in a domain (3.1.4) or subject (3.1.5)'. That means the *designation* can be seen as the label of a concept within a given *domain*. When using a 'designation (3.4.1) that represents a general concept (3.2.9) by linguistic means' it is called *term*, the common word we are usually using and will be using as well in this publication. For the sake of completeness and to close the circular argument of the quoted definitions, a *general concept* is a 'concept (3.2.7) that corresponds to a potentially unlimited number of objects (3.1.1) which form a group by reason of shared properties (3.1.3)'. To put it in a nutshell, a terminology in the ISRM domain consists of concepts related to each other that embody knowledge and terms that represent a concept in a linguistic way.

This paper attempts to review ISRM terms and concepts by examining ISRM frameworks. A framework is a document or a set of documents, which describe a system of ideas, rules and methods to enable activities of a certain domain, in this case ISRM. In this context, a framework defines its own terminology, which may or may not have an intersection with other frameworks. According to the standard on Harmonisation of concepts and terms (ISO 2007) this is inevitable, because '[c]oncepts and terms develop differently in individual languages and language communities, depending on professional, technical, scientific, social, economic, linguistic, cultural or other factors'. Since there is no universal RM or ISRM terminology, it is necessary to examine how far these terminologies differ from each other. If two or more terminologies overlap, the question is whether they only use the same terms or define the same concepts, respectively, whether there are different terms for the same concept. This 'relation between designations in different languages representing the same concept' (ISO 2007) is called *equivalence*. It can be assumed that equivalent concepts appearing in multiple, popular frameworks are important for the ISRM domain and should therefore be highlighted as key concepts. The following sections will present different ISRM frameworks, compare their terminologies and attempts to identify such key concepts.

Related work

Although terminologies are a common research topic, there are comparatively few publications that deal specifically with ISRM. Often relevant articles can also be found in the superordinate fields of IS or RM. In the following, the publications of three authors who have particularly focussed on terminology in the fields IS/RM/ISRM are presented, and their research is placed in the context of this work.

Brooks (2011) describes a comprehensive approach to identify ISRM key concepts by extracting categories that frame security knowledge. Following a quantitative approach to identify risk management categories, which was based on key topics taught in tertiary security courses, it was possible to come up with a final list of 14 categories. This list was then used by a group of experts to identify links between the categories resulting in a psychometric risk management concept map. This work provides great insight on how important a common understanding based on terminology is and that terms itself carry important concepts. The initial study was already published in 2009 (Brooks 2009) and the categories are aligned with the terminology from the 2004 Australian Risk Management Standard (AS 2004), which is by now superseded by ISO 31000. Although these studies remain valuable, the authors think an update is reasonable after more than 10 years in a fast-paced field as IS. Furthermore, the study draws its conclusion about linking the categories from expert knowledge thus representing how professionals actually understand certain concepts. While this is a sound approach, a framework based investigation may lead to a different concept model, which provides another perspective on the same issue. The strength of the document review approach presented in the next chapter is the fact that it allows for an objective analysis of concepts without including implicit assumptions of experts.

Aven (2011) analyses general RM terminology of ISO standards based on the ISO Guide 73 (ISO 2009), which was rather new at that time. The terms and their definitions are content-wise examined and checked for consistency. This raises various questions about the inherent meaning of terms and concept relations defined therein, especially concerning risk and uncertainty. It becomes apparent that the ISO ISRM terminology is not suitable for consistently representing a conceptual framework. This makes it clear how important terms are for the communication and understanding of key concepts in RM. While the publication goes into great detail on the definitions and concepts of the ISO Guide 73, other RM standards are not considered. Other publications by the author also deal with terminology and its standardisation, but with a view on RM in general and not specifically for IS.

Luko (2013b) performs a terminology review based on ANSI Z690.1:2011 (ANSI 2011), which is in fact a national equivalent of ISO Guide 73. The standard and its definitions are examined in great detail. Subsequent publications then address principles and guidelines (Luko 2013a) and assessment techniques (Luko 2014). These put emphasis on a dedicated review of the standard and the RM terms and techniques it contains. The authors had previously highlighted the importance of terminology and examined it in the context of ISO standards (Boulanger et al. 2012; Luko and Johnson 2012). Although this publication investigates the terminology provided by ISO Guide 73 for generic RM, it does not particularly address IS. Nevertheless, in its scope the review is profound and it is worthwhile to extend it with a focus on ISRM.

Investigation of existing terminology

This section explores ISRM terminology by investigating some of the most popular frameworks in the area of ISRM (Wangen and Snekkenes 2018). The analysis refers to international frameworks as these standards are essential for RM in all industrial sectors worldwide and thus form the basis of practical RM in organisations (Shameli-Sendi et al. 2016). In addition to these frameworks, there are many other publications that deal with the topic of RM or ISRM, but they mostly use already established terminology. One example is the RM glossary of the ENISA Framework (ENISA 2021), which relies mainly on ISO definitions. The vast majority of literature appears to refer to the same set of frameworks. In addition, there are many methods that deal specifically with certain activities, such as CORAS (Lund et al. 2011) or CRAMM (Yazar 2002) for risk assessment. As these only cover a sub-areas of ISRM or define specific methods, they were not considered any further. Furthermore, this review focusses specifically on ISRM and excludes generic RM standards. Despite many attempts in the past years, it has not been possible to establish a universal and overarching RM terminology (Aven 2016). One attempt is the glossary published by the Society for Risk Analysis (Aven 2018). It aims to gather and group various RM core terms, similar to the approach of the present publication, but lacks specific focus on ISRM. The attempt to unify terminology seems to be more promising in the field of ISRM as it is a much smaller branch and the terms are therefore less generic and the concepts specific to one domain.

ISO/IEC

The International Organization for Standardization (ISO) provides several internationally accepted standards for RM. In the field of IS, these are often produced in cooperation with the International Electrotechnical Commission (IEC).

The general standard for RM is ISO 31000 (ISO 2018c), from which topic specific standards (e.g. IS, quality, environment) are derived. The standard itself defines only a few terms, but refers to the generic Guide 73 (ISO 2009). This guide in turn has a national ANSI equivalent with Z690.1 Vocabulary for Risk Management (ANSI 2011). A review of the two equivalent standards has already been described by Luko (2013b). In addition, both ISO (https://www.iso.org/obp) and IEC (https://std.iec.ch/glossary) provide an online database with general and specific terms from all standards for free.

In terms of security the ISO 27000 series is a globally acknowledged standard in the area of IS Management. The ISO/IEC 27000 (ISO 2018a) standard itself provides terminology for IS in general, the ISO/IEC 27005 (ISO 2018b) specifically for RM. The procedure is derived from ISO 31000, but has a special focus on IS.

Overall, the information provided by ISO is very well structured. For the most part, the relationships between the terms are shown using inline references. Due to the standardisation and references to other standards, the ISO and IEC standards mostly use the same terms throughout, which is why they are always defined in the same way in different documents. This establishes uniformity across the ISO environment.

NIST SP 800

The Risk Framework 800-87 (NIST 2018), which belongs to the NIST SP 800 series, is a collection that logically connects several other publications from the 800 series. These include NIST SP 800-39 (NIST 2011) on IS management and the Guide for Conducting Risk Assessments NIST SP 800-30 (NIST 2012). Also, worth mentioning is the publication NIST SP 800-53 (NIST 2013), which focusses on security controls.

The NIST documents each provide a comprehensive glossary in the appendix. The terminology is mostly harmonised and applicable across all documents. However, the scope of the defined terms varies greatly. There are general (e.g. configuration item), environment-specific (e.g. federal agency) as well as IT-specific (e.g. firmware) terms. In general, the individual terms are well defined, but the relationship between individual terms is not clearly stated. Some terms are taken from related publications such as FIPS 200 (NIST 2006) or CNSSI 4009 (CNSS 2015).

RiskIT

ISACA's RiskIT Framework (ISACA 2009a) establishes a guideline for RM. It is complemented by a practice guide (ISACA 2009b) which provides implementation guidance. The recently published 2nd edition (ISACA 2020b) contains only very few

terms in the definitions & terminology section. It also states that generally accepted concepts from other frameworks are used, but the terms used may differ from these. However, the framework is written in such a way that most subchapters define and describe a specific concept, such as risk tolerance or risk response. The new version in particular refers directly to the modules 'EDM03 Ensured Risk Optimisation' and 'APO12 Managed Risk' from the COBIT framework.

COBIT describes itself as a framework for the governance of information and technology in companies. The version COBIT 5 (ISACA 2012a) was the most popular part of the series for a long time. Over the years, it was expanded to include various aspects, including the topics IS (ISACA 2012b) and RM (ISACA 2013). It has now been replaced by the COBIT 2019 (ISACA 2018a, b), which attempts to integrate IS and RM aspects more strongly. Since the framework calls itself an umbrella framework, it refers to several other frameworks. For RM, these are COSO ERM, ISO/IEC 27005 and NIST SP 800 37. There is also a general glossary (ISACA 2020a) published by ISACA, but it is neither referenced in RiskIT nor in COBIT. Since it is not clear how these terms relate to the ones defined within the frameworks, they are excluded from the further analysis.

The Enterprise Risk Management Integrated Framework published by COSO (2017) is a business framework for general RM in companies. It is a recognised and widely used framework, but does not deal specifically with the sub-area of IS. For this reason, it was not considered further in this publication.

FAIR

Factor Analysis of Information Risk (FAIR) (Freund 2015) is an ISRM approach developed by the FAIR Institute. The concept is based on the well-known risk measurement method Value at Risk (VaR). The principles of FAIR have been standardised in the Open FAIR body of knowledge by the consortium The Open Group. It consists of two publications, which define the methodology (Open Group 2013a) and the terminology (Open Group 2013b). Thus, the standardised terminology of Open FAIR is used in the context of this publication.

Open FAIR highlights the importance of a common language and generic concepts in the field of ISRM, for example, to overcome gaps between IT and business managers. The Open Group aimed to make its concepts as universally applicable and compatible as possible. So some input from OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) (Alberts and Dorofee 2002) is included, whereas a coupling with ISO 27005 is also possible. The framework emphasises its compatibility with other ISRM standards and has therefore published guides to integrate ISO/IEC 27005 (OpenGroup 2010) as well as the NIST framework (Standards 2016).

MoR

Management of Risk (MoR) (AXELOS 2012) is a pragmatic framework that is specifically designed for practitioners. It is much more compact than other frameworks

and its focus is on operationally relevant aspects of RM. Although the framework has not been updated since 2010, it does not seem to have lost its popularity in the field.

MoR defines individual terms when used and also has a glossary of core terms. However, the concepts are kept much simpler compared to the other frameworks described before. Nevertheless, the terminology is defined comparably. Due to its focus on practical aspects, MoR adds another important ISRM perspective to this review. A simple comparison of ISO 31000:2009 and MoR terms was carried for that version by the bsi group in 2013 (Dallas 2013), but with an application-oriented scope and without considering concepts.

Comparison of framework terminology

In the previous section, the document families ISO/IEC, NIST SP 800, RiskIT and MoR, their structure and related material were presented. They are referred to as the frameworks in the following. In this section, the frameworks' terminology is examined and compared to each other. It turned out that the size and scope of the terminology defined by each framework varies greatly. It is not only the number of terms that differs, but also how comprehensively they are defined and connected to each other. Often, terms are not defined explicitly, but only implicitly within their context of use. This yields the potential danger of fuzzy definitions and an inhomogeneous use of concepts.

Terminology is not just about naming and labelling, but fundamentally about terms and their meaning. Thus, it is not enough to compare the frameworks' terms like comparing labels, but their definitions which may describe a concept. The aim is to identify overlaps in their terminology, whereby there are four possible options if comparing two frameworks: (1) they have no overlaps in their terminology; (2) they use the same term for different concepts; (3) they define the same concept without using the same term; (4) they define the same concept using the same term. This is called concept harmonisation, an 'activity leading to the establishment of a correspondence between two or more closely related or overlapping concepts having professional, technical, scientific, social, economic, linguistic, cultural or other differences, in order to eliminate or reduce minor differences between them' (ISO 2007). It is expected that these overlaps actually refer to equivalent ISRM concepts, which can be gathered to define a set of ISRM key concepts.

In this terminology comparison, only explicitly defined terms were used without considering implicitly defined concepts by considering only glossaries, terminology documents and other document parts that clearly define terms. Schmidt et al. (2019) present a method to perform an in-depth content analysis in the service management domain, but state that external knowledge is often required to implement a framework in practice in order to fill logical gaps. Taking into account terms that are implicitly defined within the content of the frameworks would yield unwanted risks. Making assumptions about the concepts to be examined could produce terms that are described but not defined or concepts without terms. In terms of a terminology review it should be avoided to introduce

any external knowledge by interpreting terms that are not explicitly made by the framework itself. If one wants to specifically investigate terminology based on expert knowledge, an approach as described by Brooks (2011) could be used. The purpose of this publication is to identify terms explicitly defined by these frameworks to identify core terms and compare designated concepts to identify key concepts.

Since some frameworks consist of several documents, they are considered as a unit in regard to their terminology. Therefore, the documents mentioned in section 4 were grouped as follows:

FAIR	OpenFAIR Risk Taxonomy
ISO	ISO/IEC 27000, ISO/IEC 27001, ISO/IEC 27005, ISO 31000, ISO Guide 73
MoR	Management of Risk: Guidance for Practitioners
NIST	NIST SP 800-30, NIST SP 800-37, NIST SP 800-39
RiskIT	Risk IT Framework v1, Risk IT Framework v2

Unless a specific document is named, all further mentions of a framework refer to the group in this list. Some frameworks provide general terms that are not necessary for ISRM. In order to create a meaningful and comparable overview, the collection of terms was sanitised by removing all terms that are not directly related to ISRM. These terms could be scope specific or originate from related areas, for example *assurance* or *system* in the NIST framework.

The terminologies of the frameworks were examined according to the grouping, i.e. each framework provides one set of terms. After listing the terms for each framework, the next step was to investigate them to identify equal concepts across the frameworks. For this purpose, all definitions of terms were semantically examined and the characteristics of the concepts described were compared with each other. For example, the MoR (AXELOS 2012) term *impact* is defined as the 'result of a particular threat or opportunity actually occurring'. The referenced *threat* defines an 'uncertain event that could have a negative impact on objectives or benefits'. Both definitions combined show that the *impact* describes a concept about influence of an event on objectives. This is the same as the 'outcome of an event affecting objectives', which is the ISO (ISO 2018a) definition of *consequence*. It can be concluded that both frameworks refer to the same concept, i.e. concept equivalence. This procedure was carried out for all terms in order to create a comprehensive mapping of the frameworks' terminologies.

The aim of this analysis is to identify ISRM key concepts, i.e. concepts shared across frameworks. This requires reducing the compilation created during concept mapping to remove concepts that only occur in few frameworks. The Definition

Count (DC) was therefore established as an indicator of the significance of a concept. It describes the number of frameworks that define a given concept, regardless of whether they use the same or a different term. At least three of the five frameworks have to define a concept (DC≥3), presuming a key concept must be used in the majority of frameworks. Consequently, all concepts that are only used in a few frameworks (DC<3) are not considered key concepts and were removed from the compilation. The remaining ones were split into the categories fully covered (DC5), mostly covered (DC4) and partly covered (DC3) concepts. The outcome of this procedure is presented in Table 1. Each row represents an identified concept, each column the term used in the respective framework, if available. Bold terms indicate core terms, i.e. terms used predominantly, which will be used later on. In the first column, all concepts were arranged according to their DC. As a result of this consolidation, the entire terminology collection could be reduced to 42 unique terms assigned to 21 concepts. In the following, insights and anomalies discovered during this analysis are discussed in more detail.

It turned out that most terms in the ISO standards are indeed defined uniformly across the various documents of the framework. Only new terms are added to documents in the framework hierarchy, but inherited definitions are usually not changed. However, there are some inconsistencies between documents. *Vulnerability* listed in Table 1, for example, is defined in ISO 27000 as 'weakness of an asset or control [...] that can be exploited by one or more threats' (ISO 2018a) while Guide 73 defines it as 'intrinsic properties of something resulting in susceptibility to a risk source [...] that can lead to an event with a consequence' (ISO 2009). Still, ISO remains the most consistent and well-structured framework in this analysis.

Dealing with risks after their assessment is a key activity in RM, in which the informed acceptance of risks plays a central role. RiskIT uses the term *risk acceptance* in this context, while MoR uses *retention*. ISO (2009), on the other hand, defines both with *risk acceptance* as an 'informed decision to take a particular risk' and *risk retention* as the 'acceptance of the potential benefit of gain, or burden of loss, from a particular risk'. However, based on the definitions it was not possible to distinguish whether and how the two concepts differ. One interpretation would be that risk acceptance is about the decision to accept, i.e. the activity, while risk retention is the circumstance that a risk is accepted, i.e. its state. However, this is only an assumption based on the ISO definitions, which is neither backed by any of the other frameworks nor used consistently within the frameworks process activities. In its own documents, however, ISO mainly uses the term *risk acceptance*. NIST makes use of the term *risk acceptance* in its standards, but does not even explicitly define this term. It seems that *risk acceptance* and *retention* actually refer to the same concept, just the ISO definition of both terms is irritating. An expert evaluation could help to determine whether practitioners in fact distinguish between the terms or concepts.

As previously stated, various document families such as ISO 31000/27000 and NIST 800 were reviewed as a group and terms defined in one or more documents were consolidated to create the mapping in Table 1. This revealed, however, that it is unclear when a term that has been already defined in a superordinate document was mentioned again in a subordinate document. For example, ISO 27005

Table 1 ISRM key concepts derived from framework terminology mapping

	FAIR	ISO	MoR	NIST	RiskIT
DC5 - Fully Covered	Loss magnitude	Consequence	Impact	Impact	Impact
	Threat event	Event	Risk event	Threat event	Event
	Risk	Level of risk	Risk	Risk	Risk/business risk
	Loss event frequency	Likelihood/probability/frequency	Probability	Likelihood of occurrence	Likelihood/frequency
	Threat agent	Risk source	Risk cause	Threat source	Threat
	Threat	Threat	Threat	Threat	Threat event
DC4 - Mostly Covered	–	Residual risk	Residual risk	Residual risk	Residual risk
	Asset	Asset	–	Asset	Asset
	Risk assessment approach	Risk management process	Risk management process guide	Risk assessment methodology	–
	–	Risk mitigation/reduction	Reduction	Risk mitigation	Risk mitigation
	–	Risk treatment	Risk response	Risk response	Risk disposition
	Vulnerability	Vulnerability	–	Vulnerability/weakness	Vulnerability
DC3 - Partly Covered	Action	Attack	–	(Cyber) attack	–
	Control	Control	–	Control/countermeasure	–
	–	Risk acceptance/retention	Retention	–	Risk acceptance
	–	Risk appetite	Risk appetite	–	Risk appetite
	–	Risk avoidance	Removal	–	Risk avoidance
	–	Risk financing	Transfer	–	Risk transfer
	–	Risk register	Risk register	–	Risk portfolio view
	–	Risk tolerance	Risk tolerance	–	Risk tolerance
	–	–	Severity of risk	Impact level/value	Magnitude

is supposed to inherit the terminology from ISO 27000 as well as Guide 73: *event* is defined in all three documents, *vulnerability* only in 27000 and *hazard* in ISO Guide 73. Yet, all terms seem to be relevant to RM, IS and ISRM. Since the ISO 27000 documents are newer than Guide 73, this would explain at least the introduction of new terms, but not the other inconsistencies. Similar examples can be found for NIST. This suggests that the document families are not fully integrated or synchronised. This confirms the impression of Aven (2011), who already stated that the terminology established by ISO documents is not suitable on their own to create a consistent conceptual framework for RM. Whether these inconsistencies are actually relevant in the implementation of ISRM or whether this could cause different terms to become accepted to different degrees in practice cannot be assessed.

The concept of an asset was difficult to assess, which was a surprise, because it often appears to be a fundamental concept of ISRM. Although four of the frameworks use this concept, only RiskIT and FAIR define it explicitly. Both NIST and ISO use the term *asset* quite frequently and establish concept relations as part of other term definitions, but do never define it. However, there are documents of the ISO 27000 family not related to RM that define an *asset* as 'anything that has value to an individual, an organisation or a government' (ISO 2012), but surprisingly none of the risk related ones, i.e. 27005, 31000 or Guide 73. Strangely, the ISO 27005 version of 2005 contained an *asset* definition, which was then removed in the current version. MoR neither uses the term *asset*, nor does it seem to adopt an associated concept. Instead, it identifies threats and opportunities according to whether the organisation can achieve its objectives. We assume that these are not competing concepts, but that assets are merely a vehicle to derive the otherwise difficult to measure uncertainty to achieve objectives. In this case, assets would not be essential for ISRM if the impact on business objectives can be assessed differently.

A surprising observation is that the well-known objectives of IS, *confidentiality*, *integrity* and *availability* (CIA) are not always defined terms. The so-called CIA triad or golden triangle plays a central role in the application and teaching of IS as well as asset-based ISRM (Shameli-Sendi et al. 2010). In particular, the *integrity* objective is only defined by NIST. A look at the frameworks content sections shows that although integrity (of information) is often addressed, it does not seem to be perceived as an essential concept for RM. The objectives *availability* and *confidentiality* are only defined by ISO and NIST. The fact that CIA is only defined in ISO and NIST might be because these frameworks also cover general IS while FAIR, MoR and RiskIT are ISRM specific.

One finding of Brooks (2011) was that the term *threat* was recognised by the experts as a key concept, but it was not defined in any of the prevailing standards at that time. It turned out that this has changed in the meantime. Today, all five frameworks have a *threat* concept and even use a similar term. On the one hand this shows that the frameworks still evolve based on developments and experiences in the field of ISRM, on the other hand it indicates that the ISRM concepts have not been stable so far.

Composition of risk

Since the concept of risk is at the core of ISRM, this section compares the concepts and terms of the frameworks. The approach is analogous to that in the previous chapter, but the results are discussed in more detail. The term *risk* is often used or explained in conjunction with the terms *likelihood/probability* and *impact/magnitude*. To analyse the concept of risk, the definitions of the terms *risk, likelihood, impact* and *magnitude* from Table 1 are listed in Table 2. Besides the use of different terms for equal concepts, it can be seen that the fundamental definition of risk is similar or even the same in most of the frameworks. On closer inspection though, the concept relations turn out to be different for the Risk IT and ISO frameworks in particular.

All frameworks describe a risk as the result of a combination of *likelihood* and *impact*. Figure 1 illustrates the different risk concepts based on the definition of *risk* in Table 2. They are depicted using the same structure to facilitate graphical comparison of the concept relationships. The concepts of *[r]isk*, *[l]ikelihood* and *[i]mpact* are highlighted. Placing the definitions side by side in this way, it becomes clear that the structure and connection of these concepts is basically the same. Only when looking at the ISO definitions it is noticeable that there is another ISO-specific risk concept which is different from the others, as described later. It should be noted that although RiskIT defines and uses a similar risk concept, it does not explicitly define the term *likelihood* itself. However, this is only the case in the latest version, as the framework changed some terms with the latest upgrade (see label old in Table 2). Previously, instead of *risk* the term *business risk* was used, and the time-based *frequency* was used instead of *likelihood*.

Of particular interest is the ISO definition, which differs from the others. The ISO distinguishes between the terms *risk* and *level of risk (LoR)*. This introduces a new meta concept that is not included in the other frameworks. While in the other definitions *risk* is understood as a combination of *impact* and *likelihood*, in the ISO this fits the *LoR*. *Risk* is defined as an 'effect of uncertainty on objectives' (ISO 2009), which has a *LoR*. So this *LoR* is not the *risk* itself, but a feature of a *risk*, i.e. related concept. This distinction influences not only the concept of risk, but especially the use of its terms. A different view is that the *LoR* is not a concept itself but only a property of *risk*, a question similar to whether *impact* and *likelihood* are really concepts or just properties, too. However, the assumption that they are actually concepts is more convincing, because they transport knowledge about the use of an idea and in turn have properties themselves, such as uncertainty and time. Anyway, ISO is the only framework that has a risk concept that goes beyond the calculation of a value described by *impact* and *likelihood*. Aven (2011) analyses in detail the meaning and consequence of those concepts with special attention to *uncertainty*. He concludes that the meaning of the ISO definition of risk is not clearly defined, which is a main problem, because it enables different interpretations of the concept. This conclusion matches the findings presented in this paper, as the comparison with other frameworks also shows that the ISO concept cannot be clearly placed in or compared to other ISRM concepts.

Table 2 Definition of risk—concept comparison of 5 ISRM frameworks

	FAIR	ISO	MoR	NIST	RiskIT
Risk	**Risk** The probable frequency and probable magnitude of future loss.	**Level of Risk** Magnitude of a risk, expressed in terms of the combination of consequences and their likelihood	**Risk** An uncertain event or set of events that, should it occur, will have an effect on the achievement of objectives. A risk is measured by a combination of the probability of a perceived threat or opportunity occurring and the magnitude of its impact on objectives.	**Risk** A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence.	**Risk** The combination of the likelihood of an event and its impact **Business Risk** *(old)* A probable situation with uncertain frequency and magnitude of loss (or gain)
Likelihood	**Loss Event Frequency** The probable frequency, within a given timeframe, that a threat agent will inflict harm upon an asset.	**Likelihood** chance of something happening	**Probability** This is the evaluated likelihood of a particular threat or opportunity actually happening, including a consideration of the frequency with which this may arise.	**Likelihood of Occurrence** A weighted factor based on a subjective analysis of the probability that a given threat is capable of exploiting a given vulnerability or a set of vulnerabilities.	**Likelihood** — **Frequency** *(old)* A measure of the rate by which events occur over a certain period of time
Impact	**Loss Magnitude** The probable magnitude of loss resulting from a loss event.	**Consequence** outcome of an event affecting objectives	**Impact** Impact is the result of a particular threat or opportunity actually occurring.	**Impact/Potential Impact** With respect to security, the effect [...] of a loss of confidentiality, integrity, or availability of information or a system.	**Business Impact** The net effect, positive or negative, on the achievement of business objectives
Magnitude	—	—	**Risk effect** A description of the impact that the risk would have on the organisational activity should the risk materialise.	**Impact Level** The magnitude of harm that can be expected to result from the consequences [...]	**Magnitude** A measure of the potential severity of loss or the potential gain from a realised IT-related event/scenario

Table 2 (continued)

	FAIR	ISO	MoR	NIST	RiskIT
ISO Risk	—	**Risk** Effect of uncertainty on objectives	—	—	—

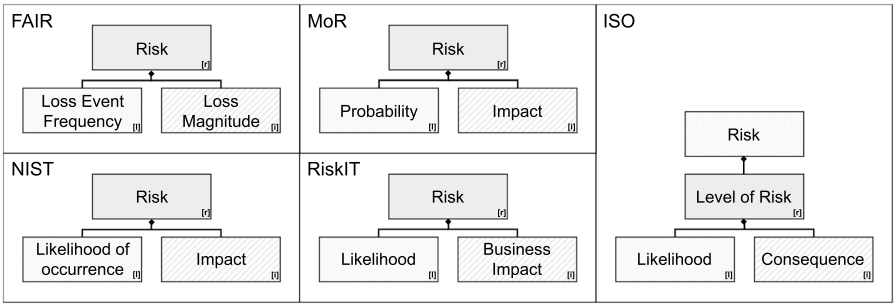

Fig. 1 Definition of risk—concept diagrams of 5 ISRM frameworks risk concept

As stated, the definition of risk is basically composed of the terms *impact* and *likelihood*. However, a closer look at their definition shows that these concepts are indeed related to a *risk*, but do not actually describe it. Instead, the *likelihood* describes the chance of an *event* occurring and the *impact* describes its effect. This shows that the risk concept cannot simply be explained without the use of additional terms. Thus, any ISRM terminology needs to include at least the terms *risk, impact, likelihood* and *event* to be capable to define a minimum viable risk model.

Some frameworks also include the so-called *magnitude* or a similar term (see Table 2). This concept is established either individually or in combination with *impact*. However, the terms are used differently and are also not consistent in the frameworks themselves. FAIR, for example, uses the term *loss magnitude* instead of *impact*. MoR speaks in its risk definition of the *magnitude of its impact on objectives*. These are more than just the use of different terms, but different concepts. RiskIT describes *magnitude* as the severity of the scenario, which is very similar to the NIST definition of *impact level*. It can be seen that there is no common understanding of the concept *magnitude* in the literature, but there is a general idea shared across the frameworks about what this concept is supposed to be. Maybe it will evolve in future, however, the concept (relations) is not sufficiently defined, and the associated terms remain inconsistent at this stage.

Despite the specific differences mentioned above, the comparison shows that the definition of risk is in general quite similar and well established across the various frameworks. It indicates that the underlying concept of risk is well known and stable in the area of ISRM. The ISO approach to focus on uncertainty aspect of events may drive future development in the field, even if it is by no means a new idea in RM, but an unusual approach in the IS domain. In other areas, risk and uncertainty has been discussed since the dawn of RM, like Knight (1921) who discussed their connections and differences already in 1921. However, as the illustrated risk definitions have shown, ISRM has evolved towards describing the *impact/likelihood* of an *event*, which is a much more tangible concept than the uncertainty to achieve objectives. It remains to be seen whether the ISO will adapt its definition in IS-related standards to follow the common industry practice or whether the *uncertainty* concept will become more important in ISRM in the future.

Key concepts & relations

After the terminologies of the frameworks have been harmonised, key concepts identified (Table 1) and the risk concept understood (Table 2), the final step is to investigate the relations of the remaining concepts. Although the frameworks define terms, describe and use concepts, the concept relations are often not sufficiently outlined. Brooks (2011) shows that experts often interpret context or mix concepts with their own experience to reach a conclusion about concept relations. Thus, it is not always clear which statement about concepts are actually based on definitions (by frameworks) and which are an (educated) assumption of the expert. At least ISO established a clear cross-referencing system to refer to terms by using unique identifiers, but other frameworks do not even always highlight terms used in the definition of other terms. This makes it difficult to understand the connection of terms and therefore derive the concept relations. In this section, the relations of the previously identified key concepts are examined to show the structure of the ISRM key concept terminology they constitute.

Usually, it is necessary to identify concept relations by interpreting the definition of terms, similar to the approach in sections 5 and 6. For example, in the previous section, the *risk* concept was examined and concluded that it mainly relates to the two concepts *likelihood* and *impact*, a fact that became obvious after comparing the five concept diagrams (Fig. 1). Luko (2013b) makes also use of concept diagrams to visualise concept relations, which provide an overview of the structure of a terminology. It seems appropriate to pursue this approach and create a concept diagram for all the key concepts.

To create the key concept diagram, all terms from Table 1 were used. As with the risk concept diagram, the concepts represented by term definitions were analysed and the concept relations were derived accordingly. A notation based on the Unified Modelling Language (UML) was chosen to visualise the concept diagram. Brownsword and Setchi (2011) also use the UML to depict their RM ontology and in the SID Information Framework (TMF 2019) UML class diagrams are used to visualise the relationships between business entities, so it seems an appropriate choice.

Since the frameworks use different terms for the same concept, it was necessary to select one term for the diagram. Therefore, the most frequently used term was used as representative of the concept. If there is no majority, because all frameworks use a different term, the one from ISO was used. The terms used in the diagram are highlighted bold in Table 1.

Figure 2 shows the created concept diagram. The result is a coherent and cohesive model that graphically represents the key concepts of ISRM according to the frameworks in this analysis. It can be seen that starting with the top category fully covered (DC5) every DC forms a self-contained conceptual model. This property is retained when it is extended to mostly covered (DC4), which only adds additional concepts and establishes terminated concept relations. This supports the assumption that these concepts are actually essential elements in the ISRM domain. Otherwise, it would be expected to see some orphans that are not tightly

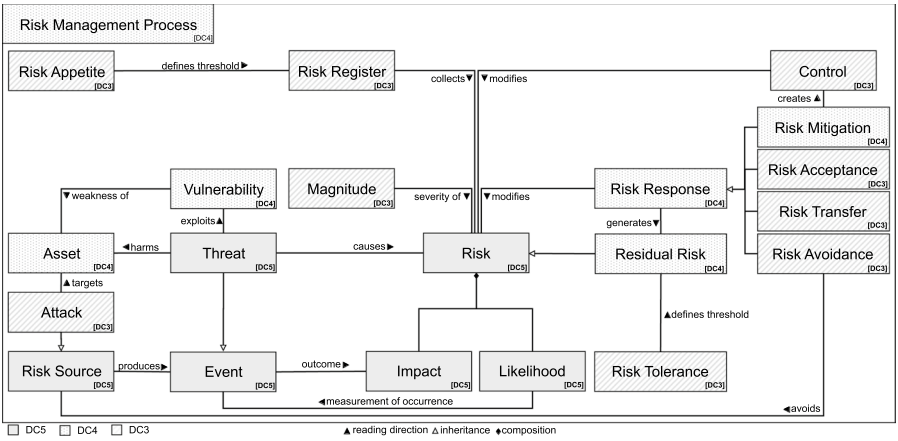

Fig. 2 ISRM key concept diagram

coupled. It can be assumed that further concepts, as seen in DC3, only refine the ISRM model, but do not change it. Consequently, the DC5 terminology could be fundamental and would represent a minimum viable model of ISRM.

Due to the often inadequate or only superficially implied concept relations, the creation of this concept diagram proofed difficult. Especially the ISO standards define concept relations poorly, despite the fact that the framework is well structured for the rest. For example, ISO states that an *event* is an 'occurrence or change of a particular set of circumstances' (ISO 2018a), i.e. does not define any association. On the one hand, ISO 27005 defines *likelihood* as 'chance of something happening' (ISO 2018b). On the other hand, Guide 73 adds the *frequency* as 'number of events or outcomes per defined unit of time' (ISO 2009). Both terms seem to define the same concept to describe probability using a numerical value and thus were aggregated in Table 1, but only one definition adds clear reference to an *event*. The consideration that in this context 'something' could also mean an 'occurrence' is good guess, but difficult to proof on its own. Similar effects can be observed for the other frameworks, too. It seems that the concept relations remain weakly defined and arise significantly from the context of use rather than from the semantics of terms.

This is surprising, as the understanding of the relations between terms and concepts is often presented in a uniform way when applied in practice. In the industry it is common knowledge that risks consists of threats acting against a vulnerability of an asset. In fact, this relationship can be derived from the activities described in the content of the ISRM frameworks, but it is not explicitly defined as part of the terminology. Once again, the question arises whether these differences are actually perceived, interpreted and applied by practitioners. In terms of academic purposes, a well-defined information model would enable to clearly define the semantic associations of ISRM.

Figure 2 shows that it is possible to create a reasonable, generic ISRM key concept diagram by just considering ISRM key concepts and defined concept relations. Since the diagram is basically framework independent and the terms are translatable

to other frameworks using Table 1, it can be used as a generic tool across different organisations and sectors. Researchers can refer to the concept diagram in their academic work if they intend to use generic terms or need to reference specific concepts. Finally, the concept diagram in combination with the table of terms helps researchers, scholars and practitioners to better understand and apply ISRM terminology.

The communication challenge, however, is not specific to ISRM, but applies to any RM domain. As mentioned before, other RM disciplines suffer from this state of ambiguousness, too, but were not able to agree on a uniform terminology yet (Aven 2016). This becomes particularly a problem, if companies aim to build a comprehensive Enterprise Risk Management (ERM) across multiple domains within their organisation. Since ERM combines risks of different areas (D'Arcy and Brogan 2001), like hazards, financial, operational and strategic, a common interface is necessary but complex to design. ISRM, for example, relies almost entirely on qualitative risk assessment, because it is still very difficult to apply quantitative methods. Yet, the latter is the de facto standard in some other disciplines, which poses a challenge if they are to produce comparable results. While it is likely that such methodical issues will disappear as the field evolves, the subject-specific language will remain. The natural development will take its time, but as a first step the mapping of terms and concepts can facilitate a better collaboration within the enterprise. Still, other RM domains struggle with fragmented terminologies, too. In order to improve the incorporation of various fields into one ERM, it would require other RM domains to validate their terminology as well. Although an overarching RM terminology has not been successfully defined so far, each field can probably identify its own set of core terms and key concepts. Clarifying the relation between these, providing a straight approach to map and translate between RM domains can improve collaboration in ERM. In this regard, the presented terms, concepts and concept relations shed light on the ISRM domain. Since the introduced method is generically applicable, it could be used in other domains as well. In the end, a better understanding will most likely boost communication within the enterprise or even enable collaboration activities like risk information sharing across organisations.

Conclusion

In this publication, the current terminology in the field of ISRM was examined based on a review of popular frameworks and industry standards. Their terms, definitions and established concepts were analysed and compared with each other to identify key concepts, i.e. equal concepts commonly used in most frameworks ($DC \geq 3$). As assumed, these key concepts exist, but fewer than expected: only 6 concepts are used across all frameworks and another 15 are used in at least 3 frameworks, all other concepts are specific to one or two frameworks. Furthermore, it has been shown that the central concept of *risk* is defined in a largely uniform manner (Fig. 1). Although the definition is often very similar in each framework (Table 2), it is not exactly the same, most notably in the ISO standards. Small but significant differences can be found in regard to the terms *likelihood* and *magnitude*, with ISO as the only framework that introduces the term *level of*

risk and a *risk* concept based on uncertainty. Finally, the relations of the identified key concepts were investigated, whereby it became apparent that many relations arise rather from the context of the process than clear definitions. Although concept relations are not well defined in the frameworks, it was possible to derive and visualise them in a concept diagram (Fig. 2). The chain of relations in the model terminates for each DC, i.e. there is a self-contained model for every level, but each level adds additional concepts to the previous one. It can be assumed that fully covered key concepts (DC5) are fundamental to the ISRM process, which means that they are mandatory in every ISRM process, an assumption that may be verified in a case study.

The produced key concept model, consisting of a table of concepts (Table 1) and a concept diagram (Fig. 2), enables cross-sector and inter-organisational discussion and thus the application or investigation of the corresponding management approaches. The derived key concept diagram can be used as a generic tool for understanding ISRM, especially in the academic environment, and the discovered issues in regard to terms and concepts may help to remove ambiguity. A future investigation could compare the key concepts and their relations with the perceived concepts of ISRM experts. In order to do this, experts would need to describe their own ISRM terminology and key concepts, which are then compared with the presented concept model. The comparison could provide an insight into the overlap between terminology theory and practice, which is an indicator of the maturity of ISRM concepts.

It remains a challenge to include ISRM, which is a comparatively young field, into the larger RM context. Unambiguous definitions of terms and concepts are a prerequisite to any integration efforts. Operative risks are an important part of any ERM and need to be aligned with other RM processes to be effective as a whole. The proposed ISRM core terminology supports organisations to integrate information and cyber risks more effectively into their enterprise risk strategy. The same or a similar approach may be used in other fields as well to align their concepts and provide a comparable terminology. In general, a better understanding of different risk domains will improve coordination and collaboration of RM activities.

Furthermore, the key concept model can be applied to specific use cases. Particularly distributed or federated service providers, which provision services from different locations cross-organisational as well as inter-organisational, communication can be simplified and standardised in this way. The authors plan to create an information and communication model based on the key concepts that can be used across organisational boundaries. The presented model is a first step to establish a common but framework-independent information flow, which allows organisations to cooperate in ISRM without adjusting their internal processes. In the long term, this aims to enable risk-based inter-organisational collaboration by defining standardised entities for each concept to integrate outbound interfaces into the ISRM process. Without a common and framework-independent understanding of terms and concepts, inter-organisational ISRM remains difficult, but the presented key terminology can help to fill the gap.

Funding Open Access funding enabled and organized by Projekt DEAL.

Declarations

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

References

Alberts, Christopher and Dorofee Audrey. 2002. Managing Information Security Risks: The OCTAVE Approach. Addison-Wesley Professional. ISBN: 0-321-11886-3.

American National Standards Institute [ANSI]. 2011. ANSI/ASSE Z690.1. Vocabulary for Risk Management.

Aven, Terje. 2011. On the new ISO guide on risk management terminology. Reliability Engineering & System Safety 96(7): 719-726. ISSN: 0951-8320. https://doi.org/10.1016/j.ress.2010.12.020.

Aven, Terje. 2016. Risk assessment and risk management: Review of recent advances on their foundation. European Journal of Operational Research 253(1): 1-13. ISSN: 0377-2217. https://doi.org/10.1016/j.ejor.2015.12.023.

Aven, Terje et al. 2018. Society for Risk Analysis Glossary. SRA. https://www.sra.org/riskanalysis-introduction/risk-analysis-glossary/

AXELOS. 2012. Management of Risk: Guidance for Practitioners. TSO. ISBN: 9780113312740.

Boulanger, Michele, Mark E. Johnson, and Stephen N. Luko. 2012. Statistical Standards and ISO, Part 1. *Quality Engineering* 24 (1): 94–101. https://doi.org/10.1080/08982112.2012.623956.

Brooks, David. 2009. *Key concepts in security risk management: A psychometric concept map to approach to understanding*. Saarbrücken: VDM Verlag.

Brooks, David. 2011. Security risk management: A psychometric map of expert knowledge structure. *Risk Management* 13: 17–41. https://doi.org/10.2307/41289355.

Brownsword, Mike, and Rossi Setchi. 2011. A Formalised Approach to the Management of Risk: Process Formalisation. *International Journal of Knowledge and Systems Science* 2: 63–80. https://doi.org/10.4018/jkss.2011070105.

Committee of Sponsoring Organizations of the Treadway Commission [COSO]. 2017. Enterprise Risk Management - Integrated Framework. https://www.coso.org/(visited on 06/08/2021).

Committee on National Security Systems [CNSS]. 2015. CNSS Glossary. 4009. https://rmf.org/wp-content/uploads/2017/10/CNSSI-4009.pdf.

D'Arcy, Stephen, and John C. Brogan. 2001. Enterprise Risk Management. *Journal of Risk Management of Korea* 12: 207–228.

Dallas, Michael. 2013. Management of Risk: Guidance for Practitioners and the International Standard on Risk Management, ISO 31000:2009. The British Standards Institution.

European Union Agency for Cybersecurity [ENISA]. 2021. Risk Management Glossary. https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/glossary (visited on 01/08/2021).

Freund, J. 2015. Measuring and Managing Information Risk: A FAIR Approach. Butterworth- Heinemann. ISBN:978-0-12-420231-3.

Audit, Information Systems, Control Association, and [ISACA]. 2009. *Risk IT Framework*. IL: Rolling Meadows 978-1-60420-111-6.

Information Systems Audit and Control Association [ISACA]. 2009b. Risk IT Practitioner Guide. ISBN: 978-1-60420-116-1.
Information Systems Audit and Control Association [ISACA]. 2012a. COBIT 5. COBIT 5. ISBN: 978-1604202373.
Information Systems Audit and Control Association [ISACA]. 2012b. COBIT 5 for Information Security. COBIT 5. ISBN: 978-1-60420-255-7.
Information Systems Audit and Control Association [ISACA]. 2013. COBIT 5 for Risk. COBIT 5. Rolling Meadows, IL. ISBN: 978-1-60420-457-5.
Information Systems Audit and Control Association [ISACA]. 2018a. COBIT 2019 Framework. Governance and Management Objectives. COBIT 2019. ISBN: 978-1-60420-764-4.
Information Systems Audit and Control Association [ISACA]. 2018b. COBIT 2019 Framework. Introduction and Methodology. COBIT 2019. ISBN: 978- 1-60420-763-7.
Information Systems Audit and Control Association [ISACA]. 2020a. Glossary. www.isaca.org/resources/glossary (visited on 07/17/2020).
Information Systems Audit and Control Association [ISACA]. 2020b. Risk IT Framework. 2nd ed. ISBN: 978-1-60420-820-7.
International Organization for Standardization [ISO]. 2007. Terminology work—Harmonization of concepts and terms. ISO 860:2007. https://www.iso.org/standard/40130.html.
International Organization for Standardization [ISO]. 2009. Risk management-Vocabulary. *ISO GUIDE* 73: 2009.
International Organization for Standardization [ISO]. 2012. Guidelines for cybersecurity. ISO/IEC 27032:2012. https://www.iso.org/standard/44375.html.
International Organization for Standardization [ISO]. 2018a. Information security management systems—Overview and vocabulary. ISO/IEC 27000:2018. https://www.iso.org/standard/54534.html.
International Organization for Standardization [ISO]. 2018b. Information security risk management. ISO/IEC 27005:2018. https://www.iso.org/standard/75281.html.
International Organization for Standardization [ISO]. 2018c. Risk Management - Guidelines. ISO 31000. OCLC: 1099576589.
International Organization for Standardization [ISO]. 2019. Terminology work and terminology science—Vocabulary. ISO 1087:2019. https://www.iso.org/standard/62330.html.
Knight, Frank Hyneman. 1921. *Risk, uncertainty and profit*. New York: Kelley.
Kockaert, Hendrik, J., and Steurs Frieda, eds. 2015. Handbook of Terminology. Vol. 1. John Benjamins. ISBN: 9789027257772. https://doi.org/10.1075/hot.1.
Luko, Stephen N. 2013. Risk Management Principles and Guidelines. *Quality Engineering* 25 (4): 451–454. https://doi.org/10.1080/08982112.2013.814508.
Luko, Stephen N. 2013. Risk Management Terminology. *Quality Engineering* 25 (3): 292–297. https://doi.org/10.1080/08982112.2013.786336.
Luko, Stephen N. 2014. Risk Assessment Techniques. *Quality Engineering* 26 (3): 379–382. https://doi.org/10.1080/08982112.2014.875769.
Luko, Stephen N., and Mark E. Johnson. 2012. Statistical Standards and ISO, Part 2 - Terminology. *Quality Engineering* 24 (2): 346–353. https://doi.org/10.1080/08982112.2012.654437.
Lund, Mass, Bjørnar. Solhaug, and Ketil Stølen. 2011. *Model-Driven Risk Analysis*. The CORAS Approach: Springer 978-3-642-12322-1. https://doi.org/10.1007/978-3-642-12323-8.
National Institute of Standards and Technology [NIST] 2006. Minimum Security Requirements for Federal Information and Information Systems. 200. https://doi.org/10.6028/NIST.FIPS.200.
National Institute of Standards and Technology [NIST]. 2011. Managing Information Security Risk. Organization, Mission, and Information System View. NIST SP 800-39. Gaithersburg, MD. https://doi.org/10.6028/NIST.SP.800-39.
National Institute of Standards and Technology [NIST]. 2012. Guide for Conducting Risk Assessments. NIST SP 800-30r1. Gaithersburg, MD. https://doi.org/10.6028/NIST.SP.800-30r1.
National Institute of Standards and Technology [NIST]. 2013. Security and Privacy Controls for Federal Information Systems and Organizations. NIST SP 800-53r4. https://doi.org/10.6028/NIST.SP.800-53r4.
National Institute of Standards and Technology [NIST]. 2018. Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy. NIST SP 800-37r2. Gaithersburg. https://doi.org/10.6028/NIST.SP.800-37r2.
Rey, Alain. 1995. Essays on Terminology. John Benjamins. ISBN: 9789027283580. https://doi.org/10.1075/btl.9.

Schmidt, Michael, Michael Brenner, and Thomas Schaaf. 2019. IT Service Management Frameworks Compared - Simplifying Service Portfolio Management. In: 2019 IFIP/IEEE Symposium on Integrated Network and Service Management (IM), pp. 421-427.

Shameli-Sendi, Alireza, Rouzbeh Aghababaei-Barzegar, and Cheriet, Mohamed. 2016. Taxonomy of information security risk assessment (ISRA). Computers & Security 57: 14-30. ISSN: 0167-4048. https://doi.org/10.1016/j.cose.2015.11.001.

Shameli-Sendi, Alireza, M. Jabbarifar, M. Shajari, and M. Dagenais 2010. FEMRA: Fuzzy Expert Model for Risk Assessment. In: 2010 Fifth International Conference on Internet Monitoring and Protection, pp. 48-53. https://doi.org/10.1109/ICIMP.2010.15.

Australia Standards. 2004. AS/NZS 4360:2004. Risk management.

The Open Group [OpenGroup]. 2010. FAIR-ISO/IEC 27005 Cookbook. https://publications.opengroup.org/c103.

Standards Australia. 2013a. Risk Analysis (O-RA). Open Group Technical Standard. https://publications.opengroup.org/c13g.

Standards Australia. 2013b. Risk Taxonomy (O-RT). 2nd ed. Open Group Technical Standard. https://publications.opengroup.org/c13k.

Standards Australia. 2016. The Open FAIR - NIST Cybersecurity Framework Cookbook. ISBN: 1-937218-80-5. https://publications.opengroup.org/g167.

TM Forum [TMF]. 2019. Information Framework (SID). Open Digital Framework (Frameworx). https://www.tmforum.org/resources/reference/gb922-information-framework-r19-0/.

Wangen, Gaute, Christoffer Hallstensen, and Snekkenes, Einar. 2018. A Framework for Estimating Information Security Risk Assessment Method Completeness: Core Unified Risk Framework, CURF. International Journal of Information Security 17(6): 681-699. ISSN: 1615-5262, 1615-5270. https://doi.org/10.1007/s10207-017-0382-0.

Yazar, Zeki. 2002. A Qualitative Risk Analysis and Management Tool - CRAMM. SANS. https://www.sans.org/reading-room/whitepapers/auditing/qualitative- risk-analysis-management-tool-cramm-83.