Current Established Risk Assessment Methodologies and Tools

Dan Ionita
SCS Group, University of Twente

Pieter Hartel
SCS Group, University of Twente

Wolter Pieters
ICT Section, Delft University of Technology

Roel Wieringa
SCS Group, University of Twente

1st of September 2013

Abstract

The technology behind information systems evolves at an exponential rate, while at the same time becoming more and more ubiquitous. This brings with it an implicit rise in the average complexity of systems as well as the number of external interactions. In order to allow a proper assessment of the security of such (sub)systems, a whole arsenal of methodologies, methods and tools have been developed in recent years. However, most security auditors commonly use a very small subset of this collection, that best suits their needs. This thesis aims at uncovering the differences and limitations of the most common Risk Assessment frameworks, the conceptual models that support them, as well as the tools that implement them. This is done in order to gain a better understanding of the applicability of each method and/or tool and suggest guidelines to picking the most suitable one.

Preface

This thesis marks the successful completion of my Master in Computer Science - Information Systems Engineering at the University of Twente, Netherlands (2011-2013). It has been a truly life-changing experience, in which I have had much to learn and understand.

The topic for the thesis was chosen due to the authors' interest in the European TREsPASS project (www.tresspass-project.eu). The project aims to design a new socio-technical Risk Assessment methodology, and as such, a comprehensive survey of the current state-of-the-art is essential. It is this goal that this thesis hopes to help achieve.

Acknowledgments

The author would like to thank Prof. Dr. Roel Wieringa for his unbounded support for the creations of this thesis and for providing me with opportunities far beyond my expectations. Furthermore, I would also like to extend my gratitude to my secondary supervisors, Pieter Hartel and Wolter Pieters, for useful comments and remarks. I would like to extend a special mention to Suse Engbers who makes everything that happens in the IS department at the UT possible thanks to her dedication and skills. However, I am and always will be most grateful to my family for the unadulterated physical, financial and emotional support which helped me get where I am now. Without you, I would be nothing! A special thanks goes to my best friend: my brother. Last but not least, I am especially grateful to my lovely girlfriend, Vincy, who stood by me whenever I felt lost and did her best to make me happy! I will be forever grateful.

I would like to make one final acknowledgment: to all the wonderful people I met while completing my Masters degree. There are to many names to mention, but you know who you are: Thank you for all the good times we've had together!

Contents

List of Figures

List of Tables

Chapter 1

Introduction

1.1 Background

In December 2012, based on EU funding, the TREsPASS project was officially launched. Consisting of 17 partners from both industry and research, the project aims to improve the way we secure information by integrating the digital, technical and social domains with the current state-of-the-art in the field of security. This is because of the impact that human behavior (be it an attacker, employee or bystander) has on the (in)security of an infrastructure. Furthermore, strict technical mechanisms can still be bypassed by using social engineering. As such, a better understanding of how these domains intertwine in the field of information security is crucial in identifying potential weak points within an organization or infrastructure.

This is where Risk Assessments come in. A Risk Assessment (RA) is a structured or semi-structured approach of analyzing the security of an infrastructure, identifying weak spots, and selecting countermeasures. Such assessments are done according to various methodologies. Currently, the sheer number of different such methodologies might be overwhelming for someone trying to get an overview of Risk Assessment methods and tools. Furthermore, each such method follows a slightly different procedure, uses different data, requires certain skills, provides different output, or is based on a different understanding of Risk all-together.

One of the first deliverables within the TREsPASS project includes a survey of the state-of-the-art in Risk Assessments. This includes both methods and tools. This master thesis is, amongst others, meant to provide input for this document. It can also serve as an introduction to Risk Assessment and Risk Management, or a glossary of relevant methods and tools.

1.2 Goals

The overall goal is obtain a better understanding of the key differences and commonalities between the various state-of-the-art Information Risk Assessment methodologies and tools. Interesting aspects are the scope, target users of the methods or tools and intended audience of the results.

We are also interested in the conceptualization and decomposition of Risk according to various methodologies and how this relates to their other characteristics.

1.2.1 Research Questions

These goals can be distilled into the following research questions:

RQ1 What are the most commonly used Risk Assessment methods?

- **SRQ1.1** What are their goals?
- **SRQ1.2** What steps do they contain?
- **SRQ1.3** What decisions do they support?
- **SRQ1.4** What is the scope of each method?

RQ2 What are the underlying conceptual models used in Risk Assessment frameworks?

- **SRQ2.1** How does each model conceptualize Risk?
- **SRQ2.2** What are the sub-components of Risk and how are they combined?
- **SRQ2.3** What are the target organizations of each model?
- **SRQ2.4** What significant differences can be found between these models?

RQ3 What are the most commonly used Risk Assessment tools?

- **SRQ3.1** What functionality does each offer?

RQ4 What are the relationships between each tool, method and model?

1.3 Approach

The core of the thesis consists of surveys of established methodologies, related tools and underlying conceptual models. Each relevant methodology, tool and conceptual model will be described and analyzed in order to create an overview of the current state-of-the-art. The analysis of individual methods/tools is followed by a comparison of key features as well as identification of commonalities and differences. Several discussion regarding the cross-compatibility between methodologies, tools and conceptual models are also included, with conclusions being drawn with regard to the observations. Finally, a guideline to choosing the most suitable method given the organization's business context and security requirements is designed. The findings are validated via expert judgment.

1.4 Structure of the report

The report is structured in 8 Chapters. This first chapter contains an introduction to the chosen topic. Chapter 2.3 contains an introduction to the field of Information Security Risk Management, of which Risk Assessments are a part of, as well as criteria for the sub-selection discussed in this thesis. Chapter 3 presents an overview of common Risk Assessment methods. Chapter 4 describes the various ways of conceptualizing risk that each framework implies. Chapter 5 indexes the software tools available and maps them to their relevant frameworks. Chapter 6 attempts to extract the key features from each of the previously identified methodologies and tools, while drawing conclusions regarding the most significant differences. Chapter 7 suggests a guideline to selecting the most suitable method. Chapter 8 draws some conclusions based on the previous analysis.

Chapter 2

Information Security Risk Management

2.1 The Risk Management process

According to the European Network and Information Security Agency (ENISA), Risk Management (RM) is "a process aiming at an efficient balance between realizing opportunities for gains while minimizing vulnerabilities and losses" [43]. Furthermore, it is an integral part of the management practice and crucial for achieving good corporate governance. Risk Management is usually a continuously re-iterating process, that typically consists of several activities. Such activities typically include identifying, analyzing and prioritizing risks and finding, evaluating and applying relevant countermeasures as well as monitoring the results. This process is either continuous or cyclical and focuses on achieving a coordinated and economical application of resources to minimize, monitor, and control the probability and/or impact of unfortunate events [26].

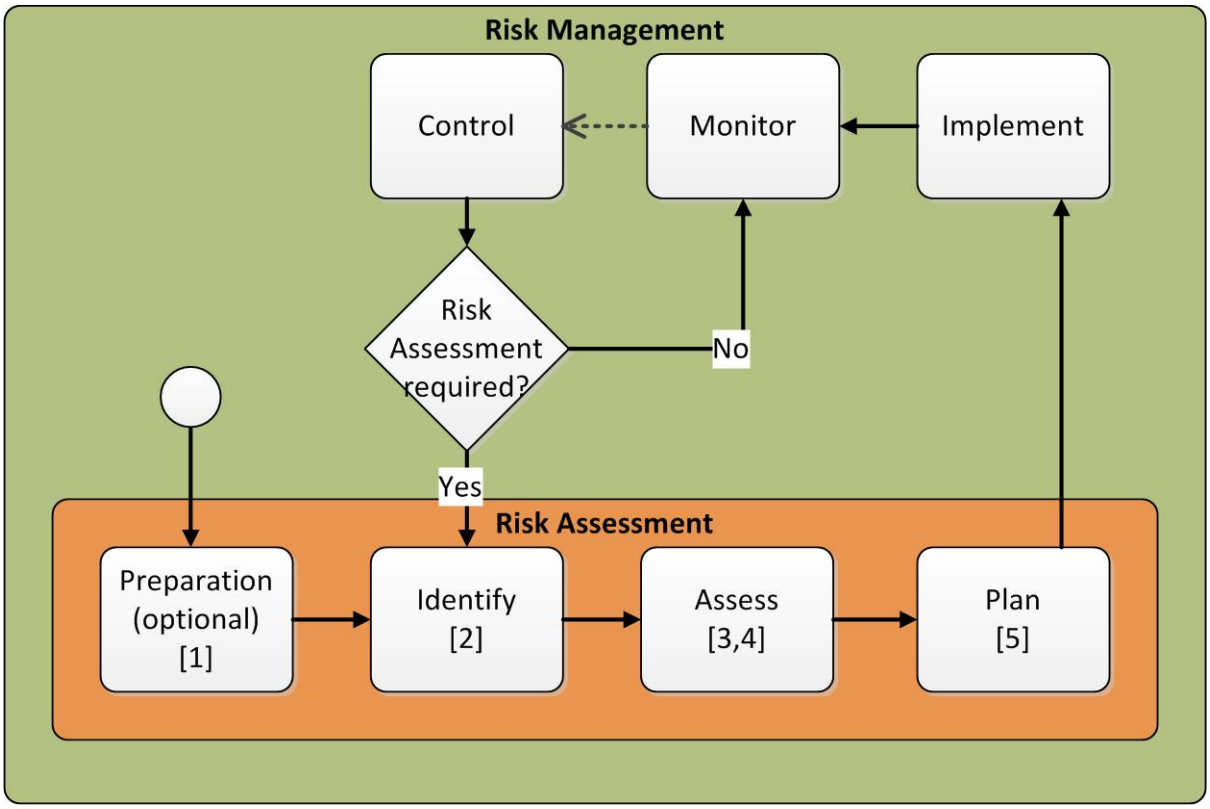
2.2 Information Security Risk Management

Risk Management and Risk Assessment are techniques that can be used to identify, monitor and control the risk level of an Information System (IS). Information Security Risk Management, in particular, can either be part of the overall organizational Risk Management process, or can be implemented separately [40]. Information Security Risk Management activities usually include implementing appropriate policies and related controls, promoting awareness, as well as monitoring and evaluating policy and control effectiveness [21]. The process is a usually cyclical. An overview of a typical Information Security Risk Management process is depicted in Figure 2.1. The dashed arrow means that the Monitor process does not stop when the Control process is started. Rather, the Monitor process is continuous and running in parallel with all other processes.

2.3 Risk Assessment

A critical step in the Information Security Risk Management process is the Risk Assessment. This involves the evaluation each IT risk as well as the total IT risk and giving them priorities.

Figure 2.1: Overview of a typical Risk Management process



While Risk Assessment is an activity that also takes place as part of the Risk Management process, it is not continuous. It is, however, a discrete activity, only being initiated when required or at regular intervals. Risk Assessments usually serve to identify and analyze possible vulnerabilities of and threats to a given system, as well as the relative value of assets and possible damage resulting from their compromise. This is done in order to estimate the risks that the owner, operator or user of the system may face. As such, its output is base for all the other Risk Management activities by eliciting new security requirements, aiding in the choice and specification of countermeasures, evaluating current Security Policies, supporting relevant management decisions, assessing existing protection mechanisms, controls, etc.

The main result of a Risk Assessment is usually a qualitative or quantitative evaluation of the possible risks that a given complex system is exposed to, taking into consideration its context and likely threats.

It should be noted that most Risk Assessments, as well as most Risk Management processes, do not aim at obtaining a fully secure system as this is often impossible. Instead, the end-goal is to reach what is perceived as an acceptable level of security at an acceptable cost (also called "good enough" security). Frameworks differ in their interpretation of this, and in the way of achieving and maintaining it.

In the most general sense, a Risk Assessment is a multidisciplinary task that might contain one or more of the following steps (Figure 2.1 maps the steps to the RM phases):

1. Establishment of context: Identifying and defining the digital, technical social and busi-

ness context in which the system operates as well as building some kind of model of the information system itself. Although the context of the IS is always relevant, this step is sometimes skipped if a satisfying specification of the IS already exists. This is usually part of the "preparation" stage in Figure 2.1. Other activities relevant for this phase are defining the scope of the assessment, security requirements, stakeholder goals, risk criteria etc.

2. Risk Identification: this is the core of any risk assessment and has to do with using available data to identify possible attack vectors and vulnerabilities of the system. This step corresponds to the "identify" stage in Figure 2.1.

3. Risk Analysis: this step has to do with understanding the probabilities, impacts, and other parameters associated with the identified risks in order to allow a better understanding of the system's vulnerabilities. This step corresponds to the "assess" stage in Figure 2.1.

4. Risk Evaluation: in this final step, risks are ranked and prioritized in order to allow decision makers to select countermeasures. This step corresponds to the "assess" stage in Figure 2.1.

5. Select countermeasures: Although this step is often considered to be outside the scope of a Risk Assessment, it is common for the results obtained from the above steps to be used for some for selection or prioritization of countermeasures, mitigation strategies, security controls or security policies. This corresponds to the planning stage in Figure 2.1.

2.3.1 Classification of Risk Assessments

Due to the large number of methodologies and frameworks available for evaluating Risk, a classification criteria would be useful in understanding the various options available. Risk Assessment or Risk Management methodologies can be grouped together based on various factors.

According to Houmb [25], Risk Assessments can be classified into three main types: *rule based, risk based (probabilistic) and judgment based.* Rule based assessments are usually based on a set of standards or checklists which are used as rules that the system should comply by. Risk based and judgment based assessments also take into consideration unknown threats and focus on assessing probabilities and impacts for each undesired event. The difference lies in the interpretation of probability: for risk based evaluations, only empirical data from similar contexts is used to estimate the probability while for judgment based assessments the subjective interpretation of the expert is used as the probability.

Zambon et al [60] introduces a framework for comparing Risk Assessment methods based on the following three parameters:

1. The scale used to evaluate risk (qualitative vs. quantitative)

2. Which factors are used to evaluate impact

3. The factors and operations used to compute risk

In this thesis, I will focus on parameters 1 and 3, as they provide a clear separation between the various types of Risk Assessments available:

Quantitative vs. Qualitative

Whether a method is considered quantitative or qualitative stems from its output (i.e. the way risk levels are measured). If risk is expressed in numbers on a ratio or interval scale, where the difference between any two values is known, then the method can be considered quantitative. If

however, risk is evaluated on an ordinal scale (e.g. high, medium, low), where only the ordering amongst values is known, then it is considered to be a qualitative method.

Qualitative risk assessments are descriptive rather than measurable. Purely quantitative methods usually rely on mathematical computations based on various metrics and thus usually require considerable amounts of data. Qualitative methods, on the other hand, can usually be performed within a shorter time, with less resources, less relevant data and require less mathematical, financial and security expertise. [55]

Risk computation

Based on the paper by Zambon et al [60], we introduce the following classification of Risk Assessment / Risk Management methodologies, based on which properties and factors are taken into account when evaluating risk, as well as how these factors are combined. In the following classification, an *Asset* is anything that is valuable for the organization, a *Threat* is regarding as any entity that can cause harm to the organization, a *Vulnerability* is any weakness that a threat might exploit to achieve its goals. While sometimes the concept of *Likelihood* is interpreted as a probability (between 0 and 1) or even as a binary indicator, in the rest of this document, I will use it with the meaning of a frequency (expected number of occurrences per period of time). This is because some events can occur multiple times in a given time frame, and as such this interpretation is more flexible. The operator $\otimes$ implies a computation between the two factors, usually a multiplication. However, specific formulas and operators are defined within individual methodology.

For an in-depth description of these concepts and factors, please refer to Section 4.3.1, although it must be kept in mind that the terms are used more loosely here. We identify 5 classes of Risk computations:

Class 1: $Risk(Threat, Asset) = Likelihood(Threat) \otimes Vulnerability(Threat, Asset) \otimes Impact(Threat, Asset)$

This is the classic way of computing Risk by taking into account the likelihood that a certain threat (i.e. attacker) will engage in an attack, the vulnerability of the target (asset) to the threat and the potential impact that the attack might have on the asset. This is commonly used in most general-purpose Risk Assessments.

Class 1 approaches evaluate Risk based on the relationship between each Asset (or group of assets) and each known threat (attacker or natural). Risk is computed by combining estimations of the likelihood that the threat will act upon the asset(s), as well as the impact that a successful such action might have on the asset(s). Furthermore, the Vulnerability of the asset with respect to the threat is taken into account.

Class 2: $Risk(Threat, Asset, Requirements) = Vulnerability(Threat, Asset) \otimes Impact(Threat, Requirements)$

This type of Risk Assessment evaluates risk based on the impact a threat might have on the Security Requirements that have been previously defined for the asset. This kind of approach is particularly useful when the assessment is done with the purpose of certification. For example, such an approach might be useful when comparing an Information System's security control to a standard benchmark (like ISO/IEC 27002) in order to establish if and by how much it deviates from the best practice recommendations.

In such approaches, "security needs" or requirements that the system must comply to have to be defined before-hand. Afterwards, the impact that each Threat might have on these Security needs is evaluated and combined with the overall vulnerability of the Asset with relation to the given threat in order to estimate Risk Level.

Class 3: $Risk(Threat, Asset) = AnnualLossExpectancy(Threat, Asset) = Likelihood(Threat, Asset) \otimes AverageLoss(Threat, Asset)$ This is the financial interpretation of risk. It is also calculated for a certain period (in this case, a year), which makes it even more applicable to cost/benefit and budget analysis. It usually requires quantitative data. An application scenario for such assessments would be the audits done by insurance companies in order to design commission and compensation schemes.

Again, Risk is evaluated for each Threat-Asset tuple. However, the term likelihood here gains the meaning of "successful attempts per year" and is combined with the average financial damage caused by each such attempt to obtain an estimation of the annual loss expectancy in monetary terms.

Class 4: $Risk(Threat, CriticalAsset) = Vulnerability(CriticalAsset) \otimes Impact(Threat, CriticalAsset)$ This is the approach usually undertaken for Security-Critical systems where probability of the threat is irrelevant as the asset needs to be fully secured against all threats at all times. Here, Risk is interpreted simply as the risk of being attacked at all. This kind of Risk Assessment might be applied to, for example, medical systems or in aerospace engineering.

For this approach, critical assets need to be identified, and for each such asset, its overall vulnerability is estimated and combined with the impact that each threat might have on the asset when successfully acting on this vulnerability.

Class 5: $Risk(Incident, Asset) = Likelihood(Incident) \otimes Impact(Incident, Asset)$ This approach is based on the traditional interpretation of Risk in safety analysis. Here, no specific threat (e.g. attacker) is taken into account. Instead, only the average frequency of negative events and their consequences are used to estimate Risk levels. Such approaches are common in, for example, risk assessment of a automotive on-board computer or other such system where the effect of environmental factors are relevant.

In Class 5 approaches risk is evaluated with relation to an incident and an asset. An incident is defined as the successful exploitation of a vulnerability. In this interpretation, each Risk can only be defined with regard to a vulnerability. This differentiates it from Class 1 approaches, where Threats can act upon assets even without the existence of a specific vulnerability. This aspect limits the scope of applicability of Class 5 Risk Analyses to weaknesses of the System.

Goal

Except for the above, another obvious classification criteria is the purpose for which the Risk Assessment is carried out. This can be one or more of the following:

- Certification
- Security audit
- Showing compliance to given rules, regulations, standards, guidelines or best practices
- Identifying corrective action(s) needed in order to achieve compliance (also called "Gap Analysis")
- Supporting security-budget (investment) decisions
- Providing up-to-date information relevant for the organization's Risk Management process

Due to the nature of the TREsPASS project, whose goal is "reducing security incidents in Europe and allowing organizations and their customers to make informed decisions about security investments", in this thesis I focus on the last three categories. However, due to the fact that the above categories are overlapping, some of the methods and tools analyzed in the following chapters could also be used for certification, audit and/or compliance. As such, the goal of each method will be related to one or more of the above, but also described in more detail.

Chapter 3

Survey of Information Security Risk Management/Assessment Methods

This chapter contains a survey of the relevant Information Security Risk Management of Risk Assessment methods used in practice. Some assumptions regarding the boundaries and scope of the survey are introduced in order to support a set of strict Inclusion and Exclusion Criteria. These are then used to filter an initial list of methods in order to restrict the analysis to only those methods that are relevant to the topic, that can be properly analyzed and that allow consistent comparison criteria to be applied.

3.1 Scope and assumptions of the survey

Due to the very large and diverse population of methodologies related to Risk Management and/or Risk Assessment, it is important to clearly state the purpose of the survey in order to apply a fair and consistent selection process and analysis.

Considering the context that this thesis was developed in (i.e. the TREsPASS project), the survey will focus on methodologies that describe step-by-step processes that can be used to conduct an enterprise-wide or system-wide socio-technical Risk Assessment as described in Section 2.2. Second, this process must deliver results which enable chief security officers and/or other management to rationalize about the need and effectiveness of security investments, as well as supporting such decisions. However, different organizations in different countries and sectors operate based on greatly varying business models and architectures. As such, it is essential that a clear definition of the assumptions made when selecting and discussing the RA/RM methods in-depth is made from the start. Based on The Open Groups document describing a framework for comparing RA processes and eliciting requirements for such methodologies [22], we state the following assumptions regarding the intended target organizations:

- The organization has a clearly defined management team which has the power and responsibility to see that high-level (business) objectives are met.
- The above described management team has a limited amount of resources available for achieving it's task

- There exists a broad spectrum of actors, threats and vulnerabilities that give rise to socio-technical information security risks which can interfere in achieving the objectives
- The management team requires reliable information that can be used to assess the risk landscape it is facing, as well as to identify various mitigation options.
- This information can be generated or derived from the application of a RA method as described in this document and used to make cost-effective decisions regarding the application of the limited resources available towards an acceptable reduction of the overall risk-level.
- The output of the risk assessment supports the defense of such decisions in front of other key stakeholders (like auditors, regulators, business partners, judges/juries, investors, shareholders, employees etc)

Of course, selected methods need to have sufficient documentation (publicly) available in English and must not be restricted to technical issues and users, nor should it be exclusively aimed at high-level management users. These, and other exclusion criteria are discussed in the next section.

3.2 Inclusion and exclusion criteria

Based on the assumptions described above (Section 3.1, a selection filter was applied to the initial list of methods. The criteria were chosen in order to make the selection as relevant to the topic as possible. Also, the criteria allow a fair and consistent comparison across all included methods. The inclusion criteria I-1 is to make sure the methods are relevant to the topic. I-2 and I-3 limit our set of methods to the ones applicable to enterprise-wide Information Systems, in order to conform with the Scope and assumptions. I-4 requires that analyzed standards or methods must include a specific step-by-step Risk Assessment method, as some only discuss general Risk Management guidelines or principles. I-5 is required in order to allow enough information about the method to be gathered. Finally, I-6 is essential in order to avoid methods designed for, and applicable to, specific national legislation, procedures or standards and encourage selection of internationally known and applicable methodologies.

Methods that are intended for the sole purpose of certification are of no interest w.r.t the topic as they were not written with the intended purpose of identifying, analyzing and evaluating IS risk, but simply to show compliance to a pre-defined standard (E-1). Lack of relevant documentation might cause difficulties in properly describing and analyzing specific aspects of a method (E-2). If such documentation is indeed available, but in languages other than English, it would make it hard, or impossible for the author to gain a good understanding of the approach and might pose threats to the validity of the conclusions or comparisons (E-3). Finally, we want to avoid methods written for a purely technical audience, such as the one intended for software development or ones focusing on the mechanics of the Information Systems while not taking into consideration aspects related to the context, the organization or its policies (E-4). Also not of interest are methods situated at the opposite end, which evaluate risk solely based on high-level issues, while ignoring technical aspects (E-5).

The methods that conform to all inclusion criteria and none of the exclusion criteria will be analyzed in-depth in Section 3.4.

- **Inclusion criteria**:

  (I-1) Describes a RA/RM method as defined in Section 2.2

  (I-2) Method takes as input an existing system or a design of a new system

(I-3) Intended users are chief security officers or other management able to make decisions regarding (security) budget

(I-4) Must contain a dedicated IS RA method

(I-5) Complete documentation available

(I-6) Method is in use in more than one country

- **Exclusion criteria**:

(E-1) Method is intended for the purpose of certification

(E-2) Lack of relevant documentation

(E-3) Documentation not available in English

(E-4) Product or system oriented method

(E-5) General management or governance oriented method

3.3 Initial list

To start with, an exhaustive list of methods that loosely conform to the inclusion criteria was generated. The list was compiled using the inventory of methods published by the European Network and Information Security Agency (ENISA) [41], as well as the work of Zambon et al. [60]. Furthermore, experienced professionals also part of the TREsPASS project helped with the selection. Finally, industry literature and surveys (e.g. [9], [34], [58] and [57] [25]) were used to identify other methods that are in use.

One thing to be noted is that most the the above literature contain surveys of risk assessment and risk management methods. However, they only compare a handful of methods each. In this thesis a union of all the methods analyzed in the industry surveys will be used to provide a complete overview of the current Risk Assessment landscape.

This initial list consists of a total 24 methods. From this initial list, we eliminate those that conform to at least one of the exclusion criteria. Table 3.1 shows the initial, exhaustive list of methods and the applicable exclusion criteria for those that are not selected for further analysis. An explanation of the exclusions follows.

The Austrian IT Security Handbook and Marion(1998) are only available in German. Furthermore, Marion was first introduced in 1983 and does not seem to be maintained or used since 1998, being replaced by MEHARI. The Dutch A&K method is only available in Dutch and only used in the Netherlands. The documentation of the ISF (i.e. Information Security Forum) methods (FIRM, IRAM, SARA and SPRINT) [29] are only available to members. MIGRA and ISAMM do not have complete documentation available, and mostly in other languages [60]. The ISO/IEC 15408:2006 (Common Criteria for Information Technology Security Evaluation) was also excluded because it is focused on evaluation the security of individual products or systems with regard to certification. ISO/IEC 27001:2005 is part of the 2700x family, but it's purpose is mostly audit and certification so it also falls outside our scope. COBIT works on a higher level of IT governance and is not explicitly designed for Risk Management. Finally, the NIST Special Publications are intended for technical users so it falls slightly outside our scope of tools that enable management to make budget decisions (according to I-3).

After the selection process we are left with 14 methods. Next, these will be described and analyzed in Section 3.4.

Method	Exclusion criteria
AS/NZS 4360 [61]	
Austrian IT Security Handbook [8]	E-3
COBIT [27]	E-5
CORAS [37]	
CRAMM [13]	
Dutch A&K Analysis [18]	E-3
EBIOS 2000 [39]	
FAIR [35]	
FRAP [49]	
ISAMM [17]	E-2, E-3
ISF Methods [29]	E-2
ISO/IEC 27001:2005 [4]	E-1
ISO/IEC 27002:2005 (formerly 17799:2000) [2]	
ISO/IEC 15408:2006 [5]	E-1, E-4
ISO/IEC 27005:2011 (incorporates ISO/IEC 13335-2) [6]	
IT Grundschutz [10]	
MAGERIT v2(2005) [44]	
Marion (1998) [14]	E-3
MEHARI [16]	
MIGRA	E-2
NIST Special Publication 800-39 [52]	E-4
OCTAVE [54]	
Risk IT[28]	
Structured Risk Analysis [38]	
TARA [51]	

Table 3.1: Initial list of methods and applicable exclusion criteria

3.4 In-depth Analysis

In this section we will be looking at the main characteristics of the previously selected RA/RM methods. Each analysis will follow a common structure. Considering the scope of this document, relevant features are the development context of the methods and their stated main objective(s). Also of interest is the Risk Assessment process itself, more specifically, the steps that need to be undertaken, as described by the method. Each description is followed by a discussion, where some unique characteristics, strong points or disadvantages specific to each method will be identified. The classification criteria described in Section 2.3.1 will also be taken into account, where relevant. Finally, for each of the analyzed methods, a summary of it's PROs and CONs will be distilled.

A complete overview of all the methods and all known characteristics is available in Annex A. Here all relevant features of the methodologies are described: Class, quantitative or qualitative, sponsor, Risk Assessment phases supported, release date, price, geographical spread, intended users, supporting tool(s), matching conceptual model, specific sector and target organization.

3.4.1 AS/NZS 4360

Name

The Australian/New Zeeland Standard for Risk Management AS/NZS 4360

Origin

The standard was introduced by Standards Australia International and Standards New Zealand in 1995, and revised in 1994. It has since been incorporated into the international standard AS/NZS ISO 3100:2009 - Principles and Guidelines.

Goal

The standard provides a generic guide to the Risk Management process at a very high-level. This allows it to be applicable to a wide rage of systems, organizations and activities. It is especially useful when used not only for Information Security Risk Management but as a uniform enterprise-wide approach to risk management.

Steps

The Australian/New Zealand Standard for Risk Management AS/NZS 4360:2004 [61] provides a generic framework for the process of managing risks which divides the elements of the risk assessment process into several sub-processes: "Establish the context", "Identify Risks", "Analyze Risks", "Evaluate Risks" and "Treat Risks" [25].The standard also describes two processes that should run in parallel with the risk assessment sessions as part of the Risk Management: "Monitoring and Review" and "Communicate and Consult". A flowchart describing this process can be found in Figure 3.1.

Discussion

The standard also puts heavy emphasis on establishing the context - both external and internal. In 2009 it was integrated into the AS/NZS ISO 3100:2009 international standard which introduces a new conceptualization of Risk: from "chance or probability of loss" to "the effect of uncertainty on objectives". The 3100 framework and it's conceptual model are discussed more in-depth in Section 4.2.1. However, in this case, it's strength can also bee seen as a weakness. Due to it's broad applicability, it offers almost no practical guidelines for it's implementation and leaves that up to the actual assessor. For non-experts this can lead to ambiguities regarding certain sub-processes and their correct implementation.

Evaluation

PROs:

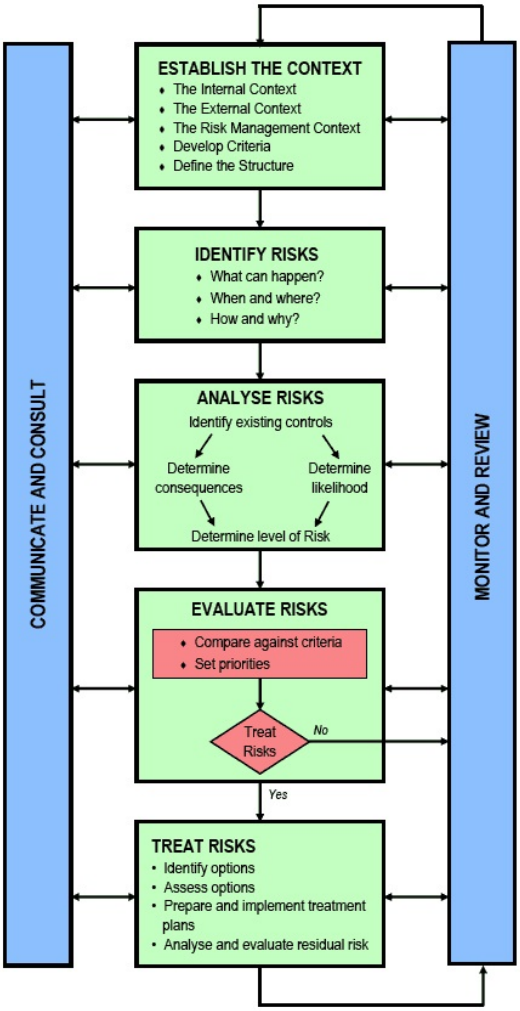
- Is supported by an extensive, standardized risk taxonomy and conceptual model (AS/NZS ISO 31000)
- Strong emphasis on “context”
- Flexible

CONs:

- Diminished focus on risk treatment

Figure 3.1: The AS/NZS 4360 Risk Management process

Source: [61]



- Lacks technical depth and more practical guidelines/tools

3.4.2 CORAS

Name

CORAS: A platform for risk analysis of security-critical systems

Origin

The CORAS method was a result of an EU-funded project, completed in 2003. Since then, the method itself has not undergone any major updates. However, the CORAS tool is still being

maintained by the OpenSource community.

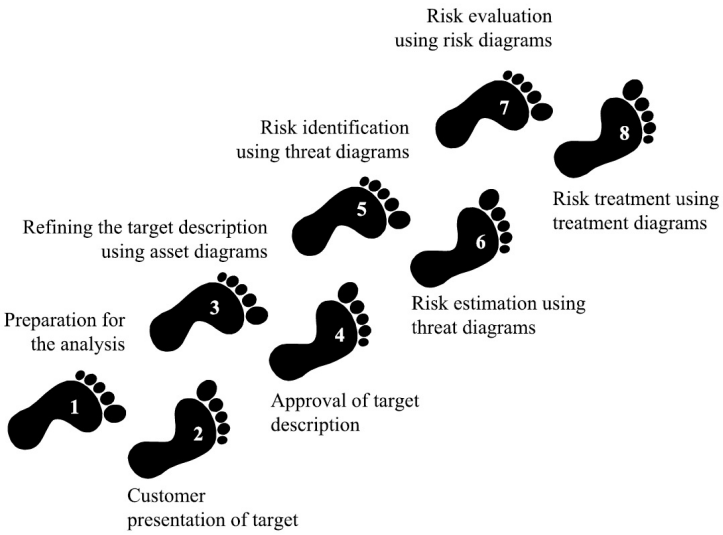
Goal

The stated goal of the CORAS project was to develop a practical model–based framework and computerized support for "precise, unambiguous and efficient risk assessment of security-critical systems" [7].

Steps

Figure 3.2: The 8 steps of the CORAS method

Source: [37]



The method describes 8 consecutive steps, visible in Figure 3.2:

1. The first step is mostly preparatory: identify the target of assessment and the depth of the analysis.
2. The second step consist of a meeting with the customer: reach a common understanding of the overall goals and planning as well as of target, focus and scope of assessment.
3. The third step further defines the target of assessment and it's most valuable assets. Some high-level threat scenarios, vulnerabilities and risks that should be investigated further are agreed upon. The refined objectives and detailed description of the target are documented using the CORAS language.
4. The fourth step is the last step before the actual risk analysis and focuses on eliciting the risk evaluation criteria to be used further on. This step also verifies that the customer approves the detailed description of the target and it's context, including assumptions and preconditions.

5. The fifth step uses the CORAS language as a basis for a multi-disciplinary brainstorming workshop. The purpose of this workshop is to identify as many risks as possible (i.e. risk identification).

6. The sixth step is aimed at estimating the risk levels (i.e risk analysis). This is also done during a cross-disciplinary brainstorming session where likelihoods and consequences of each previously identified risk are determined..

7. In the seventh step the previously defined risk evaluation criteria are used to deem each risk as either acceptable or requiring treatment (i.e. risk evaluation)

8. In the eighth step, possible treatments and mitigations are identified, evaluated and compared.

Discussion

CORAS is a model-based approach to conducting Risk Assessments. It relies on it's own modeling language which is an extension of UML that can be used in conjunction with the risk assessment to serve three purposes [50]:

- Describing the target of assessment
- As a communication medium that facilitates interaction between different groups of stakeholders
- Documenting the results and underlying assumptions

Furthermore, the method comes with a dedicated tool that facilitates documenting, maintaining and reporting analysis results through risk modeling [37]. The method was created as a result of a EU-funded project (IST-2000-25031) that was aimed primarily at risk analysis of security-critical systems. The methodology defines four kinds of diagrams (asset, threat, risk and treatment diagrams) as part of it's "model-based" approach to support various visualizations in various steps of the process. All diagrams make use of the same, relatively small, set of symbols.

The method differentiates between direct and indirect assets. Assets are the entities that need to be protected and essentially the motivation for the Risk Assessment. Furthermore, it classifies threats to these assets as:

- Human threat (accidental)
- Human threat (deliberate)
- Non-human threat

The CORAS method is based on the ISO 17799 standard (now 27002, described in Section 3.4.7) and as such is also compatible with ISO/IEC 13335 (now 27005, described in Section 3.4.7) and the AS/NZS 4360 standard (described in Section 3.4.1) [50].

It should be noted that the first 4 steps of the CORAS method are mostly concerned with defining and reaching consensus among all stakeholders regarding the target, context and goals of the assessment. It is only the second half of the analysis where the actual risk assessment is performed: Step 5 corresponds to *Risk identification*, Step 6 is *Risk analysis*, Step 7 is *Risk evaluation*, while Step 8 is where the *Risk treatment* takes place.

Evaluation

PROs:

- Free tool support
- Facilitates iterative communication and collaboration between various stakeholders
- Very thorough, suitable for security-critical systems and large organizations

CONs:

- Requires expert knowledge from various backgrounds
- Might be lengthy
- No longer developed

3.4.3 CRAMM

Name

CCTA Risk Analysis and Management Method (CRAMM).

Origin

The CRAMM method was originally developed by the Central Communication and Telecommunication Agency, a British government organization, 1985. Since then it has undergone several revisions, and is currently owned, sold and developed by a British company: Insight Consulting, a division of Siemens Enterprise Communications Ltd. [41].

Goal

CRAMM can be used to justify security investments by demonstrating need for action at management level. Secondary applications can be benchmarking the security of an organization or showing compliance to other standards (like the BS7799 - British standard for information security management) [59]. CRAMM is intended for large organizations, like government bodies and industry [41].

Steps

The CRAMM process consists of three main phases[13]:

1. Asset identification and valuation - After establishing the overall objectives of the assessment as well as the boundaries, physical and software assets are identified and valuated. This is commonly done via interviews
2. Threat and vulnerability assessment - This step covers the actual assessment of risks by identifying and analyzing possible threats to the system, assessing the vulnerability of the system to those threats and finally using the knowledge about assets, threats and vulnerabilities to compute risk.
3. Countermeasure selection and recommendation - This third stage makes use of CRAMM's countermeasure repository to identify and rank by cost and effectiveness the available mitigation strategies.

Discussion

CRAMM is a very versatile method, allowing users to achieve various tasks at various levels of complexity. The methodology come with extensive tool support, both free (CRAMM express) and professional (CRAMM expert), as well as a database of over 3000 ranked security controls (i.e countermeasures), and even certification tools [13].

CRAMM attempts a qualitative, asset-centric approach, making use of 10 predefined asset table to aid in the identification and valuation of assets [25]. Assets are classified into categories, each with a pre-defined set of known vulnerabilities and threats. Once assets have been identified and valuated, and likely threats and vulnerabilities found, the dedicated tool automatically returns possible countermeasures. However, this means that the methodology itself is of little use without the software toolkit.

CRAMM is compatible with ISO 270001 certification, and its asset-centric approach as well as its asset valuation technique have even been integrated into other methodologies (like CORAS) [25].

Evaluation

PROs:

- The complexity of the assessment can be tuned to needs
- Especially useful for large enterprise organizations
- Process is mostly automated (in software tool)

CONs:

- Expert knowledge required
- Full assessments can be lengthy or overly-complex
- Can only be used in conjunction with dedicated tool

3.4.4 EBIOS 2010

Name

Expression des Besoins et Identification des Objectifs de Sécurité (EBIOS)

Origin

The method was originally developed by the French Central Information Systems Security Division and is now maintained by a private club of experts from various fields and origins (ie. Club EBIOS). [39]

Goal

The goal of the EBIOS method is the assessment and treatment of risks associated with an IS (whether enterprise-wide or specific) in order to support management-level decision-making and to create a common ground for security discussions between various stakeholders [41].

Steps

1. The first phase deals with context establishment: the relationship between the business context and the IS (contribution to business goals, boundary, decomposition)
2. In the second phase, security requirements are determined based on the feared security events
3. In the third phase, a risk study conducted in order to identify and analyze threat scenarios
4. In the fourth phase, information from the previous steps is used to identify risks and describe the necessary and sufficient security goals relating to these risks
5. In the final phase, the necessary security controls are determined, and any residual risk is made explicit.

Discussion

One of the main strengths of the EBIOS approach is is it's modularity: it's knowledge bases can be tuned to comply to local standards and best practices, and to include external repositories of attack methods, entities or vulnerabilities [41].

EBIOS can be used both in the design stage or against existing systems [34]. Instead of a scenario-based risk analysis, EBIOS goes for a more structured approach, allowing a more exhaustive analysis through the identification of various sub-components or causes of risk (e.g. entities, vulnerabilities, attack methods, threat agents, etc). It's 5 phases can also be applied somewhat independently, allowing for only certain parts of the analysis to be (re)done (e.g. vulnerability analysis) [34].

The method is also supported by a dedicated tool: the EBIOS tool, described in Section 5.3.8. Furthermore, the method is compatible with all relevant ISO standards (13335, 15408, 17799, 31000, 27005, 27001) [39].

Evaluation

PROs:

- Generic method that allows for tuning to local standards, habits, context
- Can be applied to targets of assessment of various sizes and complexities (from entire IS to single web-site)

CONs:

- Most detailed documentation and support only available in French

3.4.5 FAIR

Name

Factor Analysis of Information Risks (FAIR).

Origin

The FAIR methodology is part of the FAIR framework described in Section, introduced by Risk Management Insight LLC. in 2005 under a Creative Commons Attribution-Noncommercial-Share Alike 2.5 License[1].

Goal

The FAIR methodology hopes to address the issue of information security being practiced "as an art rather than a science"[35]. As such, it's goal is to rely less on the practitioner's experience, intuition or best practices and instead derive output from repeatable, consistent, financially sound computations.

Steps

The FAIR Basic Risk Assessment Guide [35] describes a process comprised of ten steps, spread across four stages:

Stage 1 Identify scenario components

1. Identify the asset at risk
2. Identify the threat community under consideration

Stage 2 Evaluate Loss Event Frequency (LEF)

3. Estimate the probable Threat Event Frequency (TEF)
4. Estimate the Threat Capability (TCap)
5. Estimate Control Strength (CS)
6. Derive Vulnerability (Vuln)
7. Derive Loss Event Frequency (LEF)

Stage 3 Evaluate Probable Loss Magnitude (PLM)

8. Estimate worst-case loss
9. Estimate probable loss

Stage 4 Derive and articulate Risk

10. Derive and articulate risk

[1] **CC A-N-SA 2.5:** Anyone is free to Share (copy, distribute and transmit the work) and Remix (adapt the work) under the conditions:

- Attribution: You must attribute the work in the manner specified by the author or licensor (but not in any way that suggests that they endorse you or your use of the work).
- Noncommercial: You may not use this work for commercial purposes.
- Share Alike: If you alter, transform, or build upon this work, you may distribute the resulting work only under the same or similar license to this one.

Discussion

FAIR is, in fact, an entire framework that includes a taxonomy of the factors that make up information risk, methods for measuring such factors, computations that derive risk mathematically from the measured factors and even a simulation model that takes as input all of the above to create and analyze complete risk scenarios. In this section, we focus on the Risk Assessment methodology, as described within FAIR. The taxonomy and conceptual model it introduces will be further described in Section 4.2.2.

FAIR's Basic Risk Assessment process, as described in [35], relies extensively on tables which need to be filled in with ordinal values of the type: "low-medium-high". The ordinal values are however, defined based on intervals, described in the guide [35]. Operators are then defined on these factors by means of matrices. After step by step estimation and computation of the various factors driving risk, an evaluation of total Risk is obtained, also on a 4 level ordinal scale. This is similar to the approach undertaken in a Structured Risk Assessment (see Section 3.4.13). The key difference here is that a FAIR analysis focuses on a single assets, while an SRA first decomposes the target of assessment into components and then evaluates risk individually for each one. Furthermore, the FAIR analysis evaluates the risk for one Threat Community at a time. However, the FAIR analysis takes many more factors into account and offers a more precise evaluation of each Asset - Threat Community pair.

The Risk Assessment described above is intended for use in simple, single level risk analysis, not describing the additional steps required for a multilevel analysis [35]. A slightly more complex analysis (looking at a number of assets, or various threat communities) can of course be achieved by simply running the Basic risk assessment multiple times, once for each Asset - Threat Community pair. Documentation of performing more complex Risk Assessments is not publicly available on-line, and knowledge and qualification to perform such assessments based on FAIR can only be obtained by following training courses.

The methodology is also supported by a dedicated tool: FAIRLite (further described in Section 5.3.9 and 5.3.10).

The FAIR methodology is not in direct competition with the other methodologies. In fact, it's complementary to most other Risk Management methodologies and can be used in conjunction with NIST 800-30, ISO/IEC 27002, COBIT, ITIL or COSO [23]. Furthermore, it has been adopted as the basis for The Open Group's Risk Taxonomy [23] (described in Section 4.2.6) and is referenced in ISACA's RiskIt framework [28] (described in Section 3.4.12).

Evaluation

PROs:

- Takes into account micro factors to obtain macro results by breaking down risk into elements
- Supported by extensive taxonomy, conceptual model and Risk Management Framework
- Basic RA process is fast and does not require dedicated tools or specialized training

CONs:

- Available documentation supports only Basic RA on single assets; specific training required for conducting system-wide analyses.

3.4.6 FRAP

Name

Facilitated Risk Assessment Process (FRAP)

Origin

FRAP was first introduced by Thomas R. Peltier in 2000 [48]. Application of the FRAP method is described by Peltier in his book Information Security Risk Analysis [49], published in 2001, and further detailed in the second edition published in New York in 2005.

Goal

The goal of FRAP is to sketch how a "facilitator-led" qualitative risk analysis and assessment can be applied in order to produce findings understandable by non-experts [34].

Steps

The RA process described by FRAP if divided into three phases:[12]:

1. A pre-FRAP session where the scope and definitions of the assessment as well as how threats are to prioritized are agreed upon. In this method, the team is put together and a decision is made regarding the assets that are to be included in the analysis.

2. A FRAP session, the actual risk assessment takes place: risks are identified and risk levels are determined by taking into account the likelihood of the threat occurring

3. A post-FRAP report generation: this report contains a summary of the risks as well as suggestions on how these can be diminished.

Discussion

One of the unique aspects of FRAP is that is is a "facilitator-led" approach in the sense that the stakeholders play a big role in the assessment. Stakeholders own and drive the process, are involved in all assessment activities and it is the stakeholders' own assessment that creates the output. However, FRAP does not provide many technical details on how to conduct the assessment, and relies on the role of the Facilitator to guide the stakeholder through the process by making use of his own knowledge, experience and also other, more technical, methodologies.

FRAP operates on the idea that precisely quantifying risks is not cost effective due to the large amount of time and complexity a quantitative analysis requires and the fact that exact estimates of loss are not needed in order to determine if controls should be implemented. Furthermore, the creator of the method claims that a risk analysis using FRAP takes around 4 hours and only requires 7 to 15 people, most of which can be internal to the organization and managers [47].

The FRAP methodology is based on the assumption that security controls are not yet implemented and, as such, does not take into account the vulnerability caused by a lack of such controls. This method closely resembles Class 3 methods according to the criteria described in Section 2.3.1, although the impact is evaluated based on how it affects business operations not only based on the financial loss caused. There is also an extension of FRAP that allows for the estimation of residual risk (i.e. the risk level once a control has been selected and implemented) [12].

Evaluation

PROs:

- Highly business-driven approach, producing output relevant for stakeholders
- Requires little external assistance, most of the steps can be achieved with the organization's own employees (even if they are not security experts)
- Very fast (FRAP session can be finished in 4 hours)

CONs:

- Success highly dependent on the "facilitator", which must be a good negotiator, and posses knowledge of both business and information security.
- Works best in conjunction with a technically appropriate methodology.

3.4.7 ISO/IEC standards

There are many ISO/IEC standards related to security. However, we have restricted our list to the ones that conform to the inclusion and exclusion criteria described in Section 3.2. As such, we have narrowed down the list to only two standards: the ISO/IEC 27002 and 27005.

It is worth mentioning that other relevant standards would conform to the criteria, such as ISO/IEC 13335-3[1] and 17799[3]. However, both of these have been made obsolete and are mostly replaced or integrated with either ISO/IEC 27002[2] or 27005[6]. A time-line describing this process can be seen in Figure 3.3. From the figure we can conclude that the current up-to-date ISO/IEC standards that are relevant to either RA and/or RM are:

- ISO/IEC 27002:2005: Code of practice for Information Security Management
- ISO/IEC 27005:2011: Information security risk management
- ISO/IEC 13335-1:2004: Concepts and models for information and communication technology security management

However, the latter (13335-1:2004) is aimed at describing concepts and models that can be used to better understand and specify ICT security as well as presenting some general management issues. As such, it does not conform to the selection criteria described in Section 3.2, and will be instead treated in the section dedicated to conceptual models (i.e. Section 4).

ISO/IEC 27002:2005 (formerly 17799:2000) (incorporates BS 7799-1)

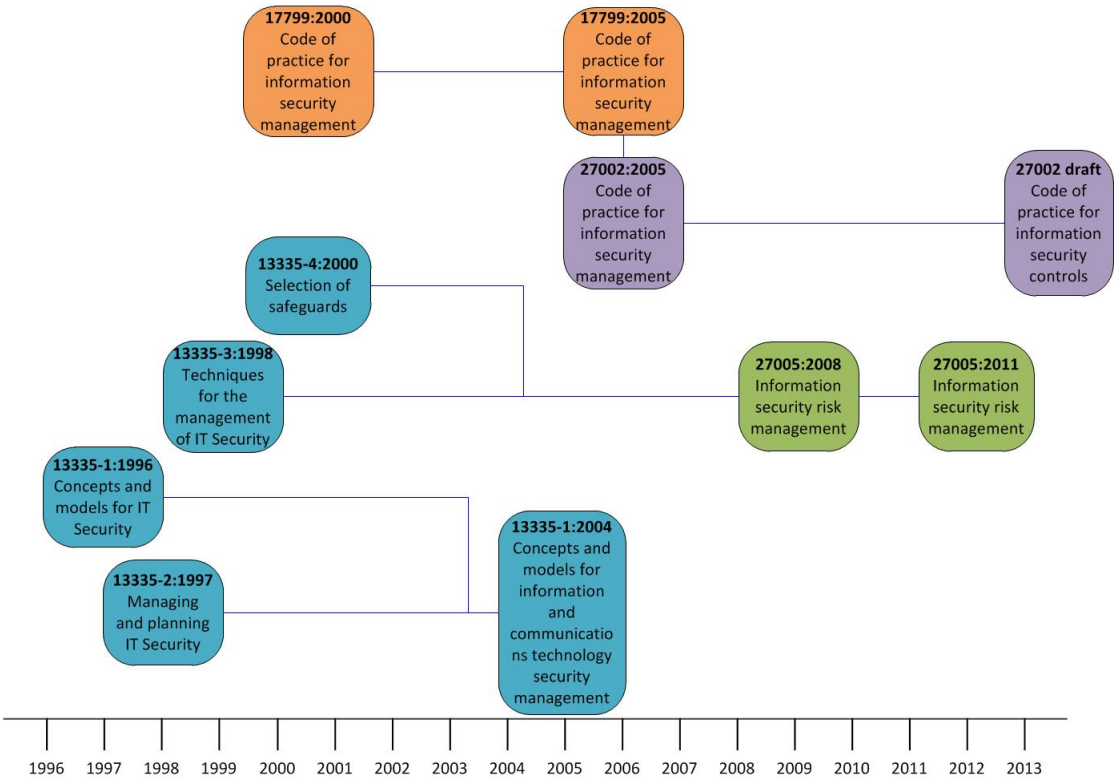
Name

ISO/IEC 27002:2005: Code of practice for Information Security Management.

Origin

ISO/IEC 27002 was is derived from the BS7799 standard, first published in the 90's. It was subsequently integrated into the ISO/IEC 17799 standard and later renamed to it's current label.

Figure 3.3: A time-line of the ISO/IEC standards relevant for Information Security RA/RM



Goal

The standard ia aimed at "establishing guidelines and general principles for initiating, implementing, maintaining, and improving information security management within an organization". The standard describes a set of 12 security clauses, each with a number of sub-categories for which control objectives are defined and guidelines on how such control can be applied are given. On top top of this, the standard gives a few best practice suggestions for conducting a formal Risk Assessment and Treatment.

Steps

The standard does not define individual steps that have to be undertaken, but does define a broad outline to which the Risk Assessment process must conform. The actions that must be part of the Risk Assessment according to ISO/IEC 27002 are:

1. Risk identification, quantification and prioritization based on objectives relevant to the organization
2. Risk analysis: estimating the magnitude of Risks
3. Risk evaluation: determine importance of risks by comparing estimated risk levels against previously defined risk criteria

4. Risk treatment: define risk acceptance criteria and use them to decide if and when treatment is indeed warranted. Then decide which approach to Risk Treatment is suitable to the organization (accept, avoid, transfer or apply controls). A large amount of such controls, grouped on clauses and categories make up the bulk of the ISO/IEC 27002 document.

Discussion

The ISO/IEC standard, while giving guidelines towards conducting Risk Assessments, does not offer sufficient practical tips towards completing such a task. Instead, it's focus is on suggesting controls for various known vulnerabilities. As such, it's focus is on Risk treatment, and it should be augmented by using a third-party Risk Assessment method before-hand, in order to get a better idea of which controls are relevant and required for your organization. Once a Risk Assessment consistent with the suggested guidelines is implemented, ISO 27002 can be used for selection and implementation of controls.

However, in practice, ISO/IEC 27002 alone can be used as a basis for Risk Assessment. This in known as ISO 27002 Gap Assessment/Analysis and the main idea is that the existing controls are compared to the ones described in the standard. Any deviation, or gap, is noted and evaluated. As a result, Risk can be estimated based on these identified gaps, and mitigation strategies can also be derived. In some sense, the standard is used as a benchmark for assessing the effectiveness of existing controls and identifying possible weak spots.

Evaluation

PROs:

- Supported by extensive taxonomy, conceptual model and Risk Management Framework (ISO 13335)

CONs:

- Only describes the Risk Assessment process at a very high level.
- Needs to be used in conjunction with a lower-level Risk Assessment methodology in order to be relevant to management users.
- Focuses mostly on Controls and Risk Treatment instead of Risk Identification and Analysis

ISO/IEC 27005:2011 (includes ISO 13335-3/4)

Name

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

Origin

The ISO/IEC 27005 standard was drafted and published by the International Organization for Standardization(ISO) and the International Electrotechnical Comission (IEC). The first version was launched in 2008 as a replacement for the Management of Information and Communications Technology Security (MICTS) standards ISO/IEC TR 13335-3:1998 plus ISO/IEC TR 13335-4:2000.

Goal

Steps

The ISO 27005 Risk Assessment process is sub-divided as follows:

1. Risk Analysis
   (a) Risk Identification - find possible sources of potential loss (primary and supporting assets, threats, existing and planned security controls, vulnerabilities, consequences and business processes) are identified.
   (b) Risk Estimation - the previously acquired knowledge is used to qualitatively or quantitatively measure the risk:
      i. assess the consequences (i.e. impact) by valuating the assets
      ii. assess the likelihood of each incident by valuating threats and vulnerabilities
      iii. assess risk by valuating consequences and likelihoods
2. Risk Evaluation - each risk level is compared to risk acceptance criteria and risk evaluation criteria; prioritized list of risks and recommended treatment options is created.
3. Risk Mitigation - measures for reducing, retaining, avoiding or transferring risk are selected and used to produce a risk treatment plan.

Discussion

While ISO 27005 gives a broad outline of a structured, systematic and rigorous Risk Assessment process that takes into account all organizational aspects (people, processes and technology), it does not provide or recommend a specific low-level method with technical detail for conducting this activity. It does not even lean towards qualitative vs. quantitative approaches, simply giving suggestions on the applicability and scope of each approach. It is geared towards high-level, management practices. [55]

An overview of the entire 27005 Risk Management process, including the Risk Assessment is available in Figure 3.4 and is obviously similar to the AS/NZS 4360 process picture in Figure 3.1. This is because both standards have been designed with the generic Risk Management guidelines and principles described in ISO 31000 in mind.

Evaluation

PROs:

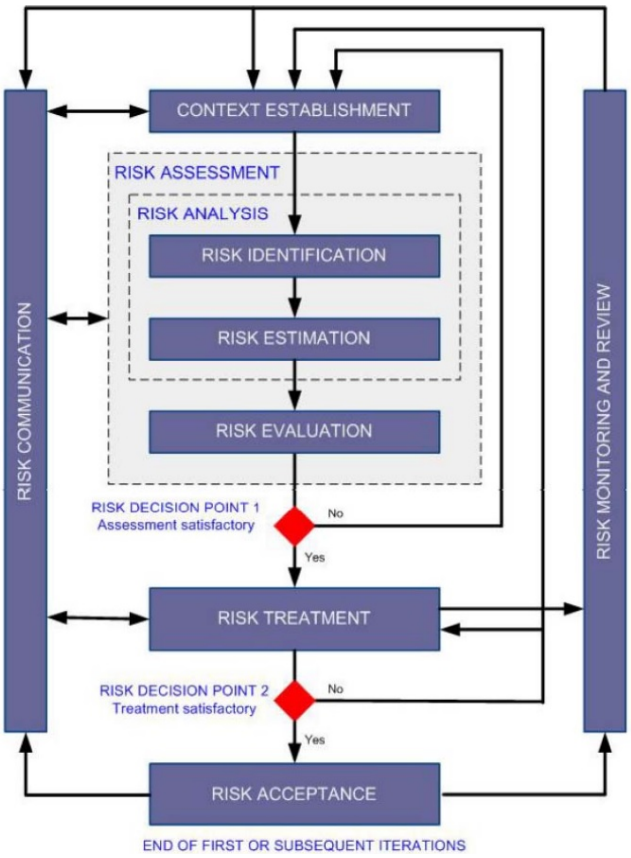
- Supported by extensive and standardized Taxonomy, Conceptual Model and Risk Management Framework (ISO 13335, 2700x and 31000)
- Flexibility in the choice of complementary low-level (technical) Risk Assessment method

CONs:

- RA process is described at a very abstract level
- Third-party RA method required in order co carry out a comprehensive RA
- Does not describe specific risk analysis method, but offers general advice on choosing and using such methods.

Figure 3.4: The ISO 27005 Risk Management workflow

Source: [6]



3.4.8 IT Grundschutz

Name

IT-Grundschutz (Former English name: IT Baseline Protection Manual)

Origin

IT-Grundschutz is part of a series of standards published by the German Federal Office for Information Security (BSI) describing "methods, processes, procedures, approaches and measures relating to information security" [10]. Apart from a more general Information Security Management methodology, BSI-Standard 100 also describes how to perform a step-by-step Risk Assessment in a manner consistent with the rest of the standard.

Goal

The goal of the IT-Grundschutz Risk Assessment is to provide a qualitative method for identification, analysis and evaluation of security incidents that might be damaging to the business, that

is also consistent and usable with the rest of the standard, and that can be applied efficiently. The standards describes a two-tier risk assessment: one is designed for reaching a "standard" level of security, while a second "supplementary risk analysis" can be undertaken by companies that desire an approach customized to their specific needs or sector or that have special security requirements.

Steps

For companies implementing a "standard" Information Security Management System based on IT-Grundschutz, the Risk Assessment is done by using the IT-Grundschutz Catalogs. These contain repositories of common threat scenarios and standard security countermeasures applicable to most IT environments, and grouped by modules corresponding to various business environments and Information System components. In order to achieve a higher level of information security, a "supplementary risk analysis based on IT-Grundschutz" can also be performed by taking the following steps[31]:

1. Prepare an overview of threats: a list of relevant threats is created for each asset that is to be analyzed by using the IT-Grundschutz catalog
2. Determine additional threats: Any threats specific to the application scenario are identified via a brainstorming session.
3. Assess the threats: The threat summary is systematically analyzed to determine if the implemented and/or planned security measures provide adequate protection for each target object and threat. Thus, all relevant security mechanisms are checked for completeness, strength and reliability.
4. Select safeguards for handling risks: Decisions are made at management level on the way risks not adequately mitigated are to be handled. Options include: reducing risk via safeguards, avoiding risk, transferring risk and accepting risk.
5. Consolidate results: The new security policy and mechanisms as a whole is verified, checked for consistency, user friendliness and adequacy to the target environment.

Discussion

The main body of the standard does not describe a specific Risk Assessment procedure, but instead gives suggestions for safeguards appropriate for typical business processes, applications and IT systems that have normal security requirements. As such, typical IT assets and components are described, including organizational, infrastructural and personnel aspects, potential threats are enumerated and necessary countermeasures suggested. In order to identify basic deficiencies in the IT security of the target system and achieve basic compliance with the IT-Grundschutz standard, the relevant modules are selected and applied to each aspect of the Information System. This allows for a fast and cost-effective way of achieving a reasonable level of security.

However, the standard also describes in detail a process it calls "Supplementary Risk Analysis" that is to be used in contexts that differ significantly from standard IT security application scenarios and requirements. It is the responsibility of the (IT) management to decide whether or not such a supplementary analysis is warranted and for which assets or components.

IT-Grundschutz is designed to be compatible with established Information Security standard ISO/IEC 27001. Although it is not the indented purpose, the IT-Grundschutz methodology can even be used to show compliance to this standard.

The two-tiered approach means that the standard can be useful for SME's trying to achieve "good enough" security with limited resources, while also allowing scaling up to a full-fledged, customized Information Security Risk Management system, suitable for large companies with extraordinary security requirements.

Evaluation

PROs:

- Two-tiered approach allows the method to be progressively applied to systems of various complexities and security requirements
- Supported by extensive Risk Management standards, guidelines and documentation
- Compatible with established Information Security Standards ISO/IEC 2700*
- large number of third-party tools compatible with the methodology are available

CONs:

- Security and technical expertise required to take advantage of some of the in-depth descriptions.

3.4.9 MAGERIT v2(2005)

Name

MAGERIT: Risk Analysis and Management Methodology for Information Systems.

Origin

MAGERIT was developed by the Spanish Higher Council for Electronic Government (CSAE) in response to the perception that the government (and society in general) is becoming more and more dependent on information technology in achieving its service objectives [44]. It was first published in 1997, with MAGERIT v2 being launched in 2005 and a third version only available in Spanish at the time of writing.

Goal

MAGERIT's stated goal is three-fold: (1) make IS stakeholders aware of the existence of risks and need for treatment, (2) offer a systematic method for analyzing these risks and (3) help in describing and planning the appropriate measures for keeping the risks under control. Furthermore, it aims to prepare the organization for the process of evaluating, auditing, certifying or accrediting as well as promoting uniformity in the reports containing findings and conclusions from risk analysis and risk management activities. [44]

Steps

MAGERIT describes the following "Risk Analysis" process:

1. Determine the relevant assets for the organization, their inter-relationships and their value (i.e. what prejudice/cost would be caused by their degradation). Assets are the resources in the information system or related to it that are necessary for the organization to operate correctly and achieve the objectives proposed by its management.

2. Determine the threats to which those assets are exposed. Threats are “things that happen.” Of all the things that could happen, those that are of interest are those that could happen to our assets and cause damage.

3. Determine what safeguards are available and how effective they are against the risk. Safeguards or counter-measures are procedures or technological mechanisms that reduce the risk.

4. Estimate the impact, defined as the damage to the asset arising from the appearance of the threat. Impact is the measurement of the damage to an asset arising from the appearance of a threat. By knowing the value of the assets (in various dimensions) and the degradation caused by the threats, their impact on the system can be derived directly.

5. Estimate the risk, defined as the weighted impact on the rate of occurrence (or the expectation of appearance) of the threat. Risk is the measurement of the probable damage to the system. Knowing the impact of the threats to the assets, the risk can be derived directly simply by taking into account the frequency of occurrence. The risk increases with the impact and with the frequency.

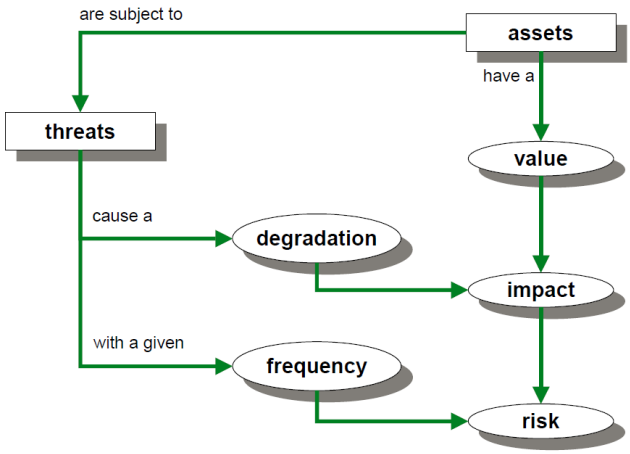
At the end of the analysis, it is recommended that step 4 and 5 be revisited in order to identify potential residual impact or residual risk.

Discussion

An conceptual overview of how each risk is estimated according to the MAGERIT methodology is depicted in Figure 3.5. This approach is consistent with both the ISO 13335 conceptual model (Section 4.2.3) and the FAIR/Open Group conceptual models (Sections 4.2.2 and 4.2.6)

Figure 3.5: Risk Analysis according to the MAGERIT method

Source: [44]



The MAGERIT method is divided across three books. The first one ([44]) describes the risk analysis methods in detail. The second one, entitles "Elements Catalog"[45] serves as a sort of repository of common asset types, dimensions and criteria for evaluating them, typical threats and best practice safeguards as well as templates. Finally, the third book, "Techniques"[46] gives

additional information and guides on some (formal) techniques often employed when carrying out risk analysis and management projects.

The documentation also describes how to carry out a planning phase in preparation for the assessment as well as tips on how to use and integrate the results into a continuous Risk Management strategy.

The MAGERIT documents describe the Risk Assessment methodology from three perspectives, each implying a certain level of granularity and abstraction. First (in Book 1, Chapter 2) the method is described at a high level, suitable for management and for understanding how the Risk Assessment needs to be integrated in a manner consistent with a Risk Management strategy. Afterwards, the process is described at an operational level, by specifying exactly which activities should be undertaken for each phase, as well as describing the outputs and inputs required. Finally, Book 1 Chapter 5 describes practical aspects arising from experience while the second and third books are focused almost exclusively on technical details, repositories and techniques that can be used by the analysis team in when actually carrying out the assessment. All this is complemented by Chapters describing how to apply such a Risk Assessment to systems under development (Book 1 chapter 4). [53]

There are also a number of both free and commercial tools capable of producing a variety of deliverables in standardized and customizable formats, both textual and graphic, that can be used to assist in the application of MAGERIT (e.g. PILAR, EAR).

Evaluation

PROs:

- Presents the Risk Assessment process at different levels of granularity and can be applied both quantitatively and qualitatively.
- Supported by technical documents describing common assets, threats, safeguards, criteria, formal techniques and templates.
- Can be applied as a stand-alone RA method, but can also be used as to implement a full-fledged Information Security Management System.

CONs:

- Version 2 has been revised by MAGERIT v3, which was only available in Spanish at the time of writing

3.4.10 MEHARI

Name

Methode Harmonisee d'Analyse de Risques (MEHARI). (Harmonised Risk Analysis Method)

Origin

The MEHARI Risk assessment methodology was developed by a non-profit information security organization, CLUSIF (i.e. Club de la Sécurité de l'Information Français in 1996. The methodology is also supported by a private company, Risicare [9].

Goal

MEHARI is mostly aimed at executive personnel (especially CISOs), and is designed to assist in the implementation of ISO/IEC 27005[6]. It was developed in compliance with other existing Information Security Standards like ISO 13335, 27001 and 27005 in order to allow a certifiable, audit-able process for analyzing scenario-based risk landscapes and provide tools for short and long term security management [16].

Steps

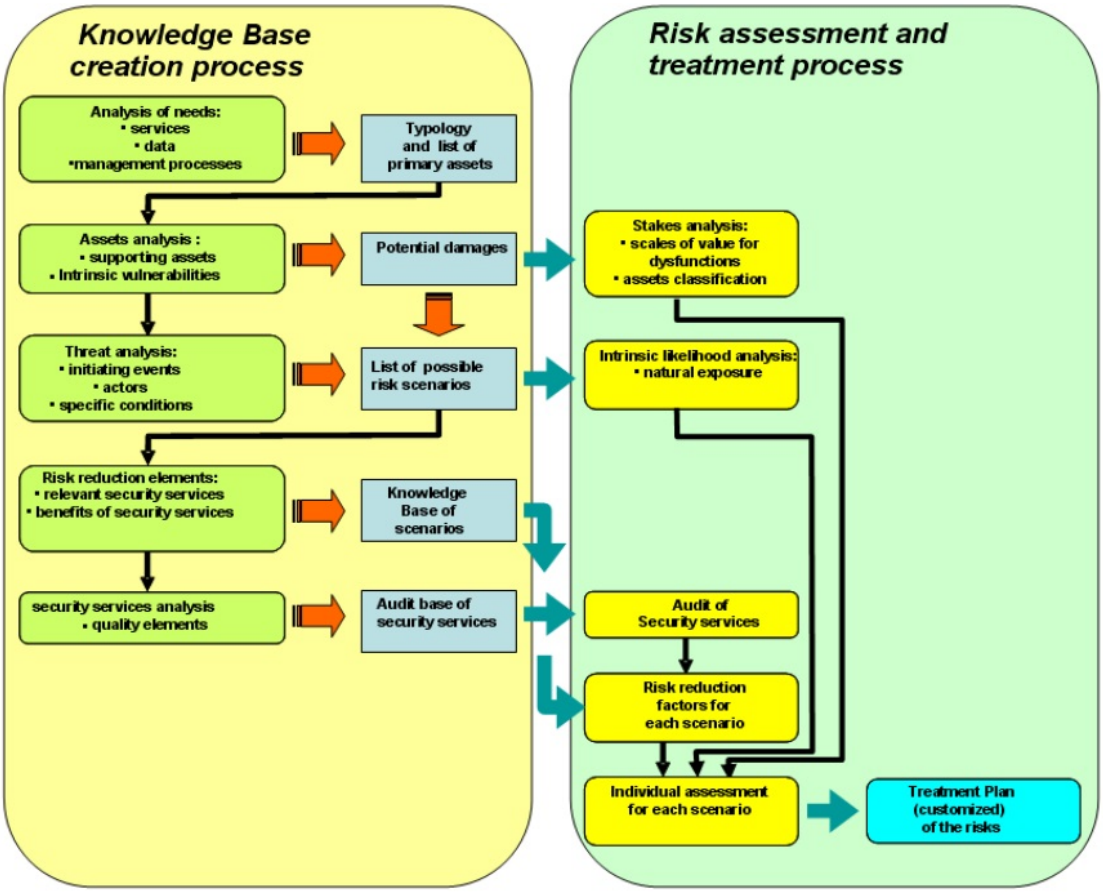
MEHARI describes a complex process, including cyclic Risk Management steps as well as the creation of a customized knowledge base. An overview of the entire process is available in figure 3.6, on page 41. After creation of the knowledge base, a separate process is started in order to analyze the risks for each individual scenario.

The actual Risk assessment process for each scenario follows the following steps, according to the description offered in [53]:

1. Identification of a risk situation (either using the knowledge base as described above or by directly, manually, identifying possible malfunctions (for faults)
2. Evaluation of natural exposure ("default" exposure from environment)
3. Evaluation of dissuasive and preventive factors
4. Evaluation of protective, palliative and recuperative factors
5. Evaluation of Potentiality (i.e. how likely the risk is)
6. Evaluation of intrinsic impact (i.e. consequences) by filling in a table
7. Evaluation of impact and impact reduction via automated computation
8. Global Risk evaluation taking into account the previous factors:
   - **Residual Likelihood** composed of the following factors:
     - Intrinsic Likelihood (from analyzing the parameters of the threat)
     - Resulting likelihood reduction (from analyzing the dissuasion and prevention capabilities of existing security measures)
   - **Residual Impact** composed of the following factors:
     - Intrinsic impact (from analyzing the consequences of each type of damage to the asset)
     - Resulting impact reduction (from analyzing the confinement and palliation capabilities of existing security measures)
9. Decision on whether risk is acceptable

Figure 3.6: The MEHARI Risk Management Process

Source: [16]



Discussion

MEHARI is designed to make use of a risk "knowledge base" in order to support semi-automated procedures for evaluating risk based on a set of input factors. These procedures are based on pre-defined formulas and parameters. This means that the method can only be used in conjunction with specially designed spreadsheets or dedicated software application [15]. The company supporting the development of MEHARI also offers a commercial software tool: RISICARE (see Section 5.3.19 for more information). A free, MS-Excel based version, called MEHARI 2010 basic tool, is also available (see Section 5.3.19 for more information).

The method supports quantitative, scenario-based analysis of risk, and the overall process is very similar to the one described in the ISO/IEC 27005 standard, further described in Section 3.4.7.

Evaluation

PROs:

- Fully compatible with all ISO Information Security standards
- Contains extensive knowledge base in Microsoft Excel format

CONs:

- Can only be used in conjunction with dedicated software or spreadsheets
- First instance of analysis requires somewhat complicated adaptation of "knowledge base"

3.4.11 OCTAVE

Name

Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE).

Origin

OCTAVE was developed within the Software Engineering Institute, part of Carnegie Mellon University (USA), by the Computer Emergency Response Team (CERT). It was initially funded by the US Department of Defense in order to address the security compliance challenges faced by the department in relation to the HIPAA[2]).

Goal

The goal of the OCTAVE suite of tools, techniques and methods is to allow "risk-based information security strategic assessment and planning" [54]. The framework consists of three OCTAVE methods, all of which rely on the same "OCTAVE criteria", but are tailored for specific application scenarios.

Steps

The main OCTAVE Risk Assessment methodology is intended for companies with 300 or more employees and consists of the following three phases and eight processes, each involving one or more workshops[34]:

Preparation involves getting senior management sponsorship, selecting the team members, defining the scope of the assessment and selecting secondary participants.

Phase 1: Build Asset-Based Threat Profiles is concerned with identifying the assets that are critical to the organization and current security mechanism in place

Process 1: Identify Senior Management Knowledge regarding important assets, perceived threats, security requirements, current security practices and organizational vulnerabilities.

Process 2: Identify Operational Area Management regarding important assets, perceived threats, security requirements, current security practices and organizational vulnerabilities.

[2]The US Health Insurance Portability and Accountability Act of 1996; The HIPAA Privacy Rule provides federal protections for individually identifiable health information held by covered entities and their business associates and gives patients an array of rights with respect to that information. The HIPAA Security Rule specifies a series of administrative, physical, and technical safeguards for covered entities and their business associates to use to assure the confidentiality, integrity, and availability of electronic protected health information.

Process 3: Identify Staff Knowledge regarding important assets, perceived threats, security requirements, current security practices and organizational vulnerabilities

Process 4: Create Threat Profiles by using the knowledge gathered in Processes 1-3. Involves selecting critical assets, refining the associated security requirements and identifying threats to those assets.

Phase 2: Identify Infrastructure Vulnerabilities is concerned with examining the information infrastructure in order to identify technological vulnerabilities that can lead to unauthorized action against critical assets.

Process 5: Identify Key Components for each critical asset and select the ones that require further evaluation

Process 6: Evaluate Selected Components and identify technology weaknesses, cross-referencing them with the critical assets and respective threat profiles.

Phase 3: Develop Security Strategy and Plans to mitigate previously identified risks to the organization's critical assets

Process 7: Conduct Risk Analysis by identifying the impact of threats to critical assets, developing criteria for evaluating these impacts and then using these criteria to evaluate the impact. The result is a risk profile for each critical asset.

Process 8: Develop Protection Strategy and Select Protection Strategy based on the findings. This step also involves obtaining management reviews and approval of the strategy and plans.

Wrap-up by complementing the protection strategy with specific implementation details and define steps for continues reviewing and improvement of the security policy.

Discussion

A survey of Information Security RA methods [9] ranked OCTAVE as the most cited such methodology.

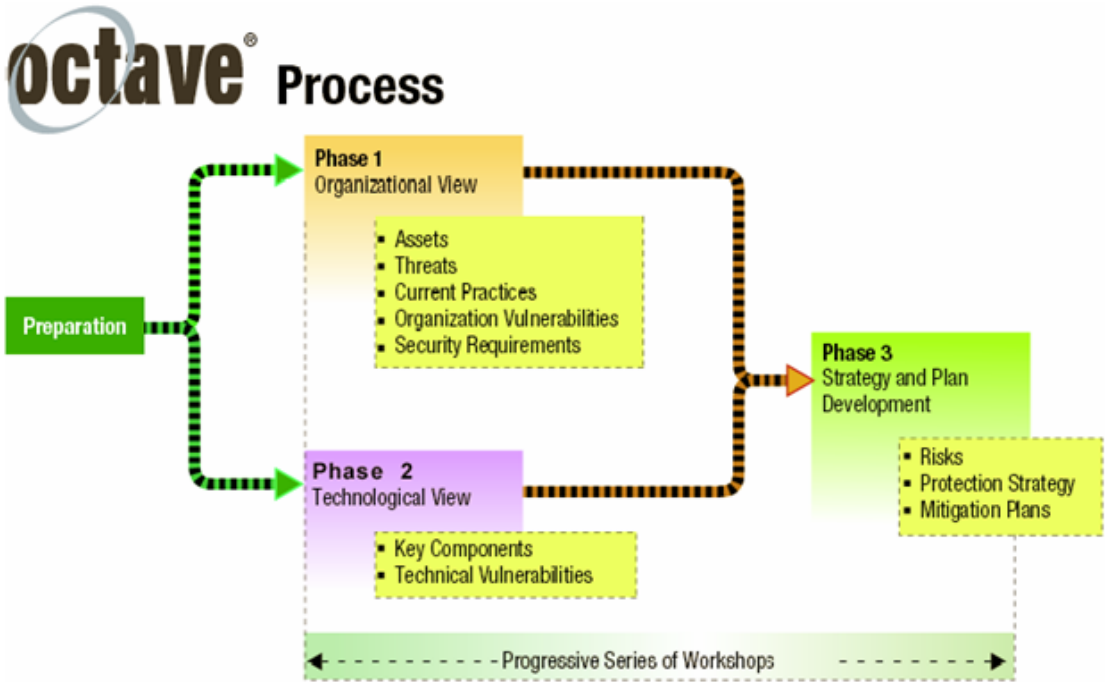
The OCTAVE methods are designed to be used by small, inter-disciplinary teams of the organization's own personnel, while also allowing use of external experts for specific activities, if necessary. [34]. The methodology describes three distinct methods:

- The main (original) OCTAVE method, described above, forms the basis for the OCTAVE body of knowledge. An overview of the method is also available in Figure 3.7
- OCTAVE-S is tailored to small and medium sized organizations (< 100 employees). Main difference is that it skips the first knowledge gathering phase and assumes such knowledge is already known by the analysis team.
- OCTAVE-Allegro offers a faster, streamlined approach that focuses on information assets. This approach covers just four simplified phases: developing risk measurement criteria, creating profiles for each critical information asset, identifying threats to these assets and finally analyze resulting risks in order to develop mitigation approaches.

All the above methods rely on a common set of criteria which specify that the assessment must be carried out by a skilled analysis team, composed of people from within the organization, that gathers input from the organization, analyzes the results and acts upon them in a structured and

Figure 3.7: The three main phases of the main OCTAVE RA method

Source: [54]



methodological manner. This process is supported by repositories of best practices (i.e. Catalog of Practices) and worksheets [58].

The original OCTAVE method is largely incompatible with frameworks that implement the traditional likelihood and consequence based risk evaluation as it assumes all possible threats will always occur. It was originally designed with defense systems in mind, which reflects in it's large body of documents (i.e. 18 volumes) as well as the multitude of worksheets and practices used for implementation. OCTAVE-S tackles most of these hurdles, making for a simplified version, with increased applicability [20].

Evaluation

PROs:

- Self-directed: can be carried out by small teams of the organization's own employees
- Flexible and context driven: contains several methods tailored for specific organizations and contexts.
- Widely used method with plenty of supporting documentation and compatible third-party tools.

CONs:

- Original OCTAVE is a heavyweight method, consisting of many volumes, worksheets and processes.

3.4.12 RiskIT

Name

Risk IT (part of the COBIT framework)

Origin

Risk IT was developed by ISACA, a non-profit professional association working on evolving the field of IT, with a focus on IT governance. It was introduced as a complement to the COBIT and Val IT frameworks in order to offer more complete IT governance guidance resources [28].

Goal

The goal of the Risk IT framework was introduced in order to fill the gap between high-level Risk Management frameworks (like AS/NZS 4360, ISO 31000) and domain-specific (e.g. security-related or project-management-related) frameworks. It aims to allow the enterprise to make appropriate risk-aware decisions by providing and end-to-end, comprehensive view of all risks related to the use of IT as well as a thorough treatment of risk management at all levels. It's goal is to enable enterprises to understand and manage all significant IT risk types and was originally designed as an educational resource for CIO's.

Steps

The "Risk Evaluation" process described in the Risk IT framework consists of three phases. It is the second phase of Risk Analysis that the actual Risk Assessment is performed, but the first and third phases are also briefly described for completeness:

1. Collect data - Identify relevant data to enable effective IT-related risk identification, analysis and reporting.
   (a) Establish and maintain a model for data collection.
   (b) Collect data on the operating environment.
   (c) Collect data on risk events.
   (d) Identify risk factors.
2. Analyze risk - Develop useful information to support risk decisions that take into account the business relevance of risk factors (i.e. Risk Assessment)
   (a) Define IT risk analysis scope: define breadth and depth of analysis
   (b) Estimate IT risk: estimate the probable frequency and probable magnitude of loss or gain associated with IT risk scenarios as influenced by applicable risk factors; consider compound scenarios and threat types; evaluate possible controls and their influence on the frequency and probable magnitude of loss and applicable risk factors; estimate residual risk levels and compare these to acceptable risk criteria
   (c) Identify risk response options: examine available range of mitigations (e.g. avoid, reduce, transfer, accept); document trade-offs; specify requirements for mitigation strategies; identify costs, benefits and responsibilities for implementation
   (d) Perform a peer review of IT risk analysis: confirm that documentation is in line with enterprise requirements; review estimates of loss/gain; verify that human factors were properly calibrated; verify that the experience level and credentials of the analysis were appropriate; extract and use peer review recommendations

3. Maintain risk profile - Maintain an up-to-date and complete inventory of known risks and attributes (e.g., expected frequency, potential impact, disposition), IT resources, capabilities and controls as understood in the context of business products, services and processes.
   (a) Map IT resources to business processes.
   (b) Determine business criticality of IT resources.
   (c) Understand IT capabilities.
   (d) Update IT risk scenario components.

Discussion

Risk IT is designed to complement COBIT, which is a generic Risk Management framework, by providing ways to identify, govern and manage IT risk. Although the framework operates mostly at a high-level of abstraction, serving as a guideline towards achieving best practices in the field of IT, not only IT security, it does describe a process for "Risk Evaluation" which can be interpreted as a Risk Assessment process. However, this "Risk Analysis" is not described at a level of granularity comparable to other dedicated methods. As such, the Risk IT framework can be rather viewed as a enterprise Risk Management framework, that can be applied to all aspects of any business IT scenario, but cannot be used as a standalone Risk Assessment methodology.

Risk IT's interpretation of Risk as frequency times probable magnitude of loss is consistent not only with the ISO 31000 conceptual model, but also with the FAIR and Open Group Taxonomies, all described in Section 4.2.

Evaluation

PROs:

- Supported by wide range of documents related to IT, and generic Risk Management, allowing easy integration with enterprise-wide Risk Management methods.
- Risk IT builds on globally recognized COBIT framework for IT governance

CONs:

- Does not describe Risk Assessment with technical detail, only gives guidelines to how such a process should be undertaken and integrated into the overall enterprise-wide RM process.
- Risk Assessment cannot be applied independently from the rest of the framework

3.4.13 Structured Risk Analysis

Name

Structured Risk Analysis (SRA).

Origin

Structured Risk Analysis was introduced by a British company, Consult Hyperion initially as an internal guideline to conducting small-scale risk assessments together with their clients.

Goal

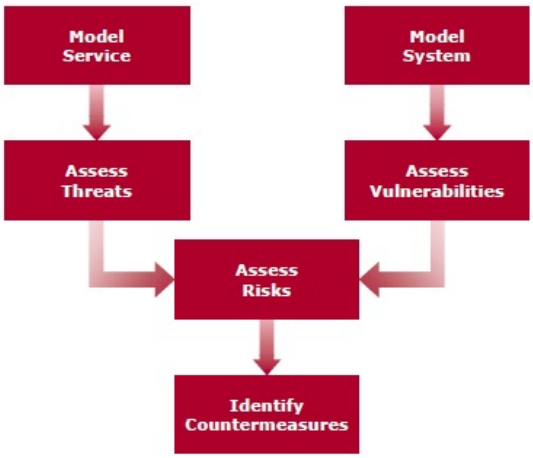
The main goal of the method is to allow on-the-spot risk assessment sessions for real or under-development systems with (financially) quantifiable output that can be used to support budget allocation decisions.

Steps

The method is made up of a small number of steps. An overview of the process can be found in Figure 3.8. In the *Model Service* step, all data entities are identified. Next, in the *Assess Threats* step for each data entity, the Damage for the customer and the Gain for an average attacker that a compromise in Confidentiality, Integrity or Availability might cause is estimated. The *Model System* step simply decomposes the physical architecture into sub-components and interfaces. The *Assess vulnerabilities* step estimated the difficulty (average cost and likelihood of capture) of an attack on each component or interface. In the *Assess risks* step, a cross-reference table is used to describe which data entities are stored, processed, or transmitted by each physical component or interface. Then, using some predefined operators, the overall risk (called Exposure) of each valid component-entity pair is automatically calculated. In the final, *Identify countermeasures* step, mitigations and treatments are manually identified for the highest risks.

Figure 3.8: The basic steps undertaken during a Structured Risk Analysis

Source: [38]



Discussion

The method is described in a [38]. As the name suggests it offers an extremely structured way of identifying and ranking risks. It's main strength comes from the fact that it uses a table-based deconstruction of the system and it's physical and digital entities. After describing this decomposition, the pre-defined table structure allows for easy identification of risks. An (expert) evaluation of each component interaction is required, but thanks to the method's pre-defined operations on the input table, the output (i.e a ranking of the most exposed risks) is easy to read and understand even by management users. This collaborative, structured way of assessing risks offers advantages in terms of speed (a complete Risk assessments can be finished in one

session), but also exhibits serious drawbacks compared to the other, more flexible methods. One such disadvantage is that the approach does not allow taking into consideration attack scenarios, but focuses on an "average attacker". A solution to this would be conducting multiple such analyses for various attacker profiles, but this still would not cover multi-step attacks (i.e attack exploiting more than one vulnerability). Furthermore, expert opinion is required for assessing the true Costs associated to each attack step. Thus, it might be necessary to re-iterate multiple times over the process described above, while taking into consideration different estimations, attacker profiles, and countermeasures.

The method defines Exposure (how serious each risk is) as a combination of other variables: taking L = Likelihood of capture, C = Cost for attacker , D = Damage to organization, G = Gain for attacker as input, calculate:

1. PNC = Probability of Not getting Caught, PNC = 1 – L
2. Pr = Profit, Pr = G – C
3. P = Probability, P = Pr x PNC
4. E = Exposure, E = D x P

Unlike most other RA methods described in this section, the SRA introduces a new way of computing risk, which is not in agreement with most higher-level Risk Management methodologies or frameworks, due to the way the concept or Risk is conceptualized. Instead, it introduces a very practical way of estimating risk based only on a hand-full of factors. This decomposition of Risk will be treated in the Section 4.2.7.

Evaluation

PROs:

- Ease of use
- Speed - full assessment can be conducted in 1 day
- Does not require dedicated tools
- Non-proprietary
- Quantitative

CONs:

- Does not take into consideration attacker profiles
- Does not take into consideration complex (multi-step) attacks
- Lacks the depth of other methodologies

3.4.14 TARA

Name

Threat Agent Risk Assessment (TARA).

Origin

TARA was introduced by the Intel Corporation in 2010 in order to tackle the problem created by the very large number of possible attacks on any given infrastructure.

Goal

The method claims to help in identifying the risks and related threat agents which could realistically succeed in actions that are most likely to cause unsatisfactory losses. Thus, the method's strong point is the prioritization of critical risks (and countermeasures) in order to maximize utilization of resources [51] and avoid over-encumbering the decision makers with every possible vulnerability.

Steps

TARA achieves it's purpose by first looking at which attack vectors or methods are more likely for the specific project/infrastructure than the "default" risks. Then this information is cross-referenced with the existing controls in order to identify exposed areas. An overview of the TARA process can be seen in Figure 3.9. More details on the steps follow:

1. Measure current threat agent risks: by using the Threat Agent Library and experts
2. Distinguish threat agents that exceed baseline acceptable risks: by using Threat Agent Library
3. Derive primary objectives of those threat agents: using Methods and Objectives library
4. Identify methods likely to manifest: using Methods and Objective library
5. Determine the most important collective exposures: using Common Exposures Library
6. Align strategy to target the most significant exposures: by using previous information to adapt security strategy and allocation of security resources.

Discussion

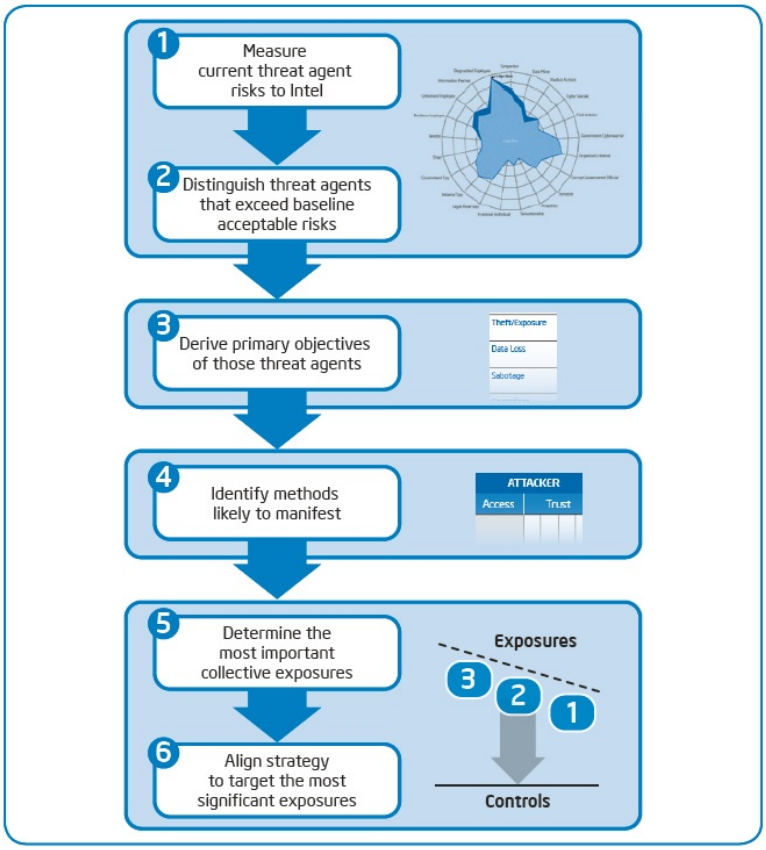
It's strong visualization techniques enable awareness dissemination amongst stakeholders, and helps reach an acceptable level of residual risk with low resources [57]. This makes it less applicable to security-critical systems, but more relevant to large enterprise scenarios, where multiple, diverse stakeholders are involved.

The method puts heavy emphasis on attacker profiles. These are defined in Intel's own *Threat Agent Library* and classified for simplicity in 22 "archetypes"'. The methodology also described how to make use of vulnerability databases, or *Common Exposure Libraries*, a number of which are available online. Finally, the method suggests using a *Methods and Objectives Library* which links the attacker profiles to common"modus operandi" and objectives.

Finally, TARA is a qualitative method and is commonly used in conjunction with other enterprise risk analysis tools, applications or processes.

Figure 3.9: The basic steps undertaken during a TARA

Source: [51]



Evaluation

PROs:

- Visualization techniques enhance awareness dissemination amongst stakeholders
- Good at distilling and prioritizing risks
- Focus on attacker profiles
- Makes good use of external libraries for up-to-date knowledge on attackers, vulnerabilities and methods

CONs:

- Not as thorough as other methods (might miss non-critical vulnerabilities)

3.5 Comparison of methods

One of the main conclusions that can be drawn from the reviews in this Chapter is that not all Risk Assessments are born equal. Besides the obvious variations in approach, scope or applica-

bility, more essential differences can be noted. Some methods are designed to be used (or usable) as stand-alone Risk Assessment methods, while others are designed to work in conjunction with more general, enterprise-wide Risk Management processes. Some describe the Risk Assessment process at a very high granularity and with technical detail, while others simply sketch high level overviews on how a Risk Assessment could be undertaken and suggest guidelines or best practices that should be taken into consideration by any such attempt. This results in an interesting conclusion: some methods can only be used in conjunction with others; others are dedicated to a certain Risk Management approach or Conceptual Model.

Most of the methods do describe the Risk Assessment process at a sufficient level of technical detail to support standalone application. Unsurprising maybe is that the methods designed as part of a standard or to comply to certain standards are the ones described at a more abstract, management oriented level. The AS/NZS 4360 and ISO/IEC 27002, 27005 are designed with Risk Management, rather than Risk Assessment in mind, and require a choice of a low-level technical method in order to support the Risk Assessment process. Furthermore the Risk IT method also requires a third-party, more technical method, in order to be successfully applied. This is because Risk IT is designed to work with COBIT, a high-level Risk Management standard. FRAP also works best in conjunction with a more technical method, but not because it is focused on Risk Management, but because it leaves it up to the key-role of the facilitator to make use of technical and RA knowledge when conducting the actual analysis. This is simply a unique feature of the FRAP approach as it does not give further indication on implementing a Risk Management process.

Furthermore, we can observe that most methods follow a process very similar to the one outlined in Section 2.3, where Risk Assessments are introduced. However, after the analyses, we can further refine the generic process to include more details. The common skeleton that most RA methodologies seem to use is the following:

1. (optional) Establishment of context
   (a) (optional) Define context, business and security requirements and the target of assessment; usually done by consulting relevant stakeholders
   (b) Identify relevant assets (including technical, digital, physical entities as well as humans and data items)
2. Risk Identification
   (a) (optional) Identify possible threats or threat agents (this is heavily dependent on the method: it can represent groups, categories by various criteria or individual threats)
   (b) Identify either individual Risks as Threat-Asset pairs or Risk Scenarios in more complex methodologies.
3. Risk Analysis
   (a) Quantify Risks such that they can be compared to each other (does not have to be on a quantitative scale).
   (b) Evaluate previously identified Risks in such a way that they can be ranked and/or prioritized with regard to the potential danger they expose the organization to.
4. Risk Evaluation
   (a) Rank and/or prioritize previously analyzed Risks based on relevant metrics.

(b) Compare Risk with certain Risk Criteria or or against the initial security requirements in order to identify areas of concern

5. Select countermeasures:

   (a) (optional) Map Risks to possible (or recommended) security controls or treatment plans

   (b) (optional) Suggest treatment plan

   (c) (optional) Underline places that require implementation of new controls based on difference between results of RA and given requirements, standards, guidelines, regulations, preferences, etc.

Chapter 4

Overview of Conceptual Models of Risk

4.1 Conceptualizing Risk

Within any Risk Assessment or Risk Management methodology, the concept or Risk occupies a central role. Variations often arise from different interpretations of this concept and what it means to an organization. Differences can also occur in the number, meaning and relationships of the factors driving risk, as well as how they can be operationalized, measured and computed in order to quantify Risk in a meaningful way.

This chapter attempts to provide an overview of some of the most common conceptualizations of Risk. The list is not exhaustive, as infinitesimal variations can result in an endless array of models, nor is it exclusive, as even the models analyzed below can be adapted, influenced or merged with one another. At the end of the chapter, an "integrated model" will be suggested that does not attempt to describe yet another conceptual model of Risk, but instead underline the entities and factors reoccurring amongst various models as well as sketch a "universal" model of Risk, that is compatible with all the ones extracted from literature.

4.2 Frameworks

In this section, a number of frameworks will be analyzed with regard to the conceptual model of Risk the introduce. Only frameworks that explicitly define and decompose Risk, as well as suggest either a taxonomy of factors or a formulas for computing Risk based on these factors are selected. The following list of frameworks were also chosen for their mutual diversity and/or relation to one or more of the methods analyzed in Chapter 3.

4.2.1 AS/NZS ISO 31000:2009

The AS/NZS ISO 31000 standard was originally launched as an attempt to promote the old AS/NZS 4360 Risk Management (discussed in Section 3.4.1) standard to an international standard. AS/NZS ISO 31000 [62] also supersedes the AS/NZS 4360:2004 by redefining risk and introducing some more general guidelines and principles applicable to (theoretically) any RM method. Furthermore, it introduced a new definition of risk, as well as the factors driving it.

To this extent, it can be considered a proper Risk Management framework, addressing all areas related to the risk management process.

Concepts

The new standard defines **Risk** itself as "the effect of uncertainty on objectives", with the following notes[62]:

- An effect is a deviation from the expected — positive and/or negative.
- Objectives can have different aspects (such as financial, health and safety, and environmental goals) and can apply at different levels (such as strategic, organization-wide, project, product and process).
- Risk is often characterized by reference to potential events (2.17) and consequences (2.18), or a combination of these.
- Risk is often expressed in terms of a combination of the consequences of an event (including changes in circumstances) and the associated likelihood (2.19) of occurrence. As such, the standard also conforms to *Class 1* approaches to Risk Management.

The AS/NZS ISO 31000:2009 standard is more focused on defining high-level concepts such as the Risk Management and Risk Assessment process, security policies and risk evaluation criteria as well as discussing the different phases involved in implementing these. The concepts are described with a management audience in mind and as such, do not go into much detail when discussing the concept of Risk iteself. While it also offers definitions for common terms used in the field or Risk Management (e.g. event, consequence, likelihood or vulnerability), it does not describe causal relationships between these concepts, nor does it suggest a decomposition or factorization of Risk. Furthermore, the standard is aimed at any Risk Management process, not necessarily one involving Information Security, making it even less relevant to our research questions. This is explainable by the fact that, from available literature, it can be concluded that the concept was designed to be compatible with (most) other Risk models and RM/RA processes. The specific factorization of Risk, as well as the taxonomy of these factors is dependent on the context-specific Conceptual Model and Risk Assessment methodlogy chosen to augment the AS/NZS 31000's general principles.

Unfortunately, the standard is also not freely available and as such, more information regarding the particualr conceptual models it is compatible with was unavailable at the time of writing.

4.2.2 FAIR

The Open Group describes FAIR as a taxonomy of the factors that contribute to risk and how they affect each other. The FAIR framework is primarily concerned with "establishing accurate probabilities for the frequency and magnitude of loss events" [23].

FAIR main document is "An Introduction to Factor Analysis of Information Risk (FAIR)"[33]. The docuement starts with a definition of Risk that is consistent with *Class 1* RA methods, as defined in section 2.3.1. That is, in order to compute risk, likelihood of the threat, the impact that the threat can have on the asset(s) as well as how vulnerable the asset is to the threat are taken into consideration. Together with a discussion regarding risk analysis at a high-level and the various interpretations of probability, it introduces the main concepts involved in Information Security. Further on, these concepts are decomposed into factors and suggestions as to how

these factors can be combines in order to estimate risk is suggested. Thus, risk is iteratively decomposed into fundamental parts. The result is a taxonomy of all possible factors that play a role in driving risk. The document also breifly discusses Controls, by dividing them across three dimensions. Finally, a discussion regarding possible challenges encountered when measuring the described factors is started.

Concepts

The FAIR framework identifies four primary components of any risk scenario: Threats, Assets, The Organization itself and The External Environment. It goes on to underline the importance of Threats and Assets. The key concepts defined in the framework are [35]:

Threat can be anything capable of acting against an *Asset* such as to cause harm. *Threat Agents* are defined as "individuals within a threat population" and can be grouped by *Threat Communities* (subsets of the overall threat agent population that share key characteristics). The framework puts heavy emphasis on defining the necessary and sufficient characteristics of such *Threat Communities*required to get an accurate estimation of the probability, nature, objective and outcome of events.

Asset is any data, device or other component supporting one or more information related-activities (such as access, misuse, disclose, modify or deny-access) such that it can result in *Loss*.

Loss can be of various forms:

Productivity: – a reduction of the organization to effectively produce goods or services in order to generate value

Response: – the resources spent while acting following an adverse event

Replacement: – the expense to substitute/repair an affected asset

Fines and judgments (F/J): – the cost of the overall legal procedure deriving from the adverse event

Competitive advantage (CA): - missed opportunities due to the security incident

Reputation: – missed opportunities or sales due to the diminishing corporate image following the event

Risk is probable frequency and probable magnitude of future loss, decomposed as follows:

Loss Event Frequency (LEF) is the probable frequency, within a given time-frame, that a threat agent will inflict harm upon an asset and can be decomposed into two factors:

Threat Event Frequency (TEF) is the probable frequency, within a given time-frame, that a threat agent will act against an asset. This is driven by two factors:

Contact is the probable frequency, within a given time-frame, that a threat agent will come into contact with an asset. Can be random, regular or intentional.

Action is the probability that a threat agent will act against an asset once contact occurs. This is influenced by the threat agent's assessment of: the *asset value*, the *level of effort* required to compromise target asset and the*probability that he might suffer negative consequences* while attempting an attack.

Vulnerability is the probability that an asset will be unable to resist the actions of a threat agent and is driven by:

Control Strength (the strength of a control as compared to a baseline measure of force)

Threat Capability (the probable level of force that a threat agent is capable of applying against an asset)

Probable Loss Magnitude (PLM) is comprised of 4 types of factors:

1. Asset Loss factors:

   Value or liability is defined as:

   - *Criticality* = the impact on the organization productivity
   - *Cost* = the cost of replacing a compromised asset
   - *Sensitivity* = the impact of disclosure of confidential information; can be of various types: Embarrassment (exposes the inappropriate behavior company management), Competitive advantage (loss of CA due to exposure), Legal/regulatory (cost of law violations) or General (other losses related to data sensitivity)

   Volume or quantity of the asset

2. Threat loss factors:

   Competence as the amount of damage threat agent is able to inflict

   Action of the Threat Agent on the Asset:

   - *Access* (read the data without proper authorization)
   - *Misuse* (use the asset without authorization and or differently form the intended usage)
   - *Disclose* (the agent let other people to access the data)
   - *Modify* (data or configuration modification)
   - *Deny* access (preventing legitimate intended users from accessing the asset)

   Internal vs. External threat agent affiliation

3. Organizational Loss Factors:

   Timing of the attack

   Due Diligence undertaken by the organization

   Response of the organization with regard to:

   - *Containment* (the ability to limit breadth and depth of an event)
   - *Remediation* (the ability to remove threat agent)
   - *Recovery* (the ability to bring things back to normal)

   Detection: of the threat in due time

4. External Loss Factors:

   Detection of the event by external entities

   Legal / Regulatory fines or judgments imposed by regulation, contract law or case law

   Competitors taking advantage of the situation

   Media reaction

   Stakeholders taking their business elsewhere

A complete overview of the decomposition of Risk as proposed by the FAIR taxonomy is visible in Figure 4.1 on page 66.

One notable difference between FAIR and most other conceptual models is that FAIR views "Vulnerability" as a probability (that the force applied by the threat exceeds the strength of

the available controls" instead of "a weakness that may be exploited". In FAIR, the weakness is defined as a "Potential Vulnerability", with the actual Vulnerability being dependent on the particular Threat and it's capabilities.

4.2.3 ISO/IEC 13335-1:2004 Concepts and models for information and communications technology security management

The standard's full title is *ISO/IEC 13335-1:2004 Information technology – Security techniques – Management of information and communications technology security – Part 1: Concepts and models for information and communications technology security management.*

According to it's abstract "ISO/IEC 13335-1:2004 presents the concepts and models fundamental to a basic understanding of ICT security, and addresses the general management issues that are essential to the successful planning, implementation and operation of ICT security. Part 2 of ISO/IEC 13335 provides operational guidance on ICT security. Together these parts can be used to help identify and manage all aspects of ICT security." [1]. In this section, however, we will focus on Part 1 as it is dedicated to discussing useful concepts and models for managing and planning IT Security. Furthermore, Part 2 as a standalone document has since been made obsolete.

Concepts

The main concepts required in any discussion about IT Security, are defined by the ISO/IEC 13335-1[1] standard as follows:

Assets are physical assets (e.g. computer hardware, communications facilities, buildings), information/data (e.g. documents, databases), software, the ability to produce some product or provide a service, people and intangibles (e.g. goodwill, image) that are considered valuable enough to warrant some degree of protection. Assets can have the following attributes: *value* and/or *sensitivity*, *safeguards*

Threats have the potential to cause an unwanted incident that may results in harm to a system or organization and it's assets. The harm can be caused by a direct or indirect attack on the information being handled by an IT system or service. Threats are classified, based on various factors:

- Depending on origin: human or environmental
- Depending on cause: deliberate or accidental
- Depending on motivation: financial, competitive advantage, etc.
- Depending on source: insider or outsider
- Depending on severity: temporary or permanent
- Depending on number of targets: one asset or many assets
- Depending on frequency of occurrence

Vulnerabilities include weaknesses in physical layout, organization, procedures, personnel, management, administration, hardware, software or information. They may be exploited by a threat in order to cause harm (either to IT system or business objectives). Not all vulnerabilities are susceptible to all threats (some vulnerabilities are only known to/exploitable by certain threats).

Impact is the consequence of an unwanted incident which affects the assets. Such consequences could be the destruction of certain assets, damage to the IT system, and loss of confidentiality, integrity, availability, non-repudiation, accountability, authenticity or reliability. Impact can be measure both quantitatively (e.g. estimating financial costs) or qualitatively (by means of ordinal scales).

Risk is the potential that a given threat will exploit vulnerabilities of an asset and thereby cause loss or damage to an organization. The methodlogy also describes *Risk Scenarios* as a description of how a particular threat or group of threats may exploit a particular vulnerability or group of vulnerabilities exposing assets to harm.

Safeguards are practices, procedures or mechanisms that may protect against a threat, reduce a vulnerability, limit the impact of an unwanted incident, detect unwanted incidents and facilitate recovery. Safeguards are responsible with performing one or more of the following functions: *prevention, deterrence, detection, limitation, correction, recovery, monitoring* and *awareness*.

Constraints set by the organization or dictated by the environment on which the organization operates. Examples: *organizational, business, financial, environmental, personnel, time, legal, technical, cultural/social*

The (causal) relationships between the concepts described above are pictured in Figure 4.2.

Risk is characterized by a combination of two factors, the probability of the unwanted incident occurring and its impact. However, no formula or indication is given as to how to estimate these values. The notion of **Residual Risk** is also discussed as the level or Risk of which a decision to accept is made. Given this decomposition, the stadard also conforms to *Class 1* approaches as described in Section 2.3.1, with Vulnerability being included in the concept of "probability".

It should be noted that these formulas allow the method to be applied both to a quantitative and to a qualitative analysis. The only difference being that in order to compute qualitative values, cross-reference tables should be pre-defined for each of the operations.

4.2.4 Microsoft Threat Model

The Microsoft Threat Modeling[32] process does not qualify as a full-fledged Risk Management or even Risk Assessment framework due to the fact that is does not offer managers output relevant for making decisions regarding the security budget nor does it take into consideration organizational or business factors. The framework does describe a simplified process for "threat modeling" at a technical level, mostly aimed at web developers.

Furthermore, the methodology also describes multiple taxonomies of factors driving Information Security Risk which is in theory applicable to Information Systems as well as distributed software applications. This, together with the definitions of key Information Security concepts, make it interesting with regard to our scope by offering yet another, more technical point of view on how to understand, conceptualize, decompose and compute IT Risk.

Concepts

Microsoft defines the following key concepts:

Asset A resource of value, such as the data in a database or on the file system. A system resource.

Threat A potential occurrence, malicious or otherwise, that might damage or compromise your assets.

Vulnerability A weakness in some aspect or feature of a system that makes a threat possible. Vulnerabilities might exist at the network, host, or application levels.

Attack/Exploit An action taken by someone or something that harms an asset. This could be someone following through on a threat or exploiting a vulnerability.

Countermeasure A safeguard that addresses a threat and mitigates risk.

The process makes use of two methodologies for characterizing and evaluating threats that implicitly introduce a conceptual model that is not only applicable to threats, but can be used when discussing Information Risk in any context [32]:

STRIDE is a classification scheme for identifying and categorizing threats based on the type of attack and the motivation of the attacker:

S poofing identity

T ampering with data

R epudiation is the ability of users to deny specific actions or transactions

I nformation disclosure

D denial of service

E scalation of privileges

DREAD is a classification scheme for computing risk associated with each threat based on the formula $Risk = (D + R + E + A + D)/5$, where:

D = Damage Potential or "How great will the damage be in case of a successful attack?

R = Reproducibility or "How easy is it to reproduce the attack?"

E = Exploit-ability or "How easy is it to launch an attack?"

A = Affected users or "How many users are affected?"

D = Discover-ability or "How easy is it to find the vulnerability?"

are evaluated on a ordinal scale (either 1-to-10 or low-medium-high). The calculation can also be extended by including optional factors like *Reputation*.

The DREAD risk computation methodology is consistent with the traditional (*Class 1*) approach to Risk evaluation. This is not immediatly obvious due to the naming of the factors. However, we could interpret Damage Potential and Affected users as metrics of the Impact. The Discover-ability of the vunerability and the Reproductibility of attack directly influence the Likelihood of such an attack taking place. Finally, the Exploitability (i.e. "how easy is it to eploit the vulnerability?") can be translated into the actual Vulnerability level.

4.2.5 OWASP Risk Rating Methodology

OWASP stands for The Open Web Application Security Project, and is a non-profit community comprised of private organizations, educational institutions and private individuals aiming at developing at improving the security of software. Same as the Microsoft Threat Modeling process, the OWASP approach is mostly geared towards software products and less towards Information

Systems and enterprise-wide security. However, the framework does describe a decomposition of Risk into driving factors as well as describe a method for computing Risk in their OWASP Risk Rating Methodology [19]. The decomposition is, in theory, applicable to a Information System as well as complex software applications.

Concepts

OWASP defines the following key concepts:

Asset A resource of value, such as the data in a database or on the file system. A system resource.

Threat Agent is used to indicate an individual or group that can manifest a threat. Each threat Agent is defined by its Capabilities, Intentions and Past Activities and can be classified into a group

Vulnerability is a hole or a weakness, which can be a design flaw or an implementation bug, that allows an attacker to cause harm to the stakeholders of an application

Attack is the techniques that attackers use to exploit the vulnerabilities

Countermeasure are defensive technologies or modules that are used to detect, deter, or deny attacks.

The OWASP methodology follows a traditional conceptualization of Risk as Likelihood X Impact and suggests the following decomposition of Risk, also described in Figure 4.3:

Likelihood is determined by:

- Threat Agent Factors

  Skill level of the Threat Agent

  Motive is influenced by the reward the Threat Agent is hoping to receive

  Opportunity reflects the amount of resources required for the Threat Agent to succeed in the Attack

  Size of the group of Threat Agents seeking similar goals w.r.t the system

- Vulnerability Factors

  Ease of discovery or how easy is it to discover a certain vulnerability

  Ease of exploit or how easy is it to successfully exploit a certain vulnerability

  Awareness or how well known is a particular vulnerability to this group of threat agents

  Intrusion detection or how likely is it to detect attack attempts

Impact is determined by:

- Technical Impact Factors

  Loss of confidentiality

  Loss of integrity

  Loss of availability

  Loss of accountability

- Business Impact Factors

Financial damage
Reputation damage
Non-compliance damage
Privacy violation

While the methodology suggests the above factors, it is also very clear on the fact that particular organizations might wish to augment the pre-defined set of factors by adding ones that are important to the organization. Furthermore, weights can be applied to each factor based on the significance it carries for the particular business model.

It is also obvious that this methodology also employs a Likelihood X Impact approach, consistent with *Class 1* methods, with Vulnerability again being viewed as a factor of Likelihood.

4.2.6 The Open Group Risk Taxonomy

The Open Group is a technology-neutral consortium, comprised of hundreds of organizations (both private and governmental) that "enables achievement of business objectives through IT standards" by striving to create what they call Boundary-less Information Flow ™. More specifically, the group works with members from all sectors of IT (customers, suppliers, regulators, standards bodies, vendors, consultants and even academia) in order to facilitate interoperability, promote open source technologies, share best practices and last but not least, promote practical, industry-wide standards and certifications.

In 2009, The Open Group introduced their own definitions and taxonomy for Information Security Risk. These are closely related to the FAIR framework (described above in Section 4.2.2): Risk Management Insight, the developers of FAIR, are members of The Open Group's Security Forum. As such, FAIR was used as the foundation for the development of the new Open Group Standard. Due to this, The Open Group Risk Taxonomy [23] cannot be considered and alternative to the FAIR taxonomy, but simply an extension.

By developing the standard, The Open Group hopes to increase consistency amongst researchers and practitioners regarding the nomenclature involved in Information Systems Risk Management, as well as promote a standardized decomposition of the factors driving risk in such systems and the relationships between them.

Concepts

The following main concepts are identified in the taxonomy [23]:

Risk The probable frequency and probable magnitude of future loss.

Threat Anything that is capable of acting in a manner resulting in harm to an asset and/or organization; for example, acts of God (weather, geological events, etc.), malicious actors, errors, failures.

Vulnerability The probability that threat capability exceeds the ability to resist the threat.

Asset Any data, device, or other component of the environment that supports information-related activities, which can be illicitly accessed, used, disclosed, altered, destroyed, and/or stolen, resulting in loss.

As it should be obvious from the above definitions, the Open Group taxonomy is fully consistent with the one introduced by FAIR and thus also a *Class 1* approach. As for the factorization of Risk, The Open Group also adopts the same one used in FAIR, as described in Section 4.2.2,

and decomposed in Figure 4.1. As a matter of fact, The Open Group Risk Taxonomy[23] is almost word-by-word identical with Risk Management Insight's "An introduction to Factor Analysis of Information Risk (FAIR)". In conclusions, the Open Group taxonomy and conceptualization of Risk is the same as FAIR's, with the Open Group's document simply aiming at increasing awareness and promoting usage of the FAIR framework.

4.2.7 Structured Risk Analysis

Structured Risk Analysis is mainly a Risk Assessment methodology introduced by Consult Hyperion, a British company. The RA process is described and analyzed in Section 3.4.13. In this section we will look at the way Risk is conceptualized and decomposed, according to the methodology.

Although the Structure Risk Analysis does not constitute a full-fledged Risk Management framework, we are including it here due to the rather unique the concept or Risk is explained, factorized and computed.

In [38], the methodologies main document, several mathematical equations are given that together can be used to estimate risk. For each risk (interpreted as a {physical entity , digital asset} tuple), the Exposure is computed on three dimensions: Confidentiality, Integrity and Availability. Exposure represents the risk level and can be expressed on a ordinal scale or numeral scale.The formula used is:

$E = D * ((G - C) * (1 - L))$

where $L =$ **Likelihood of capture**, $C =$ **Cost** for attacker , $D =$ **Damage** to organization, $G =$ **Gain** for attacker.

Gain for attacker minus Cost for attacker $(G - C)$ is interpreted as **Profit** for attacker (Pr), while the opposite of Likelihood of Capture $(1 - L)$ is interpreted as **Probability of Not Getting Caught** (PNC), which gives us the following simplified formula:

$E = D * Pr * PNC$

Profit and Probability of Not Getting Caught are further grouped together as **Probability** (P) of attack, which leads to the most simplified version of the formula:

$E = D * P$

This final formula closely resembles *Class 1* approaches to Risk Management, as described in Section 2.3.1, with the estimation of Vulnerability being implicitly assumed to be part of the "Probability" value.

4.3 Commonalities and differences

In this section, concepts that are common or similar throughout most of the reviewed methodologies will be identified. In order to achieve this, a basic model will be designed based on the key concepts that reappear and on the large variety of variables used within the frameworks. Variations in naming as well as the presence or lack of certain variables will be identified and discussed.

4.3.1 Integrated Conceptual Model

Across all the frameworks discussed in this Chapter, there are a few fundamental concepts that are reoccurring. All RA/RM frameworks seem to include the concepts of a Threat (be-it an agent/attacker, an environmental factor, or simply something that can go wrong), Asset (as a possible target for attacks, that provides value either for the organization or attackers), Vulnerability (as either as missing controls, a weakness of the system or an attack path) and

of course the actual Attack (which is often results from a combination of the previous three). These entities, as well as a clear and consistent understanding of how they are defined, appears to be required for any Security evaluation or discussion. Despite the fact that various frameworks adopt different naming or different causal relationships and computation methods, as well as introduce a number of unique factors, "integrated" model can be sketched that relates all these concepts and factors. The diagram in Figure 4.5 maps the entities, attributes and relationships found in the various decompositions and conceptualizations of Risk. We call this an integrated model due to the fact that it it contains a union of the attributes assigned by each framework to these core entities.

As all the above models take a Likelihood X Impact approach, the integrated model will obviously also be consistent with such a decomposition of Risk. Furthermore, most methodologies choose to include the influence of the Vulnerability into the estimation of Likelihood, thus slightly changing it's meaning from "likelihood that an attack is attempted" to "likelihood that an attack succeeds". Thus, if in the integrated model we also assume Vulnerability to be an intrinsic factor determining the Likelihood and/or Impact level, then this integrated model can be considered an *Class 1* approach, as described in Section 2.3.1. These core entities and the relationships between them, as well as possible attributes and their commonality are shown in Figure 4.5.

Threat is the entity that initiates the attack (it can be a human, a computer, a process or a collection of these). Furthermore, it can also include environmental factors, or natural events, and it is to accommodate such variations that the purposefully ambiguous term of Threat is used, instead of the more common "Threat Agent".

- Each Threat has a *profile* which describes it's distinctive features that are relevant for the RA and can be used to group multiple attackers or threats together into categories.
- A threat can also either be *external or internal* (outsider or insider) to the organization. The distinction of course varies depending on the type of organization and it can become blurry in certain situations, but most methodologies offer some indication as to how this can be established.

Asset is what the Threat aims at compromising. It can be either a digital or physical entity.

- it's often the case that the compromise of an asset can have a certain negative impact on the organization (depending on it's *valueForOrg*), while offering a different positive reward to the attacker (i.e. threat). As this value is dependent on the particular Threat , it is modeled as an (optional) relationship between each Threat and each Asset: *ExpectedGain*.
- Some methodologies differentiate between critical and non-critical assets.

Vulnerability is regarded by most methodologies as a weakness in the system. It can be a flaw in the design, implementation, maintenance of a system, but can also be related to the security policy or even business model.

- Most methodologies quantify the effect or severity of the Vulnerability into a Vulnerability *level*

Attack is the actual information-related activity in which the Threat attempts to compromise and Asset. It can be viewed as an association entity between a Threat, a Vulnerability and an Asset.

- It is usually classified into multiple *Types* by various methodologies (see 6th row in Table 4.1). There are also "multi-step attacks" possible, comprised of multiple Attacks, each with it's own attributes.
- Another variable usually associated with this entity are the *Threat Capability* (sometimes referred to as TCap) which reflects the skills and resources that the Threat has available for each Attack. It is sometimes regarded as a variable of the Threat, but given the fact that, for example, a Threat can have different skills for different attackTypes, I believe it is unique to each attack.
- Most taxonomies usually discuss the *Defense Strength* which is usually related to the existing controls and security policy. The same discussion applies here: while it may be intuitive to see Defense Strength as an attribute of the Asset, I chose to model it as an attribute of Attack as each Asset can have different security controls against various attack vectors and threats or multiple controls that mitigate different vulnerabilities.
- The *Frequency* of the attack usually refers to the number of attacks estimated to be attempted by the Threat in a given time-frame.
- The *Loss Type* and *Loss Magnitude* are variables usually included in the estimation of the impact or consequences that a successful attack might have on an organization and are present in all reviewed Risk taxonomies. They are also attributes of the Attack entity as the amount and type of damage that a compromise of a certain asset can bring about is dependent on the type of attack and the goals of the threat. For example, an attacker (i.e. threat) reading some private employee accounts in order to send them spam has a considerably lower impact than a hacker who launches a Denial of Service against the same records causing employees to lose access to their accounts and leading to significant drops in productivity and maybe even reputation.

An attack may exploit one or more vulnerabilities (e.g. SQL injection and Cross-Site-Scripting), but it also possible for attacks to be carried out without any knowledge of particular vulnerabilities (e.g. port scan). A threat can initiate one or more identical attacks (either simultaniously - e.g. DDoS - or in sequencially - e.g. brute force -). Furthermore a single attack can target multiple assets (such as multiple servers) and can in be one step in a complex attack. A vulnerability can affect one (e.g. weak password) or more assets (e.g. badly configured office firewall), while an asset can also be exposed by multiple vulnerabilities (e.g. weak account password + weak firewall).

4.3.2 Variations

Given the model described in the previous section, a number or taxonomic variations can be identified when comparing the reviewed Conceptual Models against it. The variations in naming and grouping of the core concepts identified as described above are shown in Table 4.1 on page 71. Due to the limited information available on the AS/NZS 31000 standard, it is omitted from this Table.

The frameworks also differ in the way they group the attributes into intermediary factors as well as in the way the use these factors to compute Risk. These differences are obvious in the descriptions and decompositions of Risk given in the dedicated sections above so they will not be treated here.

If we would attempt to distill a "core" model, consisting only of the common concepts and factors present in all discussed models (an intersection instead of a union), we would end up with only two entities: asset and threat. These are the core entities that any discussion regarding Information Security and/or Risk must address, no matter the level of granularity or

technicality. While this may appear to be obvious, it also reveals the fact that even amongst conceptual models designed to tackle the singular notion of Information Security Risk, there are significant variations. These stem not only from differences in taxonomy but can be traced down to completely different conceptualizations of Risk. While this might seem surprising, it becomes understandable if we go back to the context these models were developed in and the purpose they were developed for.

Discussion on variations

From Table 4.1 we can see that the most complete model seems to be FAIR. This is because they take intro consideration a very large number of factors. The only missing attribute is the criticality of the asset. However, this seems to be typical for general-purpose, enterprise-wide Risk Models. On the contrary, only models designed for Security Critical systems take this factor into consideration, as in that case we are not interested in achieving an overview of the Risk the organization Information Systems are facing and achieving "good enough" security, but rather in securing such critical aspects and demonstrating "as good as possible" protection.

The ISO 13335 framework also discusses similar factors, except for the Attack Cost. This seems to be ignored, as the framework is only concerned with the frequency of attacks and assumes the strength of existing controls directly influences the attack cost. This cost is then reflected back into the frequency of attack. Furthermore, threat capability is not explicitly defined, but rather implicitly assumed in the classification of Threats into groups. Each group is then defined, amongst other this, by their resources. Thus, we need not estimate specific, possibly unknown attributes of the attacker, as long as we know what impact these attributes have on the frequency and severity of attacks.

As we go on towards models designed to be used in lower-level assessments, we can see that organizational factors like asset value, and external vs. internal threat nature are ignored. The focus lies on the possible actions, and their potential consequences. SRA, as well as the Microsoft Threat Model and the OWASP methodology are also not concerned with scenarios and attacker profiles. They do not take into consideration multi-step attacks and mostly ignore factors related to the threat. They are mostly concerned with the intrinsic technical vulnerabilities and risks associated with the object of study.

As such, it becomes obvious that the most complete models, like FAIR, The Open Group taxonomy and ISO are suitable for scenarios where business factors are relevant for the Risk Assessment and the output is mostly aimed at management or meant to be useful for the organization wide Risk Management process. As such, these models are compatible with most of the Risk Assessment methods described in Section 3. Microsoft Threat Model and OWASP Risk rating methodology, as expected, are easier to apply due to the lower number of factors that require estimation, but also provide output less relevant for making security decisions. This makes them less relevant to enterprise-wide Risk Management processes. SRA is somewhere in the middle, providing limited support for decisions regarding Security Investments, while also supporting low-level technical discussions regarding individual components. However, this makes it compatible only with the dedicated Risk Assessment method, described in Section 3.4.13 and applicable to a restricted number of scenarios.

Figure 4.1: Decomposition of Risk according to the FAIR framework[35] and The Open Group taxonomy[23]

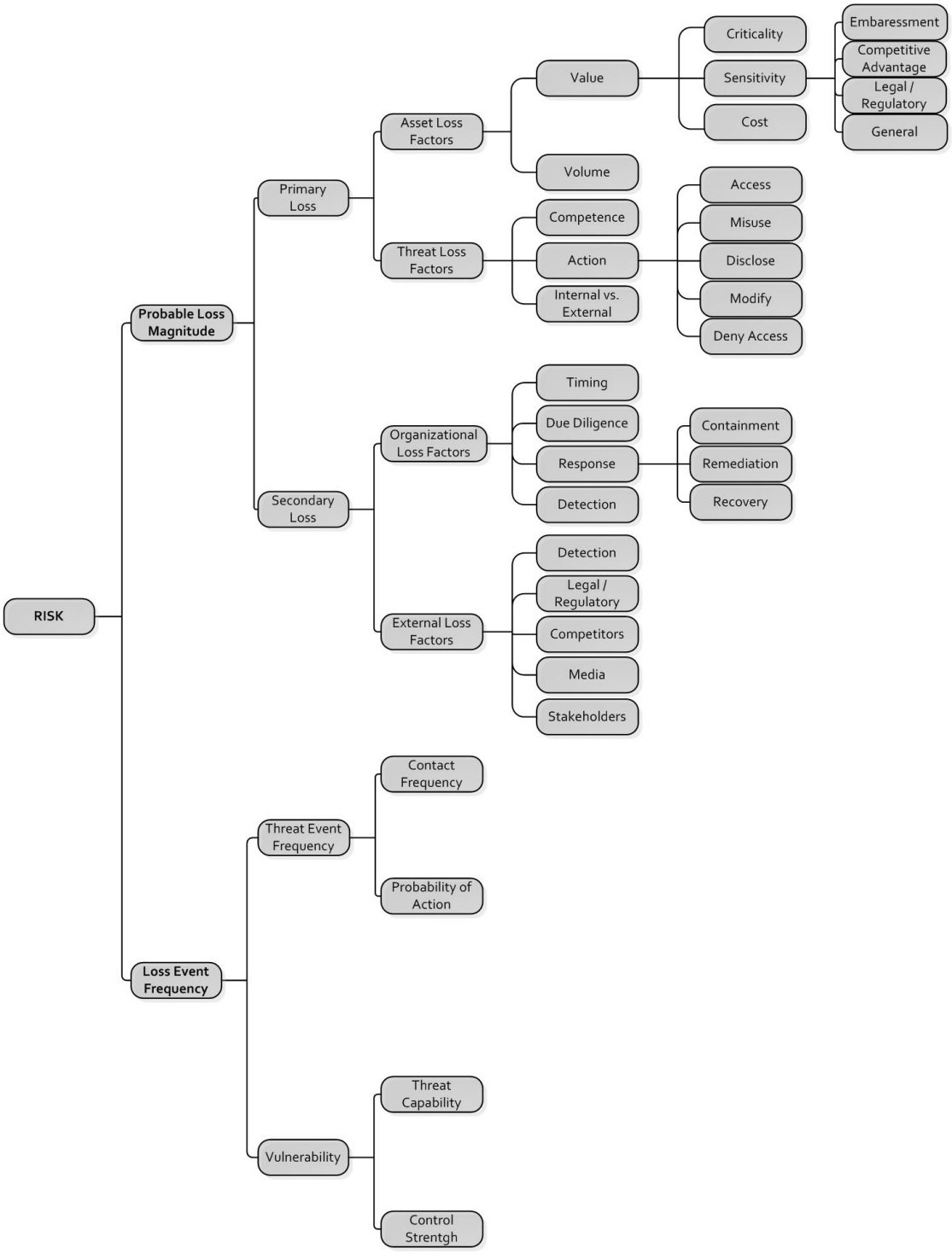


Figure 4.2: Relationships between the entities involved in RM/RA according to ISO/IEC 13335-1

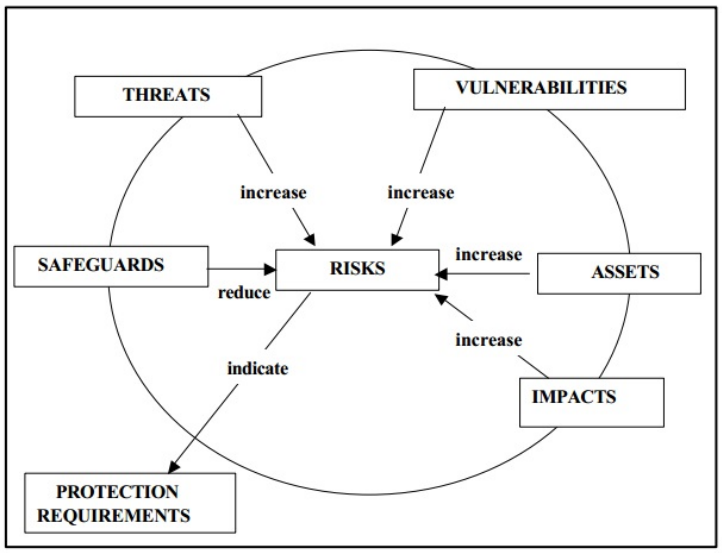


Figure 4.3: Decomposition of Risk level (Exposure) according to the OWASP [19] methodology

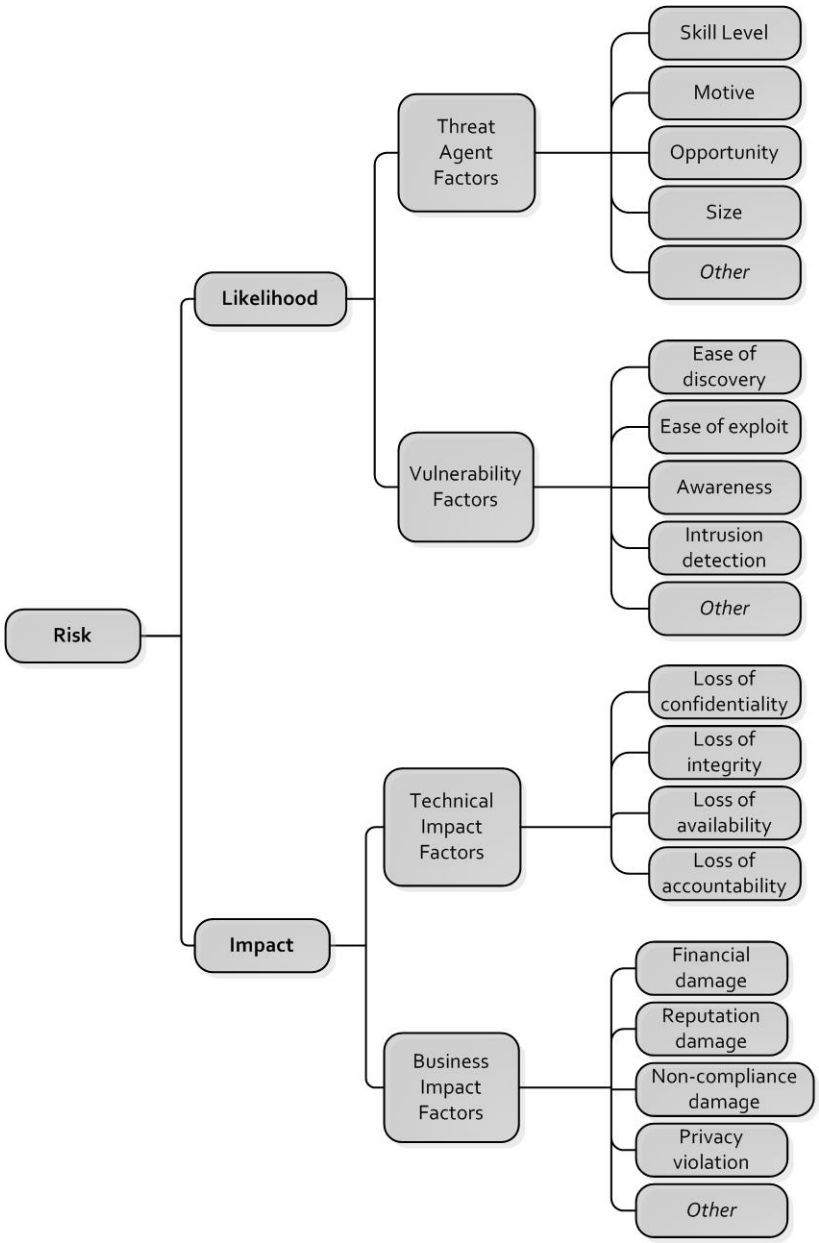


Figure 4.4: Decomposition of Risk level (Exposure) according to the SRA[38] methodology

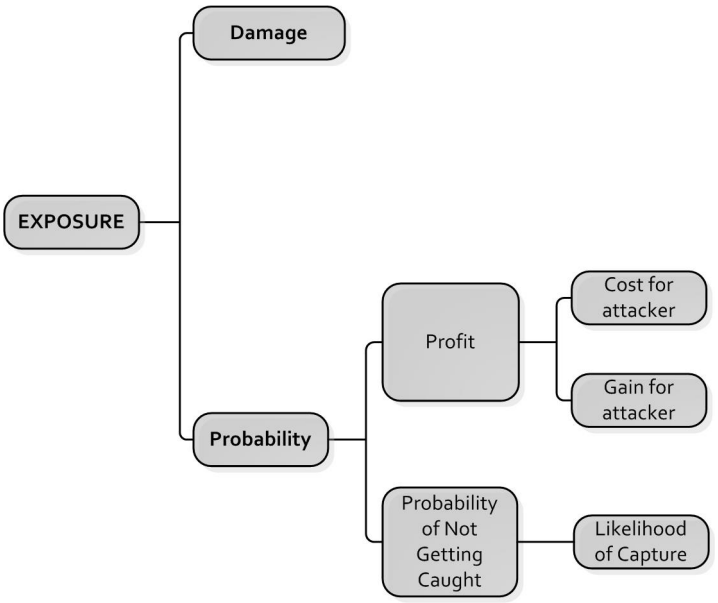
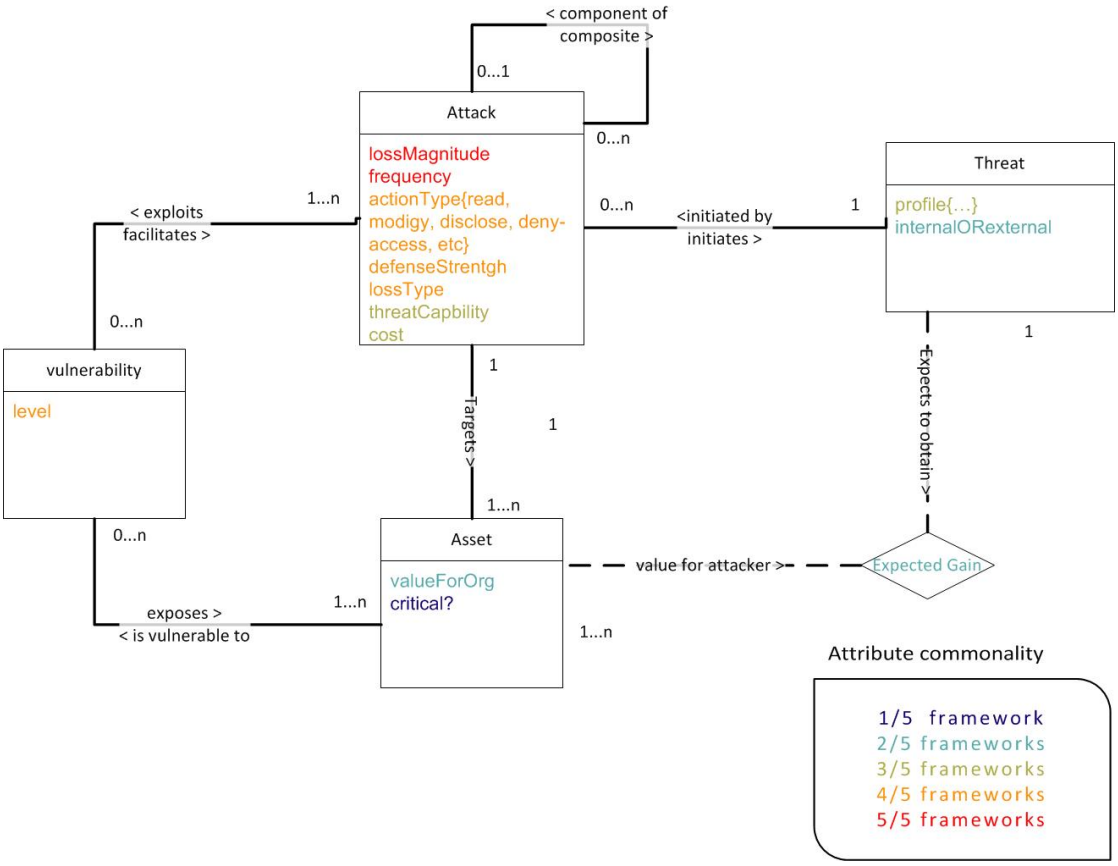


Figure 4.5: The basic entities commonly found in Information Security Conceptual Models



Integrated Model	**FAIR & Open Group**	**ISO 13335-1**	**SRA**	**Microsoft Threat Model**	**OWASP Risk Rating Methodology**
Threat	Threat Agent	Threat Agent	Attacker	N/A	Treat Agent
Threat.internalORexternal	Threat Loss Factors: internal vs. external	Threat: source	N/A	N/A	N/A
Threat.profile	Threat Community	Threat: group	N/A	N/A	Threat Agent Factors
Attack	Threat Event	Attack	Attack	Threat	Attack
Attack.actionType	Threat Loss Factors: action type	threat: numberOfAssets + threat.Severity	Attack: ThreatType {confidentiality, integrity, availability}	Threat.STRIDE{spoofing, tampering, repudiation, disclosure, DoS, elevationOfPrivilege}	Attack
Attack.threatCapability	Vulnerability: TCap	N/A	N/A	N/A	Threat Agent Skill Level + Opportunity + Size
Attack.defenseStrentgh	Vulnerability: DefenseStrentgh	Asset: Safeguards	Likelihood of Capture	N/A	Intrusion Detection
Attack.frequency	Threat Event Frequency	Threat: frequency	Attack.Probability	Reproductibility + Discover-ability	Likelihood
Attack.lossType	Loss form	Impact: consequences	Vulnerability: Type {Confidentiality, Integrity, Availability}	N/A	Technical Impact + Business Impact
Attack.lossMagnitude	Probable Loss magnitude	Impact	Damage	DamagePotential + Affected users	Impact
Attack.cost	Asset: level of effort	N/A	Cost of attack	N/A	Opportunity
Asset	Asset	Asset	Information entity	Asset	Asset
Asset.valueforOrg	Asset Loss Factors: Value	Asset: value	N/A	N/A	N/A
Asset.critical?	N/A	Asset: sensitivity	N/A	N/A	N/A
Expected gain	Asset value	Threat: motivation	Gain	N/A	Threat Agent Motive
Vulnerability	Vulnerability	Vulnerability	Vulnerability	Vulnerability	Vulnerability
Vulnerability.level	TCap - Control Strentgh	N/A	1 - Cost of attack	Exploitability	Vulnerability Factors

Table 4.1: Naming variations between Information Security Conceptual Models

4.3.3 Relationship between RA classes and the integrated model

In Section 2.3.1, a classification of RA methodologies was suggested. Next, a short comparison of each Class, and the integrated conceptual model will follow:

Class 1 approaches discuss concepts similar to the ones used in the integrated model. In order to assess Risk, they are concerned with estimating:

- $Likelihood(Threat)$ of a Threat engaging in an attack. This is represented by the attribute Attack.frequency and also influenced by the attributes of the Threat entity as well as the Expected Gain in the integrated model.
- $Vulnerability(Threat, Asset)$ by combining the attributes: Vulnerability.level and Attack.defenseStrentgh, Attack.threatCapability and Attack.cost as described in the integrated model
- $Impact(Threat, Asset)$ which corresponds to the Attack.lossMagnitude, Attack.actionType and Attack.lossType and Asset.valueforOrg attributes in the integrated model.

Class 2 approaches estimate Risk based on pre-defined Requirements. Such an entity is not present in the conceptual model. Furthermore, these types of approaches do not take any sort of Likelihood into consideration, making them significantly different from the integrated model

Class 3 approaches use a purely financial interpretation of Risk. As such, it mostly uses different attributes than the ones present in the integrated model. They only focus on one Attack.lossType, which is financial loss, and quantify Attack.lossMagnitude in monetary terms. Likelihood is also interpreted slightly different here: it is the average number of times that the given attack will succeed in the course of one year, not taking into account the factors that drive this number.

Class 4 approaches put heavy emphasis on the Asset. It is in these approaches that the Asset.critical? attribute becomes crucial, as the risk assessment is only conducted for assets which are considered to be critical. On the other hand, Attack.frequency, Attack.cost, Attack.threatCapability and Expected gain are ignored. The $Vulnerability(CriticalAsset)$ is used in the same way as the Vulnerability entity in the integrated model. The $Impact(Threat, CriticalAsset)$ thus corresponds to the Attack.lossMagnitude, Attack.actionType and Attack.lossType attributes from the integrated model.

Class 5 approaches use a factorization similar to the one in the conceptual model. The key difference here is that the Threat entity is ignored, together with its attributes, as well as the attributed dependent on it like Attack.threatCapability, Attack.cost, Attack.Defense Strength and Expected Gain

Although some methods described in Chapter 3 fall into different classes, mostly based on their scope and intended purpose, it does not seem to be the case with the conceptual models presented in this chapter. It is obvious these models most closely match the "Class 1" interpretation of Risk. Although some of the conceptual models include the influence of Vulnerability into the estimation of Likelihood, thus slightly altering it's meaning from "likelihood that an attack is attempted" to "likelihood that an attack succeeds", they still take into consideration the same factors as described in the definition of Class 1 approaches. We can thus conclude that the Class 1 interpretation of risk is the most common way Risk is computed in Information Security conceptual models.

Chapter 5

Index of Tools

5.1 Selection criteria

Similar criteria as applied to the methods will be applied here in order to trim the selection of tools. The criteria for tools are derived from the criteria used for the selection of methods. A further exclusion criteria was added to exclude tools that are not compatible with any of the methods analyzed in Section 3.4.

- **Inclusion criteria**:

  (I-1) Tool takes as input an existing system or a design of a new system

  (I-2) Intended users or beneficiaries are chief security officers or other management able to make decisions regarding (security) budget

  (I-3) Sufficient documentation available in English

- **Exclusion criteria**:

  (E-1) Tool is aimed at certification

  (E-2) Complete documentation not available in English

  (E-3) Tool is not compatible with any of the previously selected methods

  (E-4) Tools is discontinued or no longer supported

5.2 Initial list

Using the Inclusion Criteria, an initial list of currently available Risk Management and Risk Assessment software tools was created. In order to identify as many potentially relevant tools as possible, several resources were used: the ENISA inventory of RA/RM tools ([42]), literature describing or comparing various such tools ([11], [56], [34]) and various practitioners and researchers involved in the TREsPASS project.

To this initial list, the Exclusion Criteria described earlier were systematically applied in order to remove tools irrelevant to the topic and scope of this thesis. This initial list of identified methods, as well applicable Exclusion Criteria is available in Table 5.1. An explanation of the exclusions follows.

ASSET is dedicated to the NIST methods, which have been excluded from the list of reviewed methods. Casis is no longer available. COBRA was under re-development at the time of writing

and as such, relevant documentation was not available either. The ISAMM toolkit is built to work with the ISAMM methods, while MIGRA tool is designed for the MIGRA methodology. Both methods have been explicitly excluded from the in-depth analysis in Chapter 3. The OCTAVE Automated Tool is no longer available. AEXIS, the company selling RA2 no longer exists. RealISMS is designed explicitly to achieve and show compliance with the ISO/IEC 27001 standard. Resolver Risk has been made obsolete by the developer and it's features integrated into other, more comprehensive products that unfortunately are beyond this work's scope. Secu-Max, ISMS Tool Box and EISA-project are only available in German.

After applying the Exclusion criteria, we are left with 25 tools, which will al be described in more detail in the following section.

5.3 Description of tools

In this section, the tools conforming to the above Criteria will be described in more detail. Due to the fact that most tools require a (paid) license, actual testing of the entire set of relevant tools was not possible. As such, in order to identify relevant information, other resources were used. These resources include: scientific literature and reports (like [30]s, [56]), product documentation and user guides (like [36]), marketing material and presentations, third-party reviews and comparisons (like [11], [34]) and training materials .

The descriptions are taken mostly from ENISA's Inventory of Risk Assessment and Risk Management tools ([42]). Each description is accompanied by an indication as to which Risk Assessment and Risk management phases the tools are relevant to. Furthermore, the main features and functions are listed, as presented by the developers and suppliers. Compatibility with previously described methods and conceptual models is also mentioned. This compatibility, as well as the intended user group, is usually not explicitly described in product documentation, so it is sometimes derived by the author after going through product descriptions. Finally, the price is estimated in Euro, and a link is provided for the download or purchase website.

5.3.1 Acuity Stream

Description

STREAM is a comprehensive, highly configurable yet simple-to-use software product which automates the complex processes involved in managing compliance with standards and delivering effective risk management. STREAM is a multi-concurrent user, role based software tool, with a central database, used in real-time by risk managers, risk analysts, business stakeholders, control owners, and internal auditors. It is also available as a single user tool for smaller organizations and consultants. STREAM provides valuable and meaningful information for senior managers, on the status of compliance across the business with key control standards, and on the level of residual risk measured in relation to defined business appetites. It genuinely integrates compliance with risk management in a business context. It achieves this through an innovative yet simple and logical approach that is easily understood and explained. The meaningful dashboards are supplemented by a set of graphical barometers, charts and gauges, which provide clear visibility of the essential compliance and residual risk summary data. [42]

RM phases supported

1. Risk Assessment:
   (a) Risk Identification: Yes

Tool	Applicable exclusion criteria
Acuity Stream	
ASSET	E-3
Callio secura 17799	
Casis	E-4
CCS Risk Manager	
COBRA	E-2, E-4
CORAS Tool	
Countermeasures	
CRAMM	
EAR/PILAR	
Ebios tool	
EISA-Project	E-2
FAIRlite	
FAIRiq	
GSTool	
GxSGSI	
HiScout GRC Suite	
ISAMM	E-3
ISMS Tool Box	E-2
Secu-Max	E-2, E-4
Mehari 2010 basic tool	
MIGRA	E-3
Modulo Risk Manager	
MSAT	
OCTAVE Automated Tool	E-4
RA2	E-4
RealISMS	E-1
Resolver Ballot	
Resolver Risk	E-4
Risicare	
Riskwatch	
RM Studio	
SAVe	
SISMS	E-2
verinice	
vsRisk	
TRICK light	

Table 5.1: Initial list of tools and applicable exclusion criteria

(b) Risk Analysis: Yes (based on C/I/A or other custom impact)

(c) Risk Evaluation: Yes

2. Risk treatment: Yes (automatic selection of key controls and metrics for each risk)
3. Risk communication: Yes (via various reports, exports and dashboards)

Functionality

- Flexible deployment options (client-server, mobile or SaaS)
- Assets can be analyzed and classified in Asset Classes
- Risks and controls can be generated automatically onto built-in Risk registers
- Risk Registers display all of the material risks relating to a specific business unit, line of business, process, system, application or project.
- Report in real-time on: risk status against risk appetite and tolerances; compliance status against control standards, and; performance of key controls using metrics.
- Email notification on allocation of risks, controls, incidents and actions with reminders of forthcoming deadlines for actions, assessments and approvals.
- Sophisticated user-management restricts visibility of risks, controls, incidents and actions to those with appropriate permissions. Managers can see summary views with drill-down to the detail.
- Allows demonstrating compliance and achieving certification against standards or to implement a comprehensive Enterprise Risk Management solution
- Supports tracking the health of important risk mitigating controls and see how the performance of these controls affects residual risk status.

RM methods supported

ISO/IEC 27002, ISO/IEC 27005

Compatible conceptual model

ISO/IEC 13335-1

User group

Management and operational users with basic IT Security knowledge

Supplier

- Vendor name: Acuity Risk Management LLP (UK)
- Website: http://www.acuityrm.com/store/stream-software
- Price: Free; multiple paid versions also available

5.3.2 Callio secura 17799

Description

Callio Secura 17799 is a product from Callio technologies. It is a web based tool with database support that let the user implement and certify an information security management system (ISMS). It supports the ISO17799 and ISO 27001 (BS 7799-2) standards and can produce the documents that are needed for certification. Moreover it provides document Management functionality as well as customization of tool's databases. A trial version is available for evaluation. [42]

RM phases supported

1. Risk Assessment:
   (a) Risk Identification: Yes (identify vulnerabilities, threats; associate with assets)
   (b) Risk Analysis: No
   (c) Risk Evaluation: Yes
2. Risk treatment: Yes (selection of 17799 controls; list of suggested controls; create and evaluate different scenarios)
3. Risk communication: Yes (document management, awareness center portal)

Functionality

- Document Management : ISMS documentation requirements. Document approval system & version control. Document templates
- Reports Tool : Automatic report generator
- Glossary : Glossary of information security terms
- Awareness Center portal : Publish information security documents for different staff member groups.

RM methods supported

ISO 27002:2005

Compatible conceptual model

ISO 13335-1

User group

Any user group with basic IT and security knowledge

Supplier

- Vendor name: Callio technologies
- Website: http://www.callio.com
- Price: €4.495 (2 users license)

5.3.3 CCS Risk Manager

Description

Control Compliance Suite (CCS) Risk Manager enables security leaders to better understand and communicate risks to the business environment from their IT infrastructure. Risk Manager translates technical issues into risks relevant to business processes, delivers customized views of IT risk for different stakeholders, and helps prioritize remediation efforts based on business criticality rather than technical severity. [42]

RM phases supported

1. Risk Assessment:
   (a) Risk Identification: Yes (based on technical standards like ISO 27001, 27002)
   (b) Risk Analysis: Yes (multitude of tools for measuring IT risk)
   (c) Risk Evaluation: Yes (organizations can use Workflow as well as logical operations in order to evaluate, score and prioritize exposures)
2. Risk treatment: Yes
3. Risk communication: Yes (via customize-able dashboards for specific audiences, as well as other communication formats, reports and data export capabilities)

Functionality

- Ability to define a virtual business asset based on key business processes, groups, or functions you want to manage from an IT risk perspective
- Ability to group all IT assets associated with a virtual business asset and apply and monitor controls for a targeted view of IT risk posture
- Leverage a scalable data framework to easily aggregate and normalize technical and procedural controls data from multiple sources allowing you to communicate risk based on business criticality rather than technical severity
- Ability to set risk thresholds, alerts, and notifications on dashboards to better monitor IT risk levels
- Customize dashboards to illustrate different views of IT risks for multiple stakeholders including business unit leaders, Information Security and IT Operations managers
- Model risk reduction to facilitate evaluation of different remediation options
- Ability to monitor risk reduction over time as scheduled remediation activities take place

RM methods supported

AS/NZS 4346, ISO/IEC 27002, ISO/IEC 27005, FRAP, Risk IT

Compatible conceptual model

ISO/IEC 13335-1, AS/NZS 31000

User group

Tool can be used by management, operational and technical users thanks to it's customizable dashboards. General IT Security and administration skills required for use.

Supplier

- Vendor name: Symantec
- Website: http://www.symantec.com/ccs
- Price: €227.330 - Base license up to 500 users including 12 months maintenance

5.3.4 CORAS Tool

Description

The CORAS tool is a diagram editor that is designed to support on-the-fly modeling using all kinds of CORAS diagrams. [37]

RM phases supported

1. Risk Assessment:
   (a) Risk Identification: Yes, using Threat Diagrams
   (b) Risk Analysis: Yes, using Threat Diagrams
   (c) Risk Evaluation: Yes, using Risk Diagrams
2. Risk treatment: Yes, using Treatment Diagrams
3. Risk communication: No

Functionality

- Pull down menu: Offers standard functions such as open, save, copy, cut, paste, undo and print.
- Tool bar: Offers easy access to standard functions of the pull-down menu.
- Pallette: Contains all the model elements and relations for drawing CORAS diagrams.
- Drawing area: The area or canvas for drawing the CORAS diagrams.
- Properties window: Lists the properties of selected elements. Can be used to edit the values of the properties.
- Outline: Presents the project and its diagrams as a tree.

RM methods supported

CORAS

Compatible conceptual model

AS/NZS 31000

User group

All kinds of users with with decent Information Security knowledge and skills.

Supplier

- Vendor name: SINTEF ICT
- Website: http://coras.sourceforge.net/coras_tool.html
- Price: Open-Source

5.3.5 Countermeasures

CounterMeasures is a proven risk analysis solution that has been applied to address a wide range of risk disciplines including physical security and information security. The software is a scalable web-based program that is usually delivered as a pay-as-you-go web-service. The user standardizes the evaluation criteria and using a "tailor-made" assessment checklist, the software provides objective evaluation criteria for determining security posture and/or compliance. CounterMeasures is available in both networked and desktop configurations and can be evaluated through a flash demonstration and a trial version. [42]

Description

RM phases supported

1. Risk Assessment:
   (a) Risk Identification: Yes (including asset, threat and vulnerability identification and evaluation)
   (b) Risk Analysis: Yes (including estimations of Threat, Impact and Vulnerability levels)
   (c) Risk Evaluation: No
2. Risk treatment: Yes (including cost benefit analysis and re-iterating control effectiveness evaluation)
3. Risk communication: Yes (via reports)

Functionality

- User interface upgrades with offer dynamic and interactive table and chart displays
- Critical asset rating
- Threat and hazard characterization
- Security control identification
- Dynamic reports in Excel, PowerPoint, and Word with advanced graphics
- Risk mitigation tracking
- Customize-able dashboards and views (not all versions)

RM methods supported

AS/NZS 4360, ISO/IEC 27002, ISO/IEC 27005, FRAP, Risk IT

Compatible conceptual model

AS/NZS 3100, ISO/IEC 13335-1

User group

All kinds of users with decent Risk Management knowledge.

Supplier

- Vendor name: ALION Science and Technology
- Website: http://www.countermeasures.com/
- Price: €150 (basic version) to €350 (advanced version)

5.3.6 Cramm

Description

The Cramm tool provides an easy way to implement the Cramm method, developed by Insight Consulting. All three stages of the method are fully supported using a staged and disciplined approach. The tool comes in three versions: CRAMM expert, CRAMM express and BS 7799 Review. A trial version is available for evaluation. [42] CRAMM expert for executing a detailed risk assessment and CRAMM express for doing a high-level risk assessment.

RM phases supported

1. Risk Assessment:
   (a) Risk Identification: Yes
   (b) Risk Analysis: Yes
   (c) Risk Evaluation: Yes
2. Risk treatment: Yes
3. Risk communication: No

Functionality

- Comprehensive tool that supports the entire TA process
- Range of help functions and tools to help information security managers plan and manage security
- Wizards to rapidly create pro-forma information security policies and other related documentation
- 'Copy and Compare' feature allowing users to compare two reviews.

- A database of over 3000 security controls referenced to relevant risks and ranked by effectiveness and cost
- Various tools tat support the key processes involved in business continuity management
- Supports certification or compliance against ISO 27001

RM methods supported

CRAMM, ISO 27002

Compatible conceptual model

ISO 13335-1

User group

- CRAMM expert : Specialized IT Security users with knowledge of the CRAMM method described in Section 3.4.3
- CRAMM express: Basic IT Security knowledge required.

Supplier

- Vendor name: Siemens Insight Consulting (UK)
- Website: http://www.cramm.com
- Price:
  - CRAMM expert : €3.413 per copy plus €1.012 annual license
  - CRAMM express: €1.735 per copy plus €289 annual license

5.3.7 EAR / PILAR

Description

EAR / PILAR is the software that implements and expands Magerit RA/RM Methodology. It is designed to support the risk management process along long periods, providing incremental analysis as the safeguards improve. The tool is intuitive, provides fast calculations and generates a quantity of textual and graphical output. It is designed primarily to support the Magerit (see Section 3.4.9) methodology. [42] EAR provides a different versions of the PILAR tool:

- PILAR: Includes a qualitative and quantitative analysis for Risk analysis & Management and Business Impact Analysis & Continuity Management;
- μPILAR: A smaller version of PILAR for SMEs and local administrations;
- PILAR Basic: A smaller version of PILAR for SMEs and local administrations which includes only a qualitative risk analysis;
- RMAT (Risk Management Additional Tools): RMAT can be used to customize and extend PILAR with security profiles, Threat profiles and asset protection measures. This is intended to be only used by big organizations and consultants.

μPILAR, PILAR Basic and PILAR are free of charge for reading the results of a risk analysis but a commercial license is required for using the tool to run a complete risk assessment.

RM phases supported

1. Risk Assessment:
   (a) Risk Identification: Yes (including asset and threat identification and estimation)
   (b) Risk Analysis: Yes (including both qualitative and quantitative impact, potential and residual risk estimation)
   (c) Risk Evaluation: Yes (including prioritisation and presentation of results)
2. Risk treatment: Yes (both policies and procedures, including maturity evolution)
3. Risk communication: Yes (textual exports, graphical reports and exporting capabilities)

Functionality

- Quantitative and qualitative Risk Analysis and Management in several dimensions: confidentiality, integrity, availability, authenticity, and accountability.
- Quantitative and qualitative Business Impact Analysis & Continuity of Operations

RM methods supported

MAGERIT, ISO 27002, ISO 27005

Compatible conceptual model

ISO 13335-1

User group

Management users with at least basic knowledge of the Magerit[44] methodology. Can also be used by operational users.

Supplier

- Vendor name: A.L.H. J. Mañas
- Website: http://www.pilar-tools.com/en/index.html
- Price: €1.500

5.3.8 Ebios

Description

Ebios is a software tool developed by Central Information Systems Security Division (France) in order to support the Ebios method. The tool helps the user to produce all risk analysis and management steps according the five EBIOS phases method and allows all the study results to be recorded and the required summary documents to be produced. The tool is capable of matching a threat with relevant vulnerabilities and even building up risk scenarios automatically. [42]

RM phases supported

1. Risk Assessment:
   (a) Risk Identification: Yes (including identification of threats and security objectives)
   (b) Risk Analysis: Yes (including vulnerability analysis)
   (c) Risk Evaluation: Yes
2. Risk treatment: Yes (including determining security requirements)
3. Risk communication: Yes (including reports from each step)

Functionality

- Customize-able knowledge bases including vulnerabilities, threats, metrics, security requirements, etc. [30]
- Sample tutorial scenario (self-training module)
- Support for logging results and performing certain computations automatically
- Capability of producing several types of reports and deliverables based an different templates

RM methods supported

EBIOS, ISO/IEC 27005, ISO/IEC 27005

Compatible conceptual model

ISO 13335-1

User group

The tool is intended for both operational and management level users with standard RA knowledge and/or knowledge of the EBIOS method (see Section 3.4.4)

Supplier

- Vendor name: Central Information Systems Security Division (France)
- Website: https://adullact.net/projects/ebios2010/
- Price: Open-source

5.3.9 FAIRLite

Description

FAIRLite is an Excel application designed to enable simple and effective quantitative analysis of risk scenarios using the Factor Analysis of Information risk (FAIR) framework. FAIRLite is simple to use and yet flexible enough to perform powerful analyses on complex scenarios. FAIRLite leverages a widely used commercial Monte Carlo function specifically designed to analyze uncertain input data. Analysis results are then represented in both graphical and table

forms that inform management of the most likely outcomes while also accurately reflecting the degree of uncertainty associated with the analysis and the potential for "tail events". FAIRLite is primarily intended for use in analyzing discrete risk issues – i.e., those risk issues that are distilled to a single scenario. Since the merge between Risk Management Insight LLC and CXOWARE, the FAIRlite tool has been made obsolete by the new FAIRiq tool. [36]

RM phases supported

1. Risk Assessment:
   (a) Risk Identification: Yes
   (b) Risk Analysis: Yes
   (c) Risk Evaluation: Yes
2. Risk treatment: No
3. Risk communication: No

Functionality

- Scenario definition
- Analysis data input forms
- Documenting of analysis rationale
- Output of analysis results via graphs and tables

RM methods supported

FAIR

Compatible conceptual model

FAIR, The Open Group

User group

Management level users with basic understanding of Enterprise and Information Security Risk. Familiarity with FAIR (see Sections 3.4.5 and [33]) is recommended.

Supplier

- Vendor name: Risk Management Insight LLC
- Website: N/A
- Price: Free

5.3.10 FAIRiq

Description

FAIRiq is a quantitative risk analysis application and decision analysis solution based on the FAIR methodology. It is implemented as a software-as-a-service could application. FAIRiq is built as the foundational decision-analysis application enabling an organization to measure economic loss associated with information security & operational risk. The application is designed with flexible data export capability which makes it a nice compliment to the leading GRC applications on the market. Since the merge between Risk Management Insight LLC and CXOWARE, the FAIRiq tool has replaced the FAIRlite tool. According to the developers, FAIRiq helps decision-makers prioritize issues, evaluate threats, account for assets, and make sense of audit findings, all based on risk. [36]

RM phases supported

1. Risk Assessment:
   (a) Risk Identification: Yes
   (b) Risk Analysis: Yes
   (c) Risk Evaluation: Yes
2. Risk treatment: No
3. Risk communication: No

Functionality

- Centralized analysis repository – quick glance overview of risk landscape
- Constructs a view of aggregate risk
- Easy view to prioritize risk issues
- Common Asset Library Database
- Common repository for threat agents
- Common repository for scenario-based loss tables
- Enabling more consistent and accurate results across the team of analysts
- Iterative analysis capability – show risk trending over a period of time
- Dynamic reporting & Archive point-in-time reporting
- Centralized identity and access management
- Logical, easy to use, graphic scenario interfaces

RM methods supported

FAIR

Compatible conceptual model

FAIR, The Open Group

User group

Management level users with basic understanding of Enterprise and Information Security Risk. Familiarity with FAIR (see Sections 3.4.5 and [33]) is recommended.

Supplier

- Vendor name: CXOWARE
- Website: http://www.cxoware.com/solutions/
- Price: N/A

5.3.11 GSTool

Description

GStool has been developed by Federal Office for Information Security (BSI) in order to support users of the IT Baseline Protection Manual. The main goal of the software is to support preparation, administration and updating of IT security concepts according to the requirements of the IT-Grundschutz methodology. After collecting the information required, the users have a comprehensive reporting system at their disposal for carrying out structure analyses on all of their compiled data and for generating reports on paper or in electronic form. GSTOOL is a stand-alone application with database support. A trial version is available. [42]

RM phases supported

1. Risk Assessment:
   (a) Risk Identification: Yes
   (b) Risk Analysis: Yes
   (c) Risk Evaluation: Yes
2. Risk treatment: Yes
3. Risk communication: Yes (via reporting module)

Functionality

- Modeling and layer models in accordance with IT-Grundschutz
- IT system recording / structural analysis
- Assessing protection requirements
- Baseline protection modeling
- Estimation of cost, effort and residual risks
- Reporting module

- Revision support
- Encryption of user-specific data for exports

RM methods supported

IT-Grundschutz

Compatible conceptual model

ISO/IEC 13335-1

User group

Mostly management or high-level operational users with knowledge of the IT-Grundschutz methodology. No specific skills or knowledge required due to extensive user manual.

Supplier

- Vendor name: German Federal Office for Information Security (BSI)
- Website: https://www.bsi.bund.de/EN/Topics/ITGrundschutz/ITGrundschutzGSTOOL/Download/download_node.html
- Price: €887,40

5.3.12 GxSGSI

Description

GxSGSI is a Risk Management tool, which allows the identification and evaluation of threats, vulnerabilities, and impacts, the calculation of intrinsic and residual risk, the adoption of countermeasures and controls necessary for certification of a Management System of Information Security (ISMS), under ISO 27001 and ISO 27002. [42]

RM phases supported

1. Risk Assessment:
   (a) Risk Identification: Yes (including asset identification and evaluation, separation on the C/I/A dimensions, identification of existing controls, threats and vulnerabilities)
   (b) Risk Analysis: Yes
   (c) Risk Evaluation: Yes (also residual risk)
2. Risk treatment: Yes (using ISO/IEC 27001 controls)
3. Risk communication: yes (via reports)

Functionality

- Designed to automate, streamline and fully realize the security risk analysis of an organization.
- Generate all reports required in an audit of ISO 27001 certification in minutes.
- Automated data capture

RM methods supported

ISO/IEC 27002

Compatible conceptual model

ISO/IEC 27001

User group

Management and operational users with basic Information Security and Risk Management knowledge

Supplier

- Vendor name: SIGEA Sistemas de Protección de la información
- Website: http://www.sigea.es/herramientas.html
- Price: €75 per month (€750 per year)

5.3.13 HiScout GRC Suite

The HiScout GCR suite is a comprehensive toolset for Governance, Risk and Compliance Management. It's modeules cover: Business Conitnuity Management, Information Security Management, Operational Risk Managemen, Compliance Managment, Quality Management and IT-Service Management. The most notable modules are of course, the Information Security Management and Risk Management modules. These allow Risk assessments to be carried out covering both operational and enterprise Risk, as well as support the implementation of a complete ISMS.

Description

RM phases supported

1. Risk Assessment:
   (a) Risk Identification: Yes
   (b) Risk Analysis: Yes
   (c) Risk Evaluation: Yes
2. Risk treatment: Yes
3. Risk communication: Yes

Functionality

- Structured approach to collecting all relevant data for a specific risk (processes, resources involved, when/where, previous security incidents, changes in framework parameters and risk indicators, etc.) delivers better risk analyses.
- Process owners and resource owners can check any time to see what security guidelines they need to observe.
- It lets you generate security guidelines and instructions automatically or semi-automatically. This means it is less prone to errors, saves you valuable time and preserves your resources.
- It enables you to demonstrate and document at any time compliance with official requirements (laws, guidelines, standards, internal policies).
- It is highly pre-configurable but also very flexible, allowing you to make client-specific changes to parameters such as the type, number and classification of goals, as well as to methods for conducting all types of security requirements analysis.
- The module automatically calculates the overall security requirements for all company resources, and lets you use that information as the foundation for goal-oriented decisions.
- Modifiable templates for management reports and audit reports enable you to quickly demonstrate your findings

RM methods supported

IT-Grundschutz, ISO/IEC 27002

Compatible conceptual model

ISO 13335-1

User group

Management and operational users with relevat Information security, Risk management or other knowledge depending on the module and how it is used

Supplier

- Vendor name: HiSolutions AG
- Website: http://www.hiscout.com/index.php?id=3&L=1
- Price: On request

5.3.14 Mehari 2010 basic tool

Description

The worksheet of the method contains multiple formulas allowing to display step by step the results of the RA and RM activities and to propose additional controls for risk reduction. The tool is build to support the MEHARI[16] method, described in Section 3.4.10 and is built entirely in MS Excel. It is a very basic tool, with limited functionality. It can be used however, as a supporting document for a limited-purpose RA following the MEHARI methodology.

RM phases supported

1. Risk Assessment:
   (a) Risk Identification: Yes (based on assets, threats, vulnerabilities)
   (b) Risk Analysis: Yes (through scenarios)
   (c) Risk Evaluation: Yes (by quantifying level and likelihood of threats)
2. Risk treatment: Yes (limited to a simple list of suggestions)
3. Risk communication: Not by default

Functionality

- Allows assessing the seriousness level of individual risk scenarios based on impact and likelihood
- Selection of relevant countermeasures
- Knowledge base supporting Risk Assessment process.

RM methods supported

MEHARI

Compatible conceptual model

ISO 13335-1

User group

Anybody with knowledge of the MEHARI methodology.

Supplier

- Vendor name: CLUSIF
- Website: http://www.clusif.asso.fr/en/production/mehari/download.asp
- Price: Open-Source

5.3.15 Modulo Risk Manager

Description

Modulo Risk Manager™ software helps organizations streamline and automate processes required for in-depth risk assessment and compliance projects by collecting and centralizing data relating to technology assets, such as software and equipment, as well as non-technology assets such as people, processes and physical facilities within an organization to assess risk and ensure compliance. The software also allows the quick and comprehensive generation of reports resulting from the data collected. The tool features various knowledge bases customized for compliance to various standards. Modulo Risk Manager makes the calculation of risk scores easy because it contains knowledge of IT assets, best practices for the various standards and contains workable

default risk component values for every asset and control, estimated by the Modulo Security Lab. This same knowledge base simplifies the process of human interviews with prepared questionnaires. Time is saved by encapsulating these interviews with a viewer that can be emailed to the persons to be surveyed, or answer via the Web. After completion, the answers are mapped to the best practice controls for any standard and saved automatically into the secure audit repository.

RM phases supported

1. Risk Assessment:
   (a) Risk Identification: Yes (up to 70
   (b) Risk Analysis: Yes
   (c) Risk Evaluation: Yes
2. Risk treatment: Yes
3. Risk communication: Yes (28 different reports)

Functionality

- Automation of the entire RA process, including governance and compliance gap analyses, with detailed reports
- More than 4,000 automatic collectors for a variety of technological assets
- Knowledge Bases with more than 11,000 controls
- Develop a risk scorecard providing executive management with an enterprise overview of risks, including indices and metrics
- Allows risks to be viewed in different ways, as assets, parameters, business components, threats, and others
- Obtain consolidated information about compliance and risk management solutions and assessments easily through customizable, graphical risk management dashboards
- Compliance Module with standards and regulations :The MetaFramework™ allows the user to produce a score and set of reports for any of the contained standards.
- Live Up-date: feature to download the latest controls, standards and automatic collectors. Modulo's Security Research Lab updates this approximately every two weeks.
- Business Continuity Plan: BCP Module integrated in Risk Manager Solution.
- WEB Interview: For remote usage.
- Geo-referenced risk: Risk map with Google Earth.
- PDA use: Use of PDA to remote interview.

RM methods supported

AS/NZS 4346, ISO/IEC 27002, ISO/IEC 27005, FRAP, Risk IT

Compatible conceptual model

ISO/IEC 13335-1

User group

Basic Information Security knowledge required. Can be used by managers, analysts, security officers, operational users and even technical users (functionality differs according to role).

Supplier

- Vendor name: MODULO
- Website: http://www.modulo.com/risk-manager
- Price: On request

5.3.16 MSAT

Description

The Microsoft Security Assessment Tool (i.e. MSAT) is a high level security assessment tool developed by Microsoft, designed to provide information and recommendations regarding best practices for security within IT infrastructures. It is designed for SME's (50-500 employees) and is available for free. MSAT includes 200 questions covering four categories (infrastructure, applications, operations, and people). The questions, answers and recommendations of MSAT come from different sources (ISO/IEC 17799, NIST-800.x, recommendations and prescriptive guidance from the Microsoft Trustworthy Computing Group, etc.). The tool employs a holistic approach to measuring your security posture by covering topics across people, process, and technology. Findings are coupled with prescriptive guidance and recommended mitigation efforts, including links to more information for additional industry guidance The procedure of the tool is:

1. Define profile of organization by answering questions about basic information, infrastructure security, application security, operations security, people security and environment.
2. Create Risk assessment by answering questions about security controls in place.
3. SAT computes reports based on the given answers. MSAT computes a report summary, a complete report (including a business risk profile and an index based on the security measures in place) and a comparison report in order to compare the results of the assessment with a previous assessment or with assessments realized by other companies in the same sector. MSAT also calculates a security maturity of the organization. At the lower-end few security defenses are employed and actions are reactive. At the high-end, established and proven processes allow a company to be more proactive, and to respond more efficiently and consistently when needed.

MSAT cannot measure the effectiveness of the security measures employed due to the fact that MSAT only offers a baseline risk assessment approach.

RM phases supported

1. Risk Assessment:
   (a) Risk Identification: Yes
   (b) Risk Analysis: Yes
   (c) Risk Evaluation: Yes (by comparing with similar companies in the same industry)
2. Risk treatment: No
3. Risk communication: No

Functionality

- Information gathering via e-questionnaire, with 172 categorized questions.
- Three different types of reports available: Summary Report, Complete Report and Comparison Report.
- Results can be uploaded anonymously to the MSAT Web Server for comparison with similar companies.
- References recommendations and best practices from relevant standards, Microsoft's Trustworthy Computing Group as well as other security resources.
- Allows two types of assessments: Business Risk Profile Assessment and Defense in Depth Assessment.

RM methods supported

ISO/IEC 27002, FRAP

Compatible conceptual model

ISO/IEC 13335-1

User group

Operational and management users with standard IT knowledge. Can also be used by middle-management (life CTO's and CISO's) but with reduced applicability.

Supplier

- Vendor name: Microsoft Corporation
- Website: http://www.microsoft.com/en-us/download/details.aspx?id=12273
- Price: Free

5.3.17 Proteus Enterprise

Description

Proteus Enterprise is a comprehensive web server based compliance, information security and risk management, and Corporate Governance tool developed by Information Governance Ltd. The entire range of Proteus products, and its preceding versions, have been branded and distributed by the British Standards Institution since 1995, although most enterprise level sales are direct via Information Governance Ltd and its global distribution network managed by Veridion Inc., Canada. Proteus allows organizations to implement the controls of any standard or regulation, e.g. BS ISO/IEC 17799 and BS ISO/IEC 27001, BS 25999, SOX, CobiT, PCI DSS etc. [42]

RM phases supported

1. Risk Assessment:
   (a) Risk Identification: Yes
   (b) Risk Analysis: Yes
   (c) Risk Evaluation: Yes
2. Risk treatment: Yes (via "Action plans")
3. Risk communication: Yes (via PDF reports and optional RiskView module)

Functionality

- Supports both qualitative and quantitative techniques.
- Relative and Absolute risk scales can be used to adapt to corporate 'risk appetite'.
- Consists of 4 modules: Compliance module, Manager Module, RiskView and Alert Module
- Allows Compliance gap analysis, Business Impact Analysis, Business contnuity analysis, in-depth Risk Assesssments, Incident Management and Document management.
- Threat and countearmeasure template lists curtomized for all major IS standards
- Inheritance of threats and countermeasures based on location or related assets
- Action plans and work packages can be evaluated from a Return On Security Investment (ROSI) view
- Risk Matrix plotting Risk vs. Business Impact
- Large number of Graphs, charts, pictures and reports can be customised and published.

RM methods supported

AS/NZS 4346, ISO/IEC 27002, ISO/IEC 27005, FRAP, Risk IT

Compatible conceptual model

ISO/IEC 13335-1

User group

Managers and operational users with advanced Information Security and Risk Management.

Supplier

- Vendor name: Infogov (Information Governance Limited)
- Website: http://www.infogov.co.uk/solutions/proteus.htm
- Price:
  - Proteus Solo: €694 /year
  - Proteus Professional: €6942 £/year or €694 /month
  - Proteus Enterprise : on request

5.3.18 Resolver Ballot

Description

Typically used in a small meeting with a board of directors, audit committee, or with department heads, Resolver*Ballot is a group risk assessment application which allows meeting participants to anonymously voice their opinion on the impact and likelihood of risks to their organization. Accodring to the developer: "Resolver Ballot is an anonymous risk workshop assessment tool that enables groups to make better decisions in less time, with less arguing." As no two risk methodologies are identical Resolver Ballot can easily be configured to use local language, terminology, and criteria scales. Vote results are displayed on-screen real-time analysis providing rare access to all viewpoints on a topic. [42]. Although the tool is not dedicated to analyzing Information Security Risk, it's support for group discussion on Risk Assessment topics makes it useful for any methodology which involves brainstorming meetings.

1. Risk Assessment:
   (a) Risk Identification: Yes
   (b) Risk Analysis: Yes
   (c) Risk Evaluation: Yes
2. Risk treatment: No
3. Risk communication: No

Functionality

- (Remote) anonymous voting on impact, likelihood or any other criteria for each risk (from wireless keypad, mobile phone, or computer)
- Assess control effectiveness
- In-room or web based voting via computer
- Focus and facilitate discussions on topics without agreement to share viewpoints and re-vote after discussion to see the change

- Generation of standard or custom heat maps (e.g. inherent vs. residual risk or Year 1 vs. Year 2)
- Relationship Modeling: identifies and explains relationships between risks: how each key risk impacts others
- Generates over 15 different commonly used Risk Management and Decision making reports

RM methods supported

AS/NZS 4360, FRAP, ISO/IEC 27002, ISO/IEC 27005, OCTAVE, RiskIT

Compatible conceptual model

ISO/IEC 13335-1

User group

Management users (or auditors) with standard Risk Management training. In order for the tool to be applicable to Information Security Risk Assessment, knowledge about IT Security is also required.

Supplier

- Vendor name: Resolver (Canada)
- Website: http://www.resolvergrc.com/grc-software/ballot-risk-assessment/
- Price: from €1300 per year

5.3.19 Risicare

Description

Risicare assists the information risk analysis and management actions in support of MEHARI Risk Methodology (further analyzed in Section 3.4.10), options and formulas developed by CLUSIF. The functions of Risicare simulate real-world conditions and test multiple "what if" threat situations or scenarios. As a result, Risicare can be considered additionally as a risk modeling software. Moreover, Risicare allows the management of an ISMS and uses a set of control points which includes those of ISO 27002. [42]

1. Risk Assessment:
   (a) Risk Identification: Yes (according to MEHARI method)
   (b) Risk Analysis: Yes (using MEHARI knowledge bases)
   (c) Risk Evaluation: Yes
2. Risk treatment: Yes (with simulations and optimizations)
3. Risk communication: Yes (via reports, charts, tables and plans)

Functionality

- Asset identification, evaluation and classification module
- Comparison of security controls currently in place with controls recommended by ISO/IEC 13335 and ISO/IEC 27002
- Analysis and comparison of various risk mitigation strategies using novel algorithms
- Knowledge base with taxonomy of assets and catalogs of vulnerabilities and threats and connection to metric used.
- Display the risk reduction phases based on the planned improvements and the target dates for their achievements.
- Automatically produces Risk reports, mitigation action lists, contingency plans and progress reports

RM methods supported

ISO/IEC 27002, ISO/IEC 27005, MEHARI

Compatible conceptual model

ISO/IEC 13335-1

User group

Management and operational level users with standard Information Security knowledge.

Supplier

- Vendor name: BUC S.A.(France)
- Website: http://www.risicare.fr/
- Price: On request

5.3.20 Riskwatch

Description

RiskWatch for Information Systems & ISO 17799 is a IS Risk Management solution. The tool conducts automated risk analysis and vulnerability assessments of information systems. The knowledge databases that are provided along with the product are completely customizable by the user, including the ability to create new asset categories, threat categories, vulnerability categories, safeguards, question categories, and question sets. The tool includes controls from the ISO 17799 and US-NIST 800-26 standards. RiskWatch provides an online demonstration of the product. [42] It is one of the most comprehensive (and expensive) RA tools available.

RM phases supported

1. Risk Assessment:
   (a) Risk Identification: Yes (via predefined lists of threats)
   (b) Risk Analysis: Yes (by determining potential financial impact)
   (c) Risk Evaluation: Yes
2. Risk treatment: Yes (defining safeguards)
3. Risk communication: No

Functionality

- Allows both quantitative and qualitative analyses
- Industry and organization-specific libraries of pre-built standards and compliance assessment questions and controls designed to address risks relevant to a wide variety of organization types;
- Can manage all risk and compliance assessments across a client's business.
- Can work either local or as a web-based Software-as-a-Service application, both allowing real-time deployment and tracking of assessment surveys
- Provides bot top down and bottom-up views of organizational risk and compliance
- Exposes relationships between the identified risks, control and requirements.
- Covers both digital and physical security

RM methods supported

ISO/IEC 27002

Compatible conceptual model

ISO/IEC 13335-1

User group

The tool is mostly intended for management users, but is also relevant to operational-level users. Basic training is required to use the tool, and in order to guarantee relevant results, at least Basic knowledge/skills regarding Risk Management and IT are required.

Supplier

- Vendor name: RiskWatch (USA)
- Website: http://riskwatch.com/
- Price: On request (around €14.000)

5.3.21 RM Studio

Description

RM Studio is a full-featured, customizable and dynamic solution that combines business continuity management software and risk management software into one simple to use platform. RM Studio guides users through the process of risk assessment, risk treatment and risk management. Standards are easy to embed and users can easily define their company own standards. RM Studio comes with a predefined asset category library and a predefined threat library with interconnection helping users to identify important threats and select the appropriate mitigating control. RM Studio is a holistic modular solution with the option to add a risk assessment and treatment module and a business continuity module. It assists users in embedding a culture of risk management throughout the organization by combining risk management software and business continuity management software. [41]

RM phases supported

1. Risk Assessment:
   (a) Risk Identification: Yes (using Threat library)
   (b) Risk Analysis: Yes
   (c) Risk Evaluation: Yes (based on pre-defined or custom templates)
2. Risk treatment: Yes (based on pre-defined or custom standards)
3. Risk communication: Yes (via 11 different reports and result portals)

Functionality

- Analyzing and evaluating risks based on Asset-value, C/I/A, impact, probability, vulnerability or other custom criteria
- Asset Management
- Embedded standards, controls and guidelines compatible with large variety of international standards
- Step by step guide to conducting Risk Assessments
- Gap Analysis: Comparison of current controls with recommendations by any available or custom standard
- Can work "out-of-the-box", but also allows heavy customization of everything from threats and controls to standards and evaluation criteria.

RM methods supported

IT-Grundschutz, ISO/IEC 27002, ISO/IEC 27005

Compatible conceptual model

ISO/IEC 13335-1

User group

The tool is usable by all kinds of users (management, technical or operational) by providing everything from decision support and policy formulation to RM activities and implementation guides. No specific training is required, but general Risk Management knowledge is needed.

Supplier

- Vendor name: Stiki – Information Security (Iceland)
- Website: http://www.riskmanagementstudio.com
- Price: On request

5.3.22 SAVe

Description

SAVe is a Database-supported tool that implements the IT-Grundschutz methodology, but can also be used to obtain ISO 27001 OR BSI 100-2 and 100-3 results. It is supported by an extensive "IT Security Database" that allows IT security concepts to be created, applied and updated in a manner consistent manner, compatible with the IT-Grundschutz methodology. It allows the user to analyze and model the IT architecture, identify security needs, perform basic security checks and surveys. Furthermore, it can be used to perform audits and certifications against the IT-Grundschutz and ISO/IEC 27001 standards. It can be adapted to various scenarios (e.g. military or security-critical infrastructures) by extending the security model. It also contains modules that allow things like monitoring the costs of implementation, introducing custom measure and building blocks, mapping of e-business requirements, capturing of deadlines, roles and responsibilities, action planning and tracking, etc.

RM phases supported

1. Risk Assessment:
   (a) Risk Identification: Yes
   (b) Risk Analysis: Yes
   (c) Risk Evaluation: Yes
2. Risk treatment: Yes
3. Risk communication: Yes

Functionality

- Network-capable
- Multiuser
- Supports distributed development of part-concepts
- Manages multiple security concepts and part-concepts
- Flexible, role-based access control

- Revision and tracking ability
- Automatic data update for new IT-Grundschutz version
- Data export for development in Office components
- Import function to data inputs from the GSTOOL
- Interactive creation of customised report formats
- Open interface for the integration of additional modules

RM methods supported

IT-Grundschutz

Compatible conceptual model

ISO/IEC 13335-1

User group

Technical, operational and management users due to various modules and role-based access control. Users require knowledge of IT-Grundschutz methodology.

Supplier

- Vendor name: INFODAS GmbH
- Website: http://www.save-infodas.de/
- Price: €860 per license

5.3.23 TRICK light

Description

TRICK light (Tool for Risk management of an ISMS based on a Central Knowledge base) is a risk assessment & management software tool, developed in the VBA Excel environment. TRICK light enables to determine a list of security measures to implement in order to reduce the impact caused by the occurrence of possible incident scenarios. TRICK light is consistent with the ISO/IEC 27005 RM methodology and employs the "Risk Reduction Factor" (RRF) determination which enables to quantify the influence of security measures on the losses caused by threats to assets. The tool also considers cost-effectiveness of security controls by estimating Return On Security Investment (ROSI) and can derive a prioritized action plan. [42]

The main objective of the tool is to estimate the profitability of security measures in a specific context to deduce the priorities of an action plan (Risk treatment plan).

In order to have an indicator on the quality of the Information Security Management System in which the security measures will be implemented, TRICK light additionally offers the possibility to measure the maturity of the security environment of the targeted organisation. The maturity of the security environment is measured with the help of a 6 levelled maturity model and adjusts the estimated implementation rate according to the current reached maturity level.

RM phases supported

1. Risk Assessment:
   (a) Risk Identification: Yes (following ISO 27005 recommendations, including risk scenario identification)
   (b) Risk Analysis: Yes (both qualitative and quantitative)
   (c) Risk Evaluation: Yes
2. Risk treatment: Yes (either pre-defined ISO/IEC 27005 controls or custom controls from other sources)
3. Risk communication: Yes (via charts, tables, key indicators, and plans)

Functionality

- Identification of assets, threats, existing security controls, vulnerabilities through identification of missing security in previous item and consequences (List of incident scenarios & their consequences).
- Assessment of the consequences, incident likelihood and level of risk, as well as Risk Reduction Factors (i.e. influence of a security measure on the impact and occurrence of each risk scenario)
- Risk prioritization according to risk evaluation criteria in relation to the incident scenarios
- Maturity assessment of implemented security measures
- ROSI computation
- Indicators and management view of security status and implementation phases

RM methods supported

ISO/IEC 27002, ISO/IEC 27005

Compatible conceptual model

ISO/IEC 13335-1

User group

Management and operational users (including auditors) with standard Information Security knowledge.

Supplier

- Vendor name: iTrust consulting s.à r.l. (Luxembourg)
- Website: http://www.itrust.lu/index.php?p=produit_licenciable
- Price: On request

5.3.24 verinice

Description

verinice is an open-source tool that can be used to support implementation of an IT-Grundschutz or ISO 27001 compliant ISMS. The tool can be used to map important Information Security assets and identify inherent risks. It also generates reports for management and auditors. There is also a paid version: verinice.PRO. It is an additional application server for the verinice client. This server module collaborates with the client to give you a complete three-tier architecture.The verinice.PRO server acts a a central IS repository in your network, allowing you to work collaboratively on your ISMS or audits. You can assign tasks, use email notifications and a web-frontend to get feedback on completed tasks, create a central storage for policies and other documents and much more.

RM phases supported

1. Risk Assessment:
   (a) Risk Identification: Yes
   (b) Risk Analysis: Yes
   (c) Risk Evaluation: Yes
2. Risk treatment: Limited
3. Risk communication: No

Functionality

- Data import, including inventory database and lists of assets, controls or employees.
- Synchronization feature keeps verinice automatically up-to-date with all lists, inventories and directories it imports data from.
- Customize-able pre-defined reports in various formats and styles
- Audit module allows users to conduct audits of own organization or other vendors, with tracking and comparing features.
- Importing from GSTOOL, from IT-grundschutz catalogs and custom catalogs.
- Multi-user and multi-tenant capabilities including access control at various levels of granularity and Active Directory integration (only in PRO version)

RM methods supported

It-Grundschutz, ISO/IEC 27002, ISO/IEC 27005, FRAP

Compatible conceptual model

ISO/IEC 13335-1

User group

Thanks to the highly granular access control features, it can be used by various types of users simultaneously. Basic Risk Management and Information Security knowledge is required in order to make use of this software.

Supplier

- Vendor name: SerNet GMBH
- Website: http://www.verinice.org/en/download/
- Price: Open-Source; Pro version

5.3.25 vsRisk

Description

vsRisk has been designed with ISO/IEC 27001 certification in mind, but also supports Risk Assessments based on the ISO/IEC 27002 and 27005 methodologies. It is also compatible with other IS standards like BS7799-3, NIST 800-26 and 800-30, as well as the ISF standards and others.

RM phases supported

1. Risk Assessment:
   (a) Risk Identification: Yes
   (b) Risk Analysis: Yes
   (c) Risk Evaluation: Yes
2. Risk treatment: Yes
3. Risk communication: Yes (via reports)

Functionality

- Wizard-based approach to simplify and accelerate the RA process
- Asset-by-asset identification of threats, vulnerabilities
- Specific process for identification and assistance in the implementation of ISO/IEC 27001 controls as well as the ability to import additional controls
- Constantly updated threat and vulnerability databases
- Customize-able risk acceptance criteria and management scales
- Helps define scope and business requirements, policy, objectives and asset inventory of the ISMS
- Can assess confidentiality, integrity & availability (CIA) for each of business, legal and contractual aspects of information assets
- Gap analysis versus ISO/IEC standards

- Import and export of asset information
- In built Audit Trail and comparative history

RM methods supported

ISO/IEC 27002, ISO/IEC 27005, FRAP

Compatible conceptual model

ISO/IEC 13335-1

User group

Management users with standard Information Security and Risk Management knowledge.

Supplier

- Vendor name: Vigilant Software
- Website: http://www.vigilantsoftware.co.uk/
- Price: €1,323.35

5.4 Comparison of tools

Many tools are available but, as it usually is the case with software tools, most are no longer developed or even maintained. For lots of tools, the websites are down, supplier no longer exists, support has been discontinued, or the application has been replaced. The tools reviewed in the previous section were, at the time of writing, still available and maintained.

Tools seem to fall into one of three categories, with regard to the methodology they support and the conceptual models or standards they are compatible with:

Independent third-party Risk Assessment or Risk Management tools that are designed to automate or simplify one or more sub-processes, but are not explicitly designed with any method or standard in mind. These have been omitted from the analysis due to Exclusion Criteria E-3

Generic Risk Assessment or Risk Management tools designed to automate or simplify one or more sub-processes, that are not designed specifically for a particular methodology, but are compliant or consistent with one or more Information Security standards (like ISO/IEX 2700x or 13335-1, the AS/NZS 4360 or 31000 standards, COBIT, BSI standards). These type of tools are in theory usable within any method that is itself compatible with one or more of these standards.

Specialized Risk Assessment or Risk Management tools designed to support a particular methodology or method. These are, in principle, only compatible with the method they were designed for due to the fact that they make use of very specific computations or activities.

Most tools claim to provide support for all the steps involved in a Risk Assessment and even for the cyclical Risk Management phases. However, only a few software tools available actually cover all the steps required for performing an entire assessment solely within the application

(e.g. Acuity Stream, CCS Risk Manager, EAR/PILAR, GSTool, Modulo Risk Manager, Proteus, RiskWatch, RM Studio). Others are only truly useful for automating or facilitating certain sub-processes or activities (e.g. vsRisk, Resolver Ballot, FAIRiq, FAIRlite and TRICKlight, CRAMM - for RA process , MEHARI basic tool - for Risk Analysis process, Countermeasure - for Gap Analysis).

Table 5.2 provides an overview of the RA/RM tool characteristics discussed within the previous Section. The RM phases are numbered the same way as in the previous section: 1.(a) Risk identification, 1.(b) Risk Analysis, 1.(3) Risk Evaluation, 2. Risk Treatment and 3. Risk Analysis. With regard to the users, M stands for Management, O for Operational and Tfor Technical users.

Tool	RM phases supported					RM methods supported	Compatible Conceptual Model	Users				Price (per license) [€]
	1. RA			2	3			M	O	T	Skill	
	1.(a)	1.(b)	1.(c)									
Acuity Stream	X	X	X	X	X	ISO 27002, ISO 27005	ISO 13335-1	X	X		Basic	Free
Callio secura 17799	X	-	X	X	X	ISO 27002, ISO 27005	ISO 13335-1	X	X	X	Basic	2.250
CCS Risk Manager	X	X	X	X	X	AS/NZS 4346, ISO 27002, ISO 27005, FRAP, Risk IT	AS/NZS 3100, ISO 13335-1	X	X		Standard	227.330
CORAS Tool	X	X	X	X		CORAS	AS/NZS 3100	X	X	X	Standard	Open-Source
Countermeasures	X	X		X	X	AS/NZS 4346, ISO 27002, ISO 27005, FRAP, Risk IT	AS/NZS 3100, ISO 13335-1	X	X	X	Standard	350
CRAMM expert	X	X	X	X		CRAMM, ISO 27002	ISO 13335-1	X	X	X	Advanced	4413
CRAMM express	X	X	X	X		CRAMM, ISO 27002	ISO 13335-1	X	X	X	Basic	2000
EAR/PILAR	X	X	X	X	X	MAGERIT, ISO 27002, ISO 27005	ISO 13335-1	X	X		Basic	1500
Ebios tool	X	X	X	X	X	EBIOS, ISO 27002, ISO 27005	ISO 13335-1	X	X		Standard	Open-Source
FAIRlite	X	X	X			FAIR	FAIR, The Open Group	X			Basic	Free
FAIRiq	X	X	X			FAIR	FAIR, The Open Group	X			Basic	On request
GSTool	X	X	X	X	X	IT-Grundschutz	ISO 13335-1	X			Basic	887,40
GxSGSI	X	X	X	X	X	ISO 27002, ISO 27001	ISO 13335-1	X	X		Basic	750
HiScout GRC Suite	X	X	X	X	X	IT-Grundschutz, ISO 27002	ISO 13335-1	X	X		Standard	On request
Mehari 2010 basic tool	X	X	X	X		MEHARI	ISO 13335-1	X	X	X	Standard	Open-Source
Modulo Risk Manager	X	X	X	X	X	AS/NZS 4346, ISO 27002, ISO 27005, FRAP, Risk IT	ISO 13335-1	X	X	X	Standard	On request
MSAT	X	X	X			ISO/IEC 27002, FRAP	ISO 13335-1	X	X		Basic	Free
Proteus Enterprise	X	X	X	X	X	AS/NZS 4346, ISO 27002, ISO 27005, FRAP, Risk IT	ISO 13335-1	X	X		Advanced	694
Resolver Ballot	X	X	X			AS/NZS 4346, ISO 27002, ISO 27005, FRAP, Risk IT	ISO 13335-1	X	X		Standard	1300
Risicare	X	X	X	X	X	ISO 27002, ISO 27005, MEHARI	ISO 13335-1	X	X		Standard	On request
Riskwatch	X	X	X	X		ISO 27002	ISO 13335-1	X	X		Standard	14,000
RM Studio	X	X	X	X	X	ISO 27002, ISO 27005	ISO 13335-1	X	X	X	Standard	On request
SAVe	X	X	X	X	X	ISO 27002, ISO 27005	ISO 13335-1	X	X	X	Standard	860
TRICK light	X	X	X	X	X	ISO 27002, ISO 27005	ISO 13335-1	X	X		Standard	On request
verinice	X	X	X	X	X	IT-Grundschutz, ISO 27002, ISO 27005, FRAP	ISO 13335-1	X	X	X	Basic	Open-source
vsRisk	X	X	X	X	X	ISO 27002, ISO 27005, FRAP	ISO 13335-1	X			Standard	1,323.35

Table 5.2: RA/RM tools and characteristics

Chapter 6

Cross Comparison

This chapter will focus on discussing the cross-compatibility between these methodologies and the Tools identified in Chapter 5, as well as between the methodologies and the Conceptual Models from Chapter 4. Finally, suggestions on the applicability of the Methods, Tools and Conceptual Models to various contexts.

6.1 Methods and Tools

As has been pointed out in Section 5.4, the RA tools currently available fall into one of three categories with regard to the established methods: (1) *specialized* tools are designed for a specific RA method, (2) *generic* tools can be used in conjunction in the process described by one or more methods and (3) *independent* third-party not compatible with any established RA methodology. Such stand-alone tools have been excluded from the set of tools reviewed in Chapter 5 due to the exclusion criteria E-3. The other two types of tools however, were described in detail.

Furthermore, most of the tools analyzed can be used to support at least part of the RA process as it is described by the high-level RA/RM methodologies like AS/NZS 4346, ISO/IEC 27002, ISO/IEC 27005, and Risk IT. This is because most software tools aim at providing some practical tools that can support a Risk Assessment or that can provide useful output for a more general Risk Management process. As such, as long as they do not contradict any of the principles set out by these high-level methodologies, most of them can provide relevant output for, or useful automations of one or more of the sub-processes as they are abstractly defined in these standards.

One general observation is that all generic methods and even some of the specialized methods are compatible with the FRAP RA method. This is because FRAP does not go into any detail describing the assessment process and as such, can be used in conjunction with almost any tool. For more information see Section 3.4.6

In conclusion, for companies or individuals desiring to find the most suitable methodology-tool pair, it might be easier to first decide on what standardized methodology to use. If this choice is made on one of the higher-level ones, then the choice of tool is somewhat free and can be made based on the functionality and output each offers, or based on the expertise of the analysis. Otherwise, if a low-level methodology is chose, then there is usually a dedicated tool for each of these.

6.2 Tools and Conceptual Models

Most tools reviewd in this thesis were compatible with the high-level principles and conceptual model dictated by the ISO/IEC 13335-1 standard. It seems that most tool developers design their tools with one or more of the ISO/IEC Information Security or Risk Management standards. And as the ISO standards are designed to be cross-compatible, most of these tools implicitly comply with the ISO/IEC 13335-1 conceptualization of Risk.

Furthermore, most tool do not include explicit descriptions of the underlying conceptual model. Most make implicit assumptions regarding the concept of Risk as it described in established relevant standards (like the ISO/IEC 2700x series). Very few tools do not reference a particular standard or even methodology, but these have been excluded from our analysis due to the Exclusion criteria.

6.3 Methods and Conceptual Models

The FAIR method can be used in conjunction with the ISO/IEC 27005 framework by providing more practical and detailed advice on performing the Risk Analysis and Evaluation steps, as described in [24].

Having said that, it is the case that in fact all Class 1 and Class 3 methods are in principle compatible with the ISO/IEC 2700x series. This is due not only to the common interpretation of Risk as Likelihood x Impact, with Vulnerability being taken into account either explicitly or implicitly, but also because of the flexibility that the high-level ISO standards offer with regard to the Risk Assessment methodology. Furthermore, due to the extensive use of the ISO 2700x series of standards, most RA methodologies are designed with these principles in mind.

A further exception is constituted by the SRA. Its unique decomposition of Risk makes in only truly compatible with its own conceptual model.

The fact that the FAIR RA methodology is compatible with ISO/IEC 27005 does not imply however that the FAIR conceptual model and taxonomy is in turn compatible with the RA methodologies designed with ISO/IEC 27005 in mind. This is because the FAIR framework goes into sufficient technical depth to make it differ significantly from most other RA methodologies in the way it computes risk as well as in the factors it prioritizes.

The two web-oriented conceptual models of Risk. OWASP and the Microsoft Threat Model can also be considered to be compatible with the high-level methods that do not describe technical details. Even more so, these make a good addition to the abstract presentation of concepts suggested by high-level methods like: AS/NZS 4360, ISO/IEC 27002, 27005 and FRAP. As these methods provide abstract management level suggestions for the RA process, they can be easily complemented by a lower-level conceptual model describing the specific technical factors that drive risk.

Another notable observation is that while some methods describe or refer to a relevant conceptual model, others do not make any assumptions about such a model. This is the case with FRAP, as it allows the person holding the key role of "facilitator" to make use of any Risk model that suits the situation. Other methods, like OCTAVE and TARA also do not rely on an implicit or explicit conceptual model, only describing the factors involved sufficiently so that they can be estimated. Examples of methods that describe their own conceptual model as part of the same document are: SRA, FAIR, the AS/NZS 4360 standard and of course the ISO/IEC methodologies.

Chapter 7

Guidelines

In this chapter, a set of guidelines for choosing the most appropriate Risk Management or Risk Assessment framework based on the size of the organization, it's security needs, the business context, availability of experts, time-frame for conducting the analysis and other relevant factors. This will be achieved via Decision-Tables due to the large number of factors and methods yielding many possible combinations.

7.1 Decision Table

Based on the characteristics of each method, depicted in depicted in Table A.1 as well as the PROs and CONs distilled from the analyses conducted in Section 3.4, we can derive conclusions regarding the scope and applicability of each method. These conclusions are used to make recommendations regarding the suitability of each method or methodology to particular organizational contexts. This can be used by companies that are required to make a choice regarding which RA/RM methodology to implement in order to best suit their requirements and situation.

Before creating the decision table, an intermediary table was drafted mapping each method to particular selection criteria. This table is available in Appendix B

The resulting decision table is represented in Table 7.1.

The "Needs and Constraints" have the following meaning:

SME? refers to the size of the company. Any company with under 300 employee is usually considered an SME.

Days available refers to the time frame available or preferred for the assessment. Of course, methods that can be implemented in 1 day, can also be implemented in 3. As such, in case of no time constraints, selection should be made according to preferences regarding thoroughness (more lengthy methods tend to be more thorough).

Experts available refers to whether or not (usually external) Information Security and/or Risk Management experts or consultants are available for participation in the assessment

Security-Critical refers to whether or not the target of assessment is considered security-critical. Security-critical systems and critical infrastructures are systems where safety and security are paramount and are usually subject to much more thorough analysis which cover every possible Risk, no matter how unlikely.

An implicit assumption is made regarding the purpose of the Risk Assessment. The output of the Risk Assessment can be required for certification, auditing, legal compliance or even deciding about the adoption of a new technology. However, considering the scope of this thesis, as well as the Inclusion and Exclusion Criteria defined in Section 3.2, we assume that Guidelines are to be used by an organization whose main use for the Risk Assessment is security-decision-support for chief security officers or other relevant management. Secondary goals are not excluded, but this can be viewed as a "pre-selected" Need.

It should be noted that for each rule, more than one method may be suitable. However, only one method should be selected, with the exception of the methods marked with a * (i.e. X*). These, as discussed in Section 3.5, are high-level methodologies, requiring a choice of a complementary more technical method in order to be implemented. As such, any such method should only be chosen in conjunction with a second method from the same rule (column) that is not marked with a *. Given no other requirements, need or constraints, and if only interested in RA, priority should be given to stand-alone methods (without *).

However, when selecting one of more recommended methods for a given set of needs and constraints, one should also take into consideration if compliance to (certain) international standards is required or beneficial. If this is the case, priority should be given to any suitable method that is also (part of) a relevant standard. This is usually the case with methods marked with a * and only in such circumstances should such methods be selected.

Finally, any choice of method should not be made final before consulting it's description from Section 3.4 in order to verify it is indeed compatible with any other requirements not present in Table 7.1.

7.1.1 Discussion

In the Decision Table, some rather restrictive rules seem to be present. That is, sets of needs and constraints that match no method or very few methods. However, this is explainable once we take a closer look at those particular rules.

First of all, Rules 1 and 3 require a Risk Assessment of a Security-Critical infrastructure or system in less than a day. Unfortunately, no methodology suitable for such system allows a complete, thorough analysis to be completed in less than a day, even with experts available (i.e. Rule 1). This is due to the fact that Security-Critical systems/infrastructures require a much more thorough analysis before they can be proven secure. Secondly, Rules 7 and 19 would require that a security critical infrastructure/system be analyzed in 1-3 days without any experts available, which is again impossible to achieve with any of the reviewed methodologies. Finally, rules 13-16 all require a Risk Assessment for a large company (>300 employees) to be completed in less than a day. No matter the Risk Assessment methodology chose, this is most likely an impossible task simply due to the intrinsic complexity involved in an analysis of such a large company.

Rules 2 and 4 simply require a full assessment to be completed in less than a day. While this seems doable, especially with experts/consultants at hand (i.e. Rule 2), most RA/RM methodologies are simply not designed to be implemented in such a short time due to intrinsic complexities. The only method that is designed to be implemented in such a short time, given proper guidance by an expert, is the FRAP (Facilitator-led Risk Assessment Process). In the case no experts are available, it can still be applied, given at least basic Information Security knowledge and skills of the team, but a more suitable candidate, due to it's simplicity, might be the SRA. It should be noted that the meaning derived from the table is not that availability of experts restricts the choice of the method. It is simply that in the case such experts are not available, it is *recommended* to select the SRA or FRAP, while in the case such experts are indeed

available, FRAP will yield more accurate and usable results.

Although Rule 20 requires an assessment of a non-critical infrastructure/system within 1-3 days, it does so without availability of experts and for a large company. The only method designed for specifically for such scenarios is Intel's TARA. However, the method is not very thorough and will only identify the most serious risks.

DECISION TABLE	**Rules**																							
Needs & Constraints:	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
SME?	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	N	N	N	N	N	N	N	N	N	N	N
Days available	<1	<1	<1	<1	1-3	1-3	1-3	1-3	>3	>3	>3	>3	<1	<1	<1	<1	1-3	1-3	1-3	1-3	>3	>3	>3	>3
Experts available?	Y	Y	N	N	Y	Y	N	N	Y	Y	N	N	Y	Y	N	N	Y	Y	N	N	Y	Y	N	N
Security-critical?	Y	N	Y	N	Y	N	Y	N	Y	N	Y	N	Y	N	Y	N	Y	N	Y	N	Y	N	Y	N
Suitable Method:																								
AS/NZS 4346					X*	X*			X*	X*	X*	X*					X*	X*			X*	X*	X*	X*
CORAS									X	X											X	X		
Cramm																					X			
Ebios					X	X		X	X	X	X	X					X	X			X	X	X	X
FAIR								X				X												X
FRAP		X		X																				
ISO/IEC 27002:2005					X*	X*			X*	X*	X*	X*					X*	X*			X*	X*	X*	X*
ISO/IEC 27005:2011					X*	X*			X*	X*	X*	X*					X*	X*			X*	X*	X*	X*
IT-Grundschutz					X	X			X	X							X	X			X	X		
Magerit					X	X		X	X	X	X	X					X	X			X	X	X	X
Mehari																		X				X		X
Octave								X			X	X										X	X	
Risk IT					X*	X*			X*	X*	X*	X*					X*	X*			X*	X*	X*	X*
Structured Risk Analysis				X				X																
TARA								X												X				

Table 7.1: Decision table for selecting the most suitable RA method(s)

Chapter 8

Conclusions and recommendations

With the rise of the need to properly secure Information Systems has come a rise in the number and diversity of methodologies and tools to help achieve this. From national regulations to international standards and from third-party tools to Risk Management frameworks, this multitude of resources can be confusing for a company seeking to improve their information security. However, the applicability and benefits offered by each can be traced back to their original context and purpose.

In this document, a total of 14 Methodologies, 25 Tools and 7 Conceptual Models have been analyzed, described and reviewed in order to provide at least basic information regarding each of the vast amount of instruments available for conducting and supporting Risk Assessments. Furthermore, comparisons and cross-comparisons have been conducted and guidelines have been designed in order to facilitate the selection process an organization might have to go through when it decides that a Risk Assessment is required or might bring added value and security to their business. Finally, a series of conclusions can be drawn based on this work. These conclusions are grouped in the following sub-sections.

8.1 Risk Assessment

Some methodologies are designed for security-critical systems, while others are created with certification in mind. Some tools are expensive and can only be used by experts while others are free and easy to use. Some frameworks are overly complex and only suitable for large project and organizations while others can be implemented by a few skilled employees. Such criteria can be used to not only classify and understand the scope, applicability and benefits offered by each methodology, framework and tool, but also as indicators for choosing the most appropriate resource for any business environment and protection requirements. As such, guidelines, similar to the ones introduced in Section 7.1, can be designed and used to shed some light on the plethora of Risk Assessment and Risk Management frameworks, methods and tools.

One particular framework sets out from the rest. This is the ISO/IEC set of Information Security standards. The current documents with relevancy to this topic are: ISO/IEC 13335-1. ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27005. ISO/IEC 13335-1 described Risk at a conceptual level, 27001 is solely used for certification, and ISO/IEC 27002 and 27005 go into more details regarding implementing and maintaining a Information Security Risk Management,

including how to perform Risk Assessments. All these documents form a central core to which most other tools and methodologies refer or comply to. This is possible also due to the high level of abstraction the documents tend to maintain to order to allow a broader spectrum of applicability. As such, while these standards can be used to show official compliance, they are less relevant when the goal of the Security or Risk Assessment is different from this. In such situations, lower granularity is required in the descriptions of the analysis steps. This is offered by other third-party tools and methods. Of course, a hybrid solution is achieved in practice, where the high-level standards are used in conjunction with compatible implementation-level tools or more technical methodologies. In this way, desired output can be extracted from the Risk Assessment, while possibilities for certification, for showing compliance to certain rules/regulations or for performing standardized audits still remain, while also enjoying the benefits of the up-to-date, internationally sanctioned catalogs and good practices contained within the standards.

8.2 Conceptual models of Risk

Underlying most methodologies is either a generic or custom conceptual model of Risk. Differences can be seen in the way Risk and related concepts are defined and related to each other, as well as in the way Risk it-self is decomposed. The number, naming and importance of factors driving Risk, as well as the way these factors are computed in order to evaluate Risk Levels differ from one framework to the other. While some might use different names for the same concept or factor, a set of fundamental entities seem to be present in all of them: Threat, Asset, Vulnerability and of course, Attack. Each framework, and even individual methodologies disagree with regard to the attributes that are relevant for each entity, as well as how these factors can be operationalized and measured.

One other notable conclusion is that most Information Security Risk Assessment methods employ a Likelihood x Impact fundamental decomposition of Risk. Variations arise in the further decomposition of these two factors and the metrics used to estimate them. While models seem to be very closely related to the $Likelihood(Threat, Asset) \otimes Impact(Threat, Asset)$ interpretation of Risk, the concept of Vulnerability is always being taken into consideration, usually as one of the factors driving Likelihood. Thus, it seems that the basic, and most common interpretation of Risk within the field of IT is closely related to the Class 1 methodologies (as defined in Section 2.3.1). This approach stems from the traditional interpretation of Risk, outside of the IT field. However, even in general Risk Management, this approach is mostly recommended when several risks need to be evaluated in order to compare and prioritize them and does not give a good indication of absolute Risk. This is due to the fact when estimating Likelihood as probability or frequency, a certain time-frame is implied. For example: "probability of event taking place (within a year)" or "number of occurrences of event (per year)". The issue here stems from the fact that this time-frame is not always constant and sometimes not even made explicit thus creating a threat to the reproducibility of the results. Even when this is made explicit, catastrophic events make the issue of choosing the right time period in the interpretation of Likelihood as probability even more difficult: the probability of a fire destroying the archive servers within a year is very low, but within the lifetime of the infrastructure it is significant.

The ISO/IEC conceptual model of Risk mostly described in ISO/IEC 13335-1:2004, that supports all other ISO Information Security standards in the 2700x series is the most widely accepted model, and most tools and methodlogies are compatible to it and at least one 2700x RA/RM standard. It is also the most abstract one, described at a high-level with lack of technical details.

8.3 Risk Assessment tools

While a large number of methodologies that can be used to perform Information Security Risk Assessments, the number of tools that can be used in conjunction with these methodologies is even larger. With tools falling into three categories depending on their relation to a particular methodology (independent, generic or specialized), it is hard to identify what exactly are the differences between two tool falling in the same category. As such, tools should be chosen after all possible criteria have been decided upon, and the choice of RA methodology has been narrowed down as much as possible. Then, the list of functionalities can be used in conjunction with the security requirements, the skills and knowledge of the analysis team and financial considerations to decide towards a particular tool. One notable observation is that all generic tools and even some of the specialized tools are compatible with the ISO/IEC Information Security standards (especially 13335-1 and 27001).

8.4 Relationship between Risk Assessments and Security Requirements

Throughout the document, the relationship between a Risk Assessment and so-called Security Requirements is often mentioned. IT Security Requirements consist of functional and non-functional requirements that should be satisfied in order to achieve desired level of Security. In Section 2.3, I claim that the output of a RA can be used to derive Security Requirements for the overall Risk Management process. In Section 2.3.1, I define Class 2 Risk Assessments as evaluating Risk with regard to the Impact a Threat may have on given Security Requirements.

The meaning of the relationship is different, and we can identify three types of relationship possible between an RA and Security Requirements:

1. The output of an RA, especially the findings regarding asset values and threats, can be used within the Risk Management process as a base for eliciting new Security Requirements. If for example, the RA reveals that a certain database is at a high risk of being compromised via one of it's interfaces we might define a Security Requirement such as: "interface X of database Y should be protected against SQL injection". It is then up to the planning activity of the Risk Management process to implement the requirement(s).

2. If there exist security requirements, either defined by stakeholder or within regulation or standards, that the target of assessment must comply to, a Class 2 RA can be used to evaluate the Risk related to the possible compromise of these requirements. In this case, requirements are assumed to exist before-hand, and we are interested in how various Threats might invalidate these requirements. For example, HIPAA requires that "access to EPHI (Electronic Protected Health Information) must be restricted to employees who have a need for it to complete their job functions". We might then employ a Class 2 Risk Assessment to identify and evaluate the Risks related to an insider gaining access to an EPHI record he does not require do do his job.

3. A third type of relationship can be described that is actually a specific case of the previous type. Again, a Class 2 RA can be used for what is known as a "Gap Analysis". In this case, we are interested in identifying how the implementation of a system deviates from a set of pre-existing Security Requirements. The difference is, in this case we are not trying to show compliance, but instead we are trying to identify these deviations and evaluate the Risks that they pose for the IS. We might then choose to ignore or mitigate these Risks,

based on their evaluated level(s). For example, a company might desire to compare their Information Security policies and mechanisms to a more strict standard, like ISO 27001, that they are not required to comply to. As such, they might employ a Class 2 RA to evaluate the risks posed by the identified "gaps" between their Security Policy and the one described in the standard.

Bibliography

[1] Information technology – Security techniques – Management of information and communications technology security – Part 1: Concepts and models for information and communications technology security management, 2001.

[2] Information technology – Security techniques – Code of practice for information security management, 2005.

[3] Information technology – Security techniques – Code of practice for information security management, 2005.

[4] Information technology – Security techniques – Information security management systems – Requirements, 2005.

[5] Information technology – Security techniques – Evaluation criteria for IT security – Part 1: Introduction and general model, 2006.

[6] Information technology – Security techniques – Information security risk management, 2011.

[7] J.O. Aagedal, F. den Braber, T. Dimitrakos, B.A. Gran, D. Raptis, and K. Stolen. Model-based risk assessment to improve enterprise security. In *Enterprise Distributed Object Computing Conference, 2002. EDOC '02. Proceedings. Sixth International*, pages 51–62, 2002.

[8] A-SIT Austria. *Österreichisches Informationssicherheitshandbuch*. Austrian IT-Security Handbook. Chief Information Office in the Federal Chancellery, 2013.

[9] Armaghan Behnia, Rafhana Abd Rashid, and Junaid Ahsenali Chaudhry. A survey of information security risk analysis methods. February 2012.

[10] German BSI. Bsi standards 100-1, 100-2, 100-3, 100-4. https://www.bsi.bund.de/EN/Publications/BSIStandards/standards.html, 2013.

[11] A. Calder and S.G. Watkins. *Information Security Risk Management for Iso27001/Iso17799*. It Governance Ltd, 2010.

[12] Lizzie Coles-Kemp and Richard E. Overill. On the role of the facilitator in information security risk assessment. *Journal in Computer Virology*, 3(2):143–148, 2007.

[13] Central Computing and Telecommunications Agency (CCTA) of the United Kingdom. How cramm works. http://www.cramm.com/, 2011.

[14] CLUSIF (Club de la Sécurité de l'Information Français). Marion: Méthodologie d'analyse des risques informatiques et d'optimisation par niveau, 1998.

[15] CLUSIF (Club de la Sécurité de l'Information Français). Mehari 2010: Risk analysis and treatment guide. http://www.clusif.asso.fr/fr/production/ouvrages/pdf/MEHARI-2010-Principles-Specifications.pdf, August 2010.

[16] CLUSIF (Club de la Sécurité de l'Information Français). Mehari: Information risk analysis and management methodology. http://www.clusif.asso.fr/en/production/mehari/index.asp, 2010.

[17] Morrison M. Deladrière, A. The risk management challenge. http://www.bankingfinance.be/40915/default.aspx, 2010.

[18] Advies en Coördinatiepunt Informatiebeveiliging. *Handleiding afhankelijkheids- en kwetsbaarheidsanalyse: stappenplan voor de uitvoering van een A & K-analyse : werkdocument.*

[19] The OWASP Foundation. The owasp risk rating methodlogy. https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology, accessed on 9.06.2013.

[20] The OWASP Foundation. Threat risk modeling. https://www.owasp.org/index.php/Threat_Risk_Modeling,.

[21] GAO/AIMD-00-33. Information security risk assessment: Practices of leading organizations. Technical report, US Government.

[22] The Open Group. Requirements for Risk Assessment Methodologies. https://www2.opengroup.org/ogsys/jsp/publications/PublicationDetails.jsp?publicationid=12158, accessed on 17.03.2013, January 2009.

[23] The Open Group. *Technical Standard to Risk Taxonomy.* Number C081. January 2009.

[24] The Open Group. *Technical Guide: Fair - ISO/IEC 27005 Cookbook.* Number C103. October 2010.

[25] S.H. Houmb. *Decision Support for Choice of Security Solution: The Aspect-Oriented Risk Driven Development (AORDD) Framework.* PhD thesis, Norwegian University of Science and Technology, Trondheim, November 2007.

[26] D.W. Hubbard. *The Failure of Risk Management: Why It's Broken and How to Fix It.* Wiley, 2009.

[27] IT Governance Institute. *Cobit 4.1.* ISA, 2007.

[28] Isaca. *The risk IT framework.* Risk IT. Information Systems Audit and Control Association, 2009.

[29] Information Security Forum (ISF). Tools and methodologies. https://www.securityforum.org/whatwedo/publictools/#anchor5tpsat, 2013.

[30] Task Group IST-049. Improving common security risk analysis. Technical Report RTO-TR-IST-049, NATO Science and Technology Organization, September 2008.

[31] Angelika Jaschob and Lydia Tsintsifa. It-grundschutz: Two-tier risk assessment for a higher efficiency in it security management. In *ISSE 2006 — Securing Electronic Busines Processes*, pages 95–101. Vieweg, 2006.

[32] Michael Dunner Srinath Vasireddy Ray Escamilla J.D. Meier, Alex Mackman and Anandha Murukan. Improving web application security: Threats and countermeasures. http://msdn.microsoft.com/en-us/library/ff649874.aspx, 2010.

[33] Jack A. Jones. An Introduction to Factor Analysis of Information Risk (FAIR). http://riskmanagementinsight.com/media/documents/FAIR_Introduction.pdf, accessed on 16.03.2013, 2005.

[34] J. Kouns and D. Minoli. *Information Technology Risk Management in Enterprise Environments: A Review of Industry Practices and a Practical Guide to Risk Management Teams*. Wiley, 2010.

[35] Risk Management Insight LLC. *FAIR (FACTOR ANALYSIS OF INFORMATION RISK) Basic Risk Assessment Guide*. Risk Management Insight LLC, 2006.

[36] Risk Management Insight LLC. *FAIRLite High-Level Description*. Risk Management Insight LLC, 2010.

[37] M.S. Lund, B. Solhaug, and K. St2len. *Model-driven risk analysis*. Springer Berlin Heidelberg, 2011.

[38] Neil A. McEvoy and Andrew Whitcombe. Structured risk analysis. In *Proceedings of the International Conference on Infrastructure Security*, InfraSec '02, pages 88–103, London, UK, UK, 2002. Springer-Verlag.

[39] Agence nationale de la sécurité des systèmes d'information. Ebios 2010 - expression of needs and identification of security objectives. http://www.ssi.gouv.fr/en/the-anssi/publications-109/methods-to-achieve-iss/ebios-2010-expression-of-needs-and-identification-of-security-objectives.html, 2010.

[40] European Network and Information Security Agency. Introduction (risk management). http://www.enisa.europa.eu/activities/risk-management/current-risk/risk-management-inventory/introduction, February 2013.

[41] European Network and Information Security Agency. Inventory of risk management / risk assessment methods. http://rm-inv.enisa.europa.eu/methods, February 2013.

[42] European Network and Information Security Agency. Inventory of risk management / risk assessment tools. http://rm-inv.enisa.europa.eu/tools, February 2013.

[43] Technical Department of ENISA Section Risk Management. Risk management: Implementation principles and inventories for risk management/risk assessment methods and tools. Technical report, ENISA.

[44] Portughese Ministry of Public Administration. *MAGERIT - version 2. Methodology for Information Systems Risk Analysis and Management*, volume Book 1 - The Method. MINISTERIO DE ADMINISTRACIONES PÚBLICAS, 2006.

[45] Portughese Ministry of Public Administration. *MAGERIT - version 2. Methodology for Information Systems Risk Analysis and Management*, volume Book 3 - Catalogue of elements. MINISTERIO DE ADMINISTRACIONES PÚBLICAS, 2006.

[46] Portughese Ministry of Public Administration. *MAGERIT - version 2. Methodology for Information Systems Risk Analysis and Management*, volume Book 3 - Techniques. MINISTERIO DE ADMINISTRACIONES PÚBLICAS, 2006.

[47] Thomas Peltier. Effective risk analysis. In *23rd National information Systems Security Conference*.

[48] Thomas R. Peltier. *Facilitated Risk Analysis Process (FRAP)*, volume DATA SECURITY MANAGEMENT. Auerbach Publications.

[49] T.R. Peltier. *Information Security Risk Analysis, Second Edition*. Taylor & Francis, 2005.

[50] Dimitris Raptis, Theodosis Dimitrakos, Bjørn Axel Gran, and Ketil Stølen. The coras approach for model-based risk management applied to e-commerce domain. In Borka Jerman-Blazic and Tomaz Klobucar, editors, *Communications and Multimedia Security*, volume 228 of *IFIP Conference Proceedings*, pages 169–181. Kluwer, 2002.

[51] Matthew Rosenquist. Prioritizing information security risks with threat agent risk assessment. "http://www.communities.intel.com/servlet/JiveServlet/download/4693-1-3205/Prioritizing_Info_Security_Risks_with_TARA.pdf", December 2009.

[52] Gary Stoneburner, Alice Y. Goguen, and Alexis Feringa. Sp 800-30. risk management guide for information technology systems. Technical report, Gaithersburg, MD, United States, 2002.

[53] A. Syalim, Y. Hori, and K. Sakurai. Comparison of risk analysis methods: Mehari, magerit, nist800-30 and microsoft's security management guide. In *Availability, Reliability and Security, 2009. ARES '09. International Conference on*, pages 726–731, 2009.

[54] CERT (Computer Emergency Response Team). Octave® (operationally critical threat, asset, and vulnerability evaluationsm). http://www.cert.org/octave/, 2008.

[55] Anuj Tewari. Comparison between iso 27005, octave & nist sp 800-30. http://sisainfosec.com/blog/comparison-between-iso-27005-octave-nist-sp-800-30-2/, accessed on 30.06.2013, February 2013.

[56] J.R. Vacca. *Computer and Information Security Handbook*. Morgan Kaufmann series in computer security. Elsevier Science, 2009.

[57] Bob Violino. It risk assessment frameworks: real-world experience. http://www.csoonline.com/article/592525/it-risk-assessment-frameworks-real-world-experience, May 2010.

[58] Vishal Visintine. Vishal visintine. GSEC Practical Version 1.4b, SANS Institute.

[59] Zeki Yazar. A qualitative risk analysis and management tool–cramm. *SANS InfoSec Reading Room White Paper*, 2002.

[60] Emmanuele Zambon, Sandro Etalle, Roel J. Wieringa, and Pieter Hartel. Model-based qualitative risk assessment for availability of it infrastructures. *Softw. Syst. Model.*, 10(4):553–580, October 2011.

[61] Standards New Zealand. *Risk Management*. Australian/New Zealand Standard. Standards Australia International and Standards New Zealand, as/nzs 4360:2004 edition, 2004.

[62] Standards New Zealand. *Risk Management - Principles and guidelines.* Australian/New Zealand Standard. Standards Australia International and Standards New Zealand, as/nzs 31000:2009 edition, 2009.

Appendix A

Table of RA Methods and their characteristics

On the next page, a table containing all the RA methods mentioned in this thesis (including the excluded ones) is presented. For each method, all known characteristics are listed. Information that is not available or has been skipped due to the method being excluded from the analysis is marked with N/A.

The RA phases are the ones described in Section 2.3.1:

1. Context Establishment
2. Risk Identification
3. Risk Analysis
4. Risk Evaluation

The User types are:

M anagement - Guidelines for RA are given at a very generic level, suitable mostly for managers

O perational - Guidelines for RA contain enough details for planning the actual implementation and are suitable for most types of users

T echnical - Guidelines for RA are very specific, including technical, organizational, physical and human aspects of IT security and are suitable for users concerned with the actual implementation.

Method name	Excl. criteria	Class	Quant. or Qual.	Sponsor	Focus	RA phases supported				Release date		Price	Spread		Users				Supporting tools		Matching conceptual model	Stand-alone ?	Target organization		
						1	2	3	4	First v.	Latest v.		EU	Non-EU	M	O	T	Skill	Paid	Free			Gov agency	Large company	SME
AS/NZS 4360	-	Class 5	Both	Public	RM	X	X	X	X	1995	2004	€ 90	N/A	AS, NZS	X	-	-	Standard	CCS Risk Manager, Countermeasures, Modulo Risk Manager, Proteus Enterprise, Resolver Ballot	-	AS/NZS 4360 (31000)	No	X	X	X
Austrian IT Security Handbook	E-3	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
COBIT	E-5	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
CORAS	-	Class 5	Both	Public	RA	X	X	X	X	2003	2011	€ 95	?	?	X	X	X	Standard	-	CORAS Tool	AS/NZS 4360 (31000)	Yes	X	X	X
Cramm	-	Class 1	Qualitative	Public	RA	-	X	X	X	1985	2003	800 - 3000	Many	Many	X	X	X	Specialist	CRAMM expert, CRAMM express	-	ISO 13335-1	Yes	X	X	-
Dutch A&K Analysis	E-3	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Ebios	-	Class 2	Qualitative	Public + Private	RA	-	X	X	X	1995	2004	Free	Many	Many	X	X	-	Standard		Ebios tool	ISO 13335-1	Yes	X	X	X
FAIR	-	Class 1	Both	Private	RA	-	X	X	X	2001	2009	Free	Few	USA, CN	X	X	-	Basic	MS Excel	-	FAIR, ISO 13335-1, Open Group	Yes	X	X	X
FRAP	-	Class 3	Qualitative	Private	RA	-	X	X	X	2001	2005	Free	N/A	USA, CN	X	X	-	Basic	Any	Any	Any	No	-	-	X
ISAMM	E-2, E-3	Class 3	Quantitative	Private	N/A	-	X	X	X	2002			BE, FR, DE, IR, IT, LU, PT, ES, NL, UK	CN, SE, CH, TH	X	X	-	Standard	ISAMM Client tool	ISAMM Consultant tool	N/A	N/A	X	X	X
ISF Methods	E-2	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
ISO/IEC 15408:2006	E-1, E-4	N/A	N/A	N/A	RM	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	ISO 13335-1	No	N/A	N/A	N/A
ISO/IEC 27001:2005 (incorporates BS 7799-2)	E-1	N/A	Qualitative	Public	RM	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	ISO 13335-1	No	N/A	N/A	N/A
ISO/IEC 27002:2005 (formerly 17799:2000, incorporates BS 7799-1)	-	N/A	Qualitative	Public	RM	-	X	-	-	2000	2005	€ 200	Many	Many	X	-	-	Standard	CCS Risk Manager, Countermeasures, Modulo Risk Manager, Proteus Enterprise, Resolver Ballot, Risk Watch	Ebios tool	ISO 13335-1	No	X	X	X

Method name	Excl. criteria	Class	Quant. or Qual.	Sponsor	Focus	RA phases supported				Release date		Price	Spread		Users				Supporting tools		Matching conceptual model	Stand-alone ?	Target organization		
						1	2	3	4	First v.	Latest v.		EU	Non-EU	M	O	T	Skill	Paid	Free			Gov agency	Large company	SME
ISO/IEC 27005:2011 (includes ISO 13335-3/4)	-	Class 1	Both	Public	RM	-	X	X	X	1998	2011	€ 100	Many	Many	X	-	-	Standard	CCS Risk Manager, Countermeasures, Modulo Risk Manager, Proteus Enterprise, Resolver Ballot	Ebios tool	ISO 13335-1	No	X	X	X
IT-Grundschutz	-	Class 5	Qualitative	Public	RM	-	X	X	X	1994	2005	Free	Many	-	X	-	-	Standard	BSI - GSTOOl, HiScout SME, SAVe, IGS-Doku, SecuMax, Baseline-Tool, PC-Checkheft	GSTOOL (free for public authorities)	ISO 13335-1	Yes	X	X	X
Magerit	-	Class 1	Both	Public	RA	-	X	X	X	1997	2005	Free	Many	Many	X	-	-	Standard	EAR	PILAR	ISO 13335-1	Yes	X	X	X
Marion	E-3	N/A		N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Mehari	-	Class 1	Qualitative	Private	RM	X	X	X	X	1998	2010	Open-source	Many	Many	X	X	X	Standard	MEHARI 2010 basic tool	RISICARE	ISO 13335-1	Yes	X	X	-
MIGRA	E-2	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
NIST SP800-30	e-4, opposes I-3	Class 1	Qualitative		N/A	-	X	X	X	2002	2002	Free	-	USA	-	X	X	Standard	N/A	N/A	N/A	N/A	X	X	X
Octave	-	Class 4	Qualitative	Public	RA/RM	-	X	X	X	1999	2005	Free	-	USA	X	X	-	Standard	Resolver Ballot	-	None	Yes	X	X	X
Risk IT	-	Class 1	Qualitative	Public	RM	X	X	-	X	2009	2009	Free	N/A	USA	-	X	-	Standard	CCS Risk Manager, Countermeasures, Modulo Risk Manager, Proteus Enterprise, Resolver Ballot	-	ISO 31000, FAIR	No	X	X	X
Structured Risk Analysis	-	Class 1	Both	Private	RA	-	X	X	X	2002	2002	Free	UK	-	-	X	-	Basic	-	Ms Excel	SRA	Yes	-	-	X
TARA	-	Class 1	Both	Private	RA	-	X	X	X	2010	2010	Free	N/A	USA	X	X	-	Basic	-	-	None	Yes	X	X	X

Table A.1: RA/RM methods and their complete set of characteristics

Appendix B

Intermediary table used for construction of the Decision Table

Table B.1 was constructed as an intermediary table used for the construction of the Decision Table in Chapter 7.

The meaning of the symbols are:

- "-" means "don't care"
- Y means "yes"
- N means "no".
- <1 means less than one day
- 1-3 means one to three days
- >3 means more four days or more

The table represents a mapping between each RA/RM method and reach relevant context-dependent need or constraint.

Method name	Security-critical?	Experts available?	Days available	SME?
AS/NZS 4360	-	-	1-3[1], >3	-
CORAS	-	Y	>3	-
Cramm	Y	Y	>3	N
Ebios	-	-	1-3[2], >3	-
FAIR	N	-	1-3[2], >3	-
FRAP	N	N	<1	Y
ISO/IEC 27002:2005	-	-	1-3[1], >3	-
ISO/IEC 27005:2011	-	-	1-3[1], >3	-
IT-Grundschutz	-	Y	1-3, >3	-
Magerit	-	-	1-3[2], >3	-
Mehari	N	-	1-3, >3	N
Octave	-	N	1-3[2], >3	-
Risk IT	-	-	1-3, >3	-
Structured Risk Analysis	N	N	<1, 1-3	Y
TARA	N	N	1-3	-

Table B.1: Intermediary table used for construction of Decision Table

[1] >3 is normal, 1-3 possible with experts available
[2] >3 is normal, 1-3 possible with experts OR for non-security-critical SME

Appendix C

List of Acronyms

COBIT Control Objectives for Information and Related Technology

CRAMM Central Communication and Telecommunication Agency's Risk Analysis and Management Method

EBIOS Expression des Besoins et Identification des Objectifs de Sécurité

FAIR Factor Analysis of Information Risk

FRAP Facilitator-led Risk Assessment Process

MEHARI Methode Harmonisee d'Analyse de Risques

MSAT Microsoft Security Assessment Tool

MTM Microsoft Threat Model

IEC International Electrotechnical Commission

ISMS Information Security Management System

IS Information System

ISO International Standards Organization

OCTAVE Operationally Critical Threat, Asset, and Vulnerability Evaluation

OWASP Open Web Application Security Project

RA Risk Assessment

RM Risk Management

ROSI Return On Security Investment

SME Small or Medium Enterprise

TARA Threat Agent Risk Assessment

TREsPASS Technology-supported Risk Estimation by Predictive Assessment of Socio-technical Security

SRA Structured Risk Analysis