Int. J. Inf. Secur.
DOI 10.1007/s10207-017-0382-0

REGULAR CONTRIBUTION

A framework for estimating information security risk assessment method completeness

Core Unified Risk Framework, CURF

Gaute Wangen[1] · **Christoffer Hallstensen**[2] · **Einar Snekkenes**[1]

Abstract In general, an information security risk assessment (ISRA) method produces risk estimates, where risk is the product of the probability of occurrence of an event and the associated consequences for the given organization. ISRA practices vary among industries and disciplines, resulting in various approaches and methods for risk assessments. There exist several methods for comparing ISRA methods, but these are scoped to compare the content of the methods to a predefined set of criteria, rather than process tasks to be carried out and the issues the method is designed to address. It is the lack of an all-inclusive and comprehensive comparison that motivates this work. This paper proposes the Core Unified Risk Framework (CURF) as an all-inclusive approach to compare different methods, all-inclusive since we grew CURF organically by adding new issues and tasks from each reviewed method. If a task or issue was present in surveyed ISRA method, but not in CURF, it was appended to the model, thus obtaining a measure of completeness for the studied methods. The scope of this work is primarily functional approaches risk assessment procedures, which are the formal ISRA methods that focus on assessments of assets, threats, vulnerabilities, and protections, often with measures of probability and consequence. The proposed approach allowed for a detailed qualitative comparison of processes and activities in each method and provided a measure of completeness. This study does not address aspects beyond risk identification, estimation, and evaluation; considering the total of all three activities, we found the "ISO/IEC 27005 Information Security Risk Management" to be the most complete approach at present. For risk estimation only, we found the Factor Analysis of Information Risk and ISO/IEC 27005:2011 as the most complete frameworks. In addition, this study discovers and analyzes several gaps in the surveyed methods.

Keywords Information security · Risk assessment · Methodology · Completeness

✉ Gaute Wangen
gaute.wangen@NTNU.no

Christoffer Hallstensen
christoffer.hallstensen@NTNU.no

Einar Snekkenes
einar.snekkenes@NTNU.no

[1] Department of Information Security and Communication Technology, NTNU, Teknologiveien 22, 2815 Gjøvik, Norway

[2] Digital Security Section, NTNU, Teknologiveien 22, 2815 Gjøvik, Norway

1 Introduction

Information security (InfoSec) risk comes from applying technology to information [1], where the risks revolve around securing the confidentiality, integrity, and availability of information. InfoSec risk management (ISRM) is the process of managing these risks, to be more specific; the practice of continuously identifying, reviewing, treating, and monitoring risks to achieve risk acceptance, illustrated in Fig. 1. A baseline level of security can be achieved through compliance with current law and legislation, but best practice InfoSec is highly dependent on well-functioning ISRM processes [1], which requires a tailored program to suit the risk taking of the organization. Typically, risks for information systems are analyzed using a probabilistic risk analysis, where risk is a measure of the probability of occurrence of an event and the associated consequences for the organization (e.g., financial loss if a risk occurred).

InfoSec risk assessment (ISRA) practices vary between industries, disciplines, and even within the same orga-

Published online: 28 June 2017

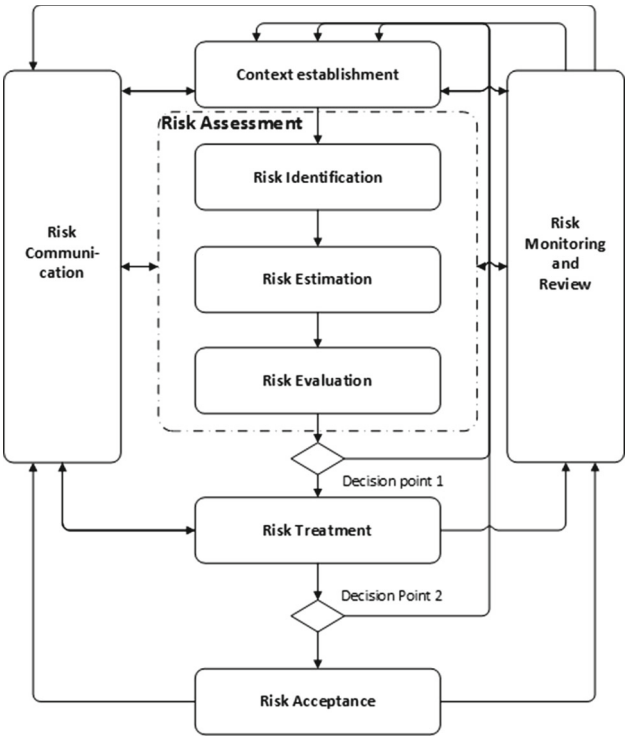

Fig. 1 The ISO/IEC 27005:2011 ISRM process, the *risk assessment* activities mark the scope of this paper

nization, which has brought a variety of ISRA methods [2] and risk definitions [3]. This article covers the risk assessment process, including risk identification, estimation, and evaluation, and compares the completeness of eleven surveyed ISRA methods. For clarification, the main difference between risk assessment and analysis is, according to ISO/IEC 27000:2016 [4], that the latter does not include the risk evaluation.Further, we develop a framework for comparing ISRA methods on their completeness. We demonstrate the utility of the framework by applying it to a collection of risk assessment methods, identifying several limitations and weaknesses of existing risk assessment approaches, of which several were previously not well known. For example, besides the FAIR approach [5] there are few detailed approaches to obtaining quantitative estimates regarding the probability of occurrence. All of the surveyed methods include an approach for qualitatively describing risk impact, while only three of the eleven methods provide guidance on how to quantify loss estimates. According to our results, asset identification and evaluation are two of the most common risk identification activities. Although business processes are defined as one of two primary assets in ISO/IEC 27005:2011 (ISO27005) [6], very few methods include the business process in the asset identification. Further, our results show that risk concepts, such as opportunity cost, cloud risk, incentive calculations, and privacy risk estimations, are only present in topic-specific methods and have a low adaptation rate in the surveyed methods. Also, none of the studied methods discuss the Black Swan concept proposed by Taleb [7], or wholly adopted the qualitative *knowledge* metric of qualitative risk assessments as suggested by Aven and Renn [8].

Note that our comparison framework is restricted to ISRA and that we apply the framework to the risk analysis and evaluation part of the surveyed methods. Thus, a comparison of non-risk assessment elements from full risk management methods is outside of scope.

Using the terminology established by Campbell and Stamp [9], the extent of this work is primarily *functional* approaches [9], which are the formal ISRA methods that focus on assessments of threats and protections, often with measures of probability and consequence. As opposed to *temporal* approaches that tests components of actual attacks, such as penetration tests and red teams, while *comparative* methods compare systems to best practices and establish security baselines. We have not evaluated accompanying software tools for each method in the Core Unified Risk Framework (CURF). Some methods, such as FAIR and CRAMM [10], come with software that expands aspects of the approach, but these are outside of scope.

The remainder of the paper is organized as follows, and Sect. 2 provides general background information on the eleven surveyed ISRA methods. In Sect. 3, we present the design science research approach applied to develop CURF. Further, in Sect. 4, we implement the framework on popular ISRA methods and show the results. Further, we discuss the completeness of each surveyed method and limitations of current approaches in Sects. 5 and 6. Lastly, we establish the relationship to other literature in Sect. 7, discuss limitations and propose future work in Sect. 8, and conclude in Sect. 9.

2 Reviewed methods

We have reviewed nine well-documented ISRA methods which all have in common that they have been specifically developed to address InfoSec risk and are well-documented. Besides, CURF contains one review of both a privacy and a cloud risk assessment method. The following is a summary of the eleven methods:

CIRA is a risk assessment method developed primarily by Rajbhandari [11] and Snekkenes [12]. CIRA frames risk as conflicting incentives between stakeholders, such as information asymmetry situations and moral hazard situations. It focuses on the stakeholders, their actions, and perceived outcomes of these actions.

CORAS is a UML (Unified Modeling Language) model-based security risk analysis method developed for InfoSec [13,14]. CORAS defines a UML language for security concepts such as threat, asset, vulnerability, and scenario, which is applied to model unwanted incidents and risks.

The CCTA Risk Analysis and Management Method (CRAMM v.5) is a qualitative ISRA method [10]. CRAMM centers on the establishment of objectives, assessment of risk, and identification and selection of countermeasures. The method is specifically built around the supporting tool with the same name and refers to descriptions provided in the repositories and databases present in the tool.

FAIR (Factor Analysis of Information Risks) is one of the few primarily quantitative ISRA approaches [5,15]. FAIR provides a risk taxonomy that breaks risks down into twelve specific factors, where each factor contains four well-defined factors for the loss and probability calculations. FAIR includes ways to measure the different factors and to derive quantitative analysis results.

The Norwegian National Security Authority Risk and Vulnerability Assessment (NSMROS) [16] approach was designed for aiding organizations in their effort to become compliant with the Norwegian Security Act. NSMROS is written in Norwegian and provides a basic description of the risk management process and associated activities.

OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) Allegro methodology is the most recent method of the OCTAVE-family [17], aimed at being less extensive than the previous installments of OCTAVE. It is a lightweight version of the original OCTAVE and was designed as a streamlined process to facilitate risk assessments without the need for InfoSec experts and still produce robust results [17] (p. 4).

The ISO/IEC 27005:2011—Information technology, Security techniques, Information security risk management [6] (ISO27005) details the complete process of ISRM/RA, with activities, inputs, and outputs of each task. It centers on assets, threats, controls, vulnerabilities, consequences, and likelihood. Since we regard ISO27005 as the industry best practice, it also provides the frame for CURF.

The current installment of the NIST SP 800-30 - Guide for Conducting Risk Assessments is at revision one [18] (NIST80030) and was developed to further statutory responsibilities under the Federal Information Security Management Act. NIST800-30 was designed to aid larger and complex organizations in information risk management. The purpose of the publication was to produce a unified information security framework for the US federal government.

The ISACA (Information Systems Audit and Control Association) Risk IT Framework and Practitioner Guide [19,20] is an ISRM/RA approach where the Practitioner Guide complements the Risk IT Framework. The former provides examples of how the concepts from the framework can be realized. It is an established approach developed by ISACA, based on ValIT and CobIT, and, therefore, has a business view on InfoSec risks, defining several risk areas and factors.

Privacy impact assessments are methods that identify and analyze specific risks to privacy in a system or a project. The Norwegian Data Protection Authority's (Datatilsynet) *risk assessment of information systems* (RAIS) [21] are ISRA guidelines that primarily are designed to aid data handlers in their effort to become compliant with the Norwegian Data Protection and Privacy Act with corresponding regulations.

Outsourcing services to the cloud bring new third-party risks to the organization. Microsoft's *Cloud Risk Decision Framework* [22] is a method designed for addressing this problem by risk assessing cloud environments. The method is derived from the ISO 31000 standard for Risk Management and provides a framework for working with cloud-associated risk.

3 Framework development

The necessity of a bottom-up approach for comparing ISRA methods became apparent when we were studying cause and effect relationships between applying an ISRA method, the work process, and the resulting output. ISRA methods are often comprehensive and comparing tasks at a sufficient level of detail is challenging. There exist multiple frameworks for comparing ISRM/RA methods [2,9,23–27]; however, these are primarily scoped to compare method content to a predetermined set of criteria. In these frameworks, evaluation proceeds from the predetermined criteria at the top to methods at the bottom. The existing approaches yield differences within the criteria and are equivalent of top-down static comparison. This approach is restrictive because the framework will overlook any tasks or parameters that the criteria do not cover. CURF's bottom-up approach solves this problem by providing a way to review each ISRA method, structure its tasks within ISO27005's risk management process, and use the complete task set as comparison criteria.

The framework idea is as follows: For each method, CURF users identify which tasks the approach covers and then combine all the tasks covered by all the surveyed methods into a combined set. For example, one method might propose to identify threats as a task, but another does not, so "threat identification" becomes a task under the risk identification group. Further, we unify all issues covered by each of the methods into a superset. An application of the framework to a risk assessment method amounts first to identify the issues covered by the method and then merging this set with the larger set of issues constructed previously. The completeness evaluation of a risk analysis method amounts to investigating the extent the said method covers all issues present in the superset constructed previously. The superset should provide the practitioner with insight into which aspects each method cover, together with an overview of where to seek knowledge

in the literature to solve other specific issues or for comparison purposes.

Further, in the following sections, we describe the choice of method for framework development, specific CURF development issues, and inclusion and exclusion criteria for the ISRA methods.

3.1 Design science research

The scientific approach applied to develop CURF overlaps with the concepts of the design science research (DSR) methodology. DSR is a problem-solving process specifically designed for research in complex information systems [28]. DSR addresses unsolved research problems experienced by stakeholders within a particular practice and solves them in unique or innovative ways [29] (p. 15). The first step of the DSR process is to define the problem and, further, to determine the requirements, design, and develop an artifact to address the problem. Followed by a demonstration and an evaluation of the artifact. This study had a defined research problem which needed an artifact to solve it, which renders DSR the obvious choice approach for this study. We both designed the artifact, the comparison framework, and continuously developed and demonstrate it through classification of ISRA methods within the framework and improving the model. We evaluate the model by applying the comparison scheme on the existing methods by adding all standalone tasks, described in Fig. 2, and deriving new knowledge. Hevner [29] (p.15) writes that *the key differentiator between professional design and design research is the clear identification of a contribution to the archival knowledge base of foundations and methodologies and the communication of the contribution to the stakeholder communities*. We consider the DSR contribution in this study as primarily the artifact, CURF, which entails a method and a data model where the application of CURF to produces a knowledge contribution to the ISRA community.

One of the keys to DSR is to develop an artifact, demonstrate, and communicate its utility. For this purpose, recent work on DSR methodology has provided the community with the DSR knowledge contribution framework [30], which defines the DSR contributions utility within four quadrants. The quadrants are described with *solution maturity* (SoM) on the Y-axis and *application domain maturity* (ADM) on the X-axis, both scored subjectively using "high" and "low."

Fig. 2 CURF development process

For example, a high ADM and SoM constitute a known solution to a known problem, referred to as a *routine design*. A high SoM and low ADM are an *exaptation*, where a known solution is applied to a new problem. A low score on both is classified as an *invention*, as it is a new solution for a new problem.

CURF represents a novel method and model for bottom-up ISRA method classification, comparison, and estimating completeness. The problems of method classification and comparisons are not unique. However, the problem of determining method completeness is novel, and CURF is a new solution to the problem which places CURF in the *invention* quadrant representing both a knowledge contribution and a research opportunity.

3.2 CURF comparisons, tables, and scores

The basis for the model was the ISO27005 model for ISRM, Fig. 1, which holds a level of acceptance in the InfoSec community [31]. The three core activities of the CURF model consist of *risk identification*, *risk estimation* and *risk evaluation*. The authors of this study evaluated each method and concept according to the following methodology: If a problem was addressed in an ISRA method, but not in the framework, we added it to the model. If a previously added item was partially addressed or mentioned to an extent in a compared method, but not defined as an individual task, we marked it is as partially present. In this way, we mapped ISRA processes with coherent tasks and compared the ISRA method to the model to see where they divert and how. This approach allowed for a detailed qualitative comparison of processes and activities for each method and provided a measure of completeness. For evaluation of tasks, CURF uses three scores: A task or issue is *addressed* when it is fully addressed with clear descriptions on how to solve it. *partially addressed* when a task or issue is suggested but not substantiated. While the *not addressed* score is applied for methods that do not mention or address a particular task at all. We converted the scores to numerals for calculations of sum, mean, and averages. The X-axis also has a "Sum"-column which displays the total score per row, which is useful to highlight how much emphasis the authors of all the methods put in sum on each task and activity.

We have divided the comparison tables into four tables, whereas Table 1 addresses *risk identification*- related issues. Table 2 addresses *risk estimation*, and Table 3 addresses *evaluation*-related issues. Table 4 summarizes the scores and addresses completeness. The two former tables list the identified tasks and activities in the Y-axis and the surveyed methods in the X-axis.

CURF also contains scores on process output from the risk identification and estimation phases; these output criteria are based on best practices and state-of-the-art research

on risk assessments [3,8,32]. We have also added a row of completeness scores without the output criteria in the results (Table 4) since these scores are derived from best practices and not a direct product of applying CURF.

3.3 Inclusion and exclusion criteria

The CURF review presented in this paper is by no means a complete overview of existing ISRA methods, as there are over one hundred different ISRA approaches at the time of writing [2]. We have restricted this study to include eleven methods as it is the idea of CURF which we consider the most important contribution of this research. However, we aimed to include a wide range of methods into CURF and chose them according to the following criteria:

- Over fifty citations in the academic literature (CRAMM, CORAS, FAIR, OCTAVE Allegro, NIST80030).
- Industry best practice (ISO27005 and RISK IT).
- Specific risk topics: incentives risk (CIRA), cloud risk (CRDF), and privacy risk (RAIS).
- Two Norwegian methods with prior familiarity for the authors (NSMROS and RAIS).
- Includes a description of the risk identification, estimation, and evaluation steps (all).
- Not older than fifteen years at a time of review (all).
- Published in English (nine) or Norwegian (two).

In addition to these criteria, the studied methods all had their dedicated publication in either peer-reviewed channel, standard, or white paper, which contained comprehensive descriptions of work flow and components. The included methods provide a broad sample of ISRA methods regarding usage, best practices, academic citations, and covered topics. This sample equips CURF with a comprehensive set of tasks to highlight differences between the methods, completeness, and exhibit the utility of CURF. A path for future work is to expand the framework with additional methods as to make the set more representative.

4 Core Unified Risk Framework (CURF)

In this section, we propose the Core Unified Risk Framework (CURF) for comparing issues in ISRA methods. Following the method outlined in Sect. 3, we surveyed each of the eleven methods described in Sect. 2 and created the CURF model. Figure 3 is a high-level representation of the results where the colored tasks indicate sub-activities which we describe in more detail in the subsequent section. Following, we outline each of CURF's descriptive categories, identified process tasks, and sub-activities. The tasks are grouped and presented in three primary categories: (i) risk identification, (ii) estimation, and (iii) evaluation.

4.1 Descriptive categories in the framework

We applied two existing risk classification frameworks to define the initial differences between the included methods before committing them to the framework. The first framework proposed by Aven [3] addresses the risk definition and historical development and was also the only approach available for this type of analysis. Aven's approach reveals fundamental properties about the method since the risk (R) definition often correlates with the product of the risk assessment process. For example, if a method uses $R = ProbabilityxConsequence$, the risk descriptions produced by the same method should estimate these variables. In addition, the historical development paths of the multiple risk definitions are an interesting topic which has not been considered in InfoSec. He proposes nine classes of risk definitions; out of these nine classes, we found five concepts relevant for our analysis: R as (i) *expected value* ($R = E$), as (ii) *probability and consequence* ($R = P\&C$), as (iii) *consequence* ($R = C$), as (iv) *uncertainty and consequence* ($R = C\&U$), and lastly, as (v) *the effect of uncertainty on objectives* ($R = ISO$). A clarification is needed between the two similar $R = E$ and $R = P\&C$. The former is motivated by the law of large numbers and represents the risk as a sum of an expected loss [3]. While $R = P\&C$ is generally described by *set of triplets*, specifically a scenario, the likelihood of that scenario, and the associated consequences [33]. The $R = P\&C$ definition allows for both subjective and statistical probabilities. In addition, we added the conflicting incentives risk analysis's risk definition, which proposes a risk as conflicting incentives ($R = CI$) [11,12].

Secondly, we have added Sandia classifications [9] of each method to indicate the properties of the surveyed functional methods regarding skill level needed. The *matrix* methods provide look-up tables to support the user, often in the form of software, which requires less expertise from the user. *Assistant* methods provide rich documentation and lists for the user to keep track of the risks but require more experience. The abstract *sequential* methods perform tasks in a sequence of activities and require more expertise from the user than the other two. Both the risk definition and the Sandia classification reveal useful properties an ISRA method; hence, they are included in the comparison tables as classifications, but they do not affect the score.

4.2 Main process 1: risk identification

The main purpose of this process is to identify relevant risk for future assessment. The risk identification process often

Table 1 Risk identification process and output comparison. Scores: XX = 2, X = 1. Max = 22 per row and Max = 50 per column

		CIRA [34] 2012 *R* = *CI* Sequence	CORAS [13,14] 2006 *R* = *P&C* Sequence	CRAMM [10] 2002 *R* = *C* Matrix	FAIR [5,15] 2014 *R* = *P&C* Sequence	NSMROS [16] 2006 *R* = *P&C* Sequence	OCTAVE A [17] 2007 *R* = *C* Assistant	ISO27005 [6] 2011 *R* = ISO Sequence	NIST 800-30 [18] 2012 *R* = *P&C* Sequence	RISK IT [19,20] 2009 *R* = *P&C* Assistant	RAIS [21] 2011 *R* = *P&C* Sequence	CRDF [22] 2012 *R* = *ISO* Sequence	Sum
PA	Preliminary assessment	XX	XX	–	X	XX	XX	–	XX	XX	–	X	14
RC	Risk criteria determin.	XX	X	X	X	X	XX	XX	–	XX	XX	XX	16
RC	Cloud-specific considera.	–	–	–	XX	–	–	–	X	–	–	XX	5
RC	Business objective Id.	–	X	–	XX	–	XX	XX	–	XX	X	X	11
RC	Key risk indicators	–	–	–	XX	–	–	–	–	XX	–	–	4
SI	Stakeholder identification	XX	XX	–	XX	–	X	XX	–	XX	–	XX	13
SI	Stakeholder analysis	XX	–	–	XX	–	–	–	–	X	–	–	5
AI	Asset identification	X	XX	XX	XX	XX	XX	XX	–	X	XX	–	16
AI	Mapping of personal data	X	–	–	X	–	X	X	X	–	XX	–	7
AI	Asset evaluation	X	XX	XX	XX	XX	X	X	X	X	X	–	14
AI	Asset owner and custo.	XX	X	XX	X	–	XX	XX	–	–	–	–	10
AI	Asset container	–	X	X	–	–	XX	–	–	–	–	–	4
AI	Business process Id.	–	X	X	–	–	–	XX	X	X	–	–	6
Vu	Vulnerability Id.	X	XX	XX	X	X	X	XX	XX	X	–	X	14
Vu	Vulnerability assessment	–	XX	XX	–	–	–	XX	XX	X	X	–	10
Th	Threat identification	XX	XX	XX	XX	XX	XX	XX	XX	XX	–	–	18
Th	Threat assessment	XX	XX	XX	–	X	XX	XX	XX	–	–	–	13
Co	Control identification	X	X	–	–	–	X	XX	XX	–	–	XX	9
Co	Control assessment	–	–	–	–	–	–	XX	–	–	–	–	2
Ou	Outcome identification	–	XX	XX	X	XX	XX	XX	XX	XX	XX	XX	19
Ou	Outcome assessment	–	X	XX	–	–	X	XX	–	XX	XX	XX	12
RS	*Asset,*	XX	XX	XX	XX	XX	XX	XX	–	XX	XX	–	18
RS	*Vulnerability,*	X	XX	XX	–	XX	XX	XX	XX	X	X	X	16
RS	*Threat,*	XX	XX	XX	XX	XX	XX	XX	XX	XX	–	–	18
RS	*Outcome*	–	XX	XX	–	XX	XX	XX	XX	XX	XX	XX	18
	Completeness	24	33	29	26	21	32	38	24	29	18	18	

XX Addressed, x Partially addressed, – Not addressed

produces many risk scenarios where some are more severe than others. The assessment team then subjects the identified scenarios to a vetting process where the primary output are the risk scenarios the assessment teams find realistic.

From the development of the unified ISRA model, we found that ISRA methods conduct subsequent tasks at different steps, such as vulnerability assessments may be carried out in either the risk identification process and/or the risk estimation process. Thus, we only define the vocabulary once, although the definitions are the same throughout the ISRA process according to where the task is conducted. Following is a description of the branches in CURF (Fig. 3):

- *Preliminary assessment* (PA) is the process of conducting a high-level or initial assessment of the ISRA target to obtain an insight into the problems and scope, for example a high-level assessment of assets, vulnerabilities, and threat agents [16].
- *Risk criteria determination* (RC) The ISRA team and/or the decision-maker decides on risk criteria for the risk evaluation process, which the team uses as terms of reference to assess the significance of the risk. This category includes measurements of risk *tolerance* and *appetite*. Several ISRA also suggests to identify *business objectives* to aid in scoping the risk assessment and increasing relevance [5,20]. Risk tolerance and appetite are derived from the objectives. *Key risk indicators* build on the predefined appetite and are metrics showing if the organization is subject to risks that exceed the risk appetite [20]. *Cloud-specific risk considerations* are made specifically for cloud migrations and operations, and these include issues related to, for example, infrastructure, platform, and application as a service risks [22].
- *Stakeholder identification* (SI) is the process of identifying and prioritizing the stakeholders that need to be contacted and included in the risk assessment [5,11,14]. Stakeholder *analysis* is the process of analyzing the stakeholders according to relevant criteria, e.g., influence and interest in the project [5].
- *Asset identification* (AI) is the process of identifying assets, while asset *evaluation* assess their value and criticality [6]. We have distinguished between *business process identification* and assets [6]. Identifying the *asset owner* helps shape the scope and target of the risk assessment, while *asset container* identifies where assets are stored, transported, and processed [17]. *Mapping of personal data* is a part of the privacy risk assessment process, where the system's handling of information assets containing personal data is mapped and assessed, for example, according to law [21].
- *Vulnerability identification* (Vu) is the process of identifying vulnerabilities of an asset or control that can be exploited by one or more threats [4]. Vulnerability *assessment* is the process of identifying, quantifying, and prioritizing (or ranking) the vulnerabilities in a system.
- *Threat identification* (Th) is the process of identifying relevant threats for the organization. A threat *assessment* comprises of methods, and approaches to determine the credibility and seriousness of a potential threat [6].
- *Control identification* (Co) is the activity of identifying existing controls in relation to, for example, asset protection. *Control (efficiency) assessment* are methods and approaches to determine how effective the existing controls are at mitigating identified risk [6].
- *Outcome identification* (Ou) is the process of identifying the likely outcome of a risk (asset, vulnerability, threat) regarding breaches of confidentiality, integrity, and availability, while outcome *assessment* incorporates methods and approaches to estimating the potential outcome(s) of an event, often regarding loss [10,19].

4.2.1 Output from risk identification process

Although the risk identification process contains several additional activities, these are not necessarily reflected in the produced risk scenario. For example, existing countermeasures/controls can be a part of the vulnerability. We define the primary output of the risk identification process as a risk scenario (RS) based on asset (including business processes), vulnerability, threat, and outcome, for which we can compare the methods. We have given scores on the RS variables as they are well-developed concepts and relevant to the granularity of the risk assessment process. For example, an asset can be vulnerable without being threatened or threatened without being vulnerable. An asset can also be both threatened and vulnerable without being critical to the organization, thus not representing any significant risk. This argument makes the granularity of the RS important to ISRA process, and the *outcome* describes the components of the risk event as proposed by the reviewed methods.

4.3 Main process 2: risk estimation

The purpose of the risk estimation process is to assign values to the probability and consequence of the risk [6] of the plausible risk scenarios from the identification process. However, reaching realistic estimates of *P&C* has been one of the major challenges of the InfoSec risk community since the very beginning [35,36], especially in the quantitative approaches [37]. We have defined the following issues and tasks for the ISRA estimation process (supplemented with issues and tasks from the risk identification process):

Table 2 Risk estimation processes and output comparison. Scores: XX = 2, X = 1, – = 0. Scores Max = 22 per row and Max = 46 per column

		CIRA	CORAS	CRAMM	FAIR	NSMROS	OCTAVE A	ISO27005	NIST 800-30	RISK IT	RAIS	CRDF	Score
AI	Asset identification and evaluation	–	–	–	–	–	–	–	X	–	–	X	2
TA	Threat willingness/motivation	XX	–	–	–	–	XX	XX	XX	X	XX	–	11
TA	Threat capability (know how)	X	–	–	XX	–	–	X	XX	—	XX	–	8
TA	Threat capacity (Resources)	X	–	–	XX	–	X	X	–	–	XX	–	7
TA	Threat attack duration	–	–	–	XX	–	–	–	–	XX	–	XX	6
Vu	Vulnerability assessment	–	–	–	XX	XX	–	–	XX	–	–	–	6
Co	Control efficiency assessment	X	–	–	XX	–	–	X	X	–	X	XX	8
PI	Subjective *P* Est. for event	–	XX	XX	XX	X	X	XX	XX	XX	XX	XX	18
PI	Quantitative *P* Est. for event	–	X	–	XX	X	–	XX	XX	XX	X	X	12
PI	Subjective impact estimation	XX	XX	XX	XX	XX	XX	XX	XX	XX	XX	XX	22
PI	Quantitative impact estimation	–	X	X	XX	XX	X	XX	–	X	–	X	11
RD	Privacy risk estimation	X	–	–	–	–	–	–	X	–	XX	–	4
RD	Utility and incentive calc.	XX	–	–	–	–	–	–	–	–	–	–	2
RD	Cloud vendor assessment	–	–	–	X	–	–	–	X	–	–	XX	4
RD	Opportunity cost	XX	–	–	–	–	–	X	–	XX	–	–	5
LRD	Level of risk determination	–	–	–	–	–	–	XX	–	XX	–	X	5
Rag	Risk aggregation	–	–	–	–	–	X	XX	XX	XX	–	–	7
A	*Event,*	XX	XX	XX	XX	XX	XX	XX	XX	XX	XX	XX	22
C	*Consequence,*	XX	XX	XX	XX	XX	XX	XX	XX	XX	XX	XX	22
U	*Uncertainty,*	–	–	–	XX	–	X	X	X	–	–	X	6
P	*Probability,*	–	XX	X	XX	XX	X	XX	XX	XX	XX	XX	18
S	*Model sensitivity,*	–	–	–	XX	–	–	X	–	–	–	–	3
K	*Knowledge about risk*	X	–	–	X	–	–	X	X	–	–	–	4
	Completeness	17	12	10	30	14	14	27	26	22	20	21	

XX Addressed, x Partially addressed, – Not addressed

- *Threat assessment* (TA) expands the definition of risk identification, and the ISRA methods can provide tools to estimate the particular threat agent's (i) *willingness/motivation* to attack [11,18], (ii) *capability* in terms of know how [5,18], (iii) *capacity* in terms of resources available to conduct the attack [5], and (iv) the potential *Attack duration* which is often related to the consequences of the attack [5,19,20]. An example of the latter is the DDoS attack where the outcome of the event will be tightly related to the threats capacity to conduct a lengthy DDoS attack.
- *Probability and impact estimation* (PI) This is one of the main parts of the risk analysis process, where the risk assessors determine the probability and consequence of each identified risk. There are primarily two approaches to probability, frequentist (quantitative) or subjective knowledge-based assessments (qualitative) [3]. The frequentist probability expresses *"the fraction of times the event A occurs when considering an infinite population of similar situations or scenarios to the one analyzed"* [3]. The subjective (qualitative) probability expresses the *"assessor's uncertainty (degree of belief) of the occurrence of an event"* [3] which also relates to *impact estimation* where the analyst can estimate based on relevant historical data (if it exists), or make knowledge-based estimates of impacts/outcomes. The subjective knowledge-based and frequentist approaches require different activities and are defined as different activities.
- *Risk-specific estimations (RD)* are method or domain-specific estimations. *Privacy risk estimation* are specific methods to estimate risks to privacy [21]. *Utility and incentive calculation* addresses issues of utility calculations regarding the risk for each involved stakeholder and calculate the incentives for acting on a strategy [11]. *Cloud vendor assessment* includes methods for assessing the cloud vendor's existing security controls and compliance [22]. *Opportunity cost estimation* are assessments of how much it will cost not to act on an opportunity, by, for example, being too risk averse [11] (pp. 99–110).
- The *Risk aggregation* (RAg) activity is conducted to roll up several linked, often low-level risks into a more general or higher-level risk [18]. During an event, interconnected individual risks can also aggregate into a more severe risk into a worst-case scenario. This activity aims to identify and assess such potential developments.
- *Level of risk determination* (LRD) consists of assigning the estimated risk (incident) scenario likelihood and consequences, and compiling a list of risks with assigned value levels [6].

4.3.1 Output from the risk estimation process

In terms of risk estimation and evaluation, Aven [32] (p. 229) [8] proposes a comprehensive tR definition for discussion and comparison in CURF. Aven describes R as a function of events (A), consequences (C), associated uncertainties (U), and probabilities (P). U and P calculations rely on background knowledge (K) which captures the underlying assumptions of the risk model; for example, a low K about a risk equals more U. Model sensitivities (S) display the dependencies on the variation of the assumptions and conditions. Thus, $R = f(A, C, U, P, S, K)$ allows for an overall output for comparison, as this definition incorporates the most common components of risk and, therefore, constitutes the risk output of the risk evaluation of CURF. For comparison, we have applied the following: A is the risk event. C is an estimate of consequence. U is an output of uncertainty expressed as a part of the risk measurement, e.g., by calculating the confidence intervals of the measurements. The surveyed ISRA method, therefore, needs to apply measurements or frequencies to incorporate U. P relates to both qualitative and quantitative probabilities. S has the same prerequisites as U and is dependent on the risk model. The K aspect is present if the method explicitly states that additional knowledge about the risk should be incorporated and applied to adjust the estimations. These have been added to CURF to assist the reader in determining what to expect as output from using each method.

4.4 Main process 3: risk evaluation

In this process, the analyzed risks are evaluated and prioritized according to the risk score derived from the risk estimation process. The risk analysis team makes their recommendation regarding treatment of risks, sometimes according to the predefined risk criteria, and the decision-maker decides where to spend the available resources.

1. *Risk criteria assessment* (RCA) is the process of either creating or revising risk criteria to evaluate risk [11] (p. 82).
2. *Risk prioritization/evaluation* (RPE) is the process of evaluating risk significance and prioritizing for risk treatments and investments [6].
3. *Risk treatment recommendation* (RTR) is the process of suggesting treatments to assessed risk. This activity is according to ISO/IEC 27000-series conducted as an own process [6], but we have included it here since several of the surveyed ISRA methods suggest treatments as a part of the risk evaluation process [10,17,19,21].

Table 3 Risk evaluation processes and output comparison. Scores: XX = 2, X = 1, – = 0. Scores Max = 22 per row and Max = 6 per column

		CIRA	CORAS	CRAMM	FAIR	NSMROS	OCTAVE A	ISO27005	NIST 800-30	RISK IT	RAIS	CRDF	
RCA	Risk criteria assessment/revision	XX	X	–	–	X	X	X	–	–	–	–	6
RPE	Risk prioritization/evaluation	XX	XX	XX	XX	XX	XX	XX	XX	XX	XX	XX	22
RTR	Risk treatment recommendation	X	–	XX	–	–	XX	–	–	XX	XX	–	9
	Completeness	5	3	4	2	3	5	3	2	4	4	2	

XX Addressed, x Partially addressed, – Not addressed

Table 4 Method process completeness according to comparison criteria according to previous scores

	CIRA	CORAS	CRAMM	FAIR	NSMROS	OCTAVEA	ISO27005	NIST 800-30	RISK IT	RAIS	CRDF	Max score	Mean
1. Risk identification	24	33	29	26	21	32	38	24	29	18	18	50	26.5
2. Risk estimation	17	12	10	30	14	14	27	26	22	20	21	46	19.4
3. Risk evaluation	5	3	4	2	3	5	3	2	4	4	2	6	3.4
Completeness sum	46	48	43	58	38	51	68	52	55	42	41	102	49.3
Without outcomes	36	34	30	43	24	37	51	38	42	31	31	82	36

5 ISRA method completeness

In this section, we evaluate the completeness of each surveyed method according to the identified activities based in the CURF, Fig. 3. The results in Tables 1, 2, and 3 form the basis for the discussion. Table 4 displays the total measure of ISRA method completeness together with the mean value. The overall most complete method is ISO27005 with FAIR scoring second highest in the risk estimation process. Following is a summary of differences between the surveyed methods and their completeness.

5.1 CIRA

The conflicting incentives risk analysis was developed based on game theory, decision theory, economics, and psychology and is with its utilitarian view entirely different from the other surveyed methods. On risk identification completeness, CIRA scores twenty-four out of fifty possible. According to our results, CIRA is a sequential method where the strength lies in the threat actor and stakeholder assessments. CIRA identifies assets for the stakeholders regarding utility but does not include the more business-related activities. CIRA does not directly conduct vulnerability and control identification, but threats and stakeholder actions are at the core of the method.

On risk estimation, CIRA scores seventeen out of forty-six possible. CIRA is primarily concerned with the threat aspects according to $R = CI$. The method avoids probability calculations and instead estimates utility from executing potential strategies with accompanying outcomes. CIRA also considers opportunity risks.

On R evaluation, CIRA scores five out of six possible. The method addresses risk criteria as defined by the risk tolerance of the risk owner. Also, the method applies an incentive graph for visualizing risk and opportunity. Compared to the completeness score for the whole set, CIRA covers a little less than half of the tasks included in CURF.

5.2 CORAS

CORAS is a sequential method, based on the $R = P\&C$ definition; *a risk is the chance of the occurrence of an unwanted incident* [13]. According to our results, CORAS has one of the most complete risk identification processes, with the second highest score of thirty-three. The method does not directly address business processes. However, it suggests to map assets into processes and facilitates business process identification as a part of the structured brainstorming process. CORAS does not provide any steps for identifying and assessing existing controls throughout the method, although identifying insufficient controls are a part of the vulnerability identification and the structured brainstorming process. Another strength is the emphasis on stakeholder communication which is an ISRA area in need of improvement [31].

Although CORAS has a robust risk identification process, it lacks in more advanced activities for risk estimation. Examples are the absence of threat assessment activities, which results in a completeness score of twelve on the estimation phase. CORAS opens for frequentist probabilities [13] (p. 56) as the risk models allow for conditional events. However, the method is primarily qualitative as it suggests to estimate $P\&C$ in workshop form.

For risk evaluation, CORAS makes use of risk matrices and scores three out of five which gives CORAS a completeness score of forty-eight, placing it in the middle of the reviewed methods.

5.3 CRAMM

As a matrix method, CRAMM depends heavily on the accompanying software to provide full support. CRAMM makes

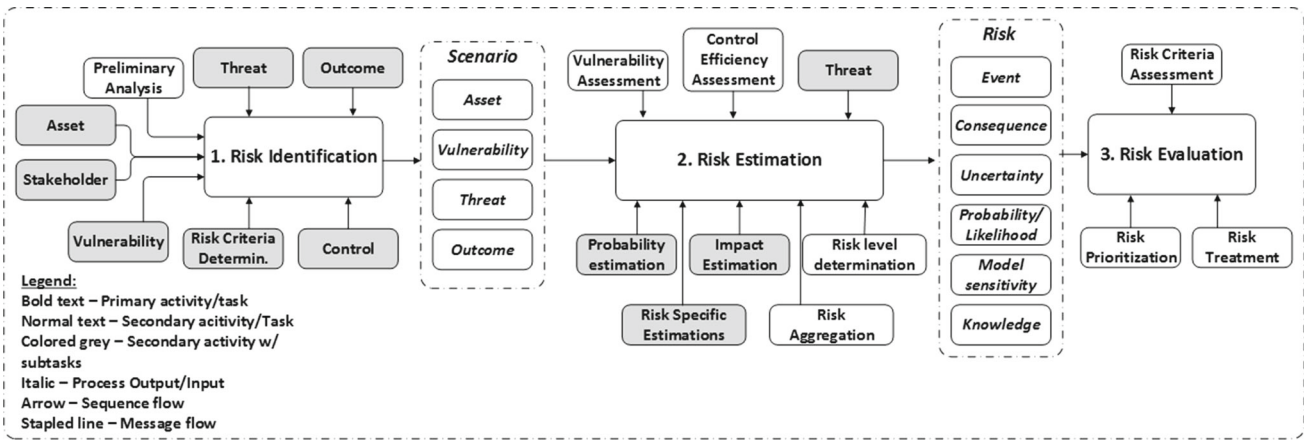

Figure 3 Top level of CURF. The generic output of the risk evaluation is prioritized risks

use of the $R = C$ definition, which is based on the "Threat * Vulnerability * Asset"-approach. The CURF results show that this definition is consistent with CRAMM's results for risk estimation, where it scores well on the AI, Vu, Th, and Ou categories. However, the preliminary assessment, business, and stakeholder-related activities are left out of the method, besides that asset models can be used to reflect business processes. The CRAMM risk identification process scores twenty-nine on completeness, which is above the average of the risk identification scores.

The risk estimation process primarily depends on subjective estimates from experts, but CRAMM also opens for quantifying losses with historical data. CRAMM does not address any threat assessment or other advanced activities for risk estimation, which puts it at the bottom for risk estimation completeness. For risk evaluation, CRAMM makes use of risk matrices. The total completeness score of thirty is the second lowest of this study.

5.4 FAIR

FAIR is a sequential method, based on the $R = P\&C$ definition *"The probable frequency and probable magnitude of future loss"* [5]. Out of the surveyed methods, FAIR stands out as the most dedicated to risk estimation and risk quantification. FAIR applies a preliminary assessment of assets and threat community to identify risk and produce scenario. The method has an average score in the risk identification phase, where, for example, the vulnerability, threat, and outcome related categories are not addressed. However, the strength of FAIR is in risk estimation where it does address threat and vulnerability. In particular, FAIR provides a comprehensive risk quantification approach which is the most mature of the surveyed methods and scores highest in completeness for risk estimation. For example, it considers all aspects of the $R = fA, C, U, P, S, K$ definition, and provides tools for risk measurement and quantification. Threat agent capability is evaluated regarding knowledge and experience requirements, and capacity resources available to the attacker. For risk evaluation, FAIR makes use of several types of risk matrices to articulate risk. FAIR is the second most complete method included in this study.

5.5 NSMROS

The Norwegian Security Authority Risk and Vulnerability Assessment is a sequential $P\&C$ approach that contains all the fundamental elements of ISRA methods. The NSMROS risk identification process is centered on assets, threat, vulnerability, and outcomes and provides few activities outside of this. The business aspects, such as activities business processes and stakeholder assessments, are not present in the method which results in NSMROS obtaining the lowest score of the full ISRA methods in risk identification. The vulnerability assessment is a part of the Risk Estimation process where it is performed as a barrier analysis. The more advanced threat assessment aspects and risk-specific estimations are missing from NSMROS. The method recommends subjective probabilities estimations, but it opens for frequentist approach to probability with a caveat of being aware of forecasting problems due to outdated statistics. NSMROS suggests gathering loss data to quantify impact estimates. NSMROS scores the second lowest on the risk estimation completeness.

For risk evaluation, NSMROS makes use of risk matrices. The control efficiency assessment (barrier analysis) and stakeholder communication are conducted in the risk treatment phase, after the risk has been estimated and evaluated, and is therefore outside of scope. NSMROS ranks the lowest on our overall completeness measurement.

5.6 OCTAVE Allegro

OCTAVE Allegro (OA)[17] is the lightweight version of the first OCTAVE and is an assistant method due to the extensive amount of worksheets it provides to the practitioner. OA bases the risk definition on the event, consequence, and uncertainty, $R = C\&U$, yet in practice both the method and worksheets put little emphasis on measurements of uncertainty, instead focusing on subjective estimates of consequence in the form of impact areas. Thus, in practice, OA is primarily a $R = C$ method. OA is an asset-centric approach, which only considers information as an asset, for example, network infrastructure, and hardware are considered as asset containers, which facilitates asset storage and flow. The risk identification process has the third highest score in completeness, with the vulnerability, control, and stakeholder assessments as the main areas lacking. OA scores low on completeness in the risk estimation process; with its' primary focus on impact estimation, it does not propose activities to address probability besides a brief mention in a worksheet. OA does not address vulnerability and threat assessments in any part of the process. However, the impact estimation is the strong suit of the method. For risk evaluation, OA makes use of risk matrices and also proposes risk treatments as a part of the evaluation. The total score of OA places two points above average.

5.7 ISO/IEC 27005:2011—Information technology—Security techniques—Information security risk management

ISO27005 is a mature ISRM standard which scored the highest on the ISRA completeness measurement. The previous versions of the standard built on a traditional PxC definition

of risk, [1] but now applies $R = ISO$ definition as the foundation for the assessment. ISO27005 is a sequential method that comes with an extensive appendix that supports the user in scoping, and asset, threat, and vulnerability assessment. The aspects that are not present in the risk identification process are key risk indicators, asset containers, preliminary assessment, and stakeholder analysis. The vulnerability and threat assessments are described as part of the identification processes and supplemented in Annex, and we, therefore, consider these as full activities in the risk identification process. ISO27005 has the highest completeness score in risk identification.

In the risk estimation process, the standard mentions the specific threat assessment activities as a part of the assessment of incident likelihood process. ISO27005 contains a description of how to conduct both a subjective knowledge-based and frequentist probabilities and impact estimations. However, for the latter, it does require prior knowledge of statistics. It does not address the risk-specific domains, but it introduces the LRD activity and recommends risk aggregation as a part of the analysis. For R, the standard mentions uncertainty, model sensitivity, and knowledge aspects as the degree of confidence in estimates. ISO27005 scores the second highest in risk estimation completeness. In the risk evaluation process, the predefined risk criteria are applied to the analyzed risks and propose several types of matrices for risk evaluation and prioritization.

5.8 NIST special publication 800-30, revision X-guide for conducting risk assessments

The NIST SP 800-30 R.1 [18] is a sequential method based on the $R = PxC$ definition of risk. The method scored two points below average completeness in the risk identification phase. It is a threat-centric method, which creates a notable absence in asset identification and evaluation processes. Assets are mentioned in conjunction with other tasks, especially threat identification, but not considered as either a main or secondary activity. NIST80030 scores well in the vulnerability and threat categories for the risk identification phase.

NIST80030 also lacks tasks for the outcome and stakeholder assessments. In the risk estimation process, the method partially identifies assets and has a comprehensive threat assessment process. It supports both subjective knowledge-based and frequentist probability estimations or a combination of the two. NIST80030 only supports subjective impact estimations regarding affected assets from the risk. The method allows for different risk models, and the components of the estimation output are dependent on the chosen model. All this results in the method scoring the third highest on completeness for the risk estimation process. In the risk evaluation process, NIST80030 suggests to evaluate and prioritize risk in tables consisting of several descriptive categories. NIST80030 ranks as number four on total completeness with a score of fifty-two.

5.9 The Risk IT framework and practitioner guide

ISACA's Risk IT is a $R = PxC$ assistant method due to the extensive documentation it provides. Risk IT scores the third highest in total completeness, but it is the least accessible of the surveyed literature, as it took us quite some time to get an overview of the content and process. An example of the method being hard to access is that assets are required to produce the risk scenarios, but there is no particular activity to identify or evaluate the assets. It is a business-centric method that covers all business-related aspects of the ISRA process, also bringing *risk indicators* into CURF. Risk IT provides a lot of tools and descriptions for the user which makes it score well on the completeness measurement. For the risk identification process, Risk IT centers on the development of risk scenarios, consisting of actors, threat type, event, asset/resource, and time. One problem is that the authors partly mix up the terminology, for example, the suggestions for events include both adverse outcomes and vulnerabilities, which are not the same thing. The scenario focus is also possibly the reason for the ISRA activities being hard to identify, whereas several tasks are embedded into others (the most comprehensive description of the process is in [19] pp. 65–76). Risk IT does not include activities for control and threat assessment in the risk identification process. Risk IT scores a little over average for risk identification.

Risk IT has the fourth highest completeness score for risk estimation. Risk IT does not consider the threat assessment or risk- specific activities, but it contributes to the CURF model with considerations of *attack duration*. Risk IT advices both frequentist and qualitative assessments, or a combination of the two, for both probability and impact. In the risk evaluation, Risk IT proposes to rank risks with risk matrices, but also to evaluate through peer reviewing inside the company as a quality assurance process.

5.10 Privacy risk assessment of information systems (RAIS)

RAIS is a sequential PxC that has been scoped primarily for assessing privacy risks; it is an asset-centric approach where the emphasis is on identification and security of personal information. The method comes with domain-specific tools for privacy and adds two additional categories to CURF: (i)

[1] "The potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organization. It is measured regarding a combination of the probability of occurrence of an event and its consequence,"—ISO:IEC 27005:2008.

Mapping of personal data and (ii) Privacy Risk Estimation. Where the former contains domain-specific tools for mapping and evaluating personal data, and the latter provides guidelines for qualitative descriptions of privacy impact. The risk identification process in RAIS scores the lowest on completeness of any method, primarily due to the lack of focus on vulnerability, threat, and controls. However, the RAIS threat assessment tools provided for the risk estimation process are comprehensive, together with a well-described process for estimating PxC, which makes the method score above average in completeness for risk estimation. The main drawbacks of the method are that it overall lacks tools for control and vulnerability analysis. RAIS emphasizes risk criteria and acceptable risk as one of the starting points for the assessment but does not suggest to revise these in the risk evaluation phase. RAIS scores third lowest in total completeness.

5.11 Microsoft Cloud Risk Decision Framework (MCRDF)

MCRDF [22] is a sequential method built on the ISO/IEC 31000-standard for general risk management and applies the $R = ISO$ definition of risk. MCRDF is scoped to support decision-making regarding cloud-based risks. The method adds two cloud-based categories to CURF: (i) cloud-specific risk domains (risk identification) and (ii) cloud vendor assessment (risk analysis).

Our analysis of the content shows that it scores low on completeness regarding common InfoSec-related tasks, such as asset evaluations and threat assessment, with the lowest score for risk identification shared with RAIS. The strong side of MCRDF is the overview of cloud-associated risks control areas and the detailed example for applying the method. The method provides easy-to-apply examples of qualitative PxC calculation examples, which are grounded in the risk control areas. One drawback with MCRDF is that it is too dependent on the tables and does not provide additional approaches for identifying and managing risks that are outside of the risk control areas. CRDF scores above average in completeness for the risk estimation phase, but places in the second last place in total completeness.

6 Scope and Limitations of the current ISRA methods

One of our most significant findings is that no method is complete in CURF, while the most complete is ISO27005 which addresses several issues in some way. However, falls short when compared to FAIR's detailed risk assessment approach. The following discussion analyzes the scope of ISRA methods, then row scores, and, lastly, the presence of modern risk concepts in the surveyed ISRA methods, starting with the risk identification process, followed by an analysis of the risk estimation and evaluation processes. Lastly, we discuss modern risk concepts in ISRA. In Tables 1, 2, and 3, we also summed each row to show where the area of focus for ISRA developers lie. We apply the ranges 0–7 = low, 8–15 = medium, and 16–22 = high, to simplify discussion.

6.1 Risk identification

Analyzing the row scores in Table 1 reveals which areas the ISRA method developers prioritize. ISRA has previously had a tendency to have a too technical scope and not address the needs of the organization [36]. Although the scope may be improving overall [31], we see from organizational and business-related categories, RC and SI, that these issues have not had a high priority. Besides, only ISO27005 fully identifies business processes as assets to the organization.

The only issue addressed by all methods in the risk identification process is threat identification. Followed by the outcome, asset, and vulnerability identification, which provides an indicator of what the output of the process should contain. Identification and assessments of assets, threats, vulnerability, and control all have high row scores in CURF, while threat identification scores highest. While the surveyed methods conduct control identification and assessment in both the risk identification and estimation parts of the ISRA, the sum of which equals existing controls in the high priority range. NSMROS suggests to do the control assessment as a part of the *risk treatment* process, which is too late as they will be left out of the assessment [38], and the existing controls have a direct influence on the risk level and should be a part of the risk estimation.

Further, risk criteria are partially or fully dealt with in all but one of the surveyed methods. These are criteria for risk evaluation and decision-making late in the process. Only four methods address the criteria in the *risk evaluation*, Table 3. One issue with defining the risk criteria in the risk identification phase and not revising them later is that when it comes to the decision-making, it is entirely up to the decision-maker(s) to consider if it is acceptable. In our experience, the risk criteria function as heuristics for the risk assessors but are not static. The severity of the risk is not the only factor that determines whether or not it is acceptable. For example, the cost of mitigating the threat may be too high, and, therefore, sways the decision to acceptance of a risk that was deemed unacceptable by the risk criteria. Thus, the cost/benefit analysis of the risk treatment is also an important factor to consider besides the criteria. Besides risk criteria, the RC tasks of CURF score in the medium to low range. For example, *key risk indicators* are also only addressed by two methods, which are strongly tied to key performance indicators in business. Further strengthening the RC area of methods will assist in practitioner business understanding

by mapping risk indicators and understanding business processes, and assist the integration of the ISRA program into the organization.

Five of the methods either propose business processes as an asset or as a central part of the risk assessment, but does not discuss the issue that protecting business processes is far more complicated than protecting an asset. Mapping out and modeling business processes require a lot of resources and will create a substantial overhead on the ISRA process at the lower abstraction layers.

CURF also shows that *stakeholder identification* is increasingly being implemented into ISRA methods. Gathering data from knowledgeable stakeholders and how to contact them is important, especially for the assessments not reliant on penetration tests for data collection.

The RS row scores in the risk identification output show that asset, threat, and the outcome being included equally, while vulnerability scores two points lower. However, two risk methods [5,16] suggest conducting the vulnerability assessment primarily in the risk estimation process, which suggests that these four areas are treated equally.

6.2 Risk estimation and evaluation

Based on the high degree of threat focus in the risk identification phase, there are surprisingly diverse approaches to the threat assessment in the risk estimation. We see from the CURF results that there is little conformity on how to conduct a threat assessment and what it should contain. CURF summed up the issues concerning threat willingness/motivation, capability, capacity, and attack durations, but no methods addressed all of these aspects on its own or propose an approach to operationalizing them. Reviewing the ISRA frameworks also revealed an ambiguous language for describing threats; for example, ISO27005 defines a threat as a type of damage or loss. In comparison, OCTAVE Allegro makes a clear distinction that the threat is either a human actor or a technical problem, while this is the "threat origin" in ISO27005. Related to threats, NIST 800-30 markets itself as a threat-based risk assessment method, but only covers two out of the four recognized TA categories in the risk estimation phase. The developers of NIST800-30 chose not to prioritize asset evaluation, which down-prioritizes one of the cornerstones of security work. Asset evaluation is essential in prioritizing security efforts, as a high-valued asset needs more protection than an asset with lower value. The threat-based approach for prioritizing security efforts will require a thorough understanding of the adversary's motivation and intent to apply it to security planning.

Related to threat motivation lies game theoretic-based estimations of utility and incentives for risk estimates, which is a field largely ignored in the surveyed ISRA methods besides CIRA. This approach can also be used to determine an adversaries willingness to attack.

The CURF results also show a difference in PxI approaches, where the qualitative methods are more utilized, especially for impact estimations. CIRA does not include probability at all, while OCTAVE Allegro mainly relies on the consequence estimate for the risk score. Probabilities are hard to determine in InfoSec [36,39]; however, the backside of leaving probability out of the risk estimate is that two risks with equal consequences may be falsely juxtapositioned if they have different rates of occurrence.

On the risk estimation itself, our results show that all methods consider event(s) and consequences. Most methods include some form of probability, while very few address uncertainty beyond probability. Descriptions of sensitivity have a model-based method as a prerequisite and are primarily an issue of quantitative methods and are only considered in FAIR, while four methods partially address the knowledge aspect, leaving S and K-aspects in the low priority range.

Cloud-specific considerations is only fully considered by the CRDF and FAIR, one of which is genre specific for the cloud. Both of the two genre-specific methods, cloud [22] and privacy [21] shows that they rely on the ISRM fundamentals, but add tasks to CURF that are unique to them. Examples are *privacy risk estimation* and *cloud vendor assessment*. FAIR is one the only generic ISRA method we found to consider cloud issues specifically. The ISO/IEC 27017:2015 standard covers cloud security controls; however, cloud issues are not present in the surveyed ISO27005.

The risk criteria determination requires the risk criteria to be defined in risk identification process and is, therefore, limited to those methods. All methods conduct risk prioritization and evaluation. While only a few propose risk treatments as a part of the risk evaluation process, common to run this as an own process, see Fig. 1).

From CURF's Risk Estimation table, we see that there is a diverse amount of tasks and few areas in which most of the methods overlap. The two most significantly overlapping areas are subjective probability and impact estimation, the latter is one of two tasks that has a full score in CURF. Quantitative estimates of P and C have the second highest scores, while the remainder of tasks is spread among the different methods. CURF shows that the most addressed area in risk estimation is PxC calculations, while the remaining RD categories are largely specific to the method that introduced it. Among the other types of estimations, the utility and incentive calculations in CIRA are closely related to threat motivation but goes deeper into these aspects by applying economic theory to threat estimation. Besides CIRA, understanding human nature is an important point that seems largely neglected by the ISRA methods. Only two approaches address the cost of lost opportunities as well. From the risk evaluation table, CURF shows that *risk prior-*

itization/evaluation is the top priority of this process. From the reviewed methods, consideration of incentives is limited to CIRA.

Based on this analysis, the development scope of ISRA methods centers on the asset, vulnerability, threat, and controls. The development also tends toward more business-related aspects. The main direction of risk assessments, besides FAIR, is developing aspects of qualitative risk assessments and methodologies for generic and specific estimations. Further, the business-related RC and SI areas in CURF currently present limitations to several methods. Threat assessments have the highest priority in CURF, but there are diverse approaches to what should be risk assessed, and no method covered all aspects within the TA category. The four RD categories consistently scored low and were specific to the methods that introduced them.

6.3 Existing methods and modern risk concepts

Several modern concepts from generic risk literature are yet to make an impact in the ISRM methodologies. Besides FAIR's Monte Carlo-based approach and ALE/SLE models (Annual and Single Loss Expectancy), there is little information on the ISRA methods on how to obtain quantitative probabilities. Related to risk quantification is the Black Swan concept proposed by Taleb [7]. None of the ISRA methods addresses Black Swan risks although the complexity and interconnectivity of the ICT systems keep growing, making them more susceptible to Black Swan events. Actively estimating risk aggregation and cascades are one mitigating activity that may reduce the impact of Black Swans. Wangen and Shalaginov [37] and Hole and Netland [39] have proposed more specific approaches for incorporating this issue into ISRA, but these have yet to be adopted into methods.

Knowledge about risk, K, is also mostly left out of the ISRA methods, meaning the descriptions of the background knowledge and assumptions that U and P are based on. As an example, a risk assessment shows a small probability of a particular threat agent committing a distributed denial-of-service (DDoS) attack occurring the coming year. Consequently, the risk will also be low. However, if the probability is based on weak knowledge and assumptions, the risk should perhaps be considered as higher. Descriptions of K are particularly important for risk estimations regarding complex systems where knowledge is limited. None of the reviewed methods addresses this aspect in full.

7 Relationship to other literature

In this section, we discuss the previous work in the research field and how our work differs and extends previously published work. There are several comparison studies of ISRM/RA methods in the related work. We have previously referenced the Sandia Report [9] which presents a classification scheme where ISRM methods are sorted in a 3-by-3 matrix by the level of expertise required and type of approach. The Sandia classification complements our results by stipulating the level of skill needed to apply an ISRA method. The historical and recent development trends of the risk concept proposed by Aven [3] also complements this framework by providing the background and foundation of each risk approach.

There exist multiple comparative studies outlining ISRA approach content to aid organizations in choosing a method, for example ENISA's high-level summary of existing methods [23] and *methodology for evaluating usage and comparison of risk assessment and risk management items* [24]. The latter is a well-developed approach for comparing and benchmarking possible ISRM processes, together with expected inputs and outputs. The benchmark follows the classic ISRM process (Fig. 1), including the six main ISRM stages and fifteen defined sub-process. There are several resemblances to CURF in the comparison method; for example, both have the ISO27005 as a starting point and apply a similar scoring system. However, they are also different as the ENISA method compares to a set of items that we interpret as best practices, while CURF compares with items present in methods and grows if the new item is added. The former ENISA comparison [23] is a high-level comparison of methods, based on four predefined categories for ISRM and ISRA, eight in total. While similarly, Syalim et al [27] have published a comparative analysis that applies four predefined generic steps of the ISRA process for comparison. Both these studies compare a set of ISRA methods within a predefined set of criteria. An approach that risks leaving important aspects out of the comparison. For example, both comparisons downplay the role of the asset identification and evaluation process, which often is the foundation of the risk assessment. The results in our paper differ from these in that ours are versatile and adaptable, allowing for other tasks and activities beyond predefined categories to be added and analyzed. In this context, Bornman and Labuschagne [25] present a very detailed framework for comparing the complete ISRM process, divided into five categories, where the *processes* category is interesting for our work. The authors built their comparison criteria on CobiT (*Control Objectives for Information and Related Technology* (COBIT) by ISACA). This framework focuses on what the compared methods address and contains about COBIT, but not differences in how they recommend solving the task, or the distinct differences between the approaches.

Another similar study was conducted by Shamala et al. [26] which defines a detailed information structure for ISRA methodology contents. This comparative framework was developed to evaluate ISRA methods primarily on the information structure regarding what is needed at a particular step

in the assessment. The contents of the framework are derived from a detailed comparison of popular ISRM/RA methods and, therefore, have a similar approach to our work, but with a different purpose and scope, and, therefore, different results regarding criteria. Whereas Shamala et al. focus on how and what information to collect, our results look at how ISRA methods address particular tasks and issues.

Agrawal [40] has published a comparative study of ISRA methods, in which the author summarizes four methods using an ontology. The paper compares the four ISRA methods to eight predefined criteria, whereas it considers if a method is primarily qualitative or quantitative, purpose, and if it is scalable. Agrawal also describes the expected input, effort, and outcome of each process step and then discusses the pros and cons of each reviewed method. This study overlaps with CURF in some of the criteria, such as methodology, outcome, and the use of Sandia classification [9]. However, the main methodology and approach to the problem are different, as Agrawal also considers a set of predefined criteria for each method.

One of the most comprehensive taxonomies of ISRA regarding reviewed methods is the Shameli-Sendi et al. [2] study, in which the authors have reviewed 125 papers. The study provides a modern taxonomy of ISRA methods based on a set of four categories identified by the authors. The first category, *appraisement*, is defined as the type of input and output of the risk calculation, such as if it is qualitative, quantitative, or a combination of both (hybrid). The second category addresses the ISRA method's *perspective*, which is either business, asset, or service driven. An additional category, *threat driven* [18], could also have been considered for the perspective category. The third category, *resource valuation*, primarily considers how the ISRA method suggests evaluating valuables: either asset, service, or business process, and if it considers functional dependencies between them. Whereas compromising one asset may inflict consequences on another, and such on. The fourth category is *risk measurement* in which the taxonomy classifies ISRA methods regarding how they consider impact propagation, meaning if the method advises considering an impact only to the asset itself (non-propagated) or if it considers dependency between assets and other resources. The Shameli-Sendi et al. taxonomy classifies an ISRA method within the predefined criteria identified by the authors, while CURF compares on criteria and tasks present in the methods. Both approaches aim to assist practitioners and organizations in the choice of ISRA approach, while Shameli-Sendi et al. are at a higher level of abstraction addressing four core issues in ISRA, and CURF provides in-depth analysis of how well each method addresses each task. Thus, these two approaches have complementary features.

On the topic of research problems, both Wangen and Snekkenes [36] and Fenz et al. [35] have published articles on current challenges in ISRM; the former is a literature review that categorizes research problems into a taxonomy. The latter discusses current challenges in ISRM, predefines a set of research challenges, and compares how the existing ISRM methods support them.

The related work contains several approaches to comparing method content. However, these are primarily studies of properties and content based on a predefined set of criteria. None of which address how to compare full ISRA processes and content beyond these criteria. Thus, the gap in the research literature lies in the lack of a bottom-up approach to compare ISRM/RA methods.

8 Limitations and future work

CURF has limitations in the abstraction layer as we chose to keep the comparison at a high level, the model does not display deeper differences between methods such as specific approaches to asset identification, vulnerability assessments, and risk estimation. For example, the new version of FAIR [5] comes with a detailed approach to risk estimation, while other methods that appear somewhat equal in the comparison, such as NSMROS [16], only describes the activity at a high abstraction which means that a closer study of the methods and a possible expansion of the tables will reveal deeper differences in scope and methodology not present in our work. This includes the time-parameter for PxI calculations suggested by one of the reviewers. A possible addition to the framework is to expand it with experience-based knowledge and to grow it by making it available to other scholars and practitioners. Comprehensiveness of activities and accessibility of the ISRA methods is not considered in this comparison, which are issues we uncovered for some of the frameworks. Another limitation is that, for example, ISO 27005:2011 scored low on the cloud-specific criteria, third-party management is covered in the supporting material (ISO/IEC 27001 and 27002 standards). This may also be true for other reviewed methods.

Although the included set adhered to our inclusion and exclusion criteria, there are several methods that we could have included in this study. We have a limitation regarding the amount of methods included in the study; however, after adding the highest scoring methods the framework started to saturate and mature. Wherein each additionally reviewed method added fewer tasks than the previous, for example, both RAIS and MCRDF were added last and each added two risk-specific tasks to CURF. A path for future work is to add new methods within specific tasks or philosophies to expand the framework and make it more representative for all ISRA methods. Among possible future additions to CURF are attack tree methods [41], the *Information Security Risk*

Analysis Method (ISRAM) [42], and *the IS risk analysis based on a business model* [43].

However, growing CURF by including more methods will increase the complexity and make it harder for the reader to obtain an understanding of the whole picture. It can be a challenge for someone who is not security literate to understand all the CURF tasks and make informed choices on methods. Although we provide a brief description of each task and sub-task, it is a limitation that the CURF user must possess a certain amount ISRA knowledge to fully utilize CURF. A path for future work to address this issue is to develop software support for CURF for collaboration and online use, in which we provide more detailed method and task descriptions. This path would make both the method and results more accessible to the ISRA community, together with an option for users to add and qualitatively score methods. There are multiple possibilities with such an approach; for example, a comprehensive overview and description of existing tasks would allow the risk practitioner to choose the parts of the framework he needs to construct a risk assessment model tailored to his requirements. Another path for future work is to apply CURF to map differences between ISRA methods, apply the methods on case studies, and then to analyze the risk assessment outcomes. This approach will allow for a study of cause (task) and effect (outcome) and allow researchers to determine how specific tasks influence the outcomes. This approach has already been partly developed [38], but additional research is required to increase the knowledge base.

Another limitation of the CURF method is that the completeness score will be dependent on the methods chosen to populate CURF. The completeness score will reflect whether it supports similar functionality to the methods already reviewed. In cases where the user wishes to assess a new method with several innovative tasks, the approach will add many several tasks to CURF, but the method is likely to obtain a low completeness score. In such cases, static evaluation criteria might be preferable as a decision basis.

Further, this work highlights the need for a more research into what the lower levels of an ISRA should consist of beyond asset, threat, vulnerability, and control assessments. For example, what are the key estimators of an asset value or a threat assessment?

9 Conclusions

To conclude this paper, we have presented CURF, which was developed inductively through reviewing eleven well-documented ISRA methods: CIRA, CORAS, CRAMM, FAIR, NSM ROS, OCTAVE, ISO27005, NIST SP 800-30, and Risk IT, in addition to two domain-specific methods, one for cloud (CRDF) and one for privacy (RAIS). Literature studies show that there exist multiple comparative assessments of ISRM/RA methods, but these are all scoped to compare method contents to a predefined set of criteria, equivalent to a top-down approach. For most cases, this is less flexible concerning tasks missing in the predefined criteria. With CURF, we have shown the utility of comparing methods and building the framework from a bottom-up point of view. Our results, therefore, consists of a larger superset of issues and tasks from all reviewed ISRA methods using ISO/IEC 27005:2011 as a reference point and then comparing the ISRA methods as a measure of completeness covering all the issues and activities added to the superset. The possibility to add new problems makes our proposed framework highly flexible to changes in future methods and for comparing methods that are very different.

No evaluated method is complete in CURF, but from all of the methods reviewed, ISO/IEC 27005:2011 is the most complete and covers most issues in one way or another. However, FAIR had the most complete risk estimation process. Another finding is that besides FAIR, there is little information on how to quantify probabilities in reviewed methods. There are several ISRA frameworks and practices; however, we find variations of asset evaluation, threat, vulnerability, and control assessments at the core of the most reviewed frameworks, while the more specific issues, such as cloud risk assessment, are primarily addressed by methods developed for that purpose. It was also interesting to find that none of the ISRA methods discuss the presence of unknown unknowns (Black Swans), which is highly relevant due to the dynamic and rapid changes in ICT systems, which continue to grow and increase complexity. Besides CIRA, the human motivational element of InfoSec and ICT systems seems mostly neglected.

Acknowledgements The Ph.D. student Gaute Wangen acknowledges the sponsorship from the COINS Research School for Information Security. The authors also acknowledge the excellent feedback and contributions from the anonymous reviewers. We also acknowledge Dimitra Anastasopoulou for her help in preparing the manuscript.

References

1. Inventory of risk assessment and risk management methods. Technical report, European Network and Information Security Agency (ENISA) (2006)
2. Methodology for evaluating usage and comparison of risk assessment and risk management items. Technical report, European Network and Information Security Agency (ENISA), (2007)
3. Aven, T.: The risk concept–historical and recent development trends. Reliab. Eng. Syst. Saf. **99**, 33–44 (2012)

4. The risk it practitioner guide. Technical report, ISACA - Information Systems Audit and Control Association (2009)
5. Freund, J., Jones, J.: Measuring and Managing Information Risk: A FAIR Approach. Butterworth-Heinemann, Oxford (2014)
6. Information technology, security techniques, information security risk management, ISO/IEC 27005:2011
7. Taleb, N.N.: The Black Swan: The Impact of the Highly Improbable, 2nd edn. Random House LLC, New York (2010)
8. Aven, T., Renn, O.: On risk defined as an event where the outcome is uncertain. J. Risk Res. **12**(1), 1–11 (2009)
9. Campbell, P.L., Stamp, J.E.: A Classification Scheme for Risk Assessment Methods. Sandia National Laboratories, Albuquerque (2004)
10. Aven, T., Renn, O.: On risk defined as an event where the outcome is uncertain. J. Risk Res. **12**(1), 1–11 (2009)
11. Blakley, B., McDermott, E., Geer, D.: Information security is information risk management. In: Proceedings of the 2001 Workshop on New Security Paradigms, pp. 97–104. ACM (2001)
12. Blank, R.M., Gallagher, P.D.: NIST special publication 800-30, information security, guide for conduction risk assessments, revision 1 (2012)
13. Den Braber, F., Brændeland, G., Dahl, H.E.I., Engan, I., Hogganvik, I., Lund, M.S., Solhaug, B., Stølen, K., Vraalsen, F.: The CORAS Model-based Method for Security Risk Analysis. SINTEF, Oslo (2006)
14. Campbell, P.L., Stamp, J.E.: A Classification Scheme for Risk Assessment Methods. Sandia National Laboratories, Albuquerque (2004)
15. Jones, J.: An introduction to factor analysis of information risk (fair). Norwich J. Inf. Assur. **2**(1), 67 (2006)
16. Risk Assessment of Information Systems (Risikovurdering av Informasjonssystem. The Norwegian Data Protection Authority (Datatilsynet) (2011)
17. Caralli, R.A., Stevens, J.F., Young, L.R., Wilson, W.R.: Introducing octave allegro: Improving the information security risk assessment process. Technical report, DTIC Document (2007)
18. Fenz, S., Heurix, J., Neubauer, T., Pechstein, F.: Current challenges in information security risk management. Inf. Manag. Comput. Sec. **22**(5), 410–430 (2014)
19. Freund, J., Jones, J.: Measuring and Managing Information Risk: A FAIR Approach. Butterworth-Heinemann, Oxford (2014)
20. Gregor, S., Hevner, A.R.: Positioning and presenting design science research for maximum impact. MIS Quart. **37**(2), 337–355 (2013)
21. Hevner, A., March, S.T., Park, J., Ram, S.: Design science in information systems research. MIS Quart. **28**(1), 75–105 (2004)
22. Hevner, A., Chatterjee, S.: Design research in information systems: theory and practice Springer **22** (2010)
23. Hole, K.J., Netland, L.H.: Toward risk assessment of large-impact and rare events. IEEE Sec. Priv. **8**(3), 21–27 (2010)
24. Jones, J.: An introduction to factor analysis of information risk (fair). Norwich J. Inf. Assur. **2**(1), 67 (2006)
25. Bornman, W.G., Labuschagne, L.: A comparative framework for evaluating information security risk management methods. In: Information Security South Africa Conference (2004)
26. Shamala, P., Ahmad, R., Yusoff, M.: A conceptual framework of info structure for information security risk assessment (isra). J. Inf. Sec. Appl. **18**(1), 45–52 (2013)
27. Lund, M.S., Solhaug, B., Stølen, K.: Risk analysis of changing and evolving systems using coras. Foundations of security analysis and design VI, pp. 231–274. Springer (2011)
28. Hevner, A., March, S.T., Park, J., Ram, S.: Design science in information systems research. MIS Quart. **28**(1), 75–105 (2004)
29. Rajbhandari, L.: Risk Analysis Using "Conflicting Incentives" as an alternative notion of Risk. Ph.D. thesis, Gjøvik University College (2013)
30. Gregor, S., Hevner, A.R.: Positioning and presenting design science research for maximum impact. MIS Quart. **37**(2), 337–355 (2013)
31. Schneier, B.: Attack trees. Dr. Dobb's J. **24**, 21–29 (1999)
32. Aven, T.: Misconceptions of Risk. Wiley, Hoboken (2011)
33. Kaplan, S., Garrick, B.J.: On the quantitative definition of risk. Risk Anal. **1**, 11–27 (1981)
34. Rajbhandari, L., Snekkenes, E.: Using the conflicting incentives risk analysis method. Security and Privacy Protection in Information Processing Systems. Springer, Berlin (2013)
35. Fenz, S., Heurix, J., Neubauer, T., Pechstein, F.: Current challenges in information security risk management. Inf. Manag. Comput. Sec. **22**(5), 410–430 (2014)
36. Suh, B., Han, I.: The IS risk analysis based on a business model. Inf. Manag. **41**(2), 149–158 (2003)
37. Syalim, A., Hori, Y., Sakurai, K.: Comparison of risk analysis methods: Mehari, magerit, NIST800-30 and microsoft's security management guide. In: International Conference on Availability, Reliability and Security, pp. 726–731 (2009)
38. Wangen, G.: Information Security Risk Assessment: A Method Comparison. IEEE Computer Society, In IEEE Computer Magazine, Special Issue - Security Risk Assessment (2017)
39. Hole, K.J., Netland, L.H.: Toward risk assessment of large-impact and rare events. IEEE Sec. Priv. **8**(3), 21–27 (2010)
40. Agrawal, V.: A comparative study on information security risk analysis methods. J. Comput. (JCP) **12**(1), 57–67 (2017)
41. Schneier, B.: Attack trees. Dr. Dobb's J. **24**, 21–29 (1999)
42. Karabacak, B., Sogukpinar, I.: ISRAM: information security risk analysis method. Comput. Sec. **24**(2), 147–159 (2005)
43. Suh, B., Han, I.: The IS risk analysis based on a business model. Inf. Manag. **41**(2), 149–158 (2003)