Residual Risk Management

A Quantitative Approach to Information Security

by Jarno Roos

FACULTY
ELEKTROTECHNIEK, WISKUNDE EN INFORMATICA
/ MANAGEMENT AND GOVERNANCE

MASTER
BUSINESS AND INFORMATION TECHNOLOGY

TRACK
ARCHITECTURES

University of Twente
Enschede - The Netherlands

Master Thesis on:

Residual Risk Management

A Quantitative Approach to Information Security

Jarno Roos
s0015032

Supervision:
Dr. P.A.T. Van Eck
University of Twente
A. Morali Msc.
University of Twente
Dr. R.M. Müller
University of Twente
Ir. I. Sarica RE CISA
KPMG EDP Auditors N.V.

Version: 1.00
January 31, 2008

In dedication to my parents.

PREFACE

> The year is 1987, and N.A.S.A launches the last of America's deep space probes. In a freak mishap, Ranger 3 and it's pilot Captain William 'Buck' Rogers are blown out of their trajectory into an orbit which freezes his life support systems, and returns Buck Rogers to Earth five-hundred years later. *(Buck Rogers in the 25th century)*

Albeit somewhat less dramatic, and certainly with less visual effects and budget, I too embarked on a remarkable journey upon starting my graduation project. After a few enjoyable years living and studying at the University of Twente in a settlement called Enschede, I was to begin with the final phase of my curriculum in 2007.

My trajectory led me to another world where knowledge from research was applied to real life problems and I was introduced to the blue-ish world of KPMG. During my stay there, I found lots of people sharing my interests. During one of the many conversations, the ideas behind this thesis emerged. While staying in at KPMG, I was to research the possibilities to take a quantitative approach to information risk management. The people there showed a practical need to get more insight in, and control over the gap between their current and desired state of information risk.

Over the previous 8 months this has been my day filling occupation. This might seem a long time for an assignment that was originally planned to span 6 months, but in my experience, it was not. In the beginning of the project there were some administrative problems concerning supervision and available material which resulted in a relatively slow start. Looking back, a development that eventually increased the quality of this research and more importantly, made doing this research more enjoyable.

Omitting a story about the ups and downs in writing this thesis (many), the amount of consumed coffee (excessive) and my remaining social life because of work-filled days (little to none), I would like to thank a few people who helped me during my research. Time constraints combined with a feeling that a preface should not be an epos on itself, prohibit me from going into too much detail.

Firstly, I am grateful to my supervisors Ayse, Ismail, Pascal and Roland. Without their efforts I am sure I would never have come this far. This might sound obvious, but help should not be underestimated nor taken for granted.

Secondly, I would like to thank the people who gave their input and ideas on the thesis and/or helped me get the information I needed. This list specifically goes on and on, forcing me to make a random selection of people I want to thank. Here goes: Amongst others I thank Ruben de Wolf, Erik Rutkens, Hans de Jong, Erik Wisloff, Mounir el Khattabi, Dulcey Sprague, Sandro Etalle, Siv Hilde Houmb, Emmanuele Zambon, Ton Spil and Dieter Hoenke.

Additionally, I am thankful to the people who made the environment in which I wrote my thesis, a pleasant one. Family, Niko Vermeer, Robert-Jan de Boer, fellow KPMG thesis-writers and my colleagues of department E1 : Thank you.

Finally, as the proverbial ‘last-but-not-least’, the two people this thesis is dedicated to. No further explanation is needed, making it an ideal closing for this preface.

Jarno Roos

Amstelveen, January 31, 2008

“Je n’ai fait celle-ci plus longue que parce que je n’ai pas eu le loisir de la faire plus courte.”
(Blaise Pascal (1623-1662) - Les Lettres Provinciales)

EXECUTIVE SUMMARY

Companies have become increasingly dependent on the correct operation of their information and communication systems. While business environments become more complex and volatile, losses increase because of mismanagement of (information) security and because of companies failing to perform effective risk management [2, 122].

Managing this information risk is not just a matter of implementing ‘good practices’. Sometimes, more risk will be present than acceptable and additional countermeasures have to be chosen to bring the risk down to an acceptable level. This brings forward the need for a method that gives control over, and a more detailed insight in the residual information risk of an organisation.

This thesis focusses on a quantitative approach to residual risk management in contrast to a qualitative approach. Earlier generations of quantitative approaches had the drawbacks of being excessively complex, unable to deal with uncertainty and being highly dependent on the availability of (sparse) information. Failing to generate useful results because of these drawbacks, the quantitative approach got the bad reputation of being overly complex, resource intensive and giving incorrect claims of loss and damage. Nevertheless, the currently often used qualitative approaches do not give the desired results in all situations, indicating the need for a different approach.

By adding an applicable (quantitative) computational method to a suitable (qualitative) risk assessment methodology, we try to get insight in the usability of a quantitative approach in the current residual information risk management practice. By conducting expert interviews and by doing extensive literature review, requirements have been formulated on the applicability of a computational method and on the suitability of current risk assessment methodologies.

Computational Method

In this thesis we work towards a quantitative risk assessment approach using *annual loss expectancies* as suggested by Lenstra and Voss [66]. This approach does not require actual event distributions or consider complex interactions. It is based on the aggregation of expected losses done by simple summation. This simplicity makes it a flexible approach that can be easily adjusted to fit a practitioner's requirements.

We modified the annual loss expectancy model from Lenstra and Voss [66] by incorporating separate threat and vulnerability components. A working example is given showing how Bayesian networks can be used in our annual loss expectancy approach, in making decisions on mitigation plans and modelling scenarios. Risk mitigation is then transformed to a binary knapsack optimization problem, allowing the selection of an ‘optimal’ set of mitigation plans under a budgetary constraint. The

results get their meaning in relationship to each other, indicating a potential increase in information security relative to a starting situation.

Risk Assessment Methodology

Based on the requirements from both the interviews and the literature, a comparative framework has been constructed to make a comparison of different methodologies and select the ones most suitable for our cause. After 9 filter iterations, 5 suitable methodologies were found. In theory, CORAS, OSSTMM-RAV, SP800-30, SPARK and SPRINT would fit our requirements. In this thesis the SPARK methodology was chosen because of the availability of workable material and its extreme ease of use.

The SPARK methodology is analysed in more detail and a quantitative branch to the methodology, representing our annual loss expectancy approach, was added. During the process, a workflow document has been constructed, using UML 2.1 activity diagrams, on how to append this quantitative branch to a suitable risk assessment methodology.

Evaluation

The resulting quantitative risk assessment model has been put against a framework that helps in evaluating the appropriateness of the decision supporting model in specific situations. Additionally, the strengths and weaknesses of our approach are evaluated by discussing 7 guiding principles in relation to our model. The discussion of these 7 guiding principles, and the application of the framework to evaluate the quantitative risk assessment model and its characteristics, gives insight in the usability of the model and defines boundaries on the application of the model in practice.

Finally, the model is discussed once again in relation to the previously defined usability requirements. Merits and possible downsides of using a quantitative approach to residual information risk management are discussed.

Conclusion

We have shown the theoretical possibility of taking a quantitative approach to get insight in, and control over the residual information risk of an organisation. With carefully defined boundaries, and taking current limitations into account the quantitative information risk assessment can be a valuable addition to the organisation who desires this insight and control.

Limitations of the earlier generation quantitative models can mostly be overcome. Additional limitations are also introduced. Some of these limitations can be overcome by doing more research on the subject. Especially certain dependencies between model components are not present in the current model, but might be in future improvements. If it is proven that adding these dependencies will sufficiently increase the value of the model's output, modifications have to be made taking under careful consideration the balance between model simplicity and a faithful representation of (a complex) reality.

The initial requirements for taking our quantitative approach are low but are dependent on the complexity of the situation. As our model allows to reason under uncertainty, one has to understand the implications of uncertainty on the eventual accuracy of the results. Further research on this uncertainty and ways to increase accuracy (under uncertainty) are desired.

Further research also includes the actual testing of the presented model in real life situations. Empirical proof of the correctness of our approach and the compliance of our model to the requirements is desired along with more formal validation of the methods used. This way we can find out what changes are necessary to realistically represent reality and get high quality results supporting the information security decision making process.

MANAGEMENTSAMENVATTING

Organisaties worden steeds afhankelijker van goed werkende informatie- en communicatiemiddelen. Terwijl de omgeving van een organisatie alsmaar complexer en meer onderhevig aan veranderingen wordt, stijgen de gemaakte verliezen door slecht beheer van (informatie) beveiliging en een slechte staat van risicobeheersing [2, 122].

Management van informatie gerelateerde risico's is niet alleen maar een kwestie van het implementeren van bewezen bestaande oplossingen ('good practices'). Soms worden bepaalde risico's niet door de standaardoplossingen afgedekt en zijn er additionele controls nodig om het risico naar een acceptabel niveau te doen dalen. Hieruit ontstaat de vraag naar een aanpak die inzicht geeft in, en controle geeft over het restrisico van een organisatie m.b.t. de informatievoorziening.

Dit proefschrift beschouwt een kwantitatieve benadering voor het beheren van restrisico's. Dit in contrast met hedendaagse veelal kwalitatieve benaderingen. Vroegere generaties van de kwantitatieve benadering waren vaak bijzonder complex, konden slecht met onzekerheden omgaan en waren zeer afhankelijk van de beschikbaarheid van (lastig te verkrijgen) informatie. Deze problemen maakte de kwantitatieve benadering vaak onwerkbaar. Zodoende kwam de kwantitatieve benadering in een kwaad daglicht te staan. Helaas geeft de hedendaags veel gebruikte kwalitatieve aanpak niet altijd het gewenste resultaat, wat de noodzaak aanduidt naar alternatieven te zoeken

Door een toepasbaar rekenkundig model te combineren met een geschikte kwalitatieve methodologie, proberen we inzicht te verkrijgen in de bruikbaarheid van een kwantitatieve aanpak in de huidige staat van informatie risicobeheersing. Door middel van het voeren van expert interviews en het doen van een extensief literatuuronderzoek, zijn de termen 'toepasbaar rekenkundig model' en 'geschikte methodologie' gedefinieerd om zodoende een bruikbaar geïntegreerd model te kunnen creëren.

Rekenkundig Model

In dit proefschrift werken we richting een kwantitatieve aanpak gebruikmakend van verwachte jaarlijkse verliezen (annual loss expectancies) zoals wordt gesuggereerd door Lenstra and Voss [66].Deze methode beschouwt geen complexe componentinteracties of distributiefuncties van gebeurtenissen. De verwachte jaarlijkse verliezen worden geaggregeerd door simpele sommatie. De eenvoud van deze aanpak zorgt ervoor dat het gemakkelijk aan een situatie aangepast kan worden.

De aanpak van Lenstra and Voss [66] is aangepast om bedreigingen en kwetsbaarheden onafhankelijk van elkaar te kunnen modelleren, iets wat niet mogelijk is in het originele model. Een werkvoorbeeld is gegeven dat gebruik maakt van een Bayesiaans netwerk om de verwachte jaarlijkse verliezen te berekenen, beslissingen te ondersteunen m.b.t. door te voeren controls en om bepaalde scenario's te simuleren. Door gebruik te maken van een binair knapzakprobleem kunnen we een optimale set controls selecteren onder een bepaalde budgetbeperking. De resultaten verkrijgen hun betekenis onderling. Dat wil zeggen: een potentieel verhoogd beveiligingsniveau is altijd relatief met een startsituatie.

Risk Assessment Methodologie

Gebaseerd op de eisen verkregen uit de expert interviews en het literatuuronderzoek is een vergelijkend raamwerk geconstrueerd dat het mogelijk maakt verschillende Risk Assessment methodologieën met elkaar te vergelijken en de meest bruikbare methodologieën voor onze doeleinden te selecteren. Na 9 filter iteraties bleven 5 geschikte kwalitatieve methodologieën over: CORAS, OSSTMM-RAV, SP800-30, SPARK en SPRINT. Uiteindelijk is de keus gevallen op de SPARK methodologie gebaseerd op de hoeveelheid beschikbare informatie en het gebruiksgemak.

De SPARK methodologie is in detail geanalyseerd en een kwantitatieve stroming die gebruikt maakt van verwachte jaarlijkse verliezen, is aan de methodologie toegevoegd. Tijdens dit proces is een document bijgehouden wat gebruik maakt van UML 2.1 activiteitsdiagrammen om weer te geven hoe deze kwantitatieve stroming toe te voegen is aan geschikte methodologieën.

Evaluatie

Het uiteindelijke geïntegreerde model is tegen een raamwerkgehouden dat het mogelijk maakt de bruikbaarheid te evalueren van het model ter ondersteuning van beveiligingsbeslissingen. Ook worden de sterke en zwakke punten van het geïntegreerde model besproken aan de hand van 7 bruikbaarheidprincipes. De discussie van deze principes in combinatie met het raamwerk, geeft inzicht in de uiteindelijke bruikbaarheid van het geïntegreerde model en geeft de grenzen aan waarbinnen het model juist kan functioneren.

Afsluitend wordt het geïntegreerde model nogmaals tegen de eerder gedefinieerde bruikbaarheideisen gehouden. Plus- en minpunten van een kwantitatieve aanpak bij het beheren van (informatie) restrisico's wordt besproken.

Conclusie

In dit proefschrift hebben we laten zien dat het theoretisch mogelijk is gebruik te maken van een kwantitatieve aanpak om inzicht te verkrijgen in, en controle te krijgen over het restrisico van een organisatie met betrekking tot de informatievoorziening. Onder zorgvuldig vastgestelde beperkingen kan de gepresenteerde aanpak een waardevolle toevoeging zijn voor een organisatie die deze controle en inzicht wenst.

Beperkingen van de vroegere generatie modellen zijn veelal te overkomen. Ook worden er nieuwe beperkingen geïntroduceerd. Enkele van deze nieuwe beperkingen zullen kunnen worden opgelost door aanpassingen verkregen uit verdere studie. Vooral met betrekking tot bepaalde afhankelijkheden van componenten in het door ons gebruikte model is vervolgonderzoek mogelijk. Als wordt aangetoond dat door het toevoegen van dusdanig complexe afhankelijkheden de kwaliteit van de uitkomsten van het model zal toenemen, zal het model aangepast moeten worden om deze situatie weer te geven. De balans tussen de eenvoud van het model en de complexiteit van de realiteit moet niet uit het zicht verloren raken.

De eisen voor het gebruik van het model zijn aanvankelijk laag te noemen. Wel zijn ze sterk afhankelijk van de complexiteit van de situatie. Omdat ons model de mogelijkheid biedt onder een bepaalde maat van onzekerheid te redeneren is het zaak de implicaties van deze onzekerheid te begrijpen. Toekomstig onderzoek over onzekerheid in het model zal hier meer inzicht in kunnen geven.

Toekomstig onderzoek omvat ook het daadwerkelijke testen van het model in realistische situaties. Empirisch bewijs van juistheid en toepasbaarheid samen met een formele validatie van de correctheid van gebruikte methoden zullen de kwantitatieve aanpak in functionaliteit, kwaliteit en waarde doen toenemen.

CONTENTS

LIST OF FIGURES

LIST OF TABLES

List of Symbols

a	Application
$A(p)$	Set of (independent) applications used in process p
c	Cumulative Threat or CumThreat
$C(a)$	Set of (independent) cumulative threats affecting application a
d	Knapsack capacity
E_t	Characteristic signature of threat t
K	Set of Information Criteria
k	Information Criterion
L	Loss amount
L^{max}	Maximum expected loss amount
M	Allowed set of mitigation plans
m	Mitigation plan
P	Set of Business Processes
p	Business Process
$P(c)$	Cumulative threat potential
$P(c_m)$	Residual cumulative threat potential
$P(t)$	Probability that a threat, once present, successfully manifests itself
$P(v)$	Probability that a vulnerability, once present, is successfully exploited
p_i	Value of item i
Q_i	Set of risk mitigation plans for the ith CumThreat
R	Risk
R_{cur}	Overall quantitative current aggregated IS risk indicator
$R_{res}(M)$	Overall quantitative residual aggregated IS risk indicator after allowed mitigation plan set M
$S(z,c)$	Information security breach probability
T	Set of (independent) threats
t	Threat
T_k	CumThreat type toggle
V	Set of (independent) vulnerabilities
v	Vulnerability
w_i	Weight of item i
z	Security investment

CHAPTER 1

INTRODUCTION

Companies have become increasingly dependent on the correct operation of their information and communication systems. These systems are “outpacing material goods as the main source of economic value in post-industrial economies” according to Tillquist and Rodgers [121].

While business environments become more complex and volatile, losses increase because of mismanagement of (information) security and because of companies failing to perform effective risk management [2, 122]. Even though around the year 2002 figures seemed to indicate that information security was growing more mature, the latest figures indicate that this assumption was way too premature by again showing increased losses [91].

A recently published risk management survey by Deloitte & Touch LLP. underlines this trend toward a strategic approach to risk management [27]. The survey shows that the industry (financials in this case) is alert to this need for better risk management, but is still struggling to get a good grip on risk issues and processes (see: Fig. 1.1).

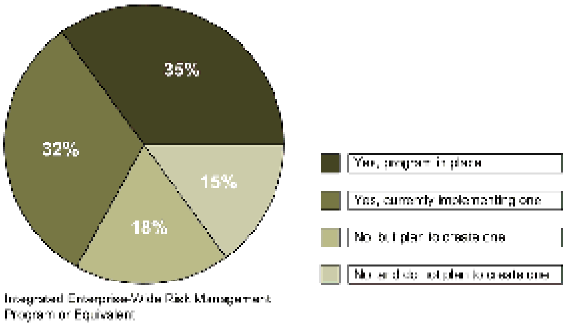


Figure 1.1: Deloitte & Touche survey result [27]

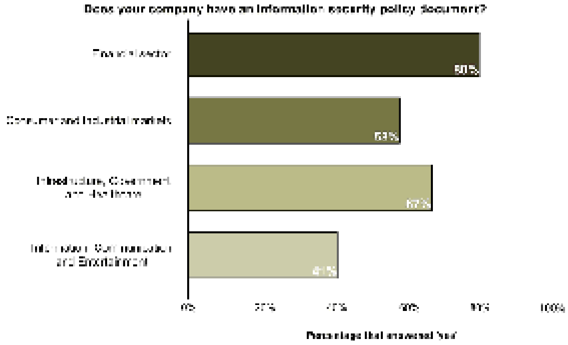


Figure 1.2: Information Security Management survey result [60]

The Pie-chart from Fig. 1.1 only addresses the Enterprise Risk Management programs in the financial sector, but this is not necessarily limiting. The financial sector has always been a pioneer in Enterprise Risk Management, meaning that other sectors score lower on the question answered in Fig. 1.1 [27].

Not surprising, taking into account the financials' Enterprise Risk Management position, is the position of the financial sector in the information security management practice (Fig. 1.2). Information security begins with a well thought-out policy, based on the risk analysis as stated above [62]. In an information security management survey done by KPMG in 2006 [59], 47% of the organisations questioned did *not* use risk analysis in determining their information security policy. Risk analysis has the reputation of being (overly) expensive and complex and needing professional practitioners to get useful results [104].

1.1 Facilitation

This research is facilitated by KPMG The Netherlands. They offer services in the fields of audit, tax and advisory to a broad group of 'major domestic and international companies' and 'medium-sized enterprises'. KPMG The Netherlands employs over 4000 people and is a member of KPMG International, the Swiss cooperative of which all the national KPMG organisations are a member.

KPMG ITA (IT Advisory), as part of Advisory Services, provides assurance and advisory services to assist clients, from all of the previously named sectors, in identifying risks and establishing appropriate controls and security measures arising from the use of information systems and technology.

KPMG ITA experiences an increased need for (information) risk analysis and advisory in the market. Because of an increased usage of information and communication systems within and between client organisations, the organisations become increasingly dependent on their correct working. So called 'information criteria' or 'reliability aspects' as availability, integrity and confidentiality are of importance in the every day practice of the organisation. Consequently, they need to be properly managed [81].

Another source of the increased need for (information) risk analysis and advisory, originates from several legislations. Increased losses by mismanagement of information security and companies failing to perform effective risk management forced legislators to react by introducing draconian laws (e.g. SOX and BASEL-*II*).

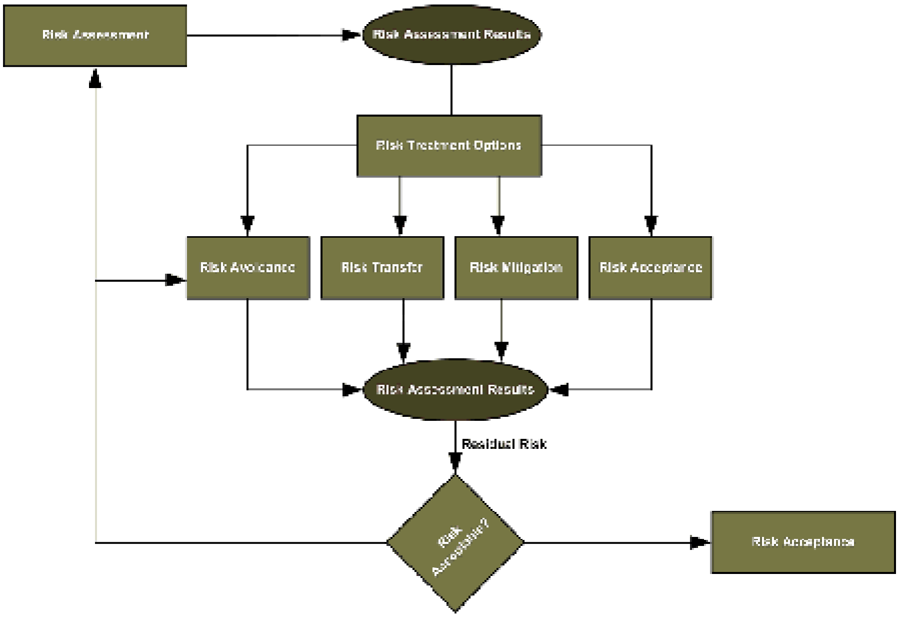


Figure 1.3: Risk Treatment Decision making Process, based on ISO/IEC TR 13335-3 [119]

1.2 Good Practices

Within the topic of IT Risk Assessment we see a great usage of so called 'good practices' and frameworks like ISO/IEC 27001:2005 [115], CobiT [49] and ITIL Security [79]. Companies want to know how they are performing, compared to others, with regard to information security. This 'gap analysis' compares a current situation (as-is) to a preferred situation or ambition (to-be) [86].

Chances are, however, that the implementation of the 'good practices' will only get an organisation to a certain point with respect to the management of risk, and more risk will be present than acceptable. We will define this remaining risk as being the *residual risk.* In a graphical representation as shown in Fig. 1.3 , the residual risk is the risk that remains after the risk assessment results, before the decision if that risk is acceptable.

KPMG ITA sees a need for a method that gives control over, and a more detailed insight in this particular gap, where controls originating from 'good practices' are put in place. KPMG ITA requires knowledge to facilitate this critical assessment on the gap. Closing the gap might help in the strategic alignment of business and IT(-security)[1] as first suggested by Henderson and Venkatraman [44].

1.3 Alignment

The strategic alignment model from Henderson and Venkatraman [44] can be seen in Fig. 1.4 . It identifies the need to specify two types of integration between business (IT demand) and IT domains (IT supply): Strategic fit (the link between the internal and external domain) and functional

[1] IT and ICT can be read interchangeably. Usage depends primarily on geographical location

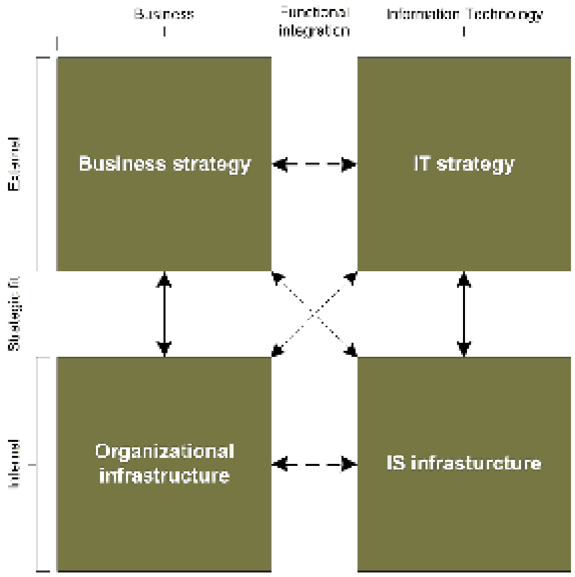


Figure 1.4: Strategic alignment model as stated by Henderson and Venkatraman [44]

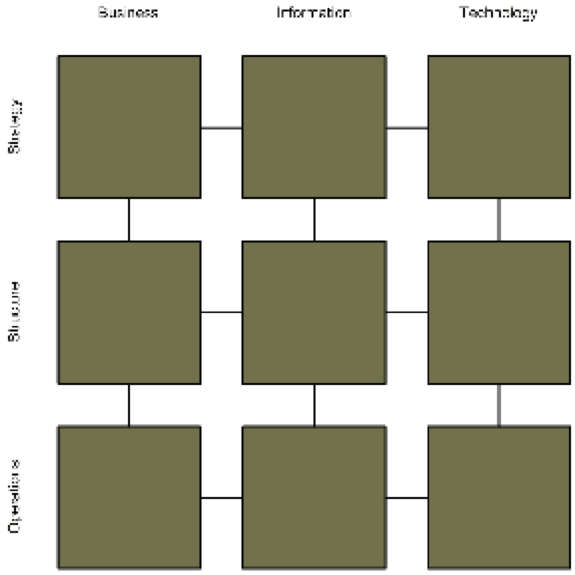


Figure 1.5: Information management integrative framework as described by Maes [68]

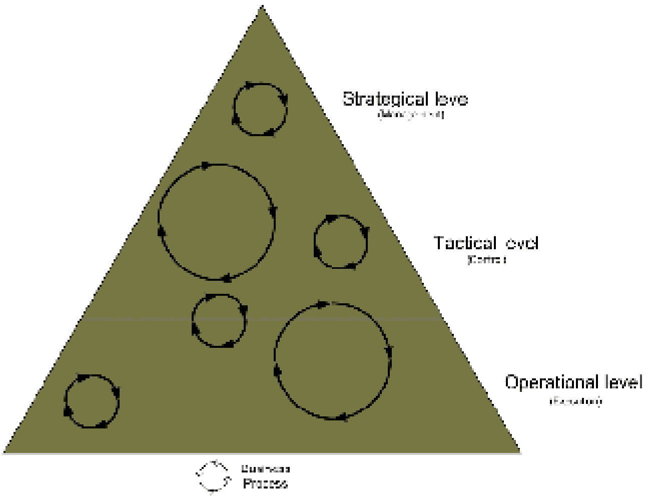


Figure 1.6: Information security on multiple levels of the organisation [81, 129]

integration (the link between business strategy and IT strategy and the link between organisational infrastructure and IS infrastructure). IT is transcending its traditional 'back office' role and is evolving toward a more strategic role [44].

A refinement of the strategic alignment model of Henderson and Venkatraman [44] (see: Fig. 1.4) is given by Maes [68]. Maes sees information security as part of the larger subject of 'information management. He extends the model as shown in Fig. 1.4 with a few information management specific domains (see: Fig. 1.5). The framework concerns strategic, structural and operational information-related issues (the vertical dimension) and relates the external and internal information and communication processes and their supporting technology to general business aspects (the horizontal dimension). The strategic integration and operational integration parts from the strategic alignment model from Henderson and Venkatraman [44] are kept but the added granularity in the model from Maes makes this version more usable in our information security management scenario.

Looking at the integrative framework(s), it is only a small step to realizing that information security actually is a large collection of processes performed on each level of the organisation. This is given a graphical representation in Fig. 1.6 . On a strategic level, information security is managed. On a tactical level information security is controlled and the actual process of information security is executed on an operational level [81, 129].

In a similar way, the horizontal dimension of the integrative framework indicates a direct mutual influence of business and IT functions [44]. The added middle column and row in the integrative framework of Maes, have been considered as dependent variables derived from adjacent columns and rows [69]. Maes et al. [69] go on defending that the added dimensions should be considered independently as they provide the 'glue' to a succesful alignment of the business and IT functions.

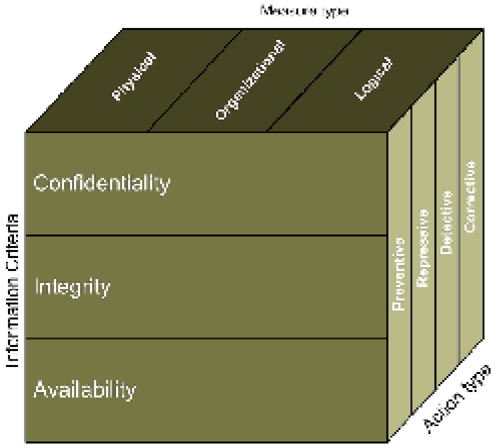


Figure 1.7: The Bautz-cube as adapted from Thiadens [120]

1.4 Security baselines and Risk Assessments

By issuing the right security measures, disruptions can be kept to a minimum. The problem lies in actually finding the 'right security measure' [87]. It depends on the situation whether to use security measures that minimize the likelihood of the threat occurring (*prevention*), or security measures that minimizes the threat's impact (*repression*). Directly linked to risk prevention and repression is the need for risk identification (*detection*) and risk amendment (*correction*)[16, 81]. Bautz attempts to summarize information this in the so called Bautz-cube Fig. 1.7 [100]. Bautz distinguishes information criteria (the reason for security), measure type (the nature of the measures) and the above named action types [120].

The previously discussed likelihood and impact are not given constants. Likelihood is influenced by many factors and impact can be direct and measurable, but also indirect and hard to measure [72]. This is why an exact calculation of the information risk experienced by an organisation is hard or even impossible. Somewhere along the line, approximations are made [37].

The more we get to know about the bigger picture, the closer we can come to an objective representation of the risk [37]. The alignment and integration of business and IT functions gave rise to processes that help in creating this bigger picture. Initially information security was more alchemy than science. It ventured between expert's gut feelings and limited scientific support [53, 103, 110]. With our better view on the bigger picture, we can find other ways to determine an organisation's information risk. When determined, countermeasures can be chosen to bring back the risk to an acceptable level [81].

Working towards an acceptable security level can be done in multiple ways [129]. A common approach is the use of so called security baselines. The security baseline is a collection of security measures that give a basic level of security on a variety of security criteria (see Fig. 1.8). Usually these baselines are directly linked to a special standard of practice. After this basic line of defence, some assets might require better protection which is achieved by introducing additional controls [105].

This brings us to the second approach, that of the risk assessment. Again, this subject can be divided

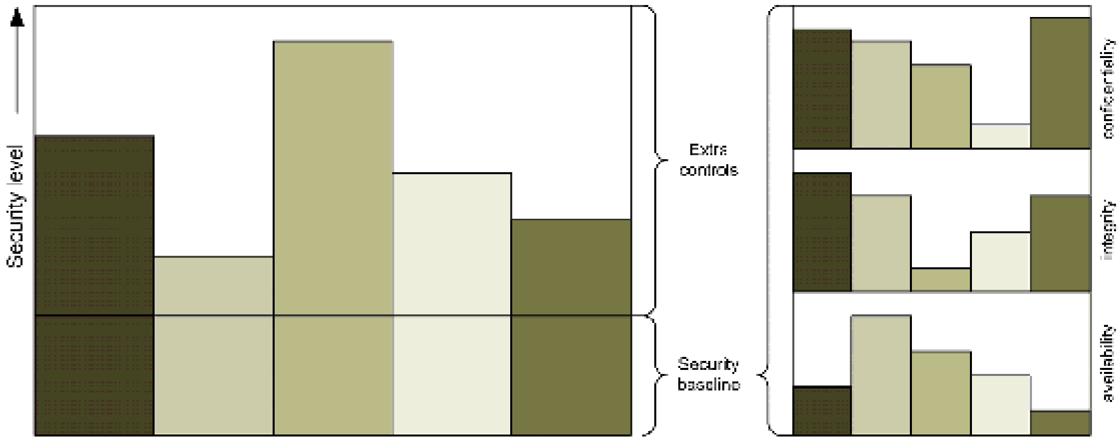


Figure 1.8: Security baseline and additional measures [129]

in roughly two subcategories [87]. A qualitative approach and a quantitative approach. Because of a variety of reasons, which will be explained later, initially qualitative approaches have had the preference of practitioners. The Qualitative approach gives a subjective view on the organisation's risk [103].

The quantitative approach uses actual figures to work towards an objective representation of the risk. The more information is available, and the higher the quality of this information, the better the representation will be [37]. Decisions to spend actual resources on hypothetical losses can then be made on actual figures instead of rough estimates [107].

CHAPTER 2

Research Design

In this chapter we intertwine the *conceptual design* and the *technical design* of the thesis. This is conform the method as provided by Verschuren and Doorewaard [126].

The conceptual design defines the content of the research by giving a clear definition of the research objectives (Section 2.1), the questions that need to be answered to reach the objectives (Section 2.2) and the framework in which the research is performed (Section 2.3).

The technical design addresses the strategy taken to come to the answers to our questions and reach our objectives. The research materials and strategy used to come to our answers are discussed in the separate phases of the research framework of Section 2.3 .

2.1 Research Objective

> *“Come to a quantitative approach that helps with getting insight in and control over the residual information risk of an organisation.”*

We started this section by giving a clear definition of the research objective. The research objective is very broad in itself. That is why it needs to be placed in context, and constraints have to be specified, in order to give the research the right scope.

In more detail, the goal of this research will be to create an understanding of the applicability of quantitative models in residual information risk management by projecting a computational method on an often used methodology for risk assessment. This will help the assessing organisation in *creating insight* in the available gap and creates a possibility for the organisation to *have more control* over it.

This high level research goal still leaves some room for interpretation. To ensure that the research will be useful for the audience and achievable within the predefined time limits, specific research questions are specified (Section 2.2) and the research framework is constructed (Section 2.3).

2.2 Research Questions

As this research focuses on reaching the research goal and validating this possible solution in terms of usability, the problem first has to be analysed. The main problem is practical in nature. There is a difference between a phenomenon and the way stakeholders desire them to be (e.g. more control and insight over residual risk) [17]. This practical problem also gives rise to some other practical problems (research issues) that form the start of the research project:

- How does one get more insight in and control over residual risk? (Possibly by taking a quantitative approach)
- How does one take a practical and usable quantitative approach? (By combining suitable models/tools with fitting computational methods)

Several research questions are defined that cover the research issues. They have been broken down in to smaller parts to provide a focus and minimize complexity.

- How to select a suitable (qualitative) tool/methodology?
  - Which (qualitative) tools/methodologies for Risk Assessment exist and what are their characteristics?
  - What are currently often used (qualitative) methodologies for Risk Assessment?
  - What kind of information is concerned in *Information Risk Management*?
  - What makes a methodology classify as ‘practical and workable’ *in practice*?
- How to select an applicable computational method?
  - Which computational methods for quantitative Risk Assessment exist and what are their characteristics?
  - What additional characteristics and/or requirements would a quantitative method need to have to make it practical and workable? (ergo: define usability criteria)
- How does the quantitative model perform on terms of usability?
  - What are the merits of using a quantitative model for residual risk management?
    - How does the model contribute to getting insight in the residual risk of an organisation?
    - How does the model contribute to getting control over the residual risk of an organisation?
  - What are the possible downsides of using a quantitative model for residual risk management?
    - What are the constraints for using a quantitative model for residual risk management?
    - What pitfalls need to be looked after?
  - What are the differences in general application of quantitative models versus qualitative models?

2.3 Research Framework

Since we have already defined the context of the research and the proclaimed research objective, it is now time to construct a framework that ensures that we will reach the proclaimed goal. The framework is as shown in Fig. 2.1 and explained in further detail in the following paragraphs.

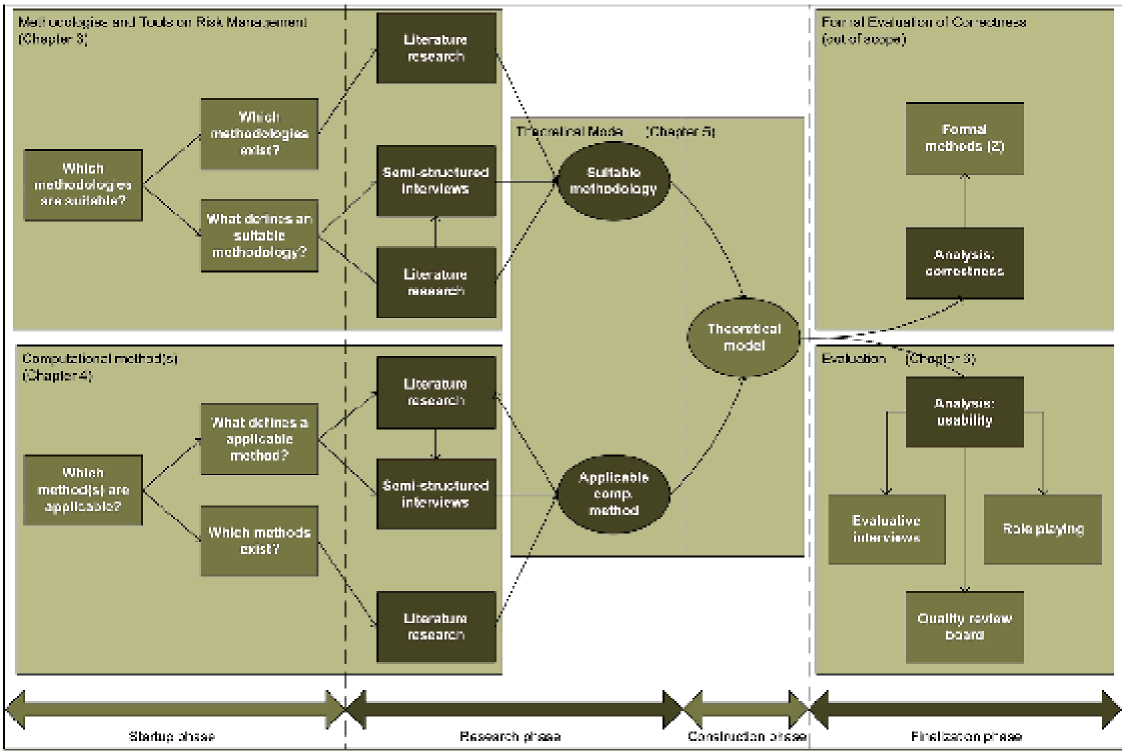


Figure 2.1: The research framework

Startup phase

The start-up phase represents the start of the research project. Here the basic information and theories are gathered for the rest of the research to build on. The problem and its research questions are analysed.

The research is started by answering the questions of ‘How to select an applicable computational method’ and ‘How to select a suitable methodology’. These two questions need to be split up into smaller questions. The availability of both the computational methods and the methodologies need to be addressed, but also insight has to be created in the definitions of ‘applicable’ and ‘suitable’.

The process of coming to an answer to these questions will be discussed in the following paragraph concerning the Research phase.

Research phase

In the Research phase an answer is given to the four main questions that have been defined during the Start-up phase. The research phase has a theoretical part and an empirical part.

The theoretical part consists of a literature research on the availability of methods and methodologies, resulting in a comparative framework of methodologies operating within the area of Risk Assessment. The same approach is taken for the computational methods; available computational methods are found doing a literature research.

The empirical part of this phase cannot be omitted. The research subject is closely coupled to the daily practice of many (information) security experts and organisation management. In order to give definitions to what is considered a 'suitable' methodology and an 'applicable' computational method, semi-structured interviews are given to people with experience in information security. This approach has the extra merit of giving extra insight in available tools and computational model use, that would be missed during the literature research.

At the end of this phase the first two research questions are answered and a base is formed for the third research question to be answered (Chapter 3). Before this is possible, a conceptual model has to be constructed which is shown in Chapter 4 .

Construction phase

In this phase, the results from the research phase are merged in a conceptual model on quantification in residual risk management (chapters 4 and 5). In contrast with the previous theoretical and empirical part of the research, this phase could be classified as being the 'design' part.

In the previous phases applicable methods and methodologies suitable for our use were identified. In this phase the two results come together. Based on a compatibility check using a comparative framework (appendices D and E), a method and methodology are combined to form a conceptual model. Assumptions and requirements for the workflow have to be clearly stated (Appendix H).

Finalization phase

During the last phase, an answer to the third research question is sought by testing the conceptual model for its usability (Chapter 6). During the research phase, information was gathered concerning usability requirements of the product. If these prove to be insufficient, additional requirements will have to be set up by consulting experts who would be using the model. The usability evaluation can take place by doing evaluative interviews, a discussion within an expert panel, and/or a game of role playing using a fictive case. The evaluation of correctness using formal methods is out of the scope of this research due to time constraints. This step of the project is discussed in this document because it is mandatory if the model is actually going to be used.

Finally, conclusions will be drawn addressing the merits and drawbacks of the model. Also, future work is discussed in greater detail (Chapter 7).

CHAPTER 3

Related Work

In this chapter we will discuss the work related to our research. Before proceeding with this chapter, it may prove useful to consult Appendix A in order to get a bird's-eye view on the relationships between important entities that will recur throughout this thesis.

In Section 3.1 we will discuss a variety of models, tools, methodologies, standards, manuals and practices in the area of risk management and risk assessment. This is necessary because a lot of these 'entities' differ in form and appearance and one might easily get lost in an attempt to get a grasp on them. In Section 3.1 we will discuss the 'entities' by its characteristics in order to structure them and increase insight.

In Section 3.2 we will take a look at an information assurance model and give an example of an implementation of such a model. We discuss possible alternatives to the example in Section 3.2 and reason towards an information security management model in Section 3.3 .

Starting from Section 3.4 we discuss the application of qualitative and quantitative risk assessment continuing in Section 3.5 with the history of the quantitative risk assessment practice. The sections thereafter will more specifically address the application of quantitative measures in *information security.*

3.1 Entities

The first thing we can notice is that the entities defined in the previous paragraphs seem to differ in their level of abstraction.

On one hand we have the big 'Risk Management Frameworks' such as COSO , M_O_R and AS/NZS 4360 [20, 78, 52]. On the other hand we have the smaller and relatively fast evolving 'methodologies'. They come in all sorts and sizes. Some are relatively large, with a broad scope and high level of detail. These might be difficult to fully understand and time-consuming to apply, but when done right they can be quite powerful and have great impact. Others are smaller, with a tighter scope, making them easier to understand, less time-consuming to apply and often more flexible and suitable for their cause.

Risk Management Frameworks

The *Risk Management Frameworks* are the largest entities which appear in the lowest numbers. They usually find their origins in a need for internal control, either voluntarily or defined by law (e.g. SOX [127]) due to corporate and accounting scandals. Perhaps the most well known example of this is the case Enron.

Enron Corporation, an American energy company, went bankrupt in late 2001. Over 21.000 people lost their jobs when it was proven that its reported financial condition was nothing close to reality. In fact, it was sustained mostly by institutionalized, systematic, and planned accounting fraud. In the process the Arthur Andersen company, at that time one of the 'Big Five' accounting firms in the world, was taken down as well. The Arthur Andersen company was convicted of obstruction of justice for shredding documents related to the audits of Enron. The 'Big Four' remain[1] (at time of writing)[43].

One of these Risk Management Frameworks, which is even suggested to be used with SOX, is COSO. As explained in the COSO Integrated Framework manual [20], the underlying premise of Enterprise Risk Management is that every entity exists to provide value for its stakeholders. All the entities face uncertainty which gives management the challenge to determine how much uncertainty is acceptable. It is this uncertainty that presents both risk and opportunity. Management tries to set strategy and objectives to create an optimal balance between growth and return goals and related risk to maximize value [77].

The COSO Cube

This section of the chapter is named 'The COSO Cube'. It is the first of many 'cubes' one will find in this chapter. Practitioners and authors of literature in the field of (Information) Risk Management seem to favour Rubix-cubes representing the multi-faceted elements of Risk Management.

This rather well known COSO-cube is as shown in Fig. 3.1 . The three dimensions of the COSO-cube represent the COSO risk management *components* on the horizontal axis, the COSO *categories* are shown on the vertical axis and the COSO *objectives* are shown on the diagonal axis.

The COSO enterprise risk management framework aims to achieve an entity's *objectives.* They appear in four categories:

Strategic: High-level goals, aligned with and supporting the mission.
Operations: Effective and efficient use of the resources.
Reporting: Reliability of reporting.
Compliance: Compliance with applicable laws and regulations.

It does so taking into account eight interrelated enterprise risk management *components* being (as taken from [20]):

[1] The 'Big Four' that remain: Ernst & Young, Deloitte Touche Tohmatsu, KPMG and PricewaterhouseCoopers

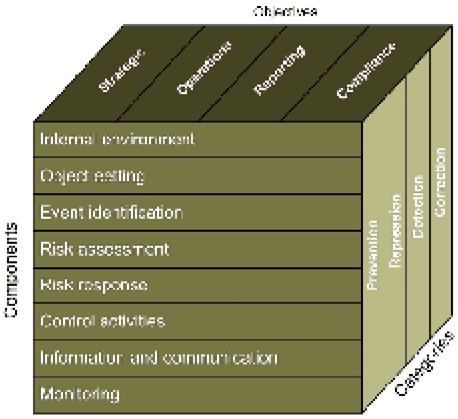


Figure 3.1: The COSO-cube [20]

Internal Environment: The internal environment encompasses the tone of an organisation, and sets the basis for how risk is viewed and addressed by an entity's people, including risk management philosophy and risk appetite, integrity and ethical values, and the environment in which they operate.

Objective Setting: Objectives must exist before management can identify potential events affecting their achievement.

Event Identification: Internal and external events affecting achievement of an entity's objectives must be identified, distinguishing between risks and opportunities.

Risk Assessment: Risks are analysed, considering likelihood and impact, as a basis for determining how they should be managed.

Risk Response: Management selects risk responses (avoiding, accepting, reducing, sharing), developing a set of actions to align risks with the entity's risk tolerances and risk appetite.

Control Activities: Policies and procedures are established and implemented to help ensure the risk responses are effectively carried out.

Information and Communication: Relevant information is identified, captured and communicated in a form and time frame that enable people to carry out their responsibilities.

Monitoring: The entirety of enterprise risk management is monitored and modifications made if necessary.

The components are relevant to the entire enterprise or to its internal units as shown by the final dimension of the COSO-cube. COSO distinguishes subsidiaries, divisions, business units and entity levels as *categories* of an entity's objectives.

Risk Assessment Frameworks

Dissecting the Risk Management Frameworks, we come across the *Risk Assessment Frameworks*. A few well known examples of the Risk Assessment Frameworks are ISO/IEC 27001 [115], ITIL [79], ISO/IEC 15408 [116] and CobiT [49]. Taking the well known CobiT Risk Assessment Framework, we see another example of cube-like representations. The CobiT-cube, as seen in Fig. 3.2 , summarizes the basic principles of the CobiT Risk Assessment Framework. In a nutshell: The *resources* are managed by *processes* to achieve the *goals* that respond to the *business requirements*.

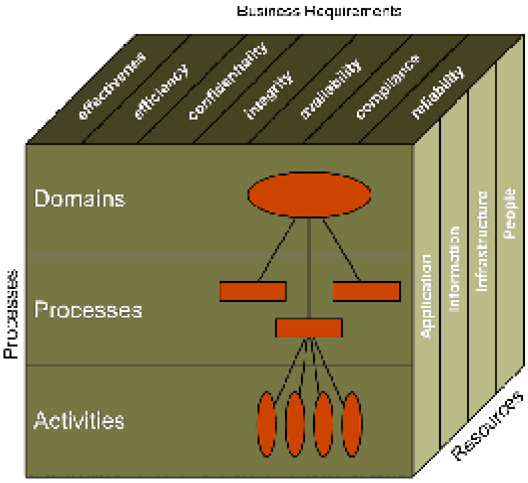


Figure 3.2: The CobiT-cube [49]

Risk Methodologies

Taking a closer look at the Risk Assessment Frameworks, we find the (Information) Risk Methodologies. Their relationship to each other is sometimes obvious, sometimes less obvious. The Information Risk Methodologies give (a partly) implementation(s) to the Risk Assessment Frameworks.

There are a lot of these methodologies to be found. The general methodologies that can be found in the literature often have a more specific (that is, with a smaller focus) sibling. The amount of different methodologies is going to be a problem if one would like to compare them all on certain characteristics. The fact that a lot of countries, or regions of countries, prefer to use their self-created methodology, often made fit-for-use to the local rules and regulations, does not help either. Nevertheless, the list in Appendix C should give an idea of the most commonly named tools and methodologies in the literature as well as interviews. A systematic overview of the above named frameworks and methodologies can be seen in Fig. C.1 in Appendix C .

In order to work conform the Rubix-cube preferences in the area of enterprise risk management, an example cube for information security management is presented. It is shown in Fig. 3.3 . It looks like the CobiT-cube because of its strong relation to it. Therefore other approaches, not working based on CobiT, could result in a different Information Security Management cube. The reasoning behind the model and the elements of the cube will be discussed in greater detail in the following paragraphs.

3.2 Information Assurance

Information Criteria

Most models will at least specify a minimal implementation of a so called information assurance model. The most commonly used criteria are denoted by their initials CIA, which in this case stands for Confidentiality, Integrity and Availability [23]. They are discussed in more detail in the following

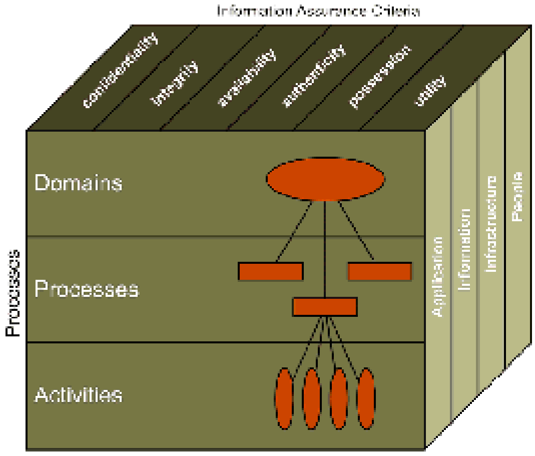


Figure 3.3: A proposed Information Security Management cube

paragraphs.

Each criterion is accompanied with an example starring a character named Sinon[2] in order to get a better feeling on how each criterion influences risk.

In the example, the character Sinon works as the Chief Information Officer (CIO) in the largest hospital of Troy. He has to ensure that all information is securely available throughout the hospital and that everything runs as smoothly as possible. He is in charge of all information systems throughout the hospital and reports to the Chief Executive Officer (CEO). *All examples are based on real life events.*

Confidentiality

Confidentiality, being part of the broader concept of privacy, refers to preventing the unauthorized access, disclosure, and use of information or even the nature or existence of the information [23]. Only the individuals, processes or devices that are intended and authorized may have access to the data. Without appropriate controls, access or theft of information can be accomplished without a trace. Therefore, confidentiality is maintained through user authentication and access control. User authentication ensures that the person trying to access the data is authorized. Access control is the process of defining which users and groups should have access to the data.
In short: Limited observation and disclosure of knowledge [18, 122].

Example: While reviewing the records of people who recently had HIV tests, the nurse on duty gets called away by a medical emergency. In the meantime, a 13 year old girl, who was told to 'go-play' finds the nurse's workstation unattended and unlocked. Since she always wanted to be a secretary, she goes on calling all the people on the nurse's list, falsely telling them they were tested HIV$^+$. Although this example might seem humorous, the breach of confidentiality here almost caused one of the tested girls to commit suicide after she heard the message [46]. After this situation, Sinon had to rethink workstation policies and implement preventive controls.

[2] Character design inspired by Vergilius Maro [124] but in this context *totally* fictional and should be regarded as a figment of the author's imagination

Integrity

Integrity is a somewhat broad phenomenon. In this case, it refers to the reliability and trustworthiness of the information in or produced by the information environment. Data integrity refers to the need to retain or preserve the information from source to destination. Source integrity refers to the verification process that is involved in ensuring that the data came from the correct source rather than from an imposter [122].

Integrity also refers to whether or not the correct data was initially entered, and whether the calculation or action will yield the same result each time.
In short: Completeness, wholeness, and readability of information and quality of being unchanged from a previous state [18, 118].

Example: Lacoön, being the head of the administration department of Troy's hospital, has access to details of all people in the hospital; both patient and employee. Since Sinon and Lacoön had an argument over lunch, Lacoön decided it would be amusing to register Sinon as being deceased in the hospital's database. Sinon found out he was virtually dead when he did not receive his monthly pay check (as he implemented a check in the payroll system which refuses to directly pay deceased people). In this case, the integrity of the Troy hospital administration was compromised [29].

Availability

Because most companies rely heavily on computers and networks, and the data and information that resides within them, availability is a critical function. Companies have to be able to rely on electronic data and communications [117]. Availability defines the timely access to data, with timely defined in terms of functional significance. It is not possible to define timely as absolute because it depends on what the data is used for.
In short: Usability of information for a purpose [18].

Example: Executive management and Sinon have decided on a capacity increase of the hospital's mainframe. New government regulations require electronic patient dossiers and that, in combination with the growing population of elderly people in Troy, asks for more capacity. During a mainframe overhaul, Sinon spills his cup of coffee, which requires immediate attention. In the ruckus, the overhaul takes ten times as long as planned, leading to the hospital's information systems being unavailable for over $1\frac{1}{2}$ hour. In the meantime, doctors could not help their patients because no information was available. This resulted in long queue's for regular patients and emergency cases had to be rerouted to other hospitals [84]. Availability in this example is compromised. Sinon did not have a functional backup system in place which would keep the system from becoming unavailable.

Alternative Criteria

The above criteria can be used to describe many important security objectives. However, many people will have difficulties combining the security objective with a criteria. Sometimes the objectives seem fitting to more criteria, or even none at all. This makes the CIA model a good starting point for the young industries, but less applicable in the more mature industries. These mature industries need a more detailed model, as for example the Parkerian Hexad [83], to cover all facets of their problem.

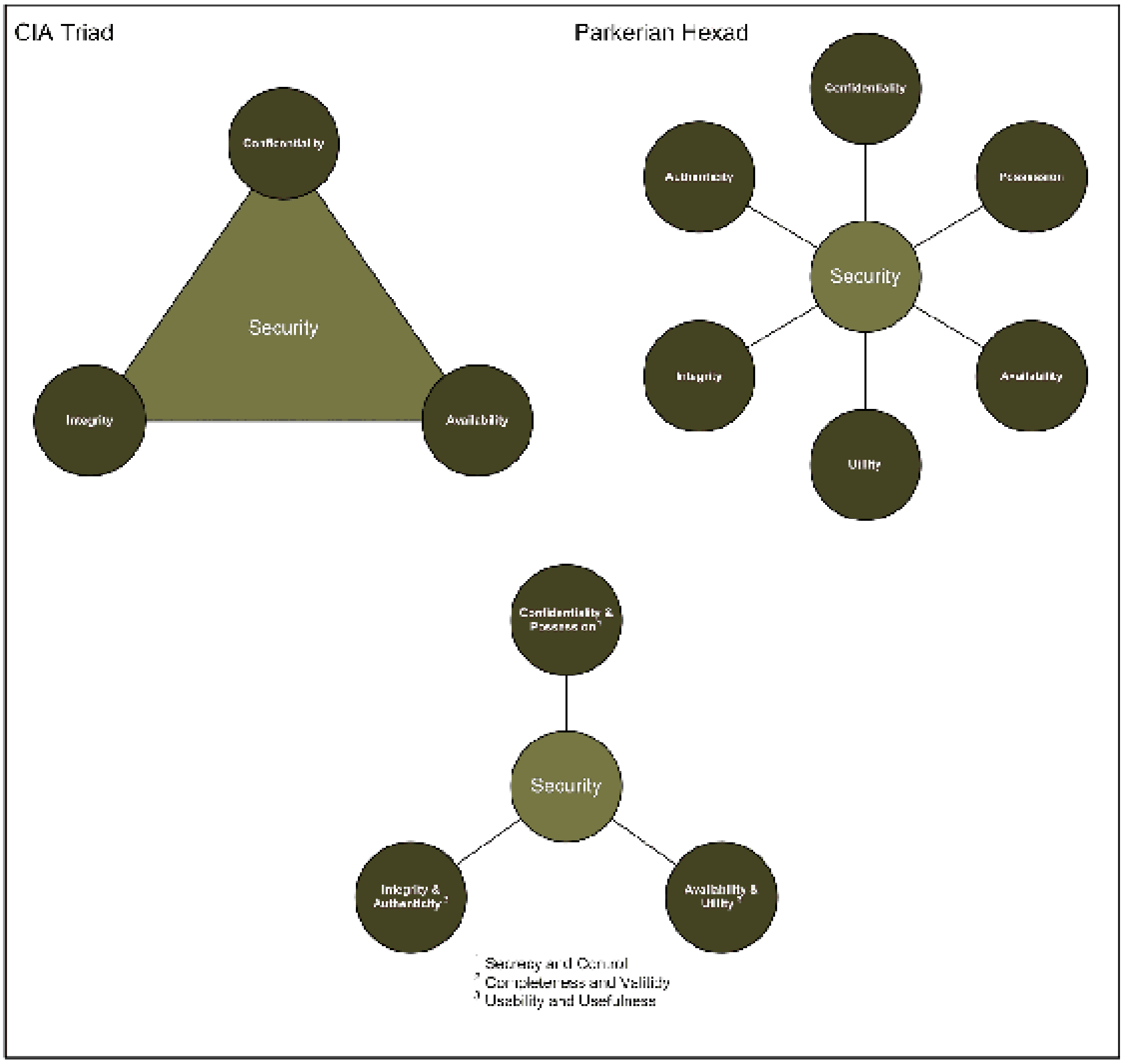


Figure 3.4: Conventional CIA and Parkerian Hexad

The conversion of the regular CIA model with the Parkerian Hexad is as shown in Fig. 3.4 as suggested by Bosworth and Kabay [18].

As can been seen from Fig. 3.4 the Parkerian Hexad adds three more criteria to the original CIA model by defining *a)* possession, *b)* utility and *c)* authenticity. Each of these criteria are briefly discussed in the following paragraphs.

Possession

Possession (or control) is often confused with confidentiality but although a breach of possession often occurs at the same time with a breach of confidentiality, they do not necessarily have to. A breach of possession results in the loss of control over the information or no longer being able to

determine who has access to the information. Data owners cannot guarantee that the data is used in an an appropriate way.
In short: Holding, controlling and having the ability to use information [18].

Example: Sinon one day received a call from the 'Bank of Troy' with the message that the hospital's ATM had been compromised. On security tapes Sinon found a young rebel who decided it was time to use the modern techniques of wireless transmitters and telelenses to pass some idle time. The boy would install an electronic transmitter in an ATM which would send the encoded information of the withdrawal card to his freshly bought laptop. Additionally, he made photographs of the hands of the people punching in their codes to get access to their accounts. This process is commonly known as 'skimming'.

Sinon called the authorities and the boy got caught and had to face a trial since his actions would have violated the criterion of confidentiality. In his defence however, his attorney stated that it could not possibly have been a breach of confidentiality since the boy never had the time, nor the intention to look at the accounts. In this case, all the other criteria were not breached [48].

Utility

Utility (or usefulness) probably is one criterion from the Parkerian Hexad that is open to some discussion. It addresses usability of the information in its form. A breach of the utility criterion makes the data less useful or unusable in that form. It denotes that having access to information (availability), and being able to use the information are clearly two different things.
In short: Usefulness of information for a purpose [18].

Example: Somewhere around the mid 1900's, Sinon thought of a way to represent a year in the programming of the information system of the hospital. He believed that the representation of the year using two digits would be sufficient for all the current and future needs and additionally save precious computer memory.

Little did he know that years later, this would prove to be the origin of the hospital's Y2k problem. Even though the system itself was long replaced, parts of the legacy software remained. Thanks to Sinon, who coded using the two digit data format, usefulness degraded. The hospital could not determine the correct age of their patients and employees because of incorrect software. The software assumed that the maximum value of a year field is 99 and will proceed with the 00 year. This proved to be rather useless since no distinction could be made any more between the year 2000 and the year 1900, leading to a gigantic increase in the amount of elderly people over night, well at least according to the hospital administration systems... [71]

Authenticity

Authenticity is a criterion often not thought about. For the data to be authentic, there should be a correspondence to its actual meaning. It is the property that ensures that the actions of an entity may be traced uniquely to the entity itself [117].
In short: Validity, conformance and genuineness of information [18].

Example: Sinon received another call from his friends at the local bank. Report got in that someone within the hospital seemed to counterfeit €50 bills. Reviewing printer logs he discovered a multifunctional printer on the payroll administration department with suspicious behaviour. With the scanner and colour printer, an employee started her fraudulent activities because she was convinced she was being paid less than needed to survive the upcoming Christmas period.

This is a case of a breach in authenticity where all other criteria are not breached. The integrity criterion is not breached since the information asset (the counterfeit €50 bill) is exactly used for what it is meant (payment), whether we agree with these fraudulent activities or not [54].

3.3 Towards the Information Security Management cube

There is not one generally accepted collection of criteria. Although most parties seem to agree on at least a minimal CIA implementation, alternatives might be better suited for a certain situation. This thesis does ***not*** suggest a specific usage of certain criteria. The Parkerian Hexad is used as ***an example*** on building an Information Security Management model. In the following chapters, the CIA criteria are used. The reasoning behind this is threefold.

1. Using the CIA criteria, which seems to be the closest thing there is to a generally agreed upon minimal implementation of information security criteria, the generalizability of the research is increased. This will make it easier for future users to adapt the model to their needs.
2. Being the most widely used set of criteria, it will feel familiar to practitioners which will increase adoptability.
3. The available time of this research is limited. By only addressing the CIA criteria time is saved while the concept is maintained.

Back to the cube that was shown in Fig. 3.3 . We already noticed that the CobiT-cube and the proposed Information Security Management cube look quite similar. This is not a coincidence. To explain this, we need to look at some CobiT internals first.

A possible reason to take the CobiT model as starting point is its appeal to different users [49]. For example:

Executive management: To obtain value from IT investments and balance risk and control investment.

Business management: To obtain assurance on the management and control of IT services provided by internal or third parties.

IT management: To provide the IT services that the business requires to support the business strategy in a controlled and managed way.

Auditors: To substantiate their opinions and provide advice to management on internal controls.

This audience covers the tactical and strategical level of an organisation. It falls short when it comes to the operational level with no clear defined linkage to line management and operators. This however is only seemingly the case. The Risk Assessment needs to be seen in context, which is shown in Fig. 3.5 , inspired by Landoll [65].

Although risk management and assessment is performed on strategical and tactical level of an organisation, the operational part of the organisation is also directly influenced by the activities performed on the other levels. This is not a one way path of influence. The risk management process covers all levels of an organisation and organisational levels are tightly coupled to each other [65].

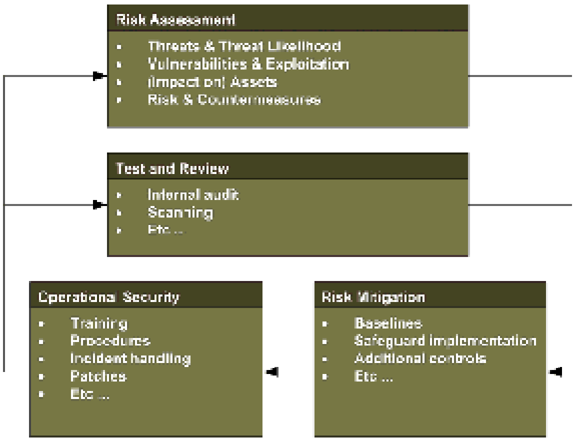


Figure 3.5: Risk Assessment in context [65]

3.4 Qualitative versus Quantitative Risk Assessment

In the first chapter we shortly introduced two families of risk assessment techniques: qualitative and quantitative. In performing risk assessments, consideration should be given to the advantages and disadvantages of qualitative and quantitative techniques [87].

The main advantage of the qualitative style is that it prioritizes the risks and identifies areas for immediate action and improvement [87]. This setting of priorities is extremely valuable [45]. The main disadvantage is that it does not provide specific measurements of the impact, making it difficult to make a cost-benefit analysis. Additionally, the findings can be considered 'too loose' or imprecise in the minds of senior management [45]. These statements are supported by the findings of the expert interviews conducted for this research (Appendix B).

The main advantages of the quantitative style are that it does provide measurements of the impact which can be used in a cost-benefit analysis of recommended controls [87]. It provides a straightforward result to support an accounting-based presentation to senior managers [45]. The downside of the quantitative measures is that the meaning of the results of the assessment is sometimes unclear. Some factors influencing risk might be hard to assess. The wrong interpretation of correct data can lead to a wrong decision, just as a right decision on wrong data can [45]. These statements are also backed-up by the results of the expert interviews (Appendix B).

3.5 History of Quantitative Measures

The idea of Information Security, even though it seems to be a rather 'hot' topic at the time of writing, is hardly new. Advances in technology both facilitate and hinder progress made in the field of Information Security. The advances made in digital computing and networking technologies introduced a new sort of information age, adding new and dynamic dimensions to information security [107]. As a result we find a significant growth in the volume of valuable information but also in the ways to compromise this information. This makes information security an even greater

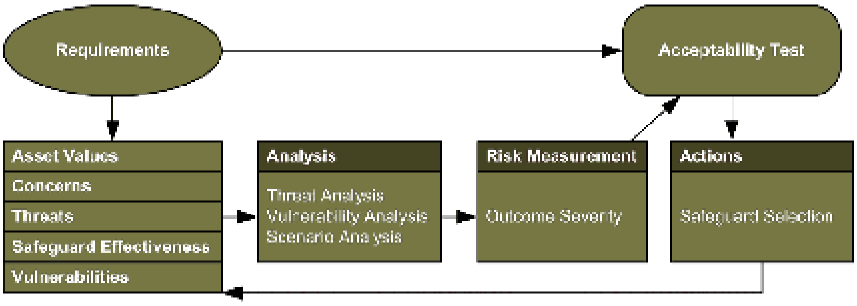


Figure 3.6: Computer System Risk Management Framework - Process Diagram [38].

challenge than it was 25 years ago when most of the current attacks against information assets were unimaginable [77].

The above named information technologies give their users the capabilities for managing, processing and communicating information. Securing the underlying technologies often proves to be a rather difficult and expensive venture. Planning, designing and implementing controls have their costs, but it also requires the participation of everyone in the organisation and is typically limiting them in their freedom. This phenomenon clearly shows the tension between security and usability where up till now usability seems to have the upper hand [107].

Information security does not necessarily has to be read in terms of computer systems and applications. In most cases however, computerized information systems are of common day practice. The importance of information security in a computer-based environment has resulted in a large stream of research that focuses on the *technical defences* associated with protecting information [7, 28, 64, 93, 98]. Additionally, research has been rapidly developing that focuses on the behavioural aspects of reducing information security breaches [31, 57, 67, 111].

Less research has been done on the *economical aspects* of information security. The work that does exist on this topic gives little guidance on investments in information security, according to Gordon and Loeb [38].

First Generation Methods

In the mid-1980's the first steps were made within the area of computer security risk-management modelling during a series of workshops provided by the National Bureau of Standards and the National Computer Security Center. The methods and tools originating from these workshops form the first generation of computer and information security risk management models and can be summarized by looking at Fig. 3.6 .

The iterative processes as shown in Fig. 3.6 starts with the identification of the security requirements, asset values, security concerns, possible threats, safeguards and vulnerabilities. This is followed by a series of analysis which involve the examination of possible threats to each asset, a vulnerability analysis[3] and scenario analysis. The scenarios are used in the risk-measurement phase to evaluate

[3] Vulnerabilities in the first generation framework are defined as the absence of specific safeguards (instead of being an independent variable)

their outcomes and their corresponding risk. The acceptability test compares the measured risk to the established requirements after which safeguard selections are made. The process is iterated.

As stated by Soo Hoo [107], the common framework is quite generic in its specification and therefore broad in its potential application. It can be adapted to either quantitative or qualitative risk assessment. Variations on the same common framework were given by Hoffman and Yoran [47] and include threat succession techniques (e.g. Jawarski [51]), networked techniques (e.g. Osgood [80]) and modelling time dependencies (e.g. Drake and Morse [30]).

Originating from inventors' bias and general challenges in modelling computer security risk, at least three drawbacks can be found in these first generation (ALE-)models[4] [107].

1. The scenario-generation mechanism created an assessment task of (at that time) infeasible proportions. The model failed to find a balance between model simplicity and faithful replication of the modelled system. This model tends to favour significantly greater detail than was efficiently feasible to describe. Assessing scenarios applying the framework results in a task with thousands to hundreds of thousands of branches with the number of scenarios growing almost exponentially with each new item considered. This was one of the reasons the above risk model failed to be widely accepted and used.[5]
2. The second drawback is based on the completely deterministic nature of the framework. It assumes that all quantities would be precisely known. Additionally, the framework models the variables as estimates, not as probabilities, limiting its usefulness for estimating uncertainty. Using (wrong) estimates became a source of misinformation derailing a company's security efforts. This had an especially large impact on popularity of the first generation methods.
3. The third drawback is the framework's dependency on information that was (and continues to be) sparse. It assumes that frequency, valuation and efficiency data is available to the practitioner.

Summarized: Excessive complexity (drawback 1), poor treatment of uncertainty (drawback 2) and data unavailability (drawback 3) are challenges that were beyond the capabilities of this framework to address [107]. The framework did provide a starting point for further research on the subject, but due to a rather bad reputation (based on the results it gave) many companies were reluctant to venture in the area of risk modelling and management again.

Second Generation Methods

If it was not for the Internet and related developments, computer and information risk management would probably not have been a big topic on a manager's agenda. The world has changed. Processors are faster, memory larger and networks are enabling communication. This resulted in a general change in the use of computers and information systems. This gave a new impulse to computer and information risk management.

Information risk was not just considered 'another additional cost' but it actually enabled new business opportunities too. This motivated people to think about the flaws from the first generation (ALE-based) methodologies. Upon developing, what was going to be the next generation of risk assessment

[4] Although not explicitly called that way, the framework works conform Annual Loss Expectancy or ALE

[5] Computational strength has increased significantly since then, but at that time the operation was to be considered *computational infeasible.*

methods, the developers' main interest was to solve the deployment and organisational acceptance issues. This process, that actually only tackles parts of the flaws from the first generation methods, resulted in a few new approaches to risk assessment.

Without going in too much detail, Soo Hoo [107] for example finds four different second generation approaches being an 'Integrated Business Risk-Management Framework' [6], 'Valuation-Driven Methodologies' [6], 'Scenario Analysis Approaches' [112] and 'Best Practices' [131]. All these approaches have in common that they provide a short-term solutions to the problems of organisational acceptance and deployment (drawback 2 of the first generation methods). The challenges with regard to the computational complexity (drawback 1 of the first generation methods) and availability of data (drawback 3 of the first generation methods) remain.

Third Generation Methods

Although relatively successful, the second generation methods still lack the means for cost justification and forecasting trends. Their weaknesses make them unsuitable to fit the needs of the insurance industry, the avoidance of legal liability and the possibility of market competition [22].

Not surprisingly, the risks of uncertainty, sparse information and technological changes has been influencing the financial markets and insurance industries [58]. They especially feel the need to measure, distribute, mitigate and accept risk. According to Soo Hoo [107] the driving forces of *insurance needs, liability exposure* and *market competition* gave birth to the third generation methods.

Insurance companies provide policies covering a large variety of risks. In order to provide service on for example information asset protection, these companies need to know the statistics on which to base the premiums of their policies. They need to develop classification mechanisms in order to be able to determine coverage and the corresponding premium. The insurance companies have to do this mainly independent from the other organisations as there seems to be tendency to keep useful information private [94].

Avoidance of legal liability is another reason for improving information security. Should it be an organisation possessing confidential or proprietary information without a specific agreement on the information, or any other variation on the subject, the organisation might be held liable. This makes it interesting for the organisation to compare the costs of *avoiding* an accident and the expected cost of the accident. This requires the availability of the necessary data to enable the cost-benefit analysis in order to justify the information security policies and strategies [73]. Risk avoidance and risk transfer are strategies that are gaining popularity fast. They work complementary to the risk mitigation strategy (see also Fig. 1.3) and will not replace it [42].

Market competition will force organisations to protect their information assets efficiently. Organisations that fail to secure their assets (cost-)effectively will not gain a competitive advantage over those that do. Organisations that over-protect will spend too much money on information security, those who under-protect will have greater losses as a result of security breaches Fig. 3.7 [15, 95]. It is believed that these developments will make the management of information risks evolve toward a quantitative *decision-based* approach not totally unlike the first generation (scenario based) methods. Again, the quantification of risks, measurement of safeguard efficiency and analysis of costs and benefits are necessary. Hopefully, the lessons learned through the previous two generations will avoid the previously experienced pitfalls.

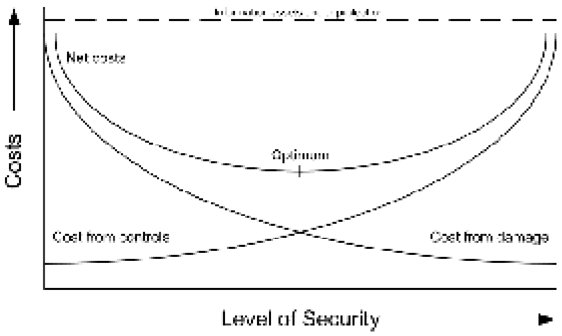


Figure 3.7: Finding the optimal information risk management strategy [55, 77]

3.6 Information Security Risk Modelling

One of the main problems of scenario based approaches is that no amount of historical research can ensure that all threats will be discovered [99]. New threat scenarios will be created or discovered by new technologies. Therefore, it is important to also look at historical data to discover the rate at which new threats are discovered. Even then, one can never be sure that all child scenarios are identified.

Along the same lines, safeguards and countermeasures do not always have the same impact as expected. Even when they are implemented correctly, they will never *totally* eliminate the threat(s). Historical data can help in estimating a safeguard's impact.

Even though the above two problems are evident, the better threats, safeguards and countermeasures can be understood, the better the effectiveness of the risk management process can be measured [99]. One cannot create a state in which there is 'perfect security'; there is no way to know if threats have been left unaddressed. One can estimate how close one comes to this goal.

3.7 Metrics

The assessment of information security risk itself is a much broader topic than one might expect. Answers have to be given to the questions of "How effective have our security efforts been in reducing the information risk?" and "How will further security efforts influence the information risk?". This often entails *estimating past values* and *forecasting future values* of elements like threats, asset value, frequency of incidents, and annual cost of the incidents.

To make decisions on information security, we must use these metrics to measure how the choices will influence the effectiveness of risk reduction within the general information security strategy [38]. This task is difficult because good statistics on factors involving information management are rare. Risk managers must convince their senior management to spend actual resources to address hypothetical losses. Because the benefits from the information security initiatives are uncertain and poorly quantifiable, senior management support is difficult to acquire.

Annual Loss Expectancy

One of the earliest used approach to risk management is the Annual Loss Expectancy (ALE). It was first introduced by the National Bureau as a Federal Information Processing Standard (FIPS) [75].

In the field of Risk Management, risk is often defined as the multiplication of the independent components of *expected loss* due to a potential event and the *likelihood* of that event occurring.

$$\text{Risk} = (\text{Cost of loss event}) \cdot (\text{Likelihood of loss event})$$

The ALE metric is based on this. An ALE can for example be calculated by computing the expected frequency of the loss event times the value of the loss event. [6] When summed over all independent loss events, one gets the total Annual Loss Expectancy as shown in eq. (3.1).

$$ALE = \sum_{i=1}^{n} L(I_i) \cdot F(I_i) \tag{3.1}$$

$$\begin{aligned} I_1,\ldots,I_n &= \text{Set of independent harmful } \textit{incidents} \\ L(I_i) &= \text{Monetary } \textit{annual loss} \text{ caused by incident } i \\ F(I_i) &= \textit{Frequency} \text{ of incident } i \end{aligned} \tag{3.2}$$

In other examples, the ALE of an event is calculated by the multiplication of the value of the loss times the probability of (independent) threats exploiting (independent) vulnerabilities (see: eq. (3.3)).

$$\begin{aligned} ALE &= (\text{Value of loss }) \cdot (\text{Threat probability}) \cdot (\text{Vulnerability probability}) \\ &= L \cdot P(t) \cdot P(v) \\ L &= \text{ Monetary loss caused by information set breach, with } L < M \\ P(t) &= \text{ Probability of threat occurring, with } t \in [0,1] \\ P(v) &= \text{ Vulnerability (probability of success once threat is realized), with } v \in [0,1] \end{aligned} \tag{3.3}$$

As we can see, there is no such thing as one rigid ALE approach. Taking a closer look at the version of ALE that is used by Gordon and Loeb [38] in eq. (3.3), we see that per situation at most one loss event will occur. This makes a difference as the monetary cost of a loss is multiplied by its likelihood (rather than the expected frequency of loss).

What makes the use of the ALE approach interesting is the combination of two risk components into one number. Hypothetically the annual loss expected from all the operations of an organisation would be the sum of the expected yearly losses that could result from each threat scenario [99].

The drawback of using ALE can be explained by looking at eq. (3.1); one is unable to distinguish low-frequency-high-impact situations with high-frequency-low-impact situations. There is a big difference in consequence between the two scenarios.

[6] Sometimes the expected frequency of the loss event is described by the term Annual Rate of Occurrence (ARO) and the value of the loss event is described by the term Single Loss Expectancy (SLE) [33].

Net Benefit

Another approach focuses on measuring the benefits of investment in safeguards. The work done by Soo Hoo [107] probably is the most cited publication on this subject on this moment. He states that the benefits of an investment in safeguards not only lie in decreased losses, but also in expected profits from new activities that could not have been profitably undertaken without the added security measures. Soo Hoo [107] proposes to define the Net Benefits under policy k (NB_k) according to eq. (3.4).

$$\begin{aligned} NB_k &= B_k - AC_k + AP_k && (3.4) \\ B_k &= \text{Benefit under policy } k \\ AC_k &= \text{Added cost under policy } k \\ AP_k &= \text{Added profit under policy } k \end{aligned}$$

The security savings are defined as a reduction in ALE as shown in eq. (3.5). The k stands for a 'basket of safeguards' or 'policy'. ALE_0, or the ALE with policy $k = 0$, stands for the situation with the current policy. Each other value of k stands for a competing collection of safeguards. This implies that the impact of each policy has to be known (calculated) beforehand.

The benefit B under policy k is given by eq. (3.5).

$$B_k = ALE_0 - ALE_k \qquad \forall k = \{1,\ldots,n\} \tag{3.5}$$

The added cost AC under policy k is given by eq. (3.6):

$$\begin{aligned} AC_k &= \sum_{j=1}^{m} C(S_j) I_k(S_j) \qquad \forall k = \{1,\ldots,n\} \quad I_k(S_j) \in \{0,1\} && (3.6) \\ C(S_j) &= \text{Cost of implementing (independent) safeguard } S_j \\ I_k(S_j) &= \text{Binary function indicating if safeguard } S_j \text{ is included in policy } P_k \end{aligned}$$

The added profit AP under policy k is given by eq. (3.7):

$$\begin{aligned} AP_k &= \sum_{j=1}^{m} R(S_j) I_k(S_j) \qquad \forall k = \{1,\ldots,n\} \quad I_k(S_j) \in \{0,1\} && (3.7) \\ R(S_j) &= \text{New profits enabled by adoption of (independent) safeguard } S_j \\ I_k(S_j) &= \text{Binary function indicating if safeguard } S_j \text{ is included in policy } P_k \end{aligned}$$

Return on Investment

Studies done by CIO insight from 2002 till 2006 with qualified Chief Information Officers (CIOs) show that the need to prove Return On Investment (ROI) is high. Many respondents reported that they are attempting to do so, but the report also gives proof that monetary and business value metrics do not fully capture the value of major IT and security related investments. The motivation is there, given that three-quarters of the respondents are under greater pressure to put a monetary value on the (sometimes intangible) benefits of security related IT investments [3, 4, 32, 56]. These findings are supported by the work done by Verhoef [125] on quantitative measures. Even though Verhoef applies these measures on IT portfolios, the measure itself stays the same.

Blakley et al. [13] define security ROI as the amount of annual benefit over its costs. They do so by assuming that the annual benefit of a security investment will be received not only in the first year, but in all subsequent years [99]. The approach taken by Soo Hoo et al. [108] is compatible with this assumption. The ROSI methodology is based on similar ROI calculations [106].

ROI is a measure based on financial return and is defined as shown in eq. (3.8) [92].

$$\begin{aligned} ROI(\%) &= \left(\frac{NB_k}{AC_k}\right) \cdot 100 \qquad \forall k = \{1,\ldots,n\} \\ &= \left(\frac{B_k + AP_k - AC_k}{AC_k}\right) \cdot 100 \\ &= \left(\frac{(ALE_0 - ALE_k) + AP_k - AC_k}{AC_k}\right) \cdot 100 \end{aligned} \tag{3.8}$$

Internal Rate of Return

The Internal Rate of Return (IRR) is the discount rate that makes the present value of the investment's income stream total to zero. Some authors prefer the use of the IRR of an investment over the use of ROI. They do so because IRR incorporates discounted cash flows for investments that have different costs and benefits in different years [14].

The IRR is closely related to the Net Present Value (NPV). A Present Value (PV) can be calculated using eq. (3.9), while the NPV of a project covering several years is calculated as shown in eq. (3.10).

$$PV = \frac{C_t}{(1+r)^t} \tag{3.9}$$

C_t = cashflow C at time t

r = discount rate

$$NPV = \sum_{t=0}^{n} \frac{NC_t}{(1+r)^t} \tag{3.10}$$

NC_t = *net* cashflow NC at time t

n = total time of the (investment) project

r = discount rate

The IRR is defined as the discount rate r at which the NPV of a stream of cashflows equals 0. In other words, the IRR is defined as the solution for r in Calculating the IRR by making the NPV equal 0 leads to eq. (3.11).

$$NPV = NC_0 + \sum_{t=1}^{n} \frac{NC_t}{(1+r)^t} = 0 \tag{3.11}$$

NC_0 = initial *net* cashflow of investment

NC_t = net cashflow NC at time t

r = discount rate

In most cases the Internal Rate of Return is a better indicator than a simple ROI calculation. However, if you can't accurately predict the timing or magnitude of the costs and benefits over the lifetime of the security investment, you will get misleading results [106].

Conclusion

Even though return calculations are becoming a fact of business life, organisations should be aware of its pitfalls. Relying solely on (seemingly) hard return figures to approve a (mitigation) project, might virtually take away the responsibility of the actual understanding of the project. Return calculations on itself do not ensure that the actions are in line with the business strategy [123]. As once stated by Einstein[7]: "Not everything that can be counted counts, and not everything that counts can be counted". Likewise, not everything is measurable in simple return components (e.g. customer satisfaction, reputation) [26].

A workaround is provided by the Basel Committee on Banking Supervision in their framework of capital measurement and capital standards. The Basel-II document [9] puts the focus on the measurement of operational (and legal) risk and explicitly excludes strategic and reputational risk. By defining operational risk as "The risk of loss resulting from inadequate or failed internal processes, people and systems or from external events", the committee basically excludes these 'hard to quantify' components from the risk management process in an attempt to 'harden' the figures. This focus on operational risk is also present in this research but should not be interpreted as 'risk management that is done solely on an operational level' as it is a process throughout the organisation as was shown in Fig. 1.6 and Fig. 3.5 .

[7] Einstein, A. 1879-1955

Chapter 4

Towards a Quantitative Model

In this research, we will be taking an approach that considers Annual Loss Expectancies (ALEs), but there are other approaches to risk management. For example, for capital management purposes it is also important to have accurate insight into the *variability of the losses* and in the *value at risk* (VaR) [50]. These approaches however cannot be used in all situations. In order to be able to accurately estimate the distribution function, one would need a significant amount of data which might be difficult to collect. Especially the high-impact-low-probability events will have limited data available to estimate a distribution function. These events typically occur in Information Security and its fast and constantly changing environment. This makes information security risk management quite different from the previously mentioned traditional insurance risk management [66].

Lenstra and Voss [66] go on explaining that although loss variation and VaR can be determined per event (based on its distribution function), aggregation of these risk related quantities is more difficult than aggregation of the expected losses. It requires knowledge of dependencies and correlations among the events. The ALE approach does not require the actual event distributions nor their interactions. Estimates for the expected losses will suffice and aggregation is done by simple summation.

Taking the ALE approach, we will work toward a model that attempts to give a good representation of the information risk of an organisation. For this, we need to be able to model the current situation as well as a situation where countermeasures to vulnerabilities and threats can be taken in order to minimize the residual information risk of an organisation.

Schematically the components of our model are as given in Fig. 4.1 . An organisation operates in an environment and knows certain business processes. In these processes, applications are used with possible vulnerabilities that can be exploited by threats. This gives a potential that a given threat will exploit a vulnerability exposing applications and assets to harm: the organisation is exposed to risk.

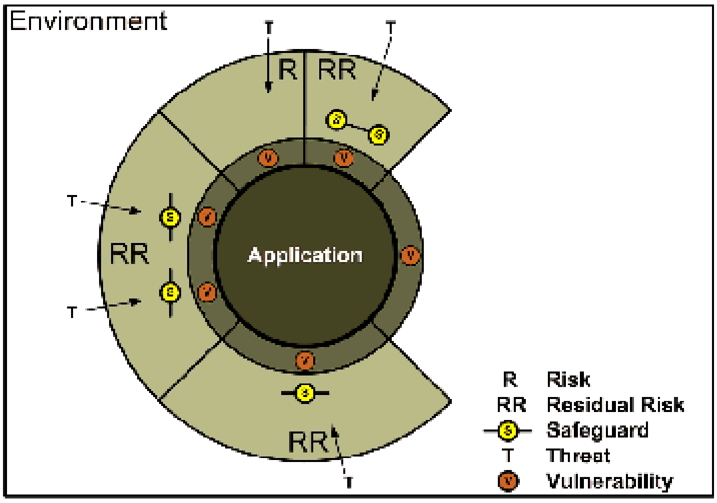


Figure 4.1: Components of the Computational Model (based on [118])

4.1 Current Risk

In the previous chapter we saw a definition of risk like:

Security Risk = (Likelihood of security breach) · (Cost of security breach)

or

Security Risk = (Security breach rate) · (Average cost per breach)

In our model we will take a look at the risk on the level of 'events', adopting the 'likelihood · cost' point of view for reasons that will be explained later. This approach is inspired on the approach taken by Lenstra and Voss [66] but adapted to fit the extra needs of a breakdown in independent threat and independent vulnerability components which will be discussed in greater detail later on. In the following sections we will first discuss the 'cost' components of the equation after which the 'likelihood' component will be discussed.

Cost of security breach

We start by giving a definition of the maximal possible loss occurring due to a security breach in a *business process*. For reasons earlier explained, we assume that a risk R originates from a breach in either confidentiality, integrity or availability (see also: Section 3.2). Therefore we need to estimate the *loss amount L* on *criterion k* for a business *process p*. We do this by calculating $L^{\max}(p) = \sum_{k \in K} \left(L_k^{\max}(p) \right)$. In our case, using the CIA criteria, this results in eq. (4.1).

$$L^{\max}(p) = L_{conf}^{\max}(p) + L_{int}^{\max}(p) + L_{avail}^{\max}(p) \tag{4.1}$$

In the above equation(s), we calculate the *maximum* expected losses per information criterion in a process. Even though this is a 'safe' approach, in some cases it might be desirable not to use the

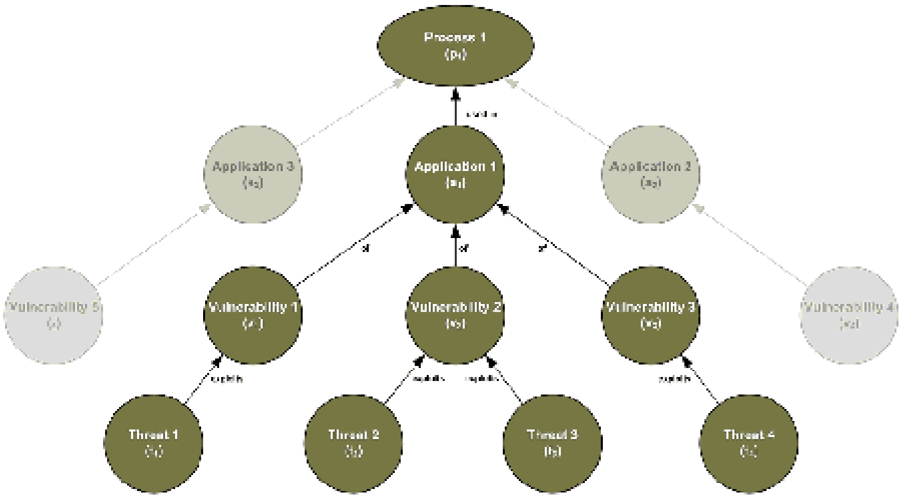


Figure 4.2: Component interaction

maximum expected losses but for example averaged expected losses. In case of multiple parties having their input in the loss expectancies, an average might provide a better approximation of the actual losses. In this publication we will use the maximum expected losses which leans to following a risk avoidance strategy. Organisations with different risk strategies (e.g. operating risk-neutral or actively participating in risk-taking) might want to review the loss expectancy function and adjust it to their strategy [81].

Another simplifying assumption made in eq. (4.1) is that of additivity of loss amounts. For now, we assume that losses add up. This might not always be the case. At some point, overlap in losses from processes can occur having influence on the eventual impact of the security breach. More research on this phenomenon where additional loss events do not have impact ('being be shot dead twice') might result in a more accurate model. It is not included in the scope of this thesis.

Likelihood of security breach

The likelihood that losses really occur, depends on the *threats* exploiting the *vulnerabilities* identified in the *applications* used in the *business process*. In his promotional thesis, Broeze [19] distinguishes two types of quantitative risk assessment approaches. The 'Classical approach' and the 'Risk assessment approach using risk indicators'. The classical approach is characterized by applying statistical calculations to a dataset as where the risk indicator approach is characterized by decomposition and abstraction.

Broeze [19] concludes that both approaches have their merits and drawbacks. It was found that the results of the risk assessment by risk indicators were consistent with the way an auditor assesses risk but on the other hand, selecting the right key indicators, and thus maximizing the predictive power of the indicators, seemed difficult.

Threats

Even though Broeze [19] has shown the difficulties of using key indicators for modelling risk, the classical approach is not always easy to apply. As long as the risk models are built based on 'what is currently known', threat and vulnerability distributions will follow a long-tailed Pareto-like distribution [99]. The long tail originates from threat agents attacking 'outside of the model' giving many different attacks with a low occurrence per attack, but with a possibility of high impact (the so called 'black swans' [113]). When the mainstream threats and vulnerabilities are well covered by countermeasures, attackers need to be creative and find those niche market attacks in order to reach their goals.

We start by defining t as being a threat with all threats being independent of each other. $P(t)$ is defined as the probability that a threat, once present, successfully manifests itself. For simplicity, we estimate this probability by giving answers to questions that define the *type* of the threat. Lenstra and Voss [66] give the characteristics as shown in Table 4.1 as an example of variables that characterize a threat:

Table 4.1: Example of threat characteristics based on [66]

Characteristic	**Explanation**	**Choice examples**
Source of threat	Indicating if the threat comes from an external or internal party.	• External (ex) • Internal (in)
Access required for threat	Indicating if remote access suffices to realize the treat or if local access is required.	• Remote (rem) • Local (loc)
Skill required for threat	Indicating the least level of skill required to realize the threat.	• Unstructured non-technical (un) • Unstructured technical (ut) • Structured non-technical (sn) • Structured technical (st)

Using the answers to these choices, we can model the type of the threat by one event with 3 different dimensions. Working along the example choices as given by Lenstra and Voss [66] we first define the following sample spaces:

$$\begin{aligned} S_{source} &= \{ex, in\} \\ S_{access} &= \{rem, loc\} \\ S_{skill} &= \{un, ut, sn, st\} \end{aligned} \tag{4.2}$$

The total set of threat types is now given by taking the Cartesian product of S_{source}, S_{access} and S_{skill} as shown in eq. (4.3).

$$S_{sas} = \left\{ \begin{array}{cccc} (ex,rem,un), & (ex,rem,ut), & (ex,rem,sn), & (ex,rem,st), \\ (ex,loc,un), & (ex,loc,ut), & (ex,loc,sn), & (ex,loc,st), \\ (in,rem,un), & (in,rem,ut), & (in,rem,sn), & (in,rem,st), \\ (in,loc,un), & (in,loc,ut), & (in,loc,sn), & (in,loc,st) \end{array} \right\} \tag{4.3}$$

A threat type (i, j, k) is said to occur if i equals the source of the threat, j equals the access required for the threat and k equals the skills required to realize the threat. We will call such an outcome a *characteristic signature* E_t (with $E_t \in S_{sas}$). We assume that every threat can be described by a characteristic signature.

Example:
A threat t_2 is characterised by the source of the threat equalling 'external', the access required for the threat to manifest equalling 'local' and the minimal skill level required for the threat to manifest equalling 'structured-technical'. An example of such a threat would be highly skilled technical person from a competing company who needs local access to an asset to cause harm to it. The characteristic signature of the threat (E_{t2}) would be as shown in eq. (4.4).

$$E_{t2} = (ex, loc, st) \tag{4.4}$$

The typing approach allows us to specify how the specific characteristics of a threat influence the eventual threat likelihood. In our example it would mean that *If* a threat t is characterised by a signature E_t, the likelihood that the threat successfully manifests itself can be determined (eq. (4.5)).

$$P(t) : Source_t \times Access_t \times Skill_t \rightarrow \mathbb{R} \tag{4.5}$$

$Source_t$, $Access_t$ and $Skill_t$ denote the separate dimensions of a signature that influence a threat to successfully manifest itself. More specifically, their influence on the probability of threat t successfully manifesting itself is given by eqs. (4.5) and (4.6).

$$\begin{aligned} Source_t &: S_{source} \rightarrow \mathbb{R} \\ Access_t &: S_{access} \rightarrow \mathbb{R} \\ Skill_t &: S_{skill} \rightarrow \mathbb{R} \end{aligned} \tag{4.6}$$

Example:
Assume the distribution functions of the separate dimensions are given by eqs. (4.7), (4.8) and (4.8):

$$Source_t = \begin{cases} 1 & \text{if } ex \in E_t \\ 0.8 & \text{if } in \in E_t \end{cases} \tag{4.7}$$

$$Access_t = \begin{cases} 1 & \text{if } rem \in E_t \\ 0.5 & \text{if } loc \in E_t \end{cases} \tag{4.8}$$

$$Skill_t = \begin{cases} 1 & \text{if } un \in E_t \\ 0.8 & \text{if } ut \in E_t \\ 0.6 & \text{if } sn \in E_t \\ 0.3 & \text{if } st \in E_t \end{cases} \tag{4.9}$$

If a threat t_2 has a signature $E_{t2} = \{ex, loc, st\}$ we get eq. (4.10) which gives us a probability of 0.15 that a threat, once present, successfully manifests itself given the fact that the threat has been characterized by event E_{t2}.

$$\begin{aligned} P(t_2) &= Source_{t2} \cdot Access_{t2} \cdot Skill_{t2} \\ P(t_2) &= 1 \cdot 0.5 \cdot 0.3 \\ P(t_2) &= 0.15 \end{aligned} \tag{4.10}$$

Vulnerabilities

The likelihood that losses really happen depends on the *vulnerabilities* being exploited by *threats*. A vulnerability has a probability to result in loss. For this to happen, the threats must first realize the exploitation of vulnerabilities leading to a breach of an information criterion resulting in loss. We therefore define v as being a vulnerability with every vulnerability being independent of each other. We then define $P(v)$ as the probability that a vulnerability, once present, is successfully exploited.

Vulnerabilities can be modelled in a similar way as threats. One could use specific components that characterize a vulnerability [24]. An example of these components is given by Bharania [11] who suggests to characterize a vulnerability using the following dimensions:

Table 4.2: Example of vulnerability characteristics

Characteristic	Explanation	Choice examples
Running affected product?	Does the organisation use the affected product in its environment?	• Yes • No
Running affected version?	Does the organisation run a version that contains the vulnerability?	• Yes • No
Vulnerable component enabled?	Is the product configured in such a way that the vulnerability is exposed, through either explicit configuration or default condition?	• Yes • No
Workaround feasible	Are methods to prevent exploitation of the vulnerability readily available and practical to implement?	• Available, practical • Available, not practical • Unavailable • Medium • Low
Workaround implemented	Are methods to prevent exploitation of the vulnerability already in place?	• In place, working • In place, should be working • Not in place
Attack confidence?	Based upon the best available information, are exploit methods available for the vulnerability?	• High • Medium • Low
Significance collateral damage?	In a worst-case scenario, would there be substantial downstream/collateral damage to other systems that might result in addition to the initial compromise of confidentiality, integrity or availability of the affected product?	• High • Medium • Low

With components as shown in Table 4.2 , we can start a vulnerability typing process in analogy to the threat typing process. After defining the sample spaces and events we can classify a vulnerability and give an estimation on the likelihood of a successful exploitation of the vulnerability. Note that, as with the threat dimensions, the vulnerability dimensions are just an example.

Typing Approaches

Defining the type of threat itself is not an easy task [101]. Two examples of approaches that one can take in identifying the right choices and values are *a)* using expert panels (e.g. [1]) and *b)* using available data (e.g. [21, 25]). An organisation would have to decide on the dimensions of a threat/vulnerability and their values. This need not necessarily be an ad-hoc decision. Research has been done on methods and techniques that can help in the automated 'learning' of the right dimensions and their values [5, 8].

If enough data of quality is present to 'learn' the variables (and their values) that characterize threat and vulnerability, the automated learning approach on available data is initially preferred because of objectivity. Keep in mind that it remains the responsibility of the experts to come to a general consensus on (the values of) the variables and propose improvements where possible. This not only helps to prevent the computational model becoming a 'black box' where a mystical number pops up upon which decisions have to be made. It also improves intra- and inter-company communication on the quantification of risk factors.

The typing approach could be successful to threats and vulnerabilities which are still relatively unknown or subjective to change. For the better known threats and vulnerabilities, it is assumed that data is present (either internally or from external sources) on the likelihood of occurrence (take for example a very specific case researched by Rabinovich et al. [90] on the estimation of Tsunami threats and risk for the coasts of Peru and northern Chile). In the latter case, one could use a given $P(t)$ or $P(v)$, if data on the separate dimensions remain sparse.

Cumulative Threat Potential

We define c as being a 'cumulative threat', which incorporates both vulnerability and threat(s). The cumulative threat potential, or $P(c)$, depicts the probability that asset security is breached by threats exploiting a vulnerability resulting in losses. This implies that a new CumThreat has to be introduced per vulnerability of an application. As tempting as it might seem, Fig. 4.2 is not suitable for the type of reasoning in our model. If we are going to refit that representation to fit our needs, we want to combine the intuitive visual representation with a sound mathematical basis. As we are reasoning under a certain amount of uncertainty, we can reach these objectives a using Bayesian network representation [76].

"Bayesian networks are directed acyclic graphs (DAGs) in which the nodes represent variables of interest and the links represent informational or causal dependencies among the variables. The strength of a dependency is represented by conditional probabilities that are attached to each cluster of parents-child nodes in the network" quoting Pearl [85]. A demonstration on the application of a Bayesian network representation is given in Appendix F .

After translation of the regular component interaction diagram (Fig. 4.2) to a Bayesian network representation with cumulative threats (Fig. 4.3), cumulative threat likelihood can be calculated relatively easily using basic mathematics. Figure 4.3 shows a part of Fig. 4.2 in greater detail and translated to a Bayesian network representation. In this example, the case around CumThreat 2 has been explored. We read the diagram from the left to the right starting with the components identifying threats and vulnerabilities and ending with an indication of the risk of loss on a process level.

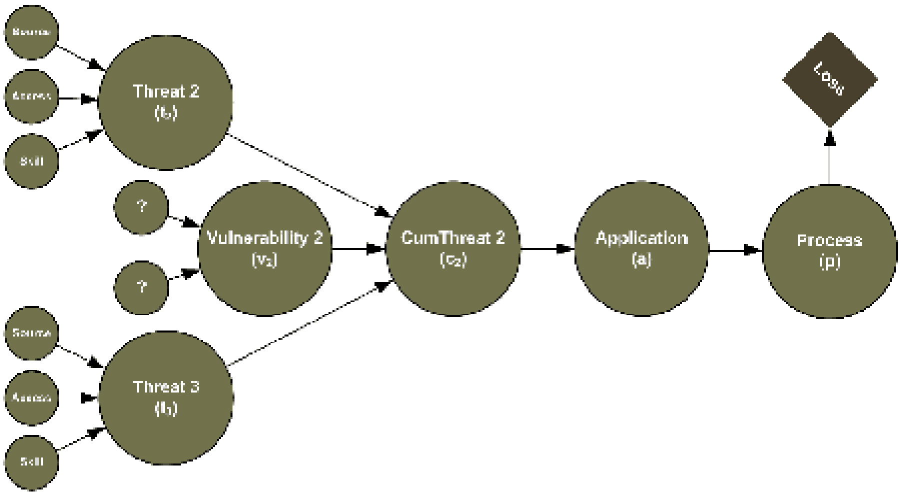


Figure 4.3: Component structure as Bayesian network

Example using Fig. 4.3 and Appendix F:
Given that the threat is typed by coming from an external party ($Source(t_2) = 1$), requiring local access ($Access(t_2) = 0.5$) and a 'structured and technical' skill level ($Skill(t_2) = 0.3$), the results are given in eq. (4.10). Threat 3 (t_3) is relatively unknown and estimated as a threat type with a probability rating of 0.5.
Vulnerability 2 (v_2) can be exploited by either of these 2 threats and has a probability that the vulnerability is successfully exploited of 0.12, based on historical data known to the organisation. The cumulative treat potential of vulnerability 2 ($P(c_2)$) equals the chance of either threat exploiting vulnerability 2. This is shown in eq. (4.11).

$$\begin{aligned} P(c) &= P(tv) = P(t) \cdot P(v) \\ P(c_2) &= P(t_2 \cup t_3) \cdot P(v_2) \end{aligned} \tag{4.11}$$

Aside from the $P(v_2)$, which is known, we have to calculate $P(t_2 \cup t_3)$ as shown in eq. (4.12).

$$\begin{aligned} P(t_2 \cup t_3) &= P(t_2) + P(\overline{t_2})P(t_3|(\overline{t_2}) \\ &= P(t_2) + (1 - P(t_2) \cdot P(t_3)) \\ &= 0.15 + ((1 - 0.15) \cdot 0.5) \\ &= 0.15 + (0.85 \cdot 0.5) \\ &= 0.575 \end{aligned} \tag{4.12}$$

We the calculate $P(c_2)$ as shown in eq. (4.13)

$$\begin{aligned} P(c_2) &= P(t_2 \cup t_3) \cdot P(v_2) \\ &= (0.575) \cdot (0.120) \\ &= 0.0690 \end{aligned} \tag{4.13}$$

Representing Current Risk

With the CumThreat approach as described above, we can now work towards a *current* information security risk indicator of process p with respect to the cumulative threat c. To indicate what type of loss can be inflicted by a *CumThreat* we first define a n-dimensional binary space and introduce a

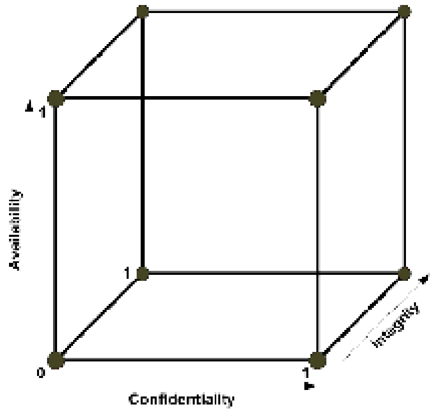


Figure 4.4: An example of a 3-dimensional binary space

dimension for each information criterion. In our example this results in the 3-dimensional binary space as depicted in Fig. 4.4 .

We can now define CumThreat type toggle T_k per information criterion based on the binary space. A CumThreat type toggle equals 1 if and only if CumThreat c may cause a breach on that specific information criterion. In our example this results in CumThreat types $T_{conf}, T_{int}, T_{avail} \in \{0,1\}$.

The current information security risk indicator of CumThreat c on process p is shown in eq. (4.14). Note how the loss function from eq. (4.1) is incorporated in this function that combines likelihood and cost.

$$R_{cur}(p,c) = \left(\sum_{k \in K} \left(T_k L_k^{\max}(p) \right) \right) \cdot P(c) \tag{4.14}$$

Which, in our case, equals eq. (4.15).

$$R_{cur}(p,c) = \left(\left(T_{conf} L_{conf}^{max}(p) \right) + \left(T_{int} L_{int}^{max}(p) \right) + \left(T_{avail} L_{avail}^{max}(p) \right) \right) \cdot P(c) \tag{4.15}$$

If we define $A(p)$ as the set of (independent) applications used in process p, and $C(a)$ as the set of (independent) cumulative threats affecting application a, the current information security risk indicator of process p is given by:

$$R_{cur}(p) = \sum_{a \in A(p)} \sum_{c \in C(a)} R_{cur}(p,c) \tag{4.16}$$

If we then assume P to be the set of all (independent) business processes, the organisation's overall quantitative current aggregated IS risk indicator is given by:

$$R_{cur} = \sum_{p \in P} R_{cur}(p) \tag{4.17}$$

4.2 Residual Risk

In a similar way the residual risk can be represented by defining a mitigation plan m countering vulnerabilities V and/or threats T (thus influencing $P(c)$). The cumulative treat potential changes because the mitigation plan works against the vulnerabilities and threats of the system. The residual cumulative threat potential $P(c_m)$ equals the chance of a vulnerability being exploited by a threat, under mitigation plan m, times the threat likelihood under mitigation plan m.

$$P(t_m) : Source_{tm} \times Access_{tm} \times Skill_{tm} \rightarrow \mathbb{R} \tag{4.18}$$

$$P(c_m) = P(v_m) \cdot P(t_m) \tag{4.19}$$

In this model we assume that the threat type toggle, is not influenced by the mitigation plan. This gives the *residual* information security risk indicator of process p with respect to cumulative threat c after mitigation plan m is carried out (eq. (4.20)).

$$R_{res}(p,c_m) = \left(\sum_{k \in K} \left(T_k L_k^{\max}(p) \right) \right) \cdot P(c_m) \tag{4.20}$$

Which, in our case, equals eq. (4.21).

$$R_{res}(p,c_m) = \left(\left(T_{conf} L_{conf}^{\max}(p) \right) + \left(T_{int} L_{int}^{\max}(p) \right) + \left(T_{avail} L_{avail}^{\max}(p) \right) \right) \cdot P(c_m) \tag{4.21}$$

If we then define an allowed set of mitigation plans M, we can now compute the residual information security risk indicator of process p with respect to cumulative threat c after the mitigation plans in M are carried out.

$$R_{res}(p,c_m,M) = \begin{cases} R_{cur}(p,c) & \text{if } M \text{ does not contain } m \text{ countering } c \\ R_{res}(p,c_m) & \text{if } M \text{ contains } m \text{ countering } c \end{cases} \tag{4.22}$$

The organisation's *residual* information security risk indicator of process p under the allowed set of mitigation plans M is defined as:

$$R_{res}(p,M) = \sum_{a \in A(p)} \sum_{c \in C(a)} R_{res}(p,c,M) \tag{4.23}$$

With P as the set of all business processes, the organisation's overall quantitative residual aggregated information security risk indicator after allowed mitigation plan set M is given by:

$$R_{res}(M) = \sum_{p \in P} R_{res}(p,M) \tag{4.24}$$

With eq. (4.24), we can find an optimal risk mitigation plan set M by minimizing $R_{res}(M)$. However, by just minimizing the residual risk, we do not take into account any budgetary constraints. For most organisations, resources for information security are not unlimited. In that case, we have to find an optimal risk mitigation plan set under a budgetary constraints.

4.3 Risk Mitigation as an Optimization Problem

Attempting to find an optimal risk mitigation plan set under budgetary constraints, we introduce the projected security investment z on mitigation plan m as given by $z(M) = \sum_{m \in M} z(m)$ and minimizing $R_{res}(M)$ under the budgetary constraint of the projected expenses of mitigation plan set M as shown in eq. (4.25).

$$\begin{array}{ll} \text{minimize} & R_{res}(M) \\ \text{subject to} & z(M) \leq Z \end{array} \tag{4.25}$$

Knapsack ILP

The knapsack problem is an important integer linear programming (ILP) problem. One could consider the situation of a camper wanting to fill up her knapsack by selecting a collection of items. Each item has a specific weight and value. The capacity of the knapsack is limited and our camper would like to maximize the total value of the items in the knapsack [63]. In short: Select a subset of items such that the total value is maximized and the total weight does not exceed the knapsack capacity [63].

Binary Knapsack Problem

According to Lenstra and Voss [66] and Pisinger [89], our optimization problem is a 'multiple-choice knapsack problem'. This multiple-choice knapsack problem is basically an integer knapsack problem where each item must be put entirely in the knapsack, or is not included at al. "Objects cannot be broken up arbitrarily... It is this 0/1 property that makes the knapsack problem hard" according to Skiena [102]. In our case, a mitigation plan is added to the collection or it is not. It is assumed that the addition of more instances of the same mitigation plan does not increase security.

The binary knapsack problem is given by eq. (4.26) [89]. It depicts a knapsack with a capacity of d units and a set of n items labelled $1,2,\ldots,n$ with item i having a weight of w_i units and a value (profit) of p_i [63].

$$\begin{aligned} \text{maximize} \quad & \sum_{i=1}^{n} p_i x_i \\ \text{subject to} \quad & \sum_{i=1}^{n} w_i x_i \leq d \\ & x_i \in \{0,1\}, \qquad i \in \{1,\ldots,n\} \end{aligned} \tag{4.26}$$

In our case, the value p_i would be the information security reduction indicator and the value w_i would be the projected expense. With n being the number of CumThreats and Q_i being the set of risk mitigation plans for CumThreat i ($i \in \{1,2,\ldots,n\}$), we can define p_{im} with $m \in Q_i$. The w_i would be illustrated by $w_{im} = w(m)$.

If c is the ith CumThreat, then

$$p_{im} = \sum_{\substack{\text{processes } p \text{ for which} \\ c \text{ affects an application} \\ \text{used by } p}} (R_{cur}(p,c) - R_{res}(p,c_m)) \tag{4.27}$$

For $0 < i \leq n$ there is a free mitigation plan m in Q_i with $w(m) = 0$ and $P(c) = P(c_m)$, corresponding to not doing anything against CumThreat c.

$$
\begin{aligned}
\text{maximize} \quad & \sum_{i=1}^{n} \sum_{m \in Q_i} p_{im} x_{im} && (4.28)\\
\text{subject to} \quad & \sum_{i=1}^{n} \sum_{m \in Q_i} w_{im} x_{im} \leq Z, \\
& \sum_{m \in Q_i} x_{im} = 1 \\
& x_{im} \in \{0,1\}, \qquad i \in \{1,2,\ldots,n\}
\end{aligned}
$$

This problem is known to be quickly solvable. Finding the optimal spending strategy will only take a few seconds at most, even for very large information security mitigation problems [70].

The optimization problem as given by eq. (4.28) considers one mitigation plan per CumThreat. Note that there is always at least one mitigation plan in place per CumThreat as the event of 'doing nothing against CumThreat' is defined as being a free mitigation plan. We could change the optimization problem to allow for more than 1 mitigation plan per CumThreat, something which would not be unthinkable in practice. For this to be workable, we would need information on overlapping impact of security measures on CumThreats. Taking the 4 types of security measures (preventive, repressive, detective and corrective) as described in Section 1.4 we can reason that impact will not (always) be a fact of simple summation.

Concluding

As also explained by Lenstra and Voss [66], the current and residual quantitative aggregated information security risk indicators cannot be interpreted as the expected loss amount for process p before and after mitigation plan set M. The current model is still too limited to compute such strong statements. It has no notice of temporal dependencies and vulnerabilities and threats are considered to be independent variables. In reality this is not always the case.

What the organisation *can* do using this model, is compare different situations to each other using eq. (4.29). This quantity gives a percentage of how much better the situation is after carrying out the mitigation plans in M, with 0% indicating no imporvement and 100% meaning that no residual aggregated information security risk is left [66]. The results are to be classified as *relative*, not *absolute* [128].

$$
\frac{100 \cdot (R_{cur} - R_{res}(M))}{R_{cur}} \qquad (4.29)
$$

For simplicity this model is deterministic in nature. If we consider the model not to be deterministic, the estimations of threat likelihood and vulnerability likelihood (type indicators) will become harder. We would have to consider other approaches using distribution functions and confidence intervals. Examples of this are given by Bier [12], who considers a game-theoretic model to analyse the level of information security. They state that, if defender and attacker are modelled as players of a game, their decisions are actually interdependent and need to be modelled as such.

Another example would be the economical model from Gordon and Loeb [38]. They define $S(z,c)$ as being the information security breach probability function (that is, the probability of an information security breach conditional on the realization of a cumulative threat c and given that the firm has made an information security investment of z to protect itself.

Concerning $S(z,c)$, we would have to make certain assumptions. As $S(z,c)$ is a probability, we must have $0 \leq S(z,c) \leq 1$. The variable z is an investment and c is a probability. Thus $z > 0$ and $0 \leq c \leq 1$. Following the work done by Willemson [130] we also define the following restrictions, based on [66, 130]:

A1 $\forall z \; S(z,0) = 0$ if initially the attack success probability is 0, it stays so after every possible investment.

A2 $\forall c \; S(0,c) = c$ if we invest no money, there will be no change in the attack success probability.

A3 The function $S(z,c)$ is continuously twice differentiable and for $c \geq 0$

$$\frac{\partial}{\partial z} S(z,c) \leq 0 \qquad \text{and,} \qquad \frac{\partial^2}{\partial z^2} S(z,c) \geq 0 \qquad \text{with} \qquad \forall c \lim_{z \to \infty} S(z,c) = 0 \tag{4.30}$$

Assumption 3 is interesting as it defines that, with increasing investments, it is possible to decrease the vulnerability level, but at a decreasing rate. In contrast to the original Gordon and Loeb model, which claims that it is impossible to decrease the information security breach probability to exactly 0 (no matter of the investment), we adopt the view from Willemson [130], who claims that it actually *is* possible to decrease the information security breach probability to (strictly) 0.[1]

If one would be able to find the right underlying vulnerability decrease function that satisfies the above assumptions, one would hypothetically be able to get good results. These functions however are strongly application area specific [130]

This leaves us with the very basic, yet widely applicable model from the previous paragraph. In this stage of the research, it is not the result that counts but the underlying cohesion of the elements used in the model. As research on this subject will progress and better data is collected to base the calculations on, it will be possible to create a usable quantitative model that can aid in information security investment decisions.

[1] e.g. if a threat is an attack by a specific person, one could get rid of that person

CHAPTER 5

SPARK

5.1 Introduction

Based on the literature review (Appendix C)and the expert interviews (Appendix B), we created a comparative framework in order to select methodologies that fit our requirements (Appendix D). After filtering the methodologies based on their characteristics, the comparative framework indicates a set of five different methodologies that fit our requirements (Appendix E). These methodologies are respectively CORAS, OSSTMM-RAV, SP800-30, SPINT and SPARK. Because all of these methodologies would hypothetically be equal in usability for our cause, a choice has to be made.

In this research the SPARK methodology is used. This choice is based on the availability on workable material of this specific methodology and its extreme ease of use. In theory every one of these methodologies could be used.

The SPARK methodology is based on the SPRINT risk analysis methodology developed by the Information Security Forum in Europe. SPARK is further enhanced and combined with ISO/IEC 27001-2005 and the more recent ISO/IEC 17799-2005 standards. Other standards (e.g. CobiT) may also be incorporated into SPARK making it very flexible. SPARK also defines additional linkages between vulnerabilities, threats and controls are defined as compared to the SPRINT methodology [61].

Decisions in the SPARK methodology are taken by the organisation's management supported by (technical) specialists. This facilitates open communication between involved parties and leads to better alignment of IT and strategy as earlier discussed in Section 1.3 [97]. The decisions are supported by a highly structured way of working, using (standard)questionnaires and documents.

Example output of the SPARK methodology can be found in Appendix G .

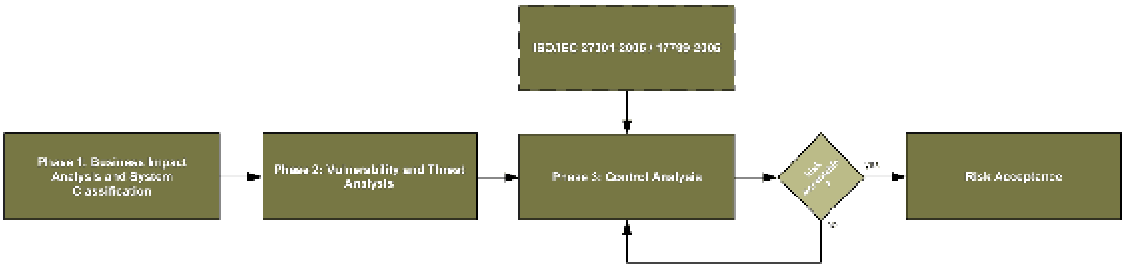

ISO/IEC 27001 2005 / 17799 2005
Phase 1: Business Impact Analysis and System Classification
Phase 2: Vulnerability and Threat Analysis
Phase 3: Control Analysis
Risk Acceptance

Figure 5.1: SPARK: Phases

5.2 Phases

SPARK currently follows a three-stage model which consists of:

Phase 0: SPARK initiation
Phase 1: Business Impact Analysis
Phase 2: Vulnerability and Threat Analysis
Phase 3: Control Analysis

For each phase, a coordinator cooperates with different persons in the organisation, in order to gain the necessary insight into the IS risk profiles associated with the selected business processes. Based on the complexity of the information system and the business process, different specialists can be included for the risk analysis [61].

Phase 0: SPARK initiation

Before a SPARK risk assessment can be done, some steps have to be taken. Because the methodology is strongly linked to the business processes and used applications and components, an analysis has to be done on these primary and secondary business processes. This phase is not SPARK-specific, but can be considered mandatory for all risk assessment methodologies using the same components.

Phase 1: Business Impact Analysis

In this phase the dependability on, and impact of information and information systems is analysed by looking at the consequences (impact) of a loss of information (in terms of confidentiality, integrity and availability) stored on, or processed by the information system. This for example can be done by interviews and workshops. Participants score an information system on the CIA constraints. This can be done on for example a three-point scale (low, medium, high). Combined with an impact table, a risk profile is started. An example is given in Table 5.1 and Table 5.2 .

Phase 2: Vulnerability and Threat Analysis

For the medium- and high-risk systems that were found in the previous phase, phase 2 is started. Based on the information system classification from the previous phase, an attempt is made at

Table 5.1: Example of SPARK business impact interpretation

Criterion	Score		
Confidentiality	*Low (protected)* Data is only accessible to a certain group	*Medium (crucial)* Data is only accessible to direct stakeholders	*High (imperative)* Business continuity is endangered on unauthorized access
Integrity	*Low (active)* Process allows limited amount of faults	*Medium (detectable)* Very limited amount of faults tolerable	*High (essential)* Process demands faultless information
Availability	*Low (desirable)* Limited unavailability is allowed	*Medium (essential)* Very limited unavailability during process times	*High (critical)* Very limited overall unavailability

Table 5.2: Example of SPARK business impact classification

Classification	Impact	Description
Low	Negligible damage (e.g. 0 ≤ damage < 10k)	Supporting system
Medium	Serious damage (e.g. 10k ≤ damage < 100k)	Important system
High	Continuity endangered (e.g. 100k ≤ damage)	Critical system

Table 5.3: Guidelines for threat/vulnerability likelihood modelling

Likelihood	Frequency
Low	Incidentally or never
Medium	Once a year
High	Multiple times a year

assessing vulnerabilities, threats and current mitigation plans in terms of confidentiality, integrity and availability of the information stored on or processed by the system [97]. Again, this can be done by workshops and interviews with stakeholders. The likelihood of the vulnerabilities and threats are modelled along the guidelines as given in Table 5.3 . The specific values can be modified to fit an organisation's special needs [61].

Phase 3: Control Analysis

In this last phase, the risk profile from the previous two phases is linked to controls as defined in ISO/IEC 270091:2005 and ISO/IEC 17799:2005 to lower the residual risk to acceptable levels. Per relevant threat and vulnerability[1] one or more controls can be chosen to mitigate the experienced risk. The eventual set of controls is formed in conjunction with the organisation's management, using structured questionnaires and reference manuals to the ISO/IEC 17799:2005 [97].

The phases are summarized in Table 5.4 . Example output of the separate SPARK phases can be found in Appendix G .

[1] SPARK does not make a clear distinction between threats and vulnerabilities.

5.3 Flowcharts

The introduction of the computational model from Chapter 4 into the SPARK methodology, will influence its original flowchart (Fig. 5.2). Starting in phase 2, a possibility is added to chose between a qualitative or quantitative approach. Following the workflow implementation as described in Appendix H figs. 5.3 and 5.4 are created. The flowcharts (figs. 5.2 5.4) clearly show the distinction between the different phases.

The (original) qualitative branch of the methodology is as shown in Fig. 5.2 . This is the flowchart we use as the base of our quantitative implementation. First we have to make an assessment of the availability of necessary components for the insertion of a quantitative branch. If a necessary component is not present, it should be incorporated in the current workflow before proceeding to the next step. This is as shown in the workflow depicted in Fig. H.1 of Appendix H .

In Fig. 5.3 we see the quantitative alternative to the second, third and fourth phase of the SPARK methodology. Phase 0 and 1 of the SPARK methodology contain all the necessary components to proceed with the creation of the quantitative branch. By following the quantitative from Chapter 4 , Fig. 5.3 is created, which is an example of a quantitative branch (and by no means the only possible solution). This results in the workflow as shown in Fig. H.2 of Appendix H .

Notice that the difference between a qualitative approach and the quantitative approach, starts directly after phase 1 of the SPARK methodology. Linking the quantitative branch to the original process flow of the SPARK methodology is just a matter of inserting a branch decision node. This way, the practitioner has the possibility to take both individual approaches or chose to do them in sequence (qualitative → quantitative). The complete flowchart with both approaches incorporated is shown in Fig. 5.4 .

Now that a complete flowchart is created, the practitioner needs to carefully review the flowchart for improvements, keeping suitability and usability of the methodology in mind. After the improvements have been identified, they can be implemented. Both steps are respectively shown as workflows in figs. H.3 and H.4 of Appendix H .

5.4 Conclusion

In this chapter we have shown that an addition of a quantitative branch to an existing qualitative methodology is not necessarily a complex task. Our combination of a quantitative model and the SPARK methodology turned out to be almost a perfect match component-wise. The workflows as given in Appendix H should make it possible to use our presented quantitative (ALE) approach in various (suitable) methodologies (see: Appendix D).

Table 5.4: SPARK phases summarized

	Phase 0	**Phase 1**	**Phase 2**	**Phase 3**
Goal	Analysing and defining information systems, processes (process owners) and assets.	Assessing corporate risks associated with the use of information systems in support of selected business processes.	Assessing threats, vulnerabilities and existing controls in the information system or related business processes.	The selection of additional security controls to reduce the identified threats and vulnerabilities found in phase 2 to a level acceptable for the organisation.
Core activities	Together with relevant employees and available formal specifications, identification of systems, processes, applications and/or assets.	Together with the process owner, identification and measurement of corporate risk associated with the use of information systems in the support of business processes by analysing the consequences of a loss of confidentiality, integrity and availability of the information stored, processed or transported by the relevant information system. Impact is measured in terms of consequences of these losses to the corporate business processes.	Together with relevant employees, identification and measurement of threats and vulnerabilities regarding the confidentiality, integrity and availability of the information systems and taking stock of the existing systems and process controls to reduce these threats and vulnerabilities.	Linking threats and vulnerabilities from the provided control sets to the residual risks identified in phase 2. Confidentiality, integrity and availability each have their own control set allowing for specific and focused reduction of threats and vulnerabilities in each of these areas.
Results	An overview of the organisation and system components including processes, information systems, applications and information criteria.	An overview of the information systems and the perceived corporate risk arising from the use of these systems, including a classification of the system in terms of availability, integrity and confidentiality.	An overview of current threats and vulnerabilities after controls according to nature and extent of potential damage. Based on these results, management can decide whether the residual level of risk is acceptable or that additional controls need to be implemented.	Overview and action lists with regards to the security controls to be implemented and identification of a time line and action owner for each action item.
Tools	To be decided.	Business Impact Assessment questionnaires.	Threat, vulnerability and control assessment questionnaire.	Control sets and action lists.
Sub-activities	*a)* Identifying information systems, *b)* Identifying business processes, *c)* Identifying business applications, *d)* Identifying information criteria	*a)* Identifying information system links with a business process, *b)*Assessment of corporate risk arising from the use of these systems, *c)* Classification of the information system	*a)* Identification of relevant employees, *b)* Collection and filing of information, *c)* Assessment of threats, vulnerabilities and existing controls, *d)* Assessment of residual risk.	*a)* Determination of non-acceptable residual risk, *b)* Selection of security controls, *c)* Filling out action lists.

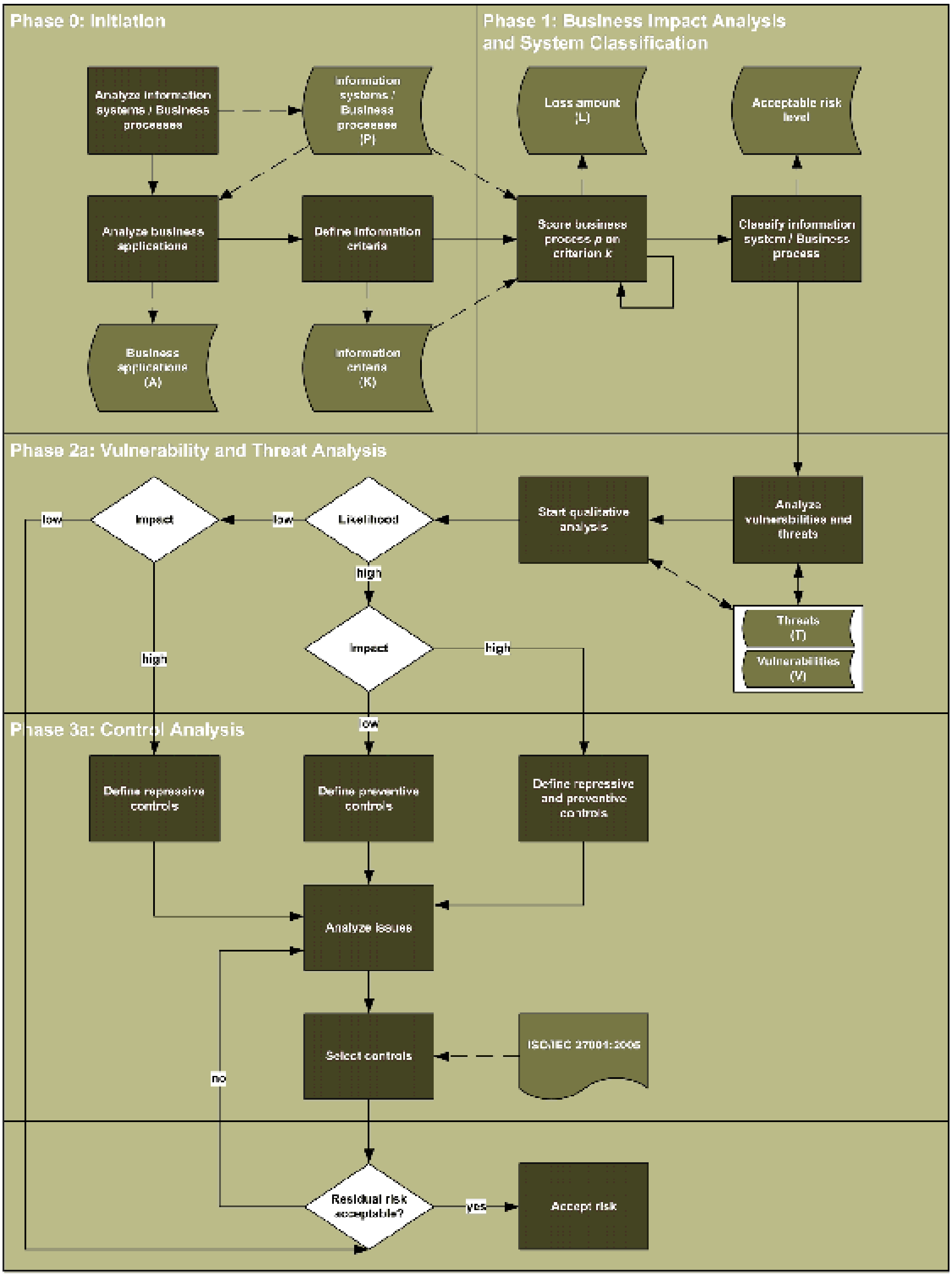

Phase 0: Initiation
Phase 1: Business Impact Analysis and System Classification
Analyze information systems / Business processes
Information systems / Business processes (P)
Loss amount (L)
Acceptable risk level
Analyze business applications
Define information criteria
Score business process p on criterion k
Classify information system / Business process
Business applications (A)
Information criteria (K)
Phase 2a: Vulnerability and Threat Analysis
low
Impact
low
Likelihood
Start qualitative analysis
Analyze vulnerabilities and threats
high
high
Impact
high
Threats (T)
Vulnerabilities (V)
Phase 3a: Control Analysis
low
Define repressive controls
Define preventive controls
Define repressive and preventive controls
Analyze issues
Select controls
ISO/IEC 27001:2005
no
Residual risk acceptable?
yes
Accept risk

Figure 5.2: SPARK: Flowchart with phases

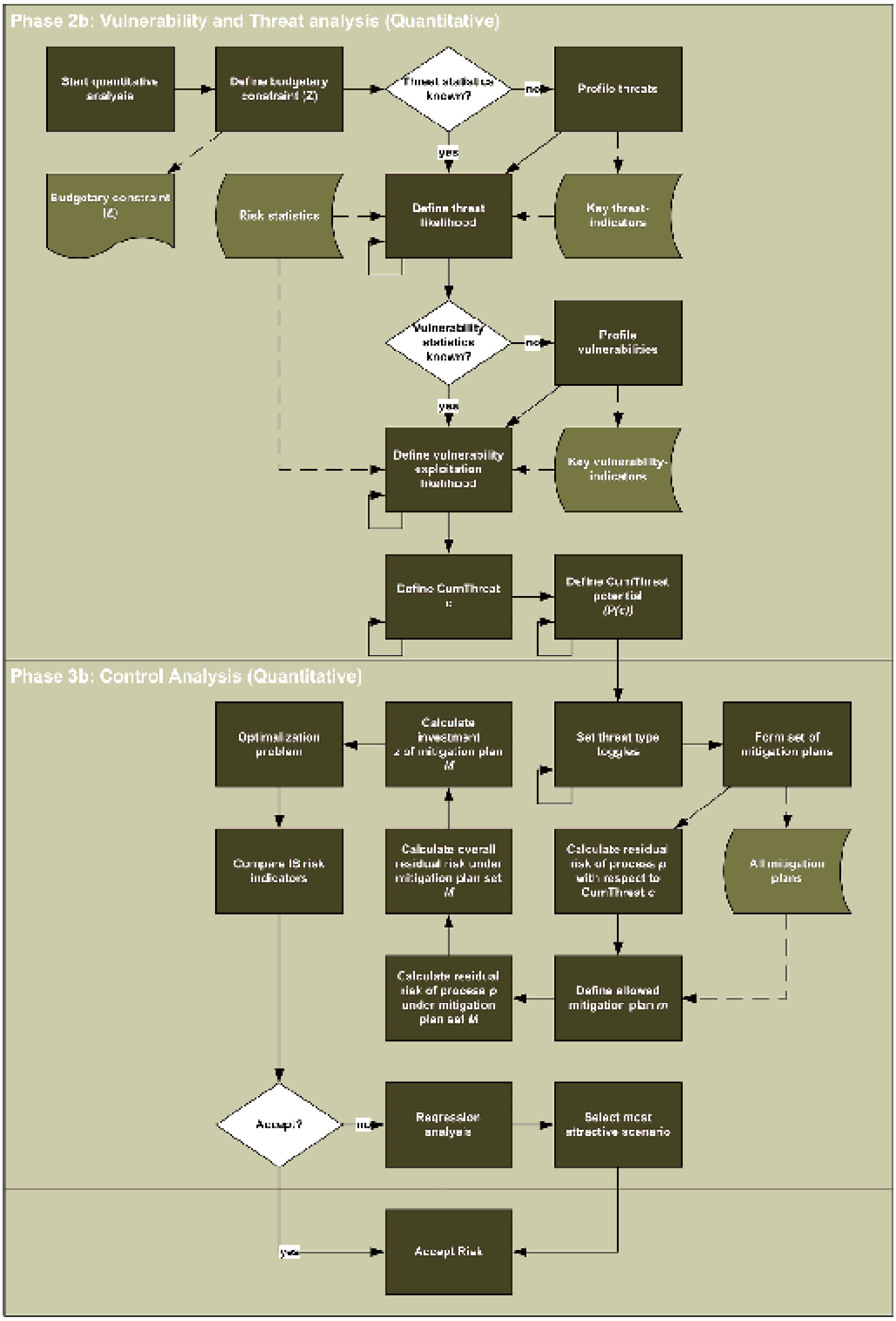

Phase 2b: Vulnerability and Threat analysis (Quantitative)
Start quantitative analysis
Define budgetary constraint (Z)
Threat statistics known?
no
Profile threats
yes
Budgetary constraint (Z)
Risk statistics
Define threat likelihood
Key threat-indicators
Vulnerability statistics known?
no
Profile vulnerabilities
yes
Define vulnerability exploitation likelihood
Key vulnerability-indicators
Define CumThreat c
Define CumThreat potential (P(c))
Phase 3b: Control Analysis (Quantitative)
Optimalization problem
Calculate investment z of mitigation plan M
Set threat type toggles
Form set of mitigation plans
Compare IS risk indicators
Calculate overall residual risk under mitigation plan set M
Calculate residual risk of process p with respect to CumThreat c
All mitigation plans
Calculate residual risk of process p under mitigation plan set M
Define allowed mitigation plan m
Accept?
no
Regression analysis
Select most attractive scenario
yes
Accept Risk

Figure 5.3: SPARK: Quantitative branch

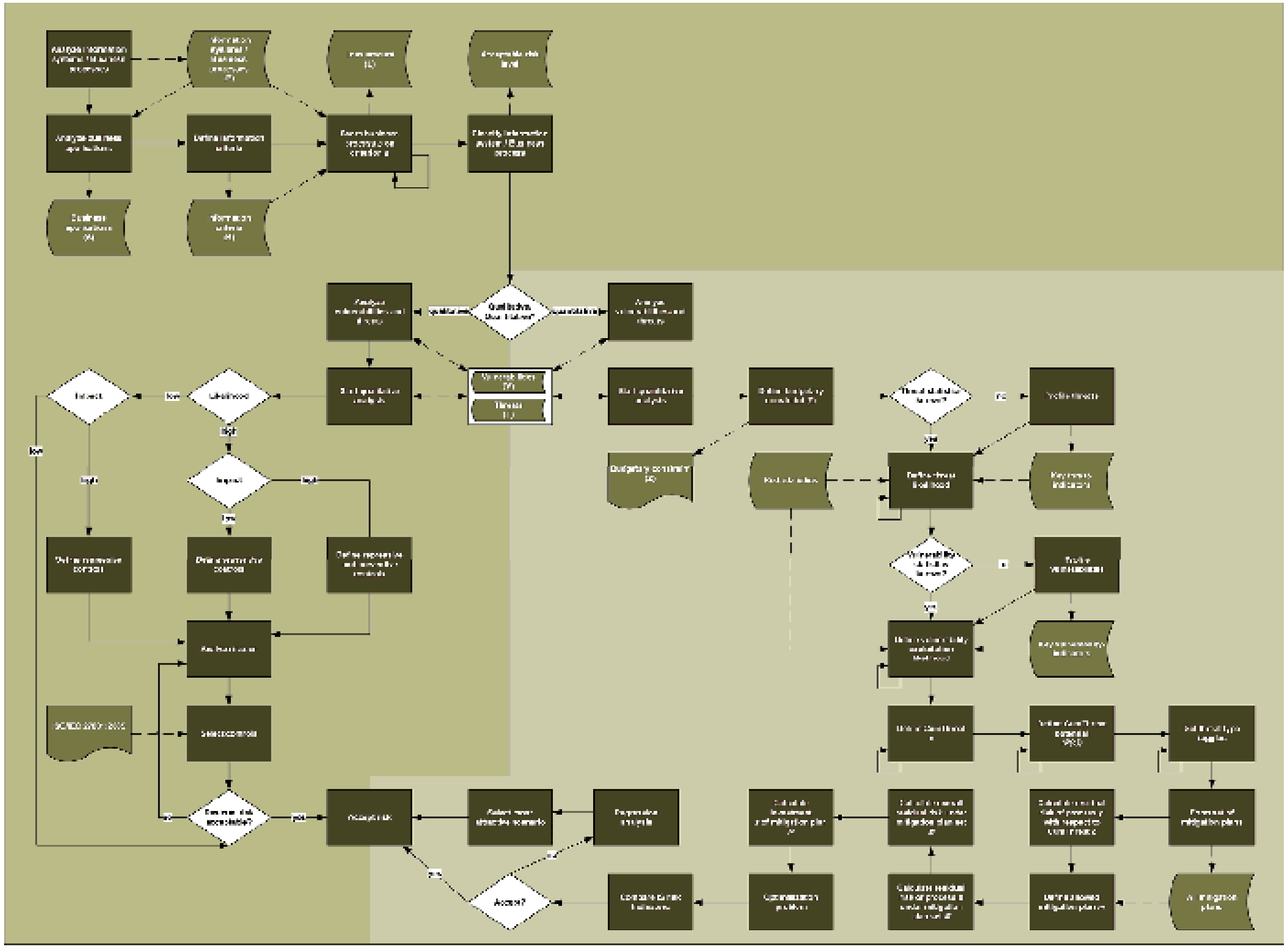


Figure 5.1: SPARK: Phased, Duo-Branched Flowchart

CHAPTER 6

EVALUATION

6.1 Evaluation of the quantitative model

Organisations have to determine appropriate protective measures to increase information security levels. These measures have to be determined keeping an optimal allocation of resources into account. These issues have been the discussion of the previous chapters. We have introduced a computational (accounting) model based on loss expectancies and added it to a popular risk assessment methodology named SPARK, forming one quantitative model.

Models (and accompanying tools), exist to assist an organisation in the above stated decision making process by giving a simplified representation of reality. For the decisions based on the model to be valid, it is essential to understand which models are appropriate for what kind of situations. The quantitative model has to be assessed and evaluated to ensure that decision-makers understand the strengths and weaknesses of the model [96].

Rue et al. [96] go on explaining that every model has its own characteristics. In order to be able to assess and compare the different models they have constructed a framework to evaluate the appropriateness of the decision supporting models in specific situations. This framework is as depicted in Table 6.1 . In the following paragraphs, the characteristics will be explained in further detail and put against the quantitative model as given in chapters 4 and 5.

Type or form

The computational structure and overall approach of the model give it it's type or form. The structure supports the way the model is applied and determines what kind of inputs are needed, how computationally complex the model is and, for example, if the model is deterministic or stochastic.

The quantitative model we have introduced in the previous chapter applies accounting principles to

Table 6.1: Framework for classifying models of information security economics (based on [96])

Characteristic	Description
Type or form	The class of model and its mathematical/computational structure
History and previous applications	When and for what purpose the model was originally developed and where it has been applied successfully
Underlying assumptions	Includes simplifications made to enable easier application
Decisions supported by the model	The types of decisions that a decision-maker would be able to substantiate through proper application of the model
Inputs and outputs	The quantities or attributes that the model manipulates
Parameter and variables	Elements that affect the way in which the model transforms inputs to outputs
Applicable domain and range	Temporal and physical ranges of inputs, outputs, parameters, and variables that the model describes
Supporting data	Evidence that the model accurately represents the phenomena of interest

information security. A basic security function is defined which takes information security expenditures as an input and gives increased security levels as an output minimizing expected loss. Parts of the model are deterministic in nature and the model applies a binary knapsack algorithm to come to the most optimal solution. The knapsack problem is one of the easier NP-hard problems [36, 88] that can be solved in pseudo-polynomial time by either branch-and-bound algorithms, dynamic programming, or a combination of both [70].

History and previous applications

The ALE accounting model on which the model in this thesis is based, has a rich history in other sectors. Before its usage in the information security sector, loss expectancies were already a frequently used tool in the determination of risk in other sectors such as the accounting and the insurance sector. These industries are influencing information risk management by offering information risk insurance policies, insuring an organisation's losses from information security breaches [39].

More information about the history and previous application can be found in Section 3.5 .

Underlying assumptions

During the construction of the quantitative model certain assumptions were made which influence the model and its applicability. Our model considers independent vulnerabilities and independent threats to form cumulative threats to assets. It is assumed that a cumulative threat can be mitigated by two scenarios. By making security investments:

1. We make the asset less vulnerable, and/or
2. We lower the threat likelihood.

With a cumulative threat potential being formed by a threat likelihood and a vulnerability exploitation likelihood as shown in eq. (4.11), we automatically make an assumption about 2 special scenarios.

1. When the threat likelihood equals 0 ($P(t) = 0$), there is no threat to an asset and cumulative threat will equal 0 ($P(c) = 0$)

2. When the vulnerability exploitation likelihood equals 0 ($P(v) = 0$), the asset is considered to be invulnerable and cumulative threat will equal 0 ($P(c) = 0$).

These scenarios can also be found in Fig. 4.1 of Chapter 4 .

The quantitative information security model as given in this thesis, assesses the organisation at one single moment in time. It is a so called one-period model [96]. We assume that security investment decisions can be made based on a snapshot of the current situation. Effective use of the model therefore requires an iterative approach, with a high frequency given the rapid changing environment of information security [109].

At some points during the construction of the current model, simplifying assumptions were made with regard to additivity and independence. For example eq. (4.1) in Chapter 4 assumes that loss amounts can be added-up. This might not always be the case and is an issue that should be taken into account upon using the model.

Decisions supported by the model

The model takes a quantitative approach to information security risk management and gives means for a meaningful interpretation of the effect of risk mitigation. Additionally, it helps in determining the optimal risk mitigation strategy by giving means to find an optimal allowed set of mitigation plans under a budgetary constraint.

Inputs and outputs

The quantitative model uses a variety of inputs. We distinguish:

- A collection of independent business processes, applications and information assets.
- Loss amounts aggregated over the assets, applications, processes and organisation.
- For each application, a calculation of the risk at hand, by assessing threat likelihood and vulnerability exploitation likelihood.
- The function that calculates annual loss expectancies to show relative increases in information security level.

The model considers disjoint sets of information assets to calculate loss expectancies. For the model to be usable, the organisation should be able to identify these distinct information assets. The same goes for the business processes and applications; they should be modelled as disjoint sets in order for the model to work correctly at this moment.

Loss amounts, or value of the assets need to be estimated. Even though the model only supports an indication of relative improvement on this moment, an attempt should be made to estimate the values with a high confidence level and low margin of error. This way, the model will be a better representation of the reality and provide better results. Consider the situation where an information asset is strongly under-valuated relative to the other information assets. This will immediately influence the loss expectancies, especially under increasing risk. It is therefore desirable that the value estimations are at least correct *in relation to each other*.

The same goes for the estimation of vulnerabilities and threats to the assets. This can be very difficult in the rapidly changing environment of information security. This calls for uniformity in the method to assess these vulnerabilities and threats which is given by phase 2 of the SPARK process.

The information security function as proposed in the previous chapters is very general in nature, making it fit for general use. The annual loss expectancy approach is a common approach in (macro) economic analysis. The function captures security levels based on these monetary loss expectancies. Monetary loss expectancies can represent a great part of the real-world situations and easily fit in budgeting activities. In some situations, monetary loss expectancies might not be representative of the real-world situations. Take for example the girl who called the people who had done the HIV tests falsely telling them they were tested positive (see Section 3.2). The losses incurred in this situation are hard to quantify. What value would be put to a loss in reputation? These situations should always be kept in mind when applying the model.

Given the inputs and the security function, the model provides an organisation with relative levels of security. The accuracy of the model therefore depends on the quality of the inputs and the correctness of the security function. The security function gives a decreased risk on lowered threat likelihood and vulnerability exploitation likelihood. It does this, not taking interdependencies into account between the elements of a set of threats, vulnerabilities and mitigation plans (independence). For example, mitigation plan x may totally mitigate vulnerability y but introduces a new vulnerability z. The model in it's current form does not take these interdependencies into account. This is a purposely introduced limitation that should be kept in mind on applying the model.

Parameters and variables

On this moment the quantitative model calculates loss expectancies based on CumThreats and information criteria. Losses on a certain information criterion are modelled by using CumThreat type toggles. A toggle is set if the CumThreat can cause losses on a criterion. It is assumed that these toggles do not change when working from a current to a future situation.

Other variables (and dimensions) are used for the characterization of threats and vulnerabilities. These variables have to be changed over time to accurately describe the threats and vulnerabilities. By using a Bayesian network, our example has the possibility to automatically update values of variables upon the introduction of new information.

Applicable domain and range

The quantitative model is to be applied to an organisation that has information assets of value and resources to protect it. Additionally an organisation needs to take into account:

- The value of their information assets (represented as monetary value)
- The vulnerability of their information assets (represented by a probability)
- The likelihood of a threat manifesting itself (represented by a probability)
- The effectiveness of the safeguard/mitigation plan (represented as decrease in loss)
- Means for determining a correct approximation of the real world scenario with the model
- *Optionally:* The values of certain threat characteristics (approximating threat likelihood)
- *Optionally:* The values of certain vulnerability characteristics (approximating vulnerability exploitation likelihood)

Supporting data

The quantitative model in its current form is rather simple. This has the merit that expected losses can be aggregated, which is much simpler than aggregation of other risk related quantities based on loss variation per event and distribution functions [66]. Expert interviews on usability requirements indicate that this simplicity is desirable in order to create a workable quantitative model in a rapidly changing environment that allows for meaningful aggregation.

Solid empirical evidence that this accounting model correctly represents the situation under research is difficult to find. Evidence can be sought in two different directions.

1. The application of the same or similar models in practices other than information security. This can show the merits and flaws of the model in other practices. It is however unsure if these cases may be directly translated to the information security practice.
2. The application of slightly different models within the practice of information security. Even though most approaches on risk assessment in the information security practice are qualitative in nature, attempts have been made to work towards a more quantitative model. Examples of this are the ROSI and ROISI models [74, 82]. Although there are similarities in the taken approach, these other models are more specific in application and this would theoretically limit general applicability.

Even though studies have been done on both the translation of similar models from other practices (e.g. [10, 34]) and different models from the same practice (e.g. [35, 114]) to the model as discussed in this thesis, this can not be seen as evidence of a correct representation.

6.2 Strengths and Weaknesses

Making the strengths and weaknesses of the quantitative model explicit will create a better understanding of the model for future developers and practitioners [96]. In order to do so, Rue et al. [96] use seven guiding principles inspired by a methodology used to compare different projects in terms of greenhouse gas emission reduction [41]. The choice of this methodology might seem illogical at first, but there are many underlying similarities. As in our information security model, economic investments have to be made in projects countering a phenomenon. In a same way, the greenhouse gas protocol takes into account vulnerabilities, threats and risks that possibly require an extensive analysis.

The following paragraph discusses the seven guiding principles from Rue et al. [96] and applies them to the model as developed in this research paper.

Is the model relevant? Does the model use data, methods, criteria, and assumptions that are appropriate for the intended use of reported information?

The model as presented in this thesis uses basic elements as independent threats, independent vulnerabilities, losses and mitigation plans to come to an output. The output of the model is only relevant in relation to other situations where the same calculations are made using the same model. Dependencies and weighing factors are omitted for reasons of simplicity and in avoidance of possible misleading assumptions.

Is the model complete? Does the model consider all relevant information that may affect the accounting and quantification of model inputs and outputs and complete all requirements?

The model is limited to quantifiable inputs. Operating within this limitation, the model iteratively supports all possible scenarios. It is the responsibility of the party who executes the model to make sure all relevant inputs are given to the model. It is made explicit how the inputs can be defined and values can be collected.

Is the model consistent? Does the model use data, methods, criteria and assumptions that allow meaningful and valid comparisons?

The methods and procedures used in the model will provide consistent relative outputs that can be compared. This holds under the assumption that internals like threat likelihood typing and vulnerability exploitation typing do not change between runs. If the internals are changed (for example: new evidence is found indicating an increased vulnerability exploitation likelihood), the calculation has to be done using the new internals. This includes all previously done calculations. If this is consequently done, the results give an accurate relative representation.

Is the model transparent? Does the model provide clear and sufficient information for reviewers to assess the credibility and reliability of a model and claims derived from it?

Depending on the actual implementation of the model, it should be transparent. Information about the usage of the model is present, which allows for a review of credibility. Should a developer decide to hide and protect some internals of the model, it should be properly documented to maintain transparency.

Is the model accurate Does the model reduce uncertainties as much as is practical?

Uncertainties with respect to input measurements, estimates and calculations should be reduced as much as is practically possible. Additionally, developers and practitioners have to avoid bias in their measurement and estimation methods. This will increase the credibility of the results of the model. If it is known that accuracy is sacrificed along the way, it is best well documented and consequently done during an assessment. This ensures that the end results will still be comparable, and that future uncertainty is minimized.

Is the model conservative Does the model use conservative assumptions, values, and procedures when uncertainty is high?

As is also discussed in Section 3.7 , the impact and results of the quantitative model should not be overestimated. Nor should it be used for transfer of responsibility. Conservative values are those that are more likely to underestimate than overestimate changes from an initial situation. When there is uncertainty, and when the costs to reduce this uncertainty are not worth the increase in accuracy, conservative estimations are favourable.

Does the model provide insight? Does the model clearly state the nature of the insights that are provided by the model?

The model serves to provide a means for decision makers to get insight in, and control over a gap between an initial and a desired state of information security. The outputs of the model are of no use on their own. They get their meaning in relation to the other outputs of the model.

6.3 Usability Requirements

The interviews as described in Appendix B resulted in, amongst other things, a list of usability requirements (see: Table B.2). They were taken into account upon developing the quantitative model. In this section the most often heard requirements are discussed and put against the quantitative model to evaluate its conformance to the given requirements.

R1: *The model should be built on (or be) a publicly available, proven standard.*
The quantitative model itself applies basic mathematical constructs to link together the components. The underlying structure is publicly available and has proven itself to be suitable in other sectors. This does not directly mean that it is suitable in the information security practice and should be tested first. During the mitigation plan set construction phase, control sets are formed. These may be made from controls as specified by the organisation itself, or from controls from some standard. In the last case, the set might not be publicly available.

R2: *The model should not be a black box.*
The components used in the quantitative model are all identifiable and their relationships are defined. The model itself is far from a black box. However, a practitioner might wish to build a tool on this model which will hide parts of the components. This issue is out of the scope of this research. This open nature of the model gives possibilities to validation of the methods used, but also gives the possibility for practitioners to 'tinker' with the internals, causing a breach in the model's integrity.

R3: *The model should give consistent, verifiable answers.*
When internals are kept constant, the quantitative model should give consistent answers. The open nature allows for the verification of the process to come to an answer.

R4: *The model should not attempt to work towards a solid claim of loss and damage.*
The output of the security function is a decrease or increase in relative security level. The quantitative model makes no claims to precise loss, profit or damage. It only described relative improvements.

R5: *The model should have a clear focus and should not have too wide a scope.*
The quantitative model has a limited scope of organisation wide information risk assessment and focusses on business processes, assets used in the business processes (and their value), vulnerabilities to the assets and threats to the vulnerabilities.

R6: *The model should not be too detailed.*
The level of detail is up to the practitioner choice. When making decisions on abstraction of variables, one must document the abstractions and have evidence that the abstractions are valid. A pitfall of the quantitative model could be to define big sets of variables. Oversight can be lost and the model will suffer from fallacies as experienced in earlier generation methodologies (see: Section 3.5).

R7: *The model should be fast to apply with low assessment costs.*
For single situations, the calculations can be done manually. Given the number of variables, the model soon becomes infeasible to handle manually. When this is the case, some sort of automated tool (e.g. a Bayesian network, Appendix F) might be used which will cost resources to acquire, implement and use. The unavailability of the necessary data might inhibit fast application of the methodology and may also require an organisation to introduce changes in their information management process. In such cases, assessment costs will rise.

R8: *The model should be as simple as possible.*
The quantitative model as described uses basic components found in risk assessment practices. They should come as no surprise to practitioners who should be able to handle them.

R9: *The model should be easy to understand by management.*
The quantitative model stimulates intra-organisation communication as described earlier in Chapter 4 . Results consist of relative improvement figures per mitigation plan and reports on the domain in which the figures are applicable (e.g. boundaries, assumptions). Awareness is an important part of the risk assessment process.

R10: *The model should have a visual component.*

The quantitative model as described in this research does not explicitly dictate the usage of a visual component. A suggestion is made to use Bayesian networks to structure and solve the problems. This remains an issue to be solved by the practitioner at this point.

R11: *The model should be usable from a strategical level to an operational level.*

The information used in the risk assessment process originates from business processes that span all layers of the organisation (see figs. 1.6 and 3.5). This makes the risk assessment a vessel of communication and a tool assisting in awareness.

R12: *The model should have a notion of an information security baseline or minimal level of security.*

The quantitative model as given in this research has a notion of an 'as-is' situation and compares this to a hypothetical future situation. This approach is as discussed in Chapter 1 . An organisation has the possibility to build scenario's without countermeasures, with an information security baseline in place and with extra controls in place, which can then be compared in terms of relative effectiveness.

R13: *The model should be aimed at business processes and information systems, with a possibility to find clusters.*

The quantitative model does indeed consider business processes and information systems in the broadest way of the definition (that is, not limited to applications, but also taking into account information, infrastructure and people as shown in Fig. 3.3). The possibility of clusters, in terms of interdependencies, is not part of the model on this moment.

R14: *The model should keep a note of 'blind spots' and weak points.*

The shortcomings, assumptions and limitations of the model as described earlier in this chapter, should always be taken into account and communicated to the parties held accountable for the decisions based on its output.

R15: *The model should have the possibility to abort the quantification if the qualitative approach should suffice.*

This requirement assumes that a quantitative risk assessment is a logical follow-up after a qualitative risk assessment. This need not always be the case, but seems a logical assumption in practice. In the SPARK example as shown in Chapter 5 , this was easily done by creating two different tracks of respectively a qualitative risk assessment and a quantitative risk assessment. When properly implemented there should be no problems on falling back to the qualitative risk assessment. Accountable parties do have to be informed of this decision, the reasoning behind it, and its implications.

R16: *The model should have a pragmatic approach.*

The quantitative model addresses a problem as found in the every day practice of information security professionals. It is up to the practitioner to mould the methodology to his desire. As the model is built on the requirements set by the information security professionals, a certain degree of pragmatism can be assumed.

R17: *The model should be able to handle a rapidly changing environment.*

The quantitative model supports a rapidly changing environment by being iterative in nature. The Bayesian network example of Appendix F has the possibility to real-time update values throughout the network upon receiving new information.

R18: *The model should retain a link to reality.*

The link to reality should always be kept in mind as the model should be a representation of the reality. On one hand there are the limitations that break the link to reality by not (yet) considering dependencies between system components. On the other hand, uncertainty *is* a part of the model.

R19: *The model should be aimed at creating awareness.*
The primary objective of the quantitative model to get insight in and control over a gap between a current and a desired state with regard to information security. This insight in the gap is a step forward in awareness. Also, the participation of people of all layers of the organisation stimulates communication and raises awareness.

R20: *The model should prioritize, not prescribe.*
The quantitative model gives relative improvements in information security as an output. It does this by comparing mitigation plan sets on their effectiveness. A mitigation plan set indicated as 'optimal' will consist of a certain amount of mitigation plans. Practitioners then have to decide if this solution is desirable or if the plans need modification. If the plan is adjusted, it should be verified once more against the model to ascertain the results.

R21: *The model Should have a notion of time.*
Due to simplifying design decisions, the element of time was not explicitly included in the model. Time dependencies would have made the initial model too complex. Time dependencies can be implemented in later stages of development to let the model more accurately describe reality.

Conclusion

As can be seen, not all requirements can be fully met by the quantitative model on this moment. We can make a distinction between between requirements that cannot be covered because of a fallacy of the approach taken in the model and requirements that cannot be covered by the model on this very moment because of time and scoping constraints. The latter reason dictates that some requirements might be covered in the future but for now remain future work.

Most requirements that were not met involve (complex) dependencies of internal components. Requirement 13 (clustering processes and assets) and requirement 21 (time dependency) are good examples of such requirements. These requirements mainly follow from the 'link to reality' requirement (R18). It is up for discussion up to what level the model should represent reality and where simplifying assumptions can be made.

Other requirements require at least some formal and/or empirical form of verification to be positively marked as 'met'. Examples can be found in requirement 3, 7 and 16.

CHAPTER 7

SUMMARY AND CONCLUSION

In this chapter we will look back at the research as performed in this thesis. Firstly, issues are discussed in combination with the context in which the research takes place. This section is followed by a section discussing the contribution of this thesis on solving the stated issues. This chapter is ended by concluding remarks and a discussion on future research.

7.1 Context

Chapter 1 described how organisations are struggling to get a good grip on risk issues and risk management processes in spite of the fact that they are aware of a need for better risk management. Increased losses on information security give the organisations reasons to worry but little research is available to these organisations to get a grip on the situation. Meanwhile, the advances in technology ensure a complex and rapidly changing environment which calls for more rigorous approaches. Standard security solutions

Current practices in residual information risk management seem to favour a qualitative approach which is easy and fast in application but lacks the support of rigid figures. This may make the approach considerably subjective and/or imprecise in the eyes of senior management. Nevertheless, the ease of application, combined with the expected cost and complexity of the quantitative approach makes the qualitative approach an often used and valuable approach to information risk management.

The bad reputation of the quantitative approach originates from the time when the approach was considered excessively complex, unable to successfully deal with uncertainty and based on information that was sparse. However, times are changing and more modern (quantitative) approaches, aided by the same technological advances as discussed earlier, can overcome (some of) the flaws of the earlier generation quantitative models and be a valuable addition to an organisation's (information) risk management toolbox.

7.2 Contribution

The objective of this research was to come to a quantitative approach that helps an organisation get insight in, and control over their residual information risk. By working towards this quantitative approach we attempt to create an understanding of the applicability of quantitative models in residual information risk management.

The process of working towards this quantitative approach entailed giving answer to the question of what makes a quantitative approach practical and usable. Within this process we combine a suitable (qualitative) methodology with a fitting computational method.

A suitable (qualitative) methodology was selected by constructing a comparative framework (Appendix D) based on an extensive literature review (Appendix C) and expert interviews (Appendix B). The comparative framework gives an overview of the existing methodologies and their characteristics. Based on certain usability requirements given by experts and suitability requirements derived from Information Risk Management research, methodologies are compared and selected (Appendix E).

Taking a similar approach, an applicable computational method was selected. This method needed to be practical and workable but also have the possibility to be combined with the methodology of choice. For this, existing computational methods were found during a literature review (Chapter 3). Characteristics of the methods were compared to usability requirements originating from experts in the field (Appendix B)and requirements related to the compatibility with the methodology. Eventually, an ALE approach was chosen and motivated (Chapter 4).

The ALE approach that was chosen first needed to be adapted to be compatible to the methodology. In its original form it was too limited to accurately describe the components of the methodology. A revised ALE approach, now making a distinction between threats and vulnerabilities, was constructed that fit the compatibility requirements. Making use of a Bayesian network-like representation with cumulative threats (Chapter 4), which consist of combined threats and vulnerabilities, definitions were given for the calculation of current and residual information risk. By translating 'risk mitigation under a budgetary constraint' to a multiple-choice binary knapsack problem, we make the initial problem quickly solvable.

Structuring the problem as a Bayesian network gave us the possibility to easily calculate the cumulative threat potential of threat-vulnerability combinations under a certain amount of uncertainty. The sound mathematical structure of conditional probabilities from the Bayesian network, combined with its intuitive visual representation, give the practitioner the building blocks needed to analyse the possible scenario's and act accordingly (Appendix F).

The (SPARK) methodology has been analysed in detail (Chapter 5 and Appendix G). The computational method, that was made compatible with the every day residual risk management practice has been added to the workflow of the SPARK methodology. Flowcharts have been created to show how the computational method can be applied within the methodology and what needs to be changed in order to facilitate this insertion.

The form of the quantitative model has been evaluated by using a framework for the classification and comparison of models that discuss security investments and related decision-making activities. This approach allows for quick comparison between models. Additionally, the internals of the quantitative model have been evaluated by discussing 7 guiding principles. From this, the strengths and weaknesses of the model are derived.

The complete quantitative model has also been evaluated on the coverage of the usability requirements as derived from the expert interviews and the literature review. Distinction was made between problems that are inherently linked to the usage of this specific model, and problems that can be addressed in the current model but remain future work.

Together, the above named elements formed the foundation for understanding the applicability and possibilities of using a quantitative approach in residual information risk management (Chapter 6). A start was made working towards a quantitative approach that can help an organisation get insight in, and control over their residual information risk.

7.3 Conclusion

The research shows that it is theoretically possible to take a quantitative approach that helps to get insight in, and control over the residual information risk of an organisation. Within boundaries we can conclude that the quantitative information risk assessment can be a valuable activity to an organisation desiring this insight, control and alignment.

The presented quantitative approach to information security risk management can give a meaningful quantitative interpretation of the effect of risk mitigation and allows for determination of the optimal risk mitigation strategy under a budgetary constraint. In the presented approach we make no solid claims of possible loss and damage to an organisation. The results are meaningful *in relation* to each other. Nevertheless, the results of the approach will be of higher quality, and have more meaning, if the inputs are sufficiently accurate.

The fallacies of the earlier generation models can be overcome. The infeasible proportions of the assessment task of earlier generation approaches can be (partly) compensated by an increase in rough computing power and by making use of more efficient system modelling. Still the balance has to be kept between model simplicity and a faithful representation.

Simplicity of the presented approach allows for a gradual learning curve making it an endeavour not limited to statistics veterans in large multinationals. Depending on the complexity of the situation, the approach will take a certain amount of resources. While some organisations will just have to perform the assessments to legally prove they are ‘in control’, other organisations might have the choice of participating in a quantitative analysis or not. These organisations might want to review the added value over a less intrusive qualitative approach in their particular situation.

The quantitative approach taken in this research allows to reason under a certain amount of uncertainty. This is different compared to the earlier generation models as not all information has to be known beforehand to get meaningful results. The unavailability of (sparse) data, or calculations where estimations are used, can have an impact on the eventual accurateness of the approach. When accuracy is (very) low, the quantitative approach might not provide enough added value compared to a qualitative approach and might not justify the added expenses.

Carefully taking the merits and drawbacks of the approach into account, a quantitative approach such as presented in this thesis can be a valuable addition to an organisation that wants to increase the insight in, and control over their residual information risk. Taking this approach, decisions on information security can be supported by actual figures based on existing data. This will strengthen the position of the information security management practice in the boardroom.

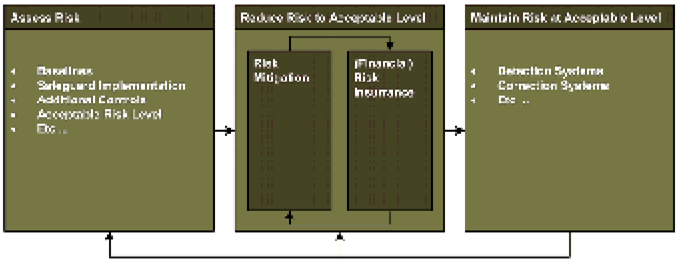


Figure 7.1: Risk Management Framework using Insurance, based on [40]

7.4 Further Research

There is still much research to be done on the topic of residual information risk management. The research at hand is built on requirements set by experts and key literature sources. The actual correctness of the approach and compliance to the requirements need to be tested in practice. This requires the formal validation of the methods used, and the integration and application of the approach in real life situations.

Along the lines of model validation we can discuss the issue of where to end the simplified representation of reality in our model, and where to start the realistic representation of the complex situations in real-life. Further research has to provide insight in this balance between model simplicity and reality complexity, optimizing the quality of the model's output.

Other further research can be sought in the nature of quantitative models. As they are based on available information and uncertainty, the availability of high quality information is important to get high quality results. If an organisation should require the usage of quantitative approaches to information risk management, it should carefully analyse what data is available. If higher accurateness is desired, the organisation might have to invest in services that can provide in this need of information. This requires further research on the influence of an organisation's (information security) maturity level in relation to the level of accuracy supported by a quantitative model.

In another attempt to increase information accuracy and availability, one might decide on the (global) collection of risk information. The availability of information is increased by the combined data collection of participating organisations. Accuracy of the information is increased by having more reports on one event. Herein lies another problem: Are organisations willing and able to share information that may indicate failure and/or weakness? This behavioural research can maybe build further one previous research done in the insurance sector.

In this research we have discussed different risk treatment options. Figure 1.3 shows that we can avoid, mitigate, accept and transfer risk. While risk avoidance, mitigation and acceptance have been discussed in the earlier chapters, less attention was given to the transfer of risk. Gordon et al. [40] incorporated risk insurance as a transfer strategy in (cyber-)risk management as shown in Fig. 7.1 . Additional research could provide insight in how to incorporate risk transfer strategies as an option in a general quantitative risk management model.

All in all, there is much future research to be performed. Chances are that this remains the case as the practice is constantly subject to change. With this thesis an attempt is made at addressing a small part of the issues experienced during the every day management practice of information security.

BIBLIOGRAPHY

[1] C. Alberts and A. Dorofee. OCTAVE-SM threat profiles. Technical report, Carnegie Mellon, Software Engineering Institute, 2001.

[2] C.J. Alberts. Common elements of risk. Technical report, Carnegie Mellon University, April 2006.

[3] A.E. Alter. Do you have any faith in your ROI numbers? CIO Insight Survey, 2003.

[4] A.E. Alter. The bitter truth about ROI. CIO Insight Survey, 2006.

[5] E.I. Altman, R.G. Haldeman, and P. Narayanan. ZETA analysis, a new model to identify bankruptcy of corporations. *Journal of Banking and Finance*, 1977.

[6] A. Andersen. *Managing Business Risks in the Information Age*. The Economist Intelligence Unit, January 1998. ISBN 0850589436.

[7] J. Anderson. Computer security technology planning study. Technical report, U.S. Air Force Electronic Systems Division Tech. Rep., October 1972.

[8] C. Apte, B. Liu, E.P.D. Pednault, and P. Smyth. Business applications of data mining. *Communications of the ACM*, 20(8), August 2002.

[9] Basel Committee on Banking Supervision. International convergence of capital measurement and capital standards - a revised framework. Technical report, Bank for International Settlements, November 2005.

[10] B.C. Beliveau. Theoretical and empirical aspects of implicit information in the market for life insurance. *The Journal of Risk and Insurance*, 51(2):286–307, June 1984.

[11] R. Bharania. Risk triage for security vulnerability announcements. Technical report, Cisco Advanced Services, 2006.

[12] V.M. Bier. Should the model for security be game theory rather than reliability theory. *Communications of the Fourth International Conference on Mathematical Methods in Reliability: Methodology and Practice*, June 2004.

[13] B. Blakley, E. McDermott, and D. Geer. Information security is information risk management. In *NSPW '01: Proceedings of the 2001 workshop on New security paradigms*, pages 97–104. ACM Press, 2001. ISBN 1581134576.

[14] A.M.M. Blommaert and J.M.J. Blommaert. *Bedrijfseconomische analyses*. Wolters-Noordhoff B.V., 2004. ISBN 9020731505.

[15] M. Boisot. *Knowledge Assets: Securing Competitive Advantage in the Information Economy*. Oxford University Press, September 1999. ISBN 019829607X.

[16] L. Bongers. Security binnen enterprise architectuur. Master's thesis, Radboud Universiteit Nijmegen, 2006.

[17] M.I. Bossworth. *Solution Selling: Creating Buyers in difficult Markets*. Irwin, 1995.

[18] S. Bosworth and M.E. Kabay. *Computer Security Handbook*. John Wiley & Sons, Inc., New York, NY, USA, 2002. ISBN 0471412589.

[19] G.B. Broeze. *Validation of Risk Assessment in Auditing.* PhD thesis, Vrije Universiteit Amsterdam, 2006.

[20] Committee of Sponsoring Organizations of the Treadway Commission. Enterprise risk management - integrated framework: Executive summary. Technical report, COSO, 2004.

[21] T. Cooper and J. Collman. Managing information security and privacy in healthcare data mining. *Integrated Series in Information Systems*, 8:95–137, 2005. ISSN 1471-0270.

[22] R.D. Cooter. Economic theories of legal liability. *Journal of Economic Perspectives*, 5(3):11–30, 1991.

[23] R.H. Courtney. Some informal comments about integrity and the integrity workshop. In *Report of the Invitational Workshop on Data Integrity*, NIST Special Publication 500-168. NIST, 1989.

[24] J Davis. Security patch management. In *Information Security Management Handbook, 5th edition*, pages 689–695. Auerbach Publications, 2004.

[25] M.S. De-Silva, D.J. Parish, P. Sandford, and J.M. Sandford. Automated detection of emerging network security threats. *ICN apos'07 - Sixth International Conference on Networking*, April 2007.

[26] S. Dekleva. Justifying investments in it. *Journal of Information Technology Management*, 2005. ISSN 1042-1319.

[27] Deloitte & Touch LLP. *Global Risk Management Survey: Fifth Edition (Financial Services).* Deloitte & Touch LLP., March 2007.

[28] D.E.R. Denning. *Cryptography and Data Security.* Addison-Wesley, June 1982. ISBN 0201101505.

[29] D.E.R. Denning. *Information Warfare and Security.* Addison-Wesley Longman Ltd., Essex, UK, 1999. ISBN 0-201-43303-6.

[30] D.L. Drake and K.L. Morse. The security specific eight stage risk assessment methodology. *Proceedings of the 17th National Computer Security Conference*, 1994.

[31] T.S. Dunn. Methodology for the optimization of resources in the detection of computer fraud. Master's thesis, University of Arizona, 1982.

[32] Editors of CIO Insight. The bitter truth about ROI. CIO Insight Survey, 2004.

[33] C.F. Endorf. Measuring ROI on security. In *Information Security Management Handbook, 5th edition*, pages 685–688. Auerbach Publications, 2004.

[34] C.F. Endorf. Outsourcing security: The need, the risk, the providers and the process. *Information Systems Security*, 2004.

[35] S. Foster and B. Pacl. Analysis of return on investment for information security. Technical report, Getronics, 2003.

[36] M.R. Garey and D.S. Johnson. *Computers and Interactibility: A Guide to the Theory of NP-Completeness.* W.H. Freeman and Co, 1979.

[37] P. Glasserman, P. Heidelberger, and P. Shahabuddin. Portfolio value-at-risk with heavy-tailed risk factors. *Mathematical Finance*, 12(3):239–269, 2002.

[38] L.A. Gordon and M.P. Loeb. The economics of information security investment. *ACM Transactions on Information and System Security*, 5(4):438–457, November 2002.

[39] L.A. Gordon, M.P. Loeb, and T. Sohail. A framework for using insurance for cyber-risk management. *Communications of the ACM*, 46(3), 2003.

[40] L.A. Gordon, M.P. Loeb, and T. Sohail. A framework for using insurance for cyber-risk management. *Communications of the ACM*, 46(3):81–85, March 2003.

[41] S. Greenhalgh, D. Broefkhoff, M. Acharya, and L. Corbier. The GHG protocol for project accounting. Technical report, The World Resource Institute and The World Business Council For Sustainable Development, 2005.

[42] S. Gritzalis, C. Lambrinoudakis, and T. Yannacopoulos. Modelling and economics of it risk management and insurance. Laboratory of Information and Communication Systems Security Presentation, 1997.

[43] P.M. Healy and K.G. Palepu. The fall of enron. *Journal of Economic Perspectives*, 17(2):3–26, 2003.

[44] J.C. Henderson and N. Venkatraman. Strategic alignment: leveraging information technology for transforming organizations. *IBM Systems Journal*, 32(1), 1993.

[45] K. Henry. Risk management and analysis. In *Information Security Management Handbook, 5th edition*, pages 751–758. Auerbach Publications, 2004.

[46] G. Heymong. Of rows and confidentiality, 1999.

[47] L.J. Hoffman and A. Yoran. Role-based risk analysis. *Proceedings of the 20th National Computer Security Conference*, October 1997.

[48] Fair Isaac. The evolving threat of card skimming. *Fair Isaac Whitepapers*, 2005.

[49] ITGI. *CobiT 4.1*. ITGI USA, 2007. ISBN 1933284722.

[50] S.R. Jaschke and Y. Jiang. Approximating value at risk in conditional gaussian models. In *Applied Quantitative Finance Theory and Computational Tools*, pages 1–33, 2002.

[51] L.M. Jawarski. Tandem threat scenarios: A risk assessment approach. *Proceedings of the 16th National Computer Security Conference*, September 1993.

[52] Joint Technical Committee OB-007. *Risk management, AS/NZS 4360:2004, Third edition*. Standards Australia/Standards New Zealand, 2004. ISBN 0-7337-5904-1.

[53] C.G. Jung. *Psychology and Alchemy*. Routledge, December 1980. ISBN 0415034523.

[54] M.E. Kabay. Infosec year in review 1998, 2003.

[55] R. Kaplan. A matter of trust. In *Information Security Management Handbook, 5th edition*, pages 727–740. Auerbach Publications, 2004.

[56] T.A. Kirkpatrick. How do CIOs figure ROI. CIO Insight Survey, 2002.

[57] H. Klete. Some minimum requirements for legal sanctioning systems with special emphasis on detection. *Deterrence and Incapacitation: Estimating the Effects of Criminal Santions on Crime Rates*, 1975.

[58] S.A. Klugman, H.H. Panjer, and G.E. Willmot. *Loss Models: From Data to Decisions, 2nd edition*. John Wiley & Sons, August 2004. ISBN 0471215775.

[59] KPMG EDP Auditors N.V. Information security survey, six important signals. Technical report, KPMG ITA, 2006.

[60] KPMG EDP Auditors N.V. Dilemmas in information security, survey of information security practices within dutch organizations. Technical report, KPMG ITA, 2006.

[61] KPMG IRM. K-sprint risk analysis. Technical report, KPMG, July 2003.

[62] KPMG ITA. ITRMB talkbook. Tool introduction presentation, 2006.

[63] Araya Kulanoot. *Algorithms for some hard knapsack problems*. PhD thesis, Curtin Univsersity of Technology, School of Mathematics and Statistics, 2000.

[64] B. Lampson, M. Abadi, M. Burrows, and E. Wobber. Authentication in distributed systems: theory and practice. *ACM Trans. Comput. Syst.*, 10(4):265–310, 1992. ISSN 0734-2071.

[65] D.L. Landoll. *The Security Risk Assessment Handbook, A Complete Guide for Performing Security Risk Assessments*. Auerbach Publications, 2006. ISBN 0849329981.

[66] A. Lenstra and T. Voss. Information security risk assessment, aggregation, and mitigation. *ACISP*, pages 391–401, 2004.

[67] K.D. Loch, H.H. Carr, and M.E. Warkentin. Threats to information systems: Today's reality, yesterday's understanding. *MIS Quarterly*, 16(2):173–186, June 1992. ISSN 02767783.

[68] R. Maes. An integrative perspective on information management. Technical report, University of Amsterdam, April 2007.

[69] R. Maes, Rijsenbrij D., O. Truijens, and H. Goedvolk. Redefining business - it alignment through a unified framework. Technical report, University of Amsterdam, June 2000.

[70] S. Martello, D. Pisinger, and P. Toth. New trends in exact algorithms for the 0-1 knapsack problem. Technical report, DEIS, University of Bologna, Bolgna and DIKU, University of Copenhagen, Copenhagen, April 1997.

[71] R.A. Martin. Dealing with dates: Solutions for the year 2000. *Computer*, 30(3):44–51, 1997. ISSN 0018-9162.

[72] K. Matsuura. Information security and economics in computer networks - an interdisciplinary survey and a proposal of integrated optimization of investment. Technical report, Institute of Industrial Science, University of Tokyo, Japan, 2003.

[73] M.W. Merkhofer. *Decision Science and Social Risk Management: A Comparative Evaluation of Cost-benefit Analysis, Decision Analysis, and Other Formal Decision-aiding Approaches*. Kluwer Academic Publishers, November 1986. ISBN 9027722757.

[74] A. Mizzi. Return on information security investment. Whitepaper, January 2005.

[75] National Bureau of Standards. Guideline for automatic data processing risk analysis - fips pub 65. Technical report, National Bureau of Standards Washington D.C., 1979.

[76] M. Neil, N. Fenton, and L. Nielson. Building large-scale-bayesian networks. *The Knowledge Engineering Review 2000*, 15(3):257–284, 2001.

[77] T. Nowey, H. Federrath, C. Klein, and K. Plößl. Ansätze zur evaluierung von sicherheitsinvestitionen. Technical report, Universität Regensburg, 2005.

[78] Office of Government Commerce (OGC). *Management of Risk: Guidance for Practitioners*. The Stationary Office, September 2007. ISBN 0113310412.

[79] Office of Government Commerce (OGC). *The Official Introduction to the ITIL Service Lifecycle*. The Stationery Office, August 2007. ISBN 0113310617.

[80] T.W. Osgood. A risk analysis model for the military environment. *Proceedings of the 11^{th} National Computer Security Conference*, October 1988.

[81] P. Overbeek, E. Roos Lindgreen, and M. Spruit. *Informatiebeveiliging onder controle - tweede editie*. Pearson Education Benelux, 2005. ISBN 9043006920.

[82] P. Overbeek, R. Joosten, A. Jochem, R. Kuiper, A. Moens, J. Popping, P. Ruijgrok, and J. Voeten. Return on security investment (rosi): Hoe te komen tot een bedrijfseconomische onderbouwing van uitgaven op het gebied van informatiebeveiliging?, 2006.

[83] D.B. Parker. *Fighting Computer Crime: a new Framework for Protecting Information*. John Wiley & Sons, Inc., 1998. ISBN 0-471-16378-3.

[84] D.A. Patterson. A simple way to estimate the cost of downtime. In *Proceedings of LISA '02: Sixteenth System Administration Conference*, pages 185–188, 2002.

[85] J. Pearl. *Causality*. Cambridge University Press, 2000. ISBN 0521773628.

[86] S. Peekel. Information security maturity - a qualitative framework for information security management. Master's thesis, Tilburg University, 2007.

[87] T.R. Peltier. *Information Security Risk Analysis, Second Edition*. Auerbach Publications, 2005. ISBN 0849333466.

[88] D. Pisinger. Where are the hard knapsack problems? Technical report, Department of Computer Science, University of Copenhagen, February 2003.

[89] D. Pisinger. A minimal algorithm for the 0-1 knapsack problem. Technical report, DIKU, 1994.

[90] A.B. Rabinovich, E.A. Kulikov, and R.E. Thomson. Tsunami risk estimation for the coasts of peru and northern chile. *Proceedings of the 2001 International Tsunami Symposium*, 2001.

[91] R. Richardson. 2007 CSI computer crime and security survey - the 12th annual computer crime and security survey. Technical report, Computer Security Institute, August 2007.

[92] D.F. Rico. *ROI of Software Process Improvement: Metrics for Project Managers and Software Engineers.* J. Ross Publishing, 2004.

[93] R.L. Rivest. *Cryptography*, chapter 13, pages 17–755. Elsevier and MIT Press, 1990.

[94] T. Rolski, H. Schmidli, V. Schmidt, and J.L. Teugels. *Stochastic Processes for Insurance and Finance.* John Wiley & Sons, Inc., August 1998.

[95] J.W. Ross, C.M. Beath, and D.L. Goodhue. Developing long-term competitiveness through information technology assets. Technical report, Center for Information System Research - Sloan School of Management - Massachusetts Institute of Technology, December 1995.

[96] R. Rue, S.L. Pfleeger, and D. Ortiz. A framework for classifying and comparing models of cyber securitiy investment to support policy and decision-making. Technical report, RAND Corporation, June 2007.

[97] E.P. Rutkens, H. Bouthoorn, and L.P.F. Tushuizen. Risicoanalyse gemakkelijk gemaakt. *Compact*, 1, 2004.

[98] J.H. Saltzer and M.D. Schroeder. The protection of information in computer systems. *Proceedings of the IEEE*, 63(9):1278–1308, 1975.

[99] S.E. Schechter. Computer security strength & risk: A quantitative approach. Technical report, Harvard University - Cambridge, Massachusetts, May 2004.

[100] M.F. van Schoote. Business process outsourcing in control - onderzoek naar de beheersing en besutring van uitbestede processen. Master's thesis, Universiteit Twente, 2006.

[101] C.A. Siegel, T.R. Sagalow, and P. Serritella. Cyber-risk management: Technical and insurance controls for enterprise-level security. In *Information Security Management Handbook, 5th edition*, pages 829–843. Auerbach Publications, 2004.

[102] S.S. Skiena. *The Algorithm Design Manual.* Springer, 1998. ISBN 0387948600.

[103] P. Slovic. Trust, emotion, sex, politics, and science: Surveying the risk assessment battlefield. *Risk Analysis*, 19(4), 1999.

[104] R. Von Solms. Risicoanalyse of security. *Compact*, 4, 2000.

[105] R. Von Solms. Can security baselines replace risk analysis? *Computers and Security*, 16(3), 1997.

[106] W. Sonnenreich, J. Albanese, and B. Stout. Return on security investment (ROSI): A practical quantitative model. Technical report, SageSecure LLC, 2005.

[107] K.J. Soo Hoo. How much is enough? a risk-management approach to computer security. Master's thesis, Stanford University, June 2000.

[108] K.J. Soo Hoo, A. Sudbury, and A.R. Jaquith. Tangible roi through secure software engineering. *Secure Business Quarterly*, 1(2):8–10, 2001.

[109] T.R. Stacey. *Contingency Planning Best Practices and Program Maturity*, pages 1557–1572. Auerbach Publications, 2007.

[110] C. Steel, R. Nagappan, and R. Lai. The alchemy of security design - methodology, patterns, and reality checks. In *Core Security Patterns: Best Practices and Strategies for J2EE, Web Services and Identify Management*, pages 438–531. Prentice Hall, 2006. ISBN 9780131463073.

[111] D.W. Straub. Effective is secuirity: An empirical study. *Information Systems Research*, 1(3): 255–276, 1990.

[112] A.G. Sutcliffe, N.A.M. Maiden, S. Minocha, and D. Manuel. Supporting scenario-based requirements engineering. Technical report, Center for HCI Design, School of Informatics, City University, London, 1998.

[113] N.N. Taleb. The black swan: Why don't we learn that we don't learn? Technical report, Empirica LLC and Courant Institute of Mathematical Sciences, New York University, 2004.

[114] D. Tan. Quantitative risk analysis step-by-step. Technical report, SANS Institute, December 2002.

[115] The International Organization for Standardization and The International Electrotechnical Commission. International standard ISO/IEC 27001, information technology - security techniques - information security management systems - requirements. Technical report, SO/IEC, 2005.

[116] The International Organization for Standardization and The International Electrotechnical Commission. International standard ISO/IEC 15408, information technology - security techniques - evaluation criteria for it security - part 1, introduction and general model. Technical report, ISO/IEC, October 2005.

[117] The International Organization for Standardization and The International Electrotechnical Commission. ISO/IEC 7498-2, open systems interconnection - security architecture. Technical report, ISO/IEC, 1989.

[118] The International Organization for Standardization and The International Electrotechnical Commission. ISO/IEC TR 13335-1, information technology - concepts and models for it security. Technical report, ISO/IEC, 1996.

[119] The International Organization for Standardization and The International Electrotechnical Commission. ISO/IEC TR 13335-3, information technology - guidelines for the management of it security. Technical report, ISO/IEC, 1998.

[120] Th.J.G. Thiadens. *Manage IT!* Springer, 2005. ISBN 1402036396.

[121] J. Tillquist and W. Rodgers. Using asset specificity and asset scope to measure the value of it. *Communications of the ACM*, 48(1), January 2005.

[122] H.F. Tipton and M. Krause. *Information Security Management Handbook - Fifth Edition.* Auerbach Publications, 2005. ISBN 0849319978.

[123] J. Varghese. ROI is not a formula, it is a responsibility. Technical report, INFOSYS Briefings, September 2002.

[124] P. Vergilius Maro. *Aeneis.* Athenaeum-Polak & Van Gennep, 29BC.

[125] C. Verhoef. Quantitative it portfolio management. *Science of Computer Programming*, 45:1–96, 2002.

[126] P. Verschuren and H. Doorewaard. *Het ontwerpen van een onderzoek.* LEMMA BV, 2004. ISBN 9051898986X.

[127] Vice President of the United States and President of the Senate. Sarbanes-oxley act of 2002. *Communications of the One Hundred Seventh Congress of the United States of America, Second Session*, 2002.

[128] A. Vorster and L. Labuschagne. A framework for camparing different information security risk analysis methodologies. In *Proceedings of SAICSIT 2005*, pages 95–103, 2005.

[129] A.N. de Vries. De risicoanalyse voorbij. informatiebeveiliging door standaardisatie. Master's thesis, Open Universiteit Nederland, 2002.

[130] J. Willemson. On the gordon and loeb model for information security investment. Technical report, Institute of Computer Science, University of Tartu, Estonia, 2006.

[131] C.C. Wood. *Best Practices In Internet Commerce Security.* Baseline Software, May 2001. ISBN 1881585050.

Appendices

APPENDIX A

Entity Relationship Diagram

In this thesis a great amount of terms are introduced for all relevant elements. The Entity Relationship Diagram from Fig. A.1 gives a simplified representation of the most important elements [63]. Not all elements and relationships between them are documented. This would make the entity relationship diagram unnecessarily complex.

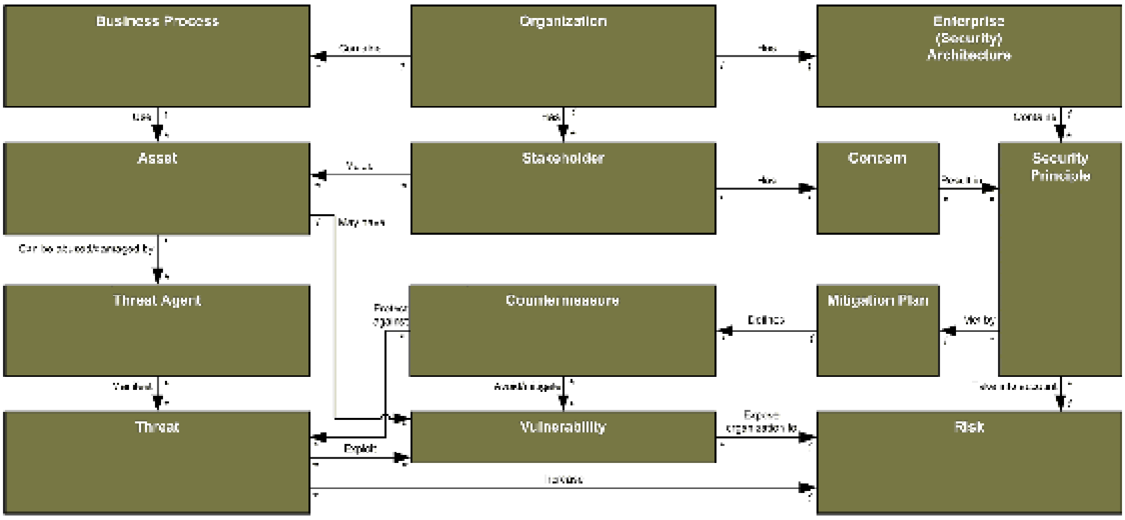


Figure A.1: Relationship between thesis elements

Elements

Organisation

"An Organisation is a distinctive type of social form in which professionals share in the determination of goals and standards" [45].

- Has various *Stakeholders.*
- Has an *Enterprise (Security) Architecture.*
- Contains *Business Processes.*

Enterprise (Security) Architecture

An Enterprise-wide architecture has to do with bridging the gap between strategy (stakeholder expectations) and implementation [64]. An Enterprise Information Security Architecture aids an enterprise in protecting the confidentiality, integrity and availability of their assets. It helps to create an understanding what threats there are to information assets are and how to allocate resources to combat these threats [61].

- Aids the *Organisation* in fulfilling *Stakeholder* expectations.
- Contains *Security Principles.*

Stakeholder

"Any group or individual who is affected by or can affect the achievement of an organisation's objectives" [15].

- Are grouped in an *Organisation.*
- Value *Assets.*
- Have specific *Concerns.*

Concern

Considerations about a system. Usually entail aspects like confidentiality, integrity and availability. Has a close relationship with security, "which has etymological roots in 'se' (without) and 'cura' (to be concerned about)" [31].

- Considerations *Stakeholders* have about a system/organisation.
- Result in the specification of *Security Principles.*

Security Principle

Fundamental, primary, or general law or truth concerning security, from which others are derived [42]. Part of this is the information security policy which is the foundation of all information security implementations that occur in the organisation [34].

- Are embedded in the *enterprise security architecture.*
- Are derived from *security concerns* from *stakeholders.*
- Take *risk* into account.
- Are met by *mitigation plan(s).*

Business Process

"A (Business) Process is simply a structured set of activities designed to produce a specified output for a particular customer or market. It implies a strong emphasis on how work is done within an *organisation,* in contrast to a product's focus on what. A process is thus a specific ordering of work activities across time and place, with a beginning, and end, and clearly identified inputs and outputs: a structure for action." [12].

- Relates to how work is done in an *Organisation.*
- During the business processes, business *Assets* are used.

Asset

In [59] assets are shortly described as "anything that has value to the organisation". The assets of an organisation include physical assets, information, software, people and intangibles [59].

- Are used and produced in *Business Processes.*
- Are valued by *Stakeholders.*
- May have *Vulnerabilities.*
- Can be abused or damaged by *Threat Agents.*

Threat Agent

"A threat agent is a person or phenomenon that can make a threat manifest" [8]. Threat agents can be natural or human. They consist of, but are not limited to, equipment malfunctions, shortages of essential services, permanent staff and outsiders [8].

- Can abuse or damage *Assets.*
- Can manifest *Threats.*

Threat

A potential cause of an unwanted incident or event which may result in harm to a system or organisation. Includes (but is not limited to) computer-assisted fraud, espionage, sabotage, vandalism, fire or flood [7, 59].

- Exploit *Vulnerabilities.*
- Increase *Risk.*
- Are manifested by *Threat Agents.*
- Are protected against by *Countermeasures.*

Vulnerability

A weakness of an asset or group of assets which can be exploited by a threat [59].

- Expose *Assets* to *Risk*.
- Can be exploited by *Threats*.
- Are avoided or mitigated by *Countermeasures*.

Mitigation Plan

A plan that describes controls or *countermeasures* to influence an *organisation's vulnerabilities* and thus *risk* exposure.

- Defines *Countermeasures*.
- Originate from an *Organisation's Security Principles*.

Countermeasure

"Means of managing risk, including policies, procedures, guidelines, practices or organisational structures, which can be of administrative, technical, management, or legal nature. Countermeasure is also used as a synonym for safeguard or control" [7].

- Are defined in a *Mitigation Plan*.
- Manages *Risk* through influencing *Vulnerabilities* and *Threats*.

Risk

"A combination of the probability of an event and its consequence" [57]. "There is a potential for events and consequences that constitute opportunities for benefit (upside) or threats to success (downside) [56]." This would mean the potential that a given threat will exploit a vulnerability exposing assets to harm.

- Is taken into account in *Security Principles*.
- Is formed by *Threats*.

APPENDIX B

SUPPORTING INTERVIEWS

During the course of the research, interviews have been given to experts in the field to get extra input and insights on the subject of information security and the application of quantitative measures. The interviews give support to the literature study that has been conducted. The description and motivation of the research methods used are given in Chapter 2

The group of experts interviewed consists of CIO's, security architects and advisers (or comparable) from different sectors and different countries. Sectors identified are government agencies, financials, telecommunication agencies and services (on both advisory and implementation side). This chapter will shortly discuss the interview and the results. The structure of the interviews is given and the questions asked are discussed and mapped to the research objectives and research questions.

B.1 Interview Structure

Introduction

- Short introduction of the research at hand
- Discussion of expert and his/her background
  - Organisation
  - Sector
  - Function and work area
  - Experience
- Description of context in which the questions need to be placed

Models and Methods on Risk Assessment

1. In your experience of Risk Assessment, which tools or methods can you name that you have used?

2. Which of the following tools or models *a)* sound familiar, *b)* have been used by you, and *c)* if used; how would you rate the tool/model on a Likert scale if the statement was 'This tool/model is very valuable for Risk Assessments in the given context'? Use the fill-in form as shown in Table B.1 .[1]
3. Considering the context as previously described, what are the main characteristics of the tool/model you would like to use?
4. What characteristics would make the tool/model *unusable* in your opinion?
5. What level of detail would you like to discuss in the tool/model? What elements should it address?

Quantification

1. Considering the context as previously described, what metrics would be useful in a quantitative model on Risk Assessment?
2. Please comment on the following statement from your own experience: "Most companies are mature enough in their Information Risk Management process to support quantitative measures".

B.2 Question-Objective Mapping

The expert interviews' main goal is to seek answers to the first two sets (out of three) of research questions. The third set of research questions will be answerable after the actual model is constructed.

The first set of questions in the interview addresses the objective of selecting a suitable methodology to use in this research. As we can see in Section 2.2 we decomposed this objective into four different research questions.

"Which methodologies for Risk Assessment exist and what are their characteristics?"

An answer to this research question is sought in the answers of question one and two. The respondent is first asked to answer questions regarding existing (used) methodologies from his/her experience in Risk Assessment. This question mainly addresses the active knowledge of the respondent.

The second question, along with the form as shown in Table B.1 , tests the passive knowledge of risk assessment methodologies per expert. If a methodology is known, it is briefly discussed.

"What are currently often used methodologies for Risk Assessment?"

In the previous question we mainly discussed the methodologies known to the expert. These may include methodologies that are not directly used by the respondent or hear-say methodologies. The answers of interview question one and two again should provide insight in this matter. The combination of interview questions one and two give an answer to research objectives one and two combined.

[1] The Likert scale: Strongly disagree, Disagree, Neither disagree nor agree, Agree, Strongly agree.

Table B.1: Fill in form, interview question 2.

Tool/Model	Known	Used	Rating				
			1	2	3	4	5
A&K Analyse	yes / no	yes / no	o	o	o	o	o
BIA	yes / no	yes / no	o	o	o	o	o
CCA	yes / no	yes / no	o	o	o	o	o
CORAS	yes / no	yes / no	o	o	o	o	o
CRAMM	yes / no	yes / no	o	o	o	o	o
DELAM	yes / no	yes / no	o	o	o	o	o
DETAM	yes / no	yes / no	o	o	o	o	o
DREAD	yes / no	yes / no	o	o	o	o	o
EBIOS	yes / no	yes / no	o	o	o	o	o
ERAM	yes / no	yes / no	o	o	o	o	o
ETA	yes / no	yes / no	o	o	o	o	o
FIRM	yes / no	yes / no	o	o	o	o	o
FMEA	yes / no	yes / no	o	o	o	o	o
FTA	yes / no	yes / no	o	o	o	o	o
HAZOP	yes / no	yes / no	o	o	o	o	o
ITRMB	yes / no	yes / no	o	o	o	o	o
MAGERIT	yes / no	yes / no	o	o	o	o	o
Markov	yes / no	yes / no	o	o	o	o	o
MEHARI	yes / no	yes / no	o	o	o	o	o
MORT	yes / no	yes / no	o	o	o	o	o
NORA	yes / no	yes / no	o	o	o	o	o
OCTAVE	yes / no	yes / no	o	o	o	o	o
OCTAVE-allegro	yes / no	yes / no	o	o	o	o	o
OCTAVE-S	yes / no	yes / no	o	o	o	o	o
OSSTMM	yes / no	yes / no	o	o	o	o	o
OSSTMM-RAV	yes / no	yes / no	o	o	o	o	o
QSM Security Expert	yes / no	yes / no	o	o	o	o	o
RAF	yes / no	yes / no	o	o	o	o	o
ROSI	yes / no	yes / no	o	o	o	o	o
ROISI	yes / no	yes / no	o	o	o	o	o
SARA	yes / no	yes / no	o	o	o	o	o
SMORT	yes / no	yes / no	o	o	o	o	o
SOMAP	yes / no	yes / no	o	o	o	o	o
SP800-30	yes / no	yes / no	o	o	o	o	o
SPARK	yes / no	yes / no	o	o	o	o	o
SPRINT	yes / no	yes / no	o	o	o	o	o
STRIDE	yes / no	yes / no	o	o	o	o	o
TRIKE	yes / no	yes / no	o	o	o	o	o

“What kind of information is concerned in Information Risk Management?”

This research question is mainly covered by the answer on the fifth interview question. In the fifth interview question the level of detail of the model is discussed along with the elements it should address. This should give an indication of what kind of information is concerned in the Information Risk Management practice, and to what extend.

“What makes a methodology classify as ‘practical and workable’ in practice?”

The main goal of this research question is to make the requirements for the eventual model as clear as possible. Usability requirements are sought in the answers of interview question three and four.

The second set of questions addresses the objective of getting more insight in the computational methods applicable for our model. Again this objective is decomposed into the following research questions:

“Which computational methods for quantitative Risk Assessment exist and what are their characteristics?”

Analogous to question one from the previous section, this question aims to broaden the view on currently used quantitative measures in information risk management. Answers are collected from interview questions six and seven covering possible metrics and measures for use in the quantitative model

“What additional characteristics or requirements would a quantitative method need, to make it practical and workable?”

In order to get a good overview of all the characteristics and requirements of the quantitative part of the research, questions with regard to usefulness are asked. Where question six directly addresses the usability criteria, question seven is aimed at provoking a discussion to identify possible hidden requirements.

Summarized, the mapping is as given in Table B.2 .

Table B.2: Research question - Interview question mapping

Interview Question	1	2	3	4	5	6	7
Research Question							
1.1	x	x					
1.2	x	x					
1.3					x		
1.4			x	x			
2.1						x	
2.2						x	x

B.3 Discussion of Results

As stated before, respondents originated from four sectors. In this section the results of the interviews will be discussed per sector. The interviews have been made anonymous. The interviewed expert will be addressed by 'the respondent' or 'he', not making any claims with regard to the gender of the respondent. The answers are those of the respondents and not of the author.[2]

Results will be given on the usability (constraints) of the quantitative model. The answers to the questions with regard to the identification of available and used methodologies and methods are incorporated in the comparative framework of Appendix D and Chapter 3 .

Sector A

The first answer set originates from a respondent working as an information management and security advisor at a local government agency. The respondent has over 10 years of experience on the subject.

Regarding Models and Methods

The respondent from the government agency suggests the following characteristics. The quantitative model:

1. Should be built on (or be) a publicly (freely) available proven standard (R1).
2. Should have a pragmatic approach (R16).
3. Should not be too detailed (R6). The model needs to have clear results that can be communicated to the organisation's management, and should not 'stall' in the process of identification of components. An optimum has to be found between detail and performance.
4. Should have a clear focus and should not have too wide a scope (R5). A wide scope will either make the model cumbersome to handle or it will result in a model without organisational impact.
5. Should be usable from a strategical level to an operational level (R11). As information security operates on all levels of the organisation (Fig. 1.6), the model should be able to support all levels from operational to strategical.

Regarding Quantification

Interesting viewpoints are given on question six and seven of the questionnaire. The respondent is sceptical on the usage of quantitative measures based on monetary values and states that when everything is translated to monetary values, the link to reality is lost (R18). Additionally he claims that most organisations are subject to an environment that is rapidly changing which makes quantitative risk assessment relatively complex and unappealing (R17). A budgetary constraint also inhibits the usability of quantitative models in this sector. Often, not enough funds are present to conduct a serious and statistically useful quantification process (R7).

[2] Even though efforts were made to represent the true contents of the interviews, in case of an error in interpretation, full responsibility is taken by the author and the respondents can not be held accountable.

Sector B

This answer set represents the view of the respondents from the financial sector. Two respondents were interviewed with experience as CISO at a bank. Both respondents report over 25 years of combined experience in the sector.

Regarding Models and Methods

The respondents from the financial sector suggest the following characteristics. The quantitative model:

1. Should not attempt to work towards a solid claim of loss and damage (R4). The model should not make false claims of accurateness. For this, there is too much uncertainty in the practice of information security which makes the results from the model difficult to take serious.
2. Should be aimed at business processes and information systems (R13), with a possibility to find clusters. The structure and the components should be made explicit.
3. Should have a notion of an information security baseline or minimal level of security (R12). It should have the possibility to take the controls that are already present into consideration.
4. Should be as simple as possible (R8). A model that is too complex to use loses its attractiveness.
5. Should not be a black box (R2). Its workings have to be understood in order to validate the model on its correctness of working.

Regarding Quantification

The respondent indicates a desire for rigid methods of quantification. On the same note he states that quantification will not be easy. As there are components that are hard to quantify into monetary units, one needs to have clear boundaries to the model. Management should not make decisions on the monetary loss indications alone but should also be presented with indications of other possible losses (e.g. reputation) (R14).

The results need to be verifiable, that is, if done a second time by other people, the same results should come up (R3). If one is to use numbers as ’return on investment’ one needs to use one strict definition of ROI. Return figures might prove to incorporate too much ‘uncertainty’ in the model, ending up with figures that are maybe right and reproducible, but are unusable because of the high level of uncertainty (R14).

Sector C

The third answer set represents the view of respondents from the telecommunication sector. The main respondent is a well respected certified operation risk management officer with affiliations in business models and disruptive change management. The respondent has over 10 years of experience in information security in the telecommunication sector aside from a history of communication technology practices within the armed services.

Regarding Models and Methods

The respondent from the telecommunication sector suggests the following characteristics. The quantitative model:

1. Should be easy to understand by management (R9). Complex mathematical structures should be avoided and the structures that are used should be logical.
2. Should have a visual component. Especially with regard to relationships between triggers, cascading events, barriers, motifs and controls visual components are desirable.
3. Should be fast to apply with low assessment cost (R7).
4. Should take controls that are already in place into account and maybe provide a possibility to use already identified residual risk figures (both accepted and unaccepted) (R12).
5. Should keep note of 'blind spots' and weak points (R14). If present, the boundaries of the model will be much clearer and decisions based on the results of the model will be better founded. This also includes statements of uncertainty.
6. Should have the possibility to abort the quantification if the qualitative approach should suffice (R15).

Regarding Quantification

The respondent indicates a discomfort with the usage of ROI figures and related representations because they can easily be manipulated and therefore lack credibility (R14/R3). The respondent is clear when it comes to measures and metrics to use in a quantitative model. Metrics should take note of:

- Available budget
- Time frame
- Staff hours,
- Machine resources
- Acceptance criteria

Additionally it is stated that many organisations do not have the required skills to perform and understand quantitative risk assessments. This, combined with the fact that the documents and statistics required for the assessment are often not present, makes quantitative risk assessments difficult (R7/R8).

Sector D

The last answer set originates from respondents from the services sector. Two respondents, one with an advisory background, the other with a more implementation focused background, report over 20 years of joined experience.

Regarding Models and Methods

The respondents from the services sector suggest the following characteristics. The quantitative model:

1. Should be aimed at creating awareness (R19). As stated by a respondent: "Awareness often is the first step to a good working information security practice."
2. Should prioritize, not prescribe (R20). It should give an indication on the benefits of certain mitigation plan, but be flexible enough to not prescribe certain countermeasures. The model needs to aid in the decision process, not be the decision maker.
3. Should be easy to understand and easy to be made understandable (R8/R9). The party using the model should be able to understand its workings in order to be able to make it understandable to stakeholders of the organisation. If one is unable to clearly explain the workings, acquiring management support will be hard.
4. Should not lose track of the non-quantifiable aspects as reputation (R14).
5. Should have a notion of time (R21). The rapidly changing nature of the environment gives raise to a need of a notion of time. Sometimes measures taken will only work for a certain amount of time, after which a new threat will occur.
6. Should have a small footprint. It should be easy to acquire and perform with little initial resource requirements (R7).
7. Should be able to incorporate standards as ISO/IEC 17799:2005 and CobiT (R1). These standards provide a basic indication of control sets and are often mandatory for organisations who want to prove they are 'in control'.

Regarding Quantification

It seems that scepticism on the use of quantitative risk assessment is also available in this sector. One respondent seriously questions the possibility of a real pragmatic quantitative approach (R16). Another issue identified comes from the fact that a quantitative approach might be possible to apply, but not all organisations will be ready to reap the benefits from it. A problem with regard to quantification is identified addressing preventive controls (risk avoidance) specifically. This strategy requires measures that model future uncertainty which might be difficult.

Table B.3: Usability requirements

rID	Description	Sector			
		A	B	C	D
R1	Should be built on (or be) a publicly available proven standard.	x			x
R2	Should not be a black box.		x		
R3	Should give consistent, verifiable answers.		x	x	
R4	Should not attempt to work towards a solid claim of loss and damage.		x		
R5	Should have a clear focus and should not have too wide a scope.	x			
R6	Should not be too detailed.	x			
R7	Should be fast to apply with low assessment costs.	x		x	x
R8	Should be as simple as possible.		x	x	x
R9	Should be easy to understand by management.			x	x
R10	Should have a visual component.			x	
R11	Should be usable from a strategical level to an operational level.	x			
R12	Should have a notion of an information security baseline or minimal level of security.		x		
R13	Should be aimed at business processes and information systems, with a possibility to find clusters.	x			
R14	Should keep note of 'blind spots' and weak points.		x	x	x
R15	Should have the possibility to abort the quantification if the qualitative approach should suffice.			x	
R16	Should have a pragmatic approach.	x			
R17	Should be able to handle a rapidly changing environment.	x			
R18	Should retain a link to reality.	x			
R19	Should be aimed at creating awareness.		x		x
R20	Should prioritize, not prescribe.				x
R21	Should have a notion of time.				x

APPENDIX C

METHODOLOGIES: LITERATURE REVIEW

This appendix gives the reader an overview of the tools and methodologies selected from the literature review quickscan. An overview of the tools and methodologies found can be seen in Fig. C.1 . The list is by no means complete. Some tools and methodologies were intentionally left out because of:

- a language barrier,
- a lack of (publicly available) documentation (often seen with proprietary methodologies),
- a proven unsuitability for this project; proven in prior research.

The following tools are examples of methodologies identified but left out of the research:

- Amenaza IT Threat Tree Modeling System (resemblance to other tree methodologies)
- ARiES (highly sector specific)
- COBRA (like CRAMM but with smaller controlset)
- MARION (Replaced by MEHARI, although still used)
- STIR (lack of (publicly available) documentation)

Other methodologies might have been forgotten, which can happen due to the nature of a quickscan.

Methodologies and Tools

A en K Analyse

A Dependability and Vulnerability Analysis (A en K Analyse) knows its origins from the Dutch 'Voorschrift Informatiebeveiliging Rijksoverheid' (VIR) where it was decided that a dependability and vulnerability analysis was mandatory for each and every information system and liability area. In the latest version from 2007 [4], this requirement has been canceled but the methodology remains important.
The A en K analyse methodology has the following characteristics [49]:

- Gives a company detailed insight in their risk exposure and controls.
- Difficult and time consuming endeavor (given that an analysis has to be done on each and every information system and liability area).
- Practically impossible to fulfill without using a good automated tool.

BIA

A BIA, or 'Business Impact Assessment' is a method of determining the possible business impact that an organisation could experience as a result of an incident that will compromise the information in a system. The BIA methodology has been designed to analyze information risk in systems (e.g. business applications) and not in other environments (e.g. networks), which severely limits its formal application domain.
The Business Impact Assessment is preferably done in a workshop, with relevant representatives in role and function, in order to get a complete overview which can be presented to the senior management. The BIA method can be used as a standalone method, but it can also be used to support other methods (e.g. IRAM) [22].

Note: In the area of risk management, the abbreviation BIA can also stand for Business Continuity Impact Analysis. Since this is more of an alternative to risk management instead of a risk management method, it is not discussed in this paper and should not be confused with Business Impact Assessment.

CCA

CCA, or 'Cause-Consequence Analysis', blends event tree analysis and fault tree analysis. CCA combines cause analysis as described by fault trees, and consequence analysis as described by event trees. Both deductive and inductive analysis methods are used. CCA has as goal the identification of chains of events that can result in undesirable consequences by documenting the failure logic of a system [10]. The CCA methodology is sometimes referred to as extended ETA and has the following characteristics:

- Provides the exact failure probability in a very calculation efficient way, and
- Does this for only one 'challenge' at a time.
- Designed for static systems, difficult to implement in dynamic system.
- Based on dependabilities (including time).

CORAS

The CORAS methodology is a risk management process based on the standardized modeling technique UML. CORAS addresses security critical systems in general but puts particular emphasis on IT security [6]. It combines, adapts, refines and extends different methods for risk analysis like FTA, Markov and HAZOP. The CORAS methodology has the following characteristics [5]:

- Particular focus on information and IT security.
- Based on a standardized modeling technique.
- Possibility to incorporate different standards such as the AS/NZS 4360:1999 [25] and ISO/IEC 27001:2005. [58]
- Publicly available and stimulates user interaction with for example an assessment repository and the possibility to make use of reusable elements.

CRAMM

CRAMM, or 'CCTA Risk Analysis and Management Method', is a best practices method providing guidance for various standards as BS7799 but also the newer ISO/IEC27000 series. CRAMM provides means for determining the likelihood and impact of threats on assets which are then used to calculate the risk value for each threat to all the assets [1]. The CRAMM methodology has the following characteristics:

- Based on best practices.
- Makes use of both qualitative and quantitative measures but cannot be considered a quantitative method.
- Considered to be a heavy-weight for most purposes, even though the general q uestionnaire base is relatively simple.
- Foundation for smaller methodologies like SPRINT and SPARK.

DELAM

DELAM, or 'Dynamic Event Logic Analytical Methodology' (sometimes referred to as DYLAM) is a methodology that explicitly models time, process variables and system behavior. It is useful for the description of behavioral system scenarios and reliability assessments with a special focus on temporal events [48]. The DELAM has the following characteristics:

- Particularly suited for situations where time is of importance.
- Problem-specific, meaning that a different simulation has to be made for each problem.
- Requires a large amount of input data (e.g. probabilities of a component being in a certain state, dependencies, state transition information).

DETAM

DETAM, or 'Dynamic Event Tree Analysis Method', is a tree-based methodology for scenario's. It is strongly time/state-based which means that it is basically a normal event tree but with allowance of branching at different points in time. A DETAM analysis provides in a causal model for errors [2]. The DETAM methodology has the following characteristics:

- Flexible tree mechanism with time dependencies.
- Due to the time dependencies, in some situations, the causal model will quickly grow too large to handle.
- Very suitable for tool based calculations, being a tree model.

DREAD

DREAD, which stands for 'Damage potential, Reproducibility, Exploitability, Affected users and Discoverability', is a tree based methodology to threat modeling. DREAD is for example used by Microsoft's[1] .Net security framework. DREAD is primarily used to get an agreement on threat ratings, clarifying the impact of the security threat and communicating them to stakeholders.

EBIOS

EBIOS, or 'Expression des Besoins des Objectifs de Sécurité', is a methodology focusing on security objectives, first intended for administrations and industries working with the Defense Ministry in France. It is a risk analysis method which aims to determine risks that threaten information systems and aids in implementing data securing policies. It can be implemented by the organisation's security expert and it can be applied to all levels of an information systems. The results of an EBIOS provide the information required for writing the security specifications of the studies systems. It also contributes to a secure operating architecture [39]. The EBIOS methodology has the following characteristics:

- Specifically sees information security as the classic CIA triad.
- Closely follows national and international standards.
- Requires formalized organisation schemes, information security policies and general system specifications to be effective.
- Flexible in a way that it can be applied to systems under design and already existing systems.
- Knows a select collection of 'best practices'.

ERAM

ERAM, or 'Enterprise Risk Assessment Methodology', is a propositioned enterprise risk assessment model mainly focused on system acquisition. ERAM tries to aid in identifying risks and potential pitfalls early in the business system development life cycle to better ensure success. It should come as no surprise that it is a tool meant for program managers to determine the root cause of specific problems. It gives the people making the program decisions insight without creating another latyer of oversight. Additionally it gives awareness on both a strategic as an operational level [28]. The ERAM methodology has the following characteristics:

- Has a clear distinction of the strategic level and the operational level (and calls this Big A and little A decisions)
- Values awareness.
- Mainly adheres to The United States / DoD directives.
- Is fast and flexible, enabling business systems to take advantage of emerging technology and deliver business capabilities faster.

[1] http://www.microsoft.com

ETA

ETA, or 'Event Tree Analysis', is considered a so called (inductive) Boolean Logic method. In cases when the probability of an event is known from past experience, statistical data can be used if the uncertainty in these data are acceptably low. In cases of rare events (which are *not* uncommon in information risk management, probabilistic failure models have to be developed [50].

FIRM

FIRM, or 'Fundamental Information Risk Management', is a methodology that aids in managing enterprise-wide, low level operational information risk and was developed by the Information Security Forum (ISF) [19, 20]. It was developed to meet the need for an effective means of keeping information risk within an enterprise under control [35]. The FIRM methodology has the following characteristics:

- Makes it possible to get the business involved in risk management with it's focus on the (monitoring of) effectiveness of information security arrangement throughout the company.
- Offers possibilities of executive risk reporting.
- After a company has established a good FIRM process, it needs minimal effort to monitor information risk and to keep it at The FIRM methodology is very flexible and can be applied in both small and large projects and companies through a good scoping process and comprehensive implementation guidelines.
- Simplicity is a key objective to the FIRM methodology and it does so by providing practical tools to enable information risk to be measured and reported (e.g. FIRM scorecards).

FMEA

FME, of 'Failure Model and Effect Analysis', is an inductive FTA-like approach. Inductive refers to the fact that this method reasons from an individual case to a general conclusion. Inductive methods are applied to determine what system states are possible [62]. The FMEA methodology has the following characteristics:

- Relatively flexible because it can be used in a design phase but also in a phase where the system is already in place.
- In actual practice, the inductive methods generally play the role over 'overview' methods.
- A full analysis is only doable for relatively small systems. Identification of all component failure modes in complex systems will be a very labor intensive task.

Note: Although this paper specifically defines FMEA as an inductive method for system analysis, other inductive methods (like FMECA, PHA, FHA and DFM) follow a similar principle and could be read instead of FMEA [62].

FTA

FTA, or 'Fault Tree Analysis' can be described as an analytical technique whereby an undesired state of a system is specified and then analyzed in the context of its environment and operation to find all credible ways in which the event can occur. It is classified as being an example of deductive system analysis: A specific system state (generally a failure state) is analyzed by defining chains of more basic faults contributing to the undesired effect. Deductive methods are applied to determine how a given system state can occur [62]. The FTA methodology has the following characteristics:

- Usually a graphical model of various parallel and sequential combinations of faults
- Not in itself a quantitative model on itself. It is a qualitative model that can be evaluated quantitatively.
- Difficult to quantify the fault tree in large systems. A possible resort is to use approximations.
- There are no dependability considerations in classic FTA.

HAZOP

HAZOP, or ‘Hazard and Operability studies’, are well known for systematic and thorough evaluation of industrial hazards. Organisations can easily justify process hazards analysis on the basis that their benefits (safety, environmental, economic) outweigh their cost. HAZOP is considered a ‘what-if’ analysis and is build on credible incident scenarios. HAZOP is usually performed by a so called ‘HAZOP review team’ which is typically made up of operators, designers, technical specialists and maintainers. The outcome of the HAZOP studies are mostly operational recommendations [9]. The HAZOP analysis has the following characteristics:

- Operates mainly on an operational level to identify operational risks.
- Does not provide in the means necessary to build a robust framework for the development of strategies to manage those risks.
- Is often used as part of a larger tool (e.g. CORAS) to overcome the above weakness.

IRAM

IRAM, or ‘Information Security Analysis Methodologies’, was developed by the Information Security Forum. It is not a risk assessment methodology at itself. It is a meta model forming an umbrella over other ISF tools as SPRINT, SARA and FIRM. It aids a company in choosing the right methodology in the right situation for the proper goal [21].

ITRMB

ITRMB, or the ‘Information Technology Risk Management Benchmark’ methodology, provides an objective and consistent means of reviewing the risks faced across and organisation in relation to its use of IT, and assesses whether they are being controlled and mitigated in an effective and efficient manner. As the name suggests, ITRMB is a benchmark. Benchmarking the risks and controls against the database population of ITRMB allows one to understand, at a high level, how the Information Security Governance approach compares against industry practice [30]. The ITRMB methodology has the following characteristics:

- Mainly focused on the financial sector.
- Enables an organisation to evaluate their position against control standards such as CobiT.
- Is questionnaire based, but not limited to pre-defined checklists.
- Has a supporting toolset.

MAGERIT

MAGERIT, or ‘Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información’, is a security management methodology of interest to people working with mechanized information and the systems that handle it. It offers a systematic method for analyzing risks that are present in these systems and helps describing and planning the appropriate measures for keeping the risks under control. Awareness of the system risk to those responsible is a direct objective of this methodology [11]. The MAGERIT methodology has the following characteristics:

- Is mainly focused on mechanized information and the information systems handling them.
- Is primarily aimed at those responsible for information systems (operational).
- Offers standardized processes for management communications.

Markov

Actually a method used by e.g. CORAS A Markov process is a stochastic process which has the Markov characteristic. Under certain circumstances, it can be used in risk management and portfolio management. The Markov characteristic says that it is not necessary to know the past, if one knows the present, to predict the future.
From all the methods listed, this probably is the most abstract one. It *is not* a complete management or analysis package. It *is* a usable methodology for use within other tools (e.g. CORAS) [32].

MEHARI

MEHARI, or ‘Méthode Harmonisée d’analyse des risques’ provides a consistent methodology, with appropriate knowledge databases, to aid Chief Information Security Officers (CISO's), general managers and security managers or other people implicated in risk reduction. It aims to provide a set of tools specifically designed for security management closely coupled to managerial actions with their respective goals [26]. The MEHARI methodology has the following characteristics:

- Is considered both qualitative as quantitative.
- Is broader that most standards. It does respond to the needs as indicated in the standards.
- Is constantly updated, meaning (amongst other things) that new standards and practices are easily implemented.

MORT

MORT, or Management Oversight Risk Tree is an analytical procedure for determining causes and contributing factors. It is a formal, decision tree like system that integrates a wide variety of safety concepts. It provides a base for communication, cooperation and planning for the company that uses the method [24, 16]. The MORT methodology has the following characteristics:

- Is a time consuming endeavor
- Needs a practitioner familiar with the method to be in a good position to make judgment based on its results.
- Has a resemblance to FTA up to a degree.
- Possible to quickly assimilate new experiences and findings, giving flexibility on this aspect.

NORA

NORA, or the ‘Network Oriented Risk Analysis’ methodology, is a network focused risk assessment methodology developed by PriceWaterhouseCoopers. It is considered to be qualitative, quantitative as well as semi-quantitative. It defines a large risk oriented vocabulary with associated methodologies [23]. The NORA has the following characteristics:

- Is partly questionnaire based.
- Offers possibilities for tree-like risk scenarios
- Has a variety of support tools.
- Concretely defines residual risk.

OCTAVE

OCTAVE, or Operationally Critical Threat, Asset and Vulnerability Evaluation, is a risk-based strategic assessment and planning technique for security. It uses risks to the most critical assets to prioritize areas of improvement and set the security strategy for the organisation. OCTAVE can be primarily considered a qualitative methodology. It does provide a possibility for the use of quantitative data, but only to construct a qualitative risk ranking. The OCTAVE methodology has the following characteristics [3]:

- Self directed.
- Leverages people’s knowledge of security-related practices and processes.
- Targeted at organisational risk and focused on static practice-related issues (in contrast to a typical technology-focused assessment).
- Includes both people from the IT department and management.

OCTAVE-S

OCTAVE-S, or OCTAVE for Smaller organisations is a smaller version of the normal OCTAVE methodology. It is designed for organisations that can empower a team of three to five people who have to do all evaluation activities without the need for formal data-gathering activities [3]. It has a few characteristics that makes it different from the normal OCTAVE methodology:

- Developed for small organisations, ranging from 20 to 80 people.
- Evaluates the company’s computing infrastructure to a lesser extent than normal OCTAVE because small organisations often outsource this function.

OSSTMM

OSSTMM, or the ‘Open Source Security Testing Methodology Manual’, is a peer-reviewed methodology for performing security tests and metrics. It focuses on the technical details of exactly which items need to be tested, what to do before, during and after a security test, and how to measure the results [17]. The OSSTMM has the following characteristics:

- Has compliance to legislations incorporated in it’s design.

- Constantly updated, making use of international best practices, laws, regulations and ethical concerns.
- Can easily be customized to situations.
- Stimulates intra-organisation communication between technical (operational) and management employees.

OSSTMM-RAV

OSSTMM-RAV, or the 'Open Source Security Testing Methodology Manual - Risk Assessment Values', considers the security metrics as defined in OSSTMM. They are considered the cornerstone of change control and information security management. The security metrics provide factual security numbers. It is an addition to the OSSTMM, giving the possibility of more detailed information to base decisions upon. For example:

OSSTMM *without* RAV's "Our main server needs to reside in a secure vault with sufficient protection against fire"

OSSTMM *with* RAV's "Our main server needs to reside in a 5x5x3m secure vault with nuclear blast doors of at least 15cm thickness, with an argon based fire protection system"

QSM Security Expert

The QSM Security Expert is part of the iQSM governance framework with a special focus on security aspects. Since the iQSM's goal is to provide a governance framework, it should not come as a surprise that most activities have a management focus and are aimed at providing management information for executive and senior levels. The compliance to standards is a second specialization of the approach, making it easy to comply to standards as CobiT, SOX and ISO27001 [36].

RAF and ARROW-II

RAF, or 'Risk Assessment Framework' is a general naming of a framework used to make risk-based regulations operational. In particular, ARROW (Advanced, Risk-Responsive Operating FrameWork) is a Risk Assessment Framework developed by the FSA (Financial Services Authority).. The ARROW-II (and RAF) program are aimed at creating greater efficiency and effectiveness in the management of risk. Improved communication, skills and supervisory knowledge are also discussed by ARROW. The ARROW processes and deliverables are mostly qualitative in nature (qualitative measures for impact and probability). It gives the possibility for a semi-quantitative approach, but only in a minimalistic way. Different approaches exist for large/medium organisations and small organisations as well as organisations in different risk categories [55].

ROSI

ROSI, or Return On Security Investments, focuses on the financial benefits and costs of a security initiative and ignores any non-financial benefit, as these cannot be quantified. By capturing and stating benefits in financial terms and comparing the benefits to the costs, ROSI provides an approach

for security professionals to quantify and communicate the financial benefits of information security initiatives to the organisation [38].
ROSI can be used to make a business case and to compare alternative security initiatives by examining the costs and reductions in business impact offered by those alternatives. Alternatively, the controls originating from ROSI can assist an organisation in meeting requirements placed on it by law or regulation (e.g. SOX, Turnbull, Basel II, King II, etc...) [46].
ROSI is driven from two directions: 'top-down' and 'bottom-up'. The 'top-down' group consists of the Senior Management, Academics developing specific implementations of the ROSI method, and audit groups. The 'bottom-up' group consists of mainly security professionals.

ROISI

ROISI, or Return On Information Security Investments, is a ROSI methodology specifically focused on information security. The ROISI uses the same approach as ROSI but has different parameters.

SARA

SARA, or Simple to Apply Risk Analysis for information systems, is a detailed risk analysis methodology developed by the Information Security Forum (ISF). The SARA methodology is intended to be used for business critical IT systems and provides a systematic process for the identification and assessment of threats and control requirements in order to support a cost justification of controls [53]. SARA has the following characteristics:

- Aims at providing management with an understanding of an organisation's exposure to losses from IT security breaches.
- Designed to assess risks for a single application as distinct from an installation or an entire organisation.
- Designed for use by IT security practitioners or system development personnel. It needs an experienced facilitator with good experience of risk analysis.(Given the application of SARA to mainly business critical systems, it has been d)
- Does *not* provide guidance on the design or selection of specific control techniques.
- Can be applied to a great variety of systems in different sizes since it is not system specific in nature.

SMORT

SMORT, or 'Safety Management Organisation Review Technique', is a simplified version of MORT. Like MORT, it is a tree-like technique with as difference that SMORT-tree's are finite in branchings and leafs, where MORT in theory is infinite. Every leaf-node of the tree has a questionnaire and checklist for it's specific level. This methodology has a relatively small userbase originating from Scandinavia. The methodology nonetheless, can be used for security audits and security baseline analysis, tho be it not it's primary point of interest [52]. Relatively little is publicly available on this methodology.

SOMAP

SOMAP, or 'Security Officers Management and Analysis Project', is not a method, model or tool in itself. The products of this project (e.g. ’the guide’ and ’the handbook’) contain descriptions and explanations on how to plan, implement and manage an information security risk strategy and information security management system. The guide and the handbook describe the risk assessment and management process in detail. They discuss the different steps of the risk analysis process and contain the formulas to calculate risk [60]. The SOMAP guidelines have the following characteristics:

- Can deal with changes over time.
- Discusses both qualitative as (semi-)quantitative method for risk prioritization.
- Can address both reactive as proactive approaches to the management of risk.

SP800-30

SP800-30, which is short for NIST Special Publication 800-30 is a risk management guide for information technology systems. It has a very low level objective of performing risk management to enable the organisation to accomplish it’s mission(s)

1. by better securing the IT systems that store, process or transmit organisational information.
2. by enabling management to make well-informed risk management decisions to justify the expenditures that are part of an IT budget.
3. by assisting management in authorizing the IT systems on the basis of the supporting documentation resulting from the performance of risk management.

As we can see from these objectives, the SP800-30 is not only for senior management, but also for CISO’s, functional and business managers, technical support personnel and programmers. The method considers the classic CIA triad and is to be considered qualitative in that it reports using rating (e.g. likelihood rating, impact rating) [51].

SPARK

SPARK, or Simplified Process for Analyzing Risk by KPMG, is a formal and relatively easy method to assess information risks using a software tool. It helps identifying adequate controls and actions to ensure confidentiality, integrity and availability. It is closely integrated with international standards [43]. The SPARK methodology has the following characteristics [29]:

- Can be done in relatively little time and is easy to learn and apply.
- Facilitates communication between specialists and senior management.
- Structured by using questionnaires. This makes the scope somewhat narrow.
- Integrated with international standards by working with ISF’s SPRINT methodology. It also has the flexibility of the SPRINT methodology.

SPRINT

SPRINT, or Simplified Process for Risk Identification, is a risk analysis methodology developed by the Information Security Forum (ISF). The SPRINT methodology is intended to be used for important, but not critical systems. (for this, the SARA methodology would be better) SPRINT should also not be used in low risk situations where standard security requirements are covered by baselines [54]. It has the following characteristics:

- Business-oriented which means that decisions about risk and controls are made by business managers in cooperation with the specialists on the matter.
- Structured by having clear defined processes and deliverables. It supports a systematical approach.
- As the abbreviation already says; The SPRINT methodology is easy to understand and simple to apply. A SPRINT risk analysis can be completed in relatively little time.
- Working from the previous point, a SPRINT risk analysis can be done by people with limited experience with risk analysis.
- Can be applied to a great variety of systems since it is not system or size specific in nature.

STRIDE

STRIDE, which stands for Spoofing, Tampering, Repudiation, Information disclosure, Denial of service and Elevation of privilege, is a tree based methodology to threat modelling. STRIDE is for example used in Microsoft's .Net security framework. It is used for the identification of threats that might affect a system and compromise assets. In the methodology, operational people are brought together to conduct an informed brainstorming session. The STRIDE methodology in this sense is goal-based where one considers the goals of a potential attacker.

TRIKE

TRIKE is a conceptual framework for security auditing from a risk management perspective through the generation of threat models and attack graphs. A security auditing team can use it to describe the security characteristics of a system from a high-level architecture point of view till a low-level implementation point of view. It enables communication among security team members and between security teams and other stakeholders by abiding to a consistent framework [44].
Sadly enough, it seems like the TRIKE methodology has been abandoned by its founders, showing little recent activity.

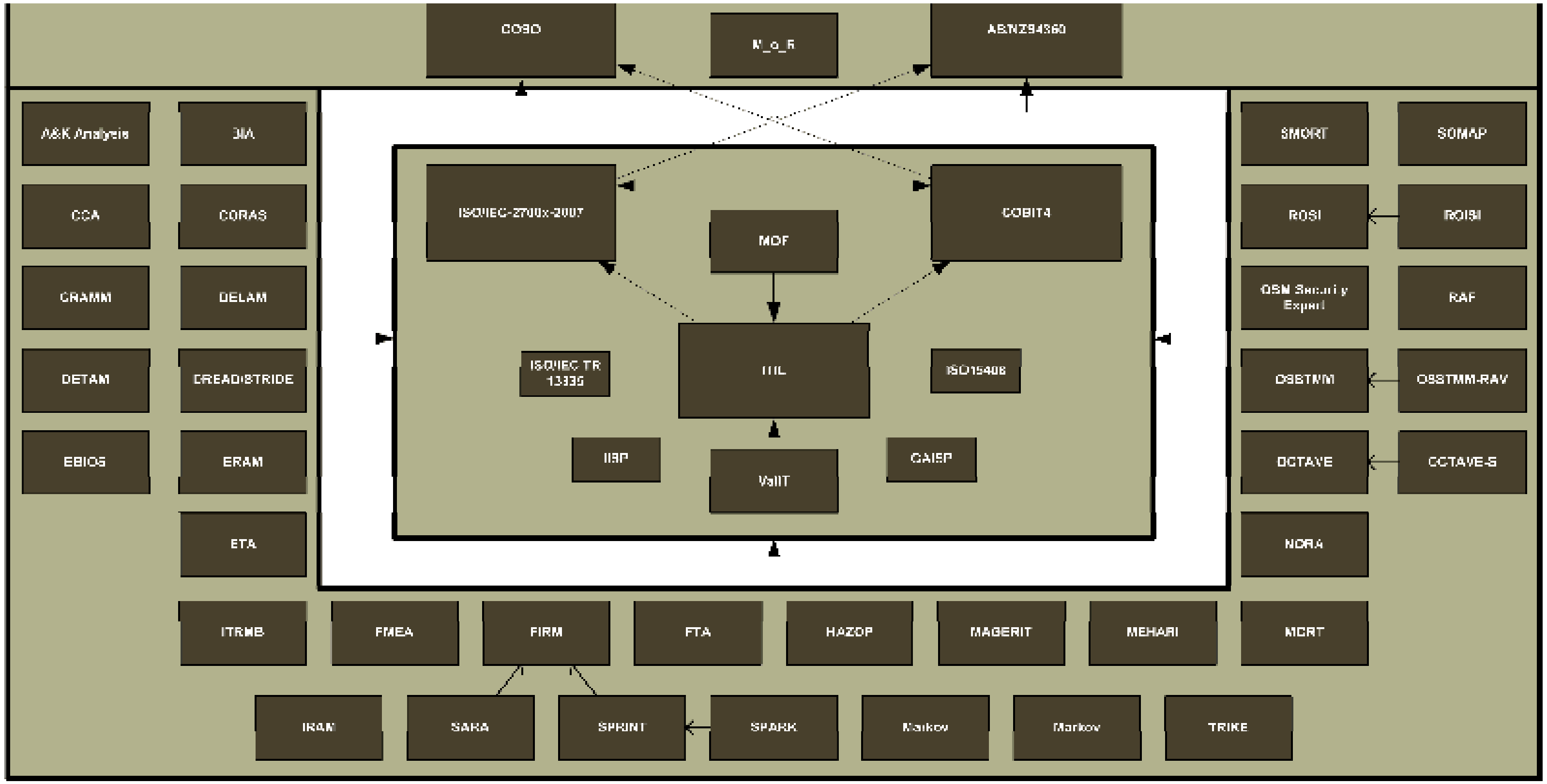


Figure C.1: [illegible] found from literature-quickscan

APPENDIX D

Methodologies: Comparative Framework

For the comparison of the rather large amount of methodologies found in the literature quickscan, a comparative framework is constructed to quickly pick the right methodologies for our need. Additional requirements were identified by conducting semi-structured interviews with experts from different sectors as shown in Appendix B .

D.1 Framework Construction

Combining the results of the interviews and literature present on the subject, a comparative framework is constructed. The comparative framework consists of the template of "Risk Management and Risk Assessment Methods" from the ENISA combined with components from CobiT. The exact details will be discussed in the following paragraphs.

ENISA

The "Risk management and Risk Assessment Methods" template from the ENISA provides a very basic foundation for the comparison of different Risk Management and Risk Assessment Methodologies. The methodologies are all compared on a high level. It discusses origin, compliance and support of different RA/RM phases, but also scope, level of detail and skill needed to use the methodology. The template was constructed and used by the ENISA Working Group (which can be considered experts in the field, originating from eight EU member states) in 2005.

Although the ENISA template provides a sturdy foundation to compare different Risk Management and Risk Assessment methodologies, it is very global in nature. If the framework is to support the decision on selecting an appropriate methodology, we need a more detailed comparison. For this purpose, elements from CobiT were added to the framework.

CobiT

If we take a look back at Chapter 3 we again see the so called CobiT-cube (see Fig. 3.2). Notice that the 'processes' dimension of the cube are largely covered by the ENISA template. The other two dimensions of the cube are not.

A direct translation of the CobiT business objectives cannot be made to our comparative framework of information risk management and assessment methodologies. The part of CobiT that addresses the assessment and management of risk (the most) is process P09 (CobiT: Plan and Organise; Assess and Manage IT Risks). The CobiT documentation states that this process primarily supports the Confidentiality, Integrity and Availability 'business requirements' (which should sound familiar after reading Chapter 3). Regardless if one is to use the limited CIA criteria, the broader Parkerian Hexad criteria or any other variety or criteria, a clear definition of the information assurance criteria is necessary for our eventual model. Therefor, this requirement is added to the comparative framework (as *Information Ass. Criteria defined*).

Building further on CobiT process P09, we see that the Risk Assessment and Management process covers all resources. In our comparative framework we therefor need to be able to select methodologies based on their coverage of resources. These resources can also be found in the comparative framework (as *Resources defined*).

D.2 Framework Elements

The comparative framework discusses the following elements:

Information Assurance Criteria defined Does the methodology explicitly define Information Assurance Criteria? [1]

Resources defined Does the methodology explicitly define the following resources: [1]

- Applications?
- Information?
- Infrastructure?
- People?

RA Phases The Risk Assessment phases that are supported by the methodology: [1]

- Risk Identification: The process of identifying assets and threats in relation to risk.
- Risk Analysis: The process of identifying dependabilities between risk elements, controls, time, etc…
- Risk Evaluation: The process of evaluating assets and threat likelihood in relation to risk.

RM Phases The Risk Management phases that are supported by the methodology: [1]

- Risk Assessment: The process of assessing the (current) risk is explicitly defined.
- Risk Treatment: The process of the treatment of risk is explicitly defined.
- Risk Acceptance: The process of the acceptance of risk is explicitly defined.
- Risk Communication: The process of the communication of risk is explicitly defined.

Target Organisation The type of the target organisation that is supported by the methodology: [1]

- Government and agencies. Organisation has a clear affiliation with the government.

[1] Ranked using: V (Yes), ~ (Somewhat), X (No)

- Large companies. Organisation with more than 250 employees.
- SME's. Small and Medium sized Enterprises.

Level coverage The level of the targeted user: [1]

- Management: uses generic guidelines.
- Operational: uses guidelines for implementation planning with a low level of detail.
- Technical: uses specific guidelines for implementation planning with a high level of detail.

Compliance to standards Is it possible to work toward compliance to standards, using the methodology? [1]

Maturity measurement Is it possibly to measure maturity based on the methodology? [1]

Tool support Is the methodology officially supported by tools? [1]

Geographical spread The geographical spread of the methodology. [2]

Skill needed The level of skill needed to apply the method successfully. [2]

Year of introduction The year the methodology was introduced.

Year of last update The year the methodology was last, formally updated.

By adding a few bits and pieces from CobiT to the comparative framework, we seemingly limit ourselves to using one specific Risk Assessment Framework. This is only partly the case since CobiT knows a great variety of possible mappings to other frameworks, standards and practices. With these linkages one could easily customize the methodology to special preferences or even expand its functionality (e.g. by working towards an *information security maturity* model)

[2] Ranked using: L (Low), M (Medium) and H (High)

control	X	X	X	✓	✓	X	X	X	X	✓	X	–	X	X	X	X	✓	X	✓	X	✓	X	X	X	X	✓	–	–	X	X	–	X	X	✓	–	–	X	–
Compliance to standards	✓	–	X	✓	✓	X	X	X	✓	✓	X	–	X	X	X	✓	✓	X	✓	X	✓	✓	–	–	–	✓	✓	–	X	X	✓	X	✓	✓	✓	✓	X	–
Maturity measurement	X	X	X	X	X	X	X	X	✓	X	X	–	X	X	X	✓	X	X	X	X	X	X	X	X	X	X	–	X	X	X	X	X	X	X	X	X	X	X
Geographic spread	L	M	M	M	H	M	M	M	H	L	H	H	M	H	H	M	M	H	M	H	M	M	L	L	M	M	L	M	H	L	H	L	L	M	M	H	H	L
Skill needed	I	I	M	M	H	H	H	I	H	M	M	I	M	M	M	I	H	H	M	H	M	M	I	I	M	M	I	M	H	H	M	M	M	M	I	I	I	I
Tool support	–	✓	–	✓	✓	–	–	X	✓	X	–	–	X	–	–	✓	✓	✓	X	✓	✓	X	✓	X	✓	✓	✓	✓	✓	✓	X	✓	✓	–	✓	–	X	X
Year of introduction	80	04	87	01	85	88	68	?	05	05	76	?	62	82	74	?	97	08	88	70	?	02	07	04	00	00	?	00	01	05	03	70	08	02	04	07	?	08
Year of last update	86	07	X	05	07	X	X	X	05	07	X	00	X	X	X	07	06	X	07	X	07	07	07	07	07	07	07	06	07	06	84	X	06	02	07	87	X	06

Table D.1: A comparative framework for SA/RM methodologies

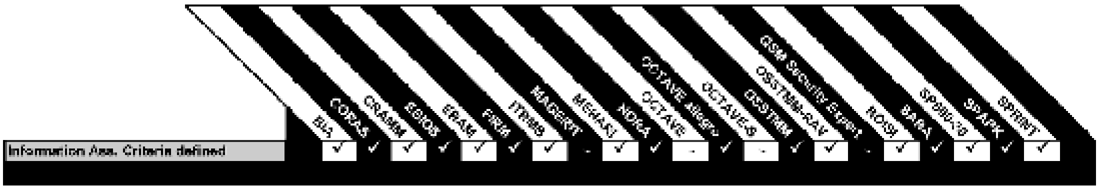
Appendix E

Methodologies: Filter Iterations

In this chapter the found methodologies from the comparative framework are filtered against a set of predefined criteria. The Criteria are as defined in Table E.1

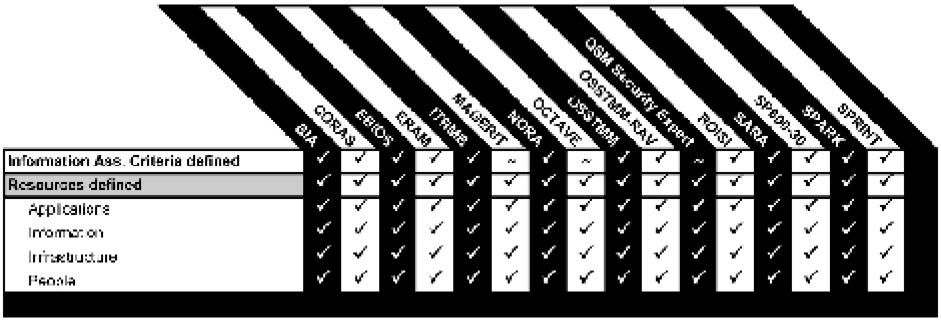
Table E.1: Iteration filter criteria

Iteration	Filter requirements
1	Should have information assurance criteria defined.
2	Should (at least) have resources defined (application, information, infrastructure, people).
3	Should provide means for identifying tangible assets and threats.
4	Should provide means for analyzing risk dependabilities.
5	Should provide means for evaluating tangible assets and threats.
6	Should provide means for risk acceptance.
7	Should be usable by small and medium enterprises. Should be usable by large companies. Should preferably be usable by government & agencies.
8	Should provide detail on management level. Should at least provide detail up to operational level. Should preferably provide detail up to technical level.
9	Skill needed is medium or low. Tool support is preferably native, or provided by third parties. Should be at least somewhat recent (last update ≤ 10 years ago)



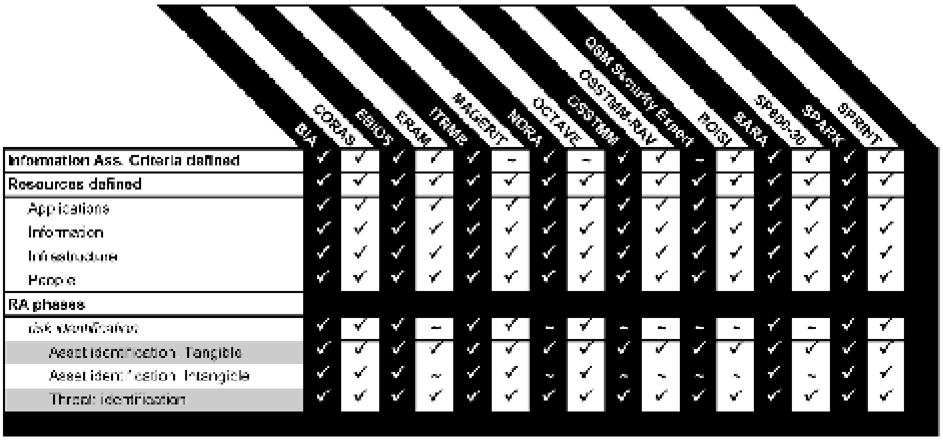
	BIA	CORAS	CRAMM	EBIOS	ERAM	FIRM	ITRMS	MAGERIT	MEHARI	NORA	OCTAVE	OCTAVE Allegro	OCTAVE-S	OSSTMM	OSSTMM-RAV	QSM Security Expert	ROISI	SARA	SP800-30	SPARK	SPRINT
Information Ass. Criteria defined	✓	✓	✓	✓	✓	✓	✓	-	✓	✓	-	✓	-	✓	✓	-	✓	✓	✓	✓	✓

Table E.2: Iteration 1: Information Assurance Criteria



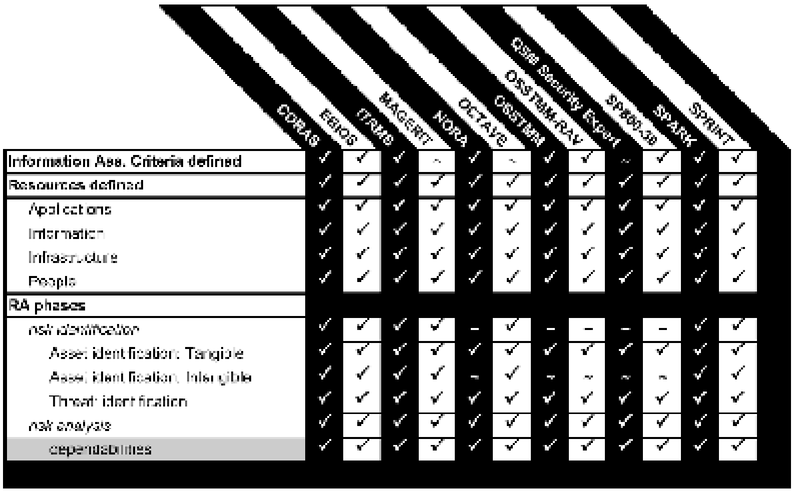
	BIA	CORAS	EBIOS	ERAM	ITRMS	MAGERIT	NORA	OCTAVE	OSSTMM	OSSTMM-RAV	QSM Security Expert	ROISI	SARA	SP800-30	SPARK	SPRINT
Information Ass. Criteria defined	✓	✓	✓	✓	✓	~	✓	~	✓	✓	~	✓	✓	✓	✓	✓
Resources defined	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Applications	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Information	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Infrastructure	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
People	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

Table E.3: Iteration 2: Resources



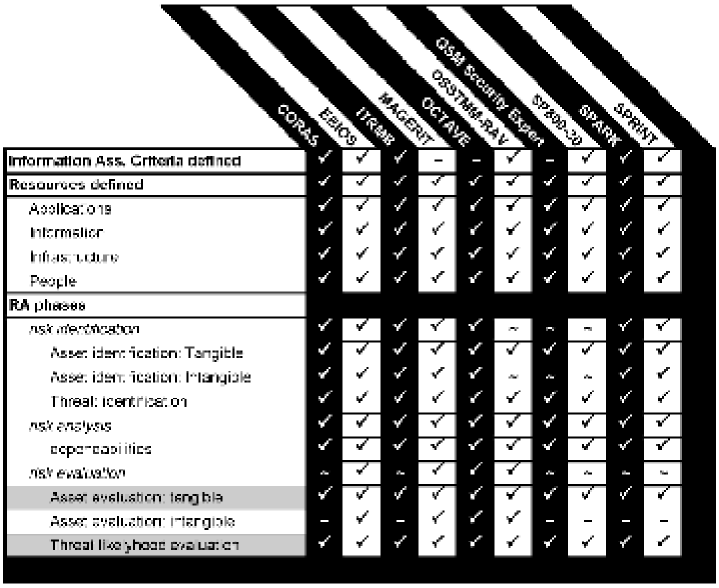
	BIA	CORAS	EBIOS	ERAM	ITRMS	MAGERIT	NORA	OCTAVE	OSSTMM	OSSTMM-RAV	QSM Security Expert	ROISI	SARA	SP800-30	SPARK	SPRINT
Information Ass. Criteria defined	✓	✓	✓	✓	✓	–	✓	–	✓	✓	–	✓	✓	✓	✓	✓
Resources defined	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Applications	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Information	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Infrastructure	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
People	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
RA phases																
risk identification	✓	✓	✓	–	✓	✓	–	✓	–	–	–	–	✓	–	✓	✓
Asset identification Tangible	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Asset identification Intangible	✓	✓	✓	~	✓	✓	~	✓	~	~	~	~	✓	~	✓	✓
Threat identification	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

Table E.4: Iteration 3: Identify tangible assets and threats



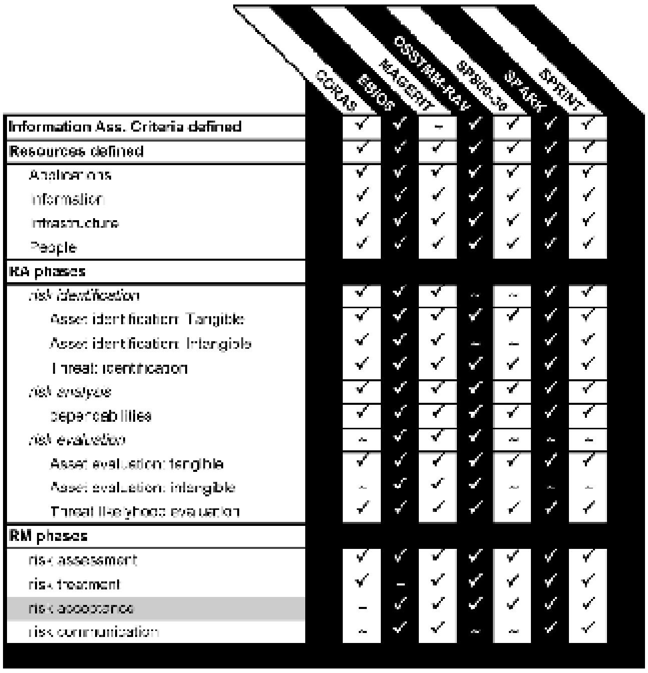
	CORAS	EBIOS	ITRMS	MAGERIT	NORA	OCTAVE	OSSTMM	OSSTMM-RAV	QSM Security Expert	SP800-30	SPARK	SPRINT
Information Ass. Criteria defined	✓	✓	✓	~	✓	~	✓	✓	~	✓	✓	✓
Resources defined	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Applications	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Information	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Infrastructure	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
People	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
RA phases												
risk identification	✓	✓	✓	✓	–	✓	–	–	–	–	✓	✓
Asset identification: Tangible	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Asset identification: Intangible	✓	✓	✓	✓	–	✓	~	~	~	~	✓	✓
Threat identification	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
risk analysis	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
dependabilities	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

Table E.5: Iteration 4: Risk dependabilities



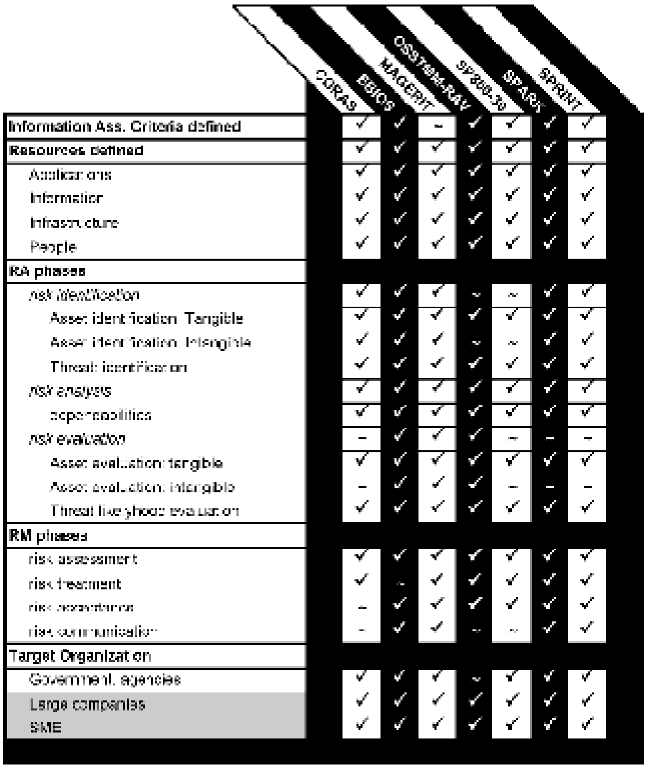
	CORAS	EBIOS	ITRMS	MAGERIT	OCTAVE	OSSTMM-RAV	QSM Security Expert	SP800-30	SPARK	SPRINT
Information Ass. Criteria defined	✓	✓	✓	–	–	✓	–	✓	✓	✓
Resources defined	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Applications	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Information	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Infrastructure	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
People	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
RA phases										
risk identification	✓	✓	✓	✓	✓	~	~	–	✓	✓
Asset identification: Tangible	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Asset identification: Intangible	✓	✓	✓	✓	✓	~	~	~	✓	✓
Threat identification	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
risk analysis	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
dependabilities	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
risk evaluation	~	✓	~	✓	✓	✓	~	~	~	~
Asset evaluation: tangible	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Asset evaluation: intangible	–	✓	–	✓	✓	✓	–	–	–	–
Threat likelyhood evaluation	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

Table E.6: Iteration 5: Evaluate tangible assets and threats



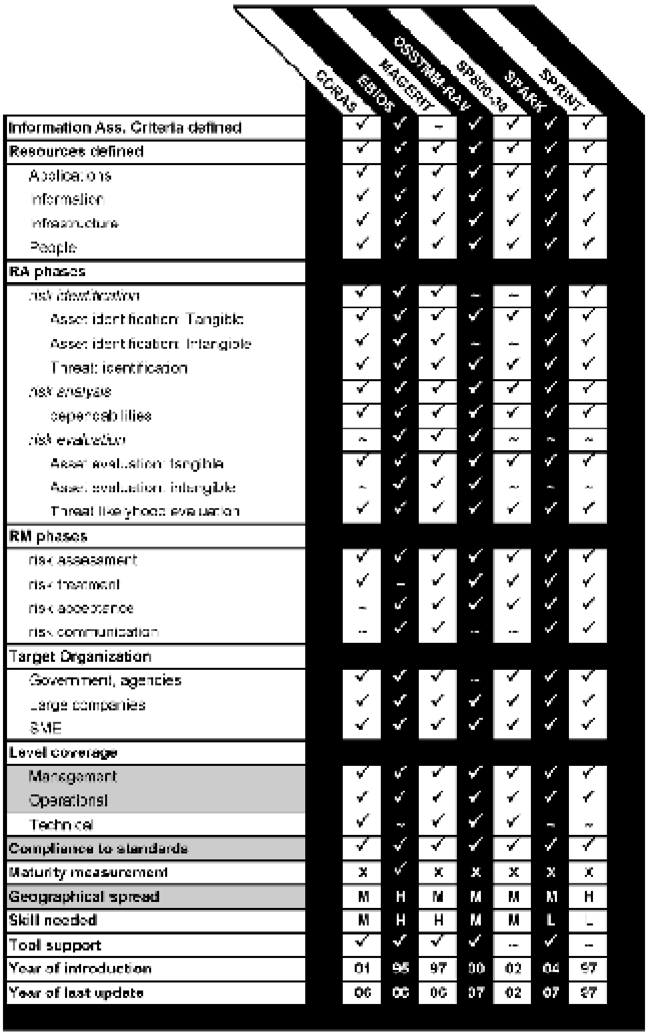
	CORAS	EBIOS	MAGERIT	OSSTMM-RAV	SP800-30	SPARK	SPRINT
Information Ass. Criteria defined	✓	✓	–	✓	✓	✓	✓
Resources defined	✓	✓	✓	✓	✓	✓	✓
Applications	✓	✓	✓	✓	✓	✓	✓
Information	✓	✓	✓	✓	✓	✓	✓
Infrastructure	✓	✓	✓	✓	✓	✓	✓
People	✓	✓	✓	✓	✓	✓	✓
RA phases							
risk identification	✓	✓	✓	~	~	✓	✓
Asset identification: Tangible	✓	✓	✓	✓	✓	✓	✓
Asset identification: Intangible	✓	✓	✓	–	–	✓	✓
Threat identification	✓	✓	✓	✓	✓	✓	✓
risk analysis	✓	✓	✓	✓	✓	✓	✓
dependabilities	✓	✓	✓	✓	✓	✓	✓
risk evaluation	~	✓	✓	✓	~	~	~
Asset evaluation: tangible	✓	✓	✓	✓	✓	✓	✓
Asset evaluation: intangible	~	✓	✓	✓	~	~	~
Threat likelyhood evaluation	✓	✓	✓	✓	✓	✓	✓
RM phases							
risk assessment	✓	✓	✓	✓	✓	✓	✓
risk treatment	✓	–	✓	✓	✓	✓	✓
risk acceptance	–	✓	✓	✓	✓	✓	✓
risk communication	~	✓	✓	~	~	✓	✓

Table E.7: Iteration 6: Risk acceptance



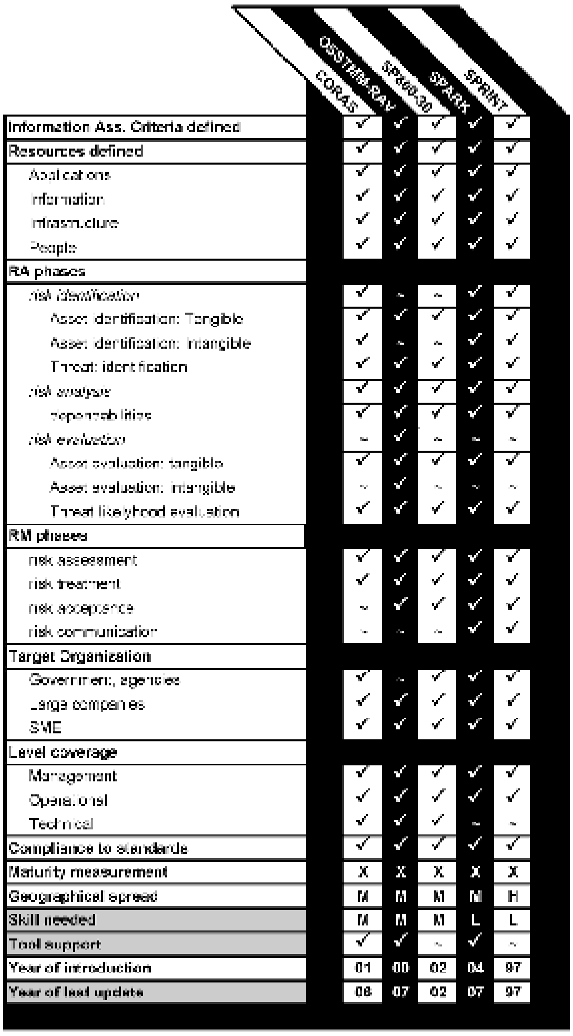
	CORAS	EBIOS	MAGERIT	OSSTMM-RAV	SP800-30	SPARK	SPRINT
Information Ass. Criteria defined	✓	✓	~	✓	✓	✓	✓
Resources defined	✓	✓	✓	✓	✓	✓	✓
Applications	✓	✓	✓	✓	✓	✓	✓
Information	✓	✓	✓	✓	✓	✓	✓
Infrastructure	✓	✓	✓	✓	✓	✓	✓
People	✓	✓	✓	✓	✓	✓	✓
RA phases							
risk identification	✓	✓	✓	~	~	✓	✓
Asset identification: Tangible	✓	✓	✓	✓	✓	✓	✓
Asset identification: Intangible	✓	✓	✓	~	~	✓	✓
Threat identification	✓	✓	✓	✓	✓	✓	✓
risk analysis	✓	✓	✓	✓	✓	✓	✓
dependabilities	✓	✓	✓	✓	✓	✓	✓
risk evaluation	–	✓	✓	✓	–	–	–
Asset evaluation: tangible	✓	✓	✓	✓	✓	✓	✓
Asset evaluation: intangible	–	✓	✓	✓	–	–	–
Threat likelyhood evaluation	✓	✓	✓	✓	✓	✓	✓
RM phases							
risk assessment	✓	✓	✓	✓	✓	✓	✓
risk treatment	✓	~	✓	✓	✓	✓	✓
risk acceptance	–	✓	✓	✓	✓	✓	✓
risk communication	~	✓	✓	~	~	✓	✓
Target Organization							
Government agencies	✓	✓	✓	~	✓	✓	✓
Large companies	✓	✓	✓	✓	✓	✓	✓
SME	✓	✓	✓	✓	✓	✓	✓

Table E.8: Iteration 7: Organisational size



	CORAS	EBIOS	MAGERIT	OSSTMM-RAV	SP800-30	SPAKK	SPRINT
Information Ass. Criteria defined	✓	✓	–	✓	✓	✓	✓
Resources defined	✓	✓	✓	✓	✓	✓	✓
Applications	✓	✓	✓	✓	✓	✓	✓
Information	✓	✓	✓	✓	✓	✓	✓
Infrastructure	✓	✓	✓	✓	✓	✓	✓
People	✓	✓	✓	✓	✓	✓	✓
RA phases							
risk identification	✓	✓	✓	–	–	✓	✓
Asset identification: Tangible	✓	✓	✓	✓	✓	✓	✓
Asset identification: Intangible	✓	✓	✓	–	–	✓	✓
Threat: identification	✓	✓	✓	✓	✓	✓	✓
risk analysis	✓	✓	✓	✓	✓	✓	✓
dependabilities	✓	✓	✓	✓	✓	✓	✓
risk evaluation	~	✓	✓	✓	~	~	~
Asset evaluation: tangible	✓	✓	✓	✓	✓	✓	✓
Asset evaluation: intangible	~	✓	✓	✓	~	~	~
Threat likelyhood evaluation	✓	✓	✓	✓	✓	✓	✓
RM phases							
risk assessment	✓	✓	✓	✓	✓	✓	✓
risk treatment	✓	–	✓	✓	✓	✓	✓
risk acceptance	~	✓	✓	✓	✓	✓	✓
risk communication	–	✓	✓	–	–	✓	✓
Target Organization							
Government, agencies	✓	✓	✓	–	✓	✓	✓
Large companies	✓	✓	✓	✓	✓	✓	✓
SME	✓	✓	✓	✓	✓	✓	✓
Level coverage							
Management	✓	✓	✓	✓	✓	✓	✓
Operational	✓	✓	✓	✓	✓	✓	✓
Technical	✓	~	✓	✓	✓	–	~
Compliance to standards	✓	✓	✓	✓	✓	✓	✓
Maturity measurement	X	✓	X	X	X	X	X
Geographical spread	M	H	M	M	M	M	H
Skill needed	M	H	H	M	M	L	L
Tool support	✓	✓	✓	✓	–	✓	–
Year of introduction	01	95	97	00	02	04	97
Year of last update	06	06	06	07	02	07	97

Table E.9: Iteration 8: Level of detail



	CORAS	OSSTMM-RAV	SP800-30	SPARK	SPRINT
Information Ass. Criteria defined	✓	✓	✓	✓	✓
Resources defined	✓	✓	✓	✓	✓
Applications	✓	✓	✓	✓	✓
Information	✓	✓	✓	✓	✓
Infrastructure	✓	✓	✓	✓	✓
People	✓	✓	✓	✓	✓
RA phases					
risk identification	✓	~	~	✓	✓
Asset identification: Tangible	✓	✓	✓	✓	✓
Asset identification: Intangible	✓	~	~	✓	✓
Threat identification	✓	✓	✓	✓	✓
risk analysis	✓	✓	✓	✓	✓
dependabilities	✓	✓	✓	✓	✓
risk evaluation	~	✓	~	~	~
Asset evaluation: tangible	✓	✓	✓	✓	✓
Asset evaluation: intangible	~	✓	~	~	~
Threat likelyhood evaluation	✓	✓	✓	✓	✓
RM phases					
risk assessment	✓	✓	✓	✓	✓
risk treatment	✓	✓	✓	✓	✓
risk acceptence	~	✓	✓	✓	✓
risk communication	~	~	~	✓	✓
Target Organization					
Government, agencies	✓	~	✓	✓	✓
Large companies	✓	✓	✓	✓	✓
SME	✓	✓	✓	✓	✓
Level coverage					
Management	✓	✓	✓	✓	✓
Operational	✓	✓	✓	✓	✓
Technical	✓	✓	✓	~	~
Compliance to standards	✓	✓	✓	✓	✓
Maturity measurement	X	X	X	X	X
Geographical spread	M	M	M	M	H
Skill needed	M	M	M	L	L
Tool support	✓	✓	~	✓	~
Year of introduction	01	00	02	04	97
Year of last update	08	07	02	07	97

Table E.10: Iteration 9: Skill needed

APPENDIX F

A BAYESIAN REPRESENTATION

This chapter gives an example on how Bayesian Networks can be used in our representation of residual risk and how the features of the Bayesian Network can aid in making decisions on mitigation plans and scenarios.

F.1 Minimal Working Example

In the minimal working example we modelled one application which has one vulnerability and two possible threats exploiting this vulnerability. These threats exploiting that specific vulnerability give rise to one CumThreat. As can be seen in Fig. F.1 , the threats are modelled by the three components Source, Access and Skill which were discussed earlier in Chapter 4 .

Examples (based on the information given in Chapter 4) of the conditional probability table are given by tables F.1 and F.2. The conditional probabilities of the threats can be derived from the event corresponding to the occurrence of the separate components. In this situation, the probability of the vulnerability being successfully exploited was known a priori.

This minimal example can already be used to condition on different observations and analyse different scenarios.

F.2 Extended Working Example

In the extended working example as shown in Fig. F.2 we add some functionality to our Bayesian Network by adding a utility node to the Application. Assuming that the loss occurring from this specific application originating from the CumThreat equals €20M, the utility node will represent that value as shown in Table F.3 .

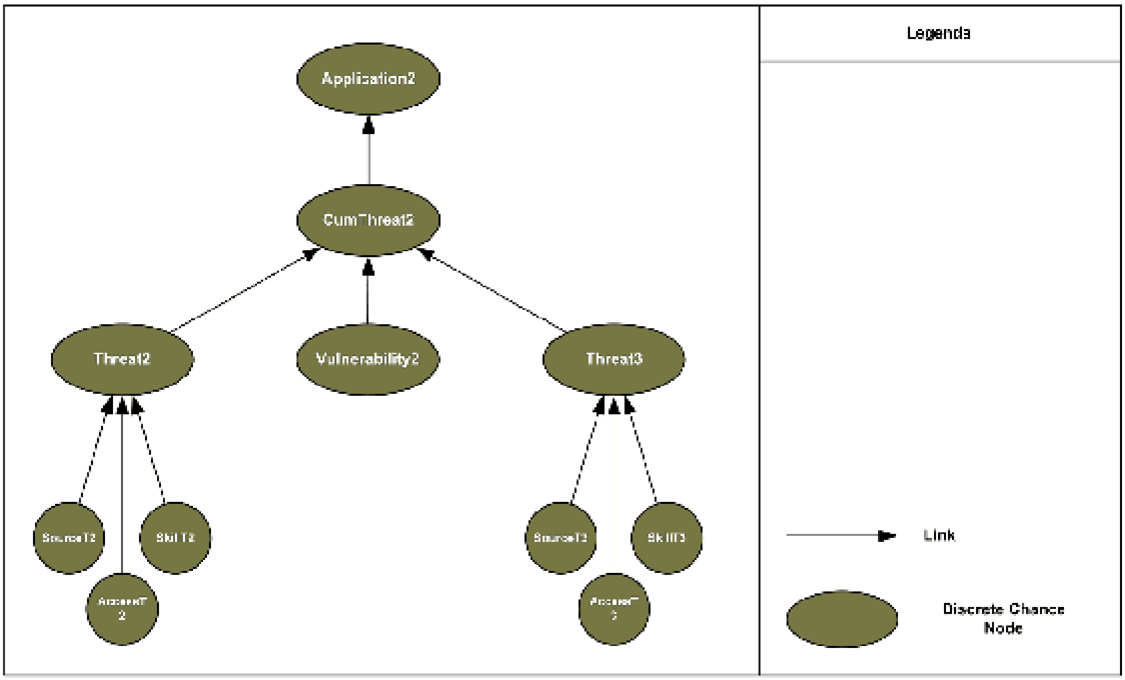


Figure F.1: Initial situation

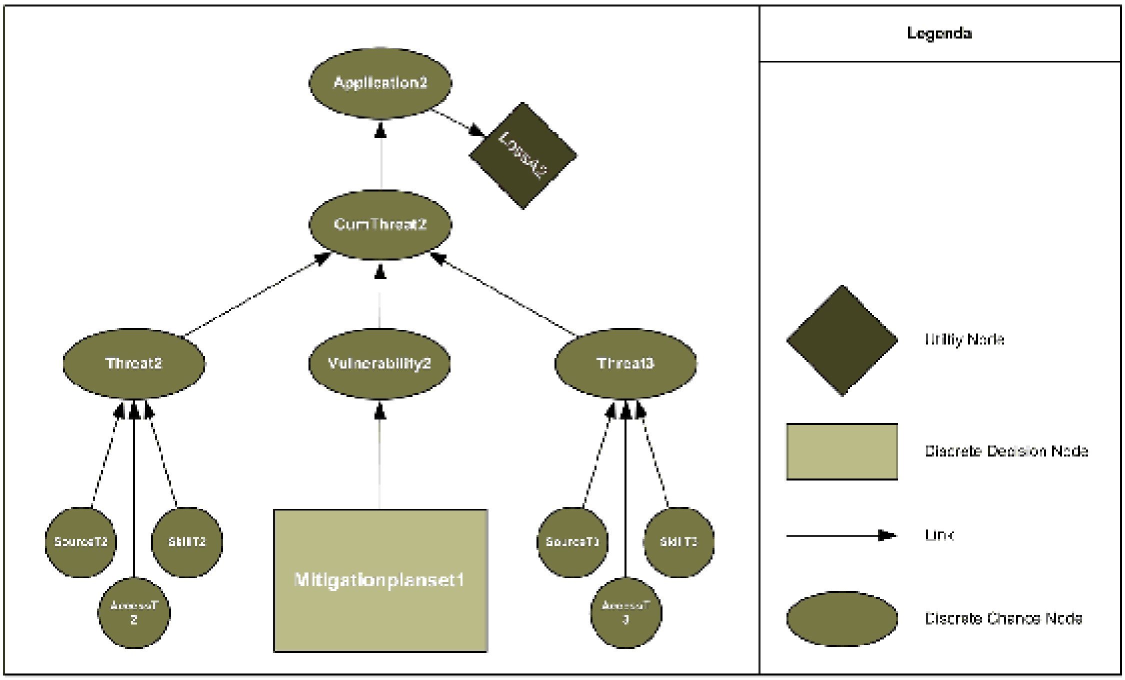


Figure F.2: Initial situation with added utility and mitigationplanset

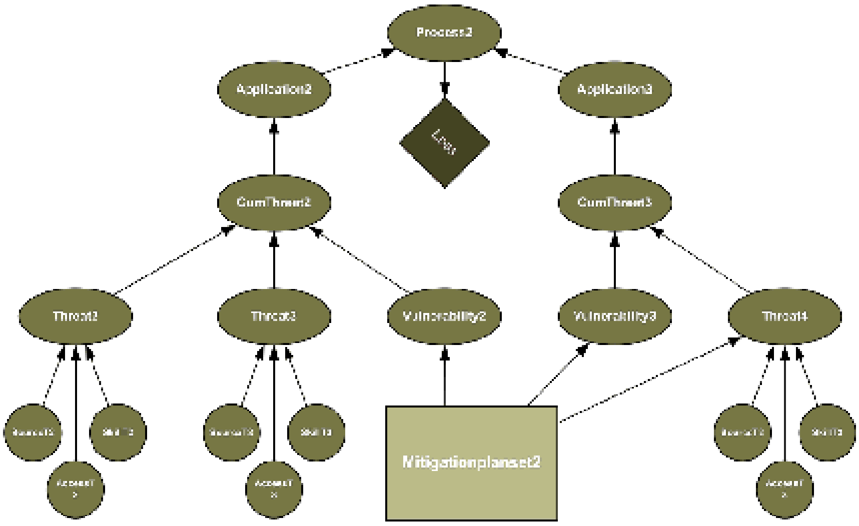


Figure F.3: Extended situation on process level

By adding a decision node, we can represent a Mitigationplanset that counters certain vulnerabilities and threats. In the example as shown in Fig. F.2 the Mitigationplanset1 mitigates Vulnerability2 as shown in Table F.4 . Initially, the probability that the vulnerability would be successfully exploited was considered to be 0.12. With the introduction of Mitigationplanset1, this can be reduced to 0.02.

Now the organisation can calculate the value of certain decisions (e.g. implement Mitigationplanset1 or not) and simulate what would happen if new information comes in (e.g. Threat2 has successfully manifested itself).

F.3 Extended Process Level Example

This final example (Fig. F.3) shows how processes spanning more applications can be incorporated in the Bayesian Network. Additionally, more complex relationships can be added. Mitigationplanset2, for example, does not only mitigate Vulnerability2 but also mitigates Vulnerability3 and Threat4 to a certain level. An additional utility node is added to represent the losses from a breach in either confidentiality, integrity or availability in Application3.

The organisation can again calculate the value of Mitigationplanset2 given the conditional probabilities in the network, the value of the applications and additional information on the occurrence of certain events. Should new information come in on (for example) a threat that has been classified as present, the network can be updated with this information to accurately represent the new values of each node, including the new value of mitigationplanset2.

Table F.1: Conditional Probability Table of Threat2/3

	Threat 2/3															
SouceT	External								Internal							
AccessT	Remote				Local				Remote				Local			
SkillT	un	ut	sn	st	un	ut	sn	st	un	ut	sn	st	un	ut	sn	st
Threat	1	0.8	0.6	0.3	0.5	0.4	0.3	0.15	0.8	0.64	0.48	0.24	0.4	0.32	0.24	0.12
NoThreat	0	0.2	0.4	0.7	0.5	0.6	0.7	0.85	0.2	0.36	0.52	0.76	0.6	0.68	0.76	0.88

Table F.2: Conditional Probability Table of CumThreat2

	CumThreat2							
Vulnerability2	Vulnerable				NotVulnerable			
Threat2	Threat		NoThreat		Threat		NoThreat	
Threat3	Threat	NoThreat	Threat	NoThreat	Threat	NoThreat	Threat	Nothreat
Lose20M	1	1	1	0	0	0	0	0
NotLose20M	0	0	0	1	1	1	1	1

Table F.3: Utility node of CumThreat2

Loss2		
CumThreat2	Lose20M	NotLose20M
Utility	-20	0

Table F.4: Conditional Probability Table of Vulnerability2

Vulnerability2		
Mitigationplanset1	yes	no
Vulnerable	0.02	0.12
NotVulnerable	0.98	0.88

APPENDIX G

SPARK OUTPUT: EXAMPLES

G.1 Phase 1: Output

This chapter gives some imaginative SPARK output for Troy Hospital's information systems. The data and representations are simplified and have a purely illustrative purpose.

The output of phase 1 consists of the classification of information systems on a Low (L) Medium (M), High (H) scale. Using the list of information systems from phase 0, combined with Table 5.1 and Table 5.2 , Table G.1 is formed.

Table G.1: SPARK classification of Troy Bank's information systems

System	Confidentiality	Integrity	Availability
High dependability (critical systems)			
1. Zeus	H	H	H
2. Cronus	H	H	H
3. Aphrodite	H	H	M
4. Athena	H	H	M
5. Apollo	H	H	L
Medium dependability (important systems)			
6. Artemis	M	M	H
7. Mermes	M	H	M
9. Persephone	M	M	H
10. Heracles	M	M	M
11. Rhea	M	H	M
12. Dionysus	L	H	M
Low dependability (supporting systems)			
13. Perseus	L	L	M
14. Minos	M	M	L
15. MarathonMail	L	M	L
16. EZchef	L	L	L

G.2 Phase 2: Output

This phase knows lists of vulnerabilities and threats as output. They are ranked on likelihood and impact of occurrence using a risk matrix as shown in Fig. G.1 .

Another product of this phase is an overview of the average risk per information system, per aspect. This is formed by adding up the risk indicators of a threat/vulnerability, per aspect, per information system and dividing this by the number of threats/vulnerabilities. Part of this is shown in Table G.3 and Fig. G.2 .

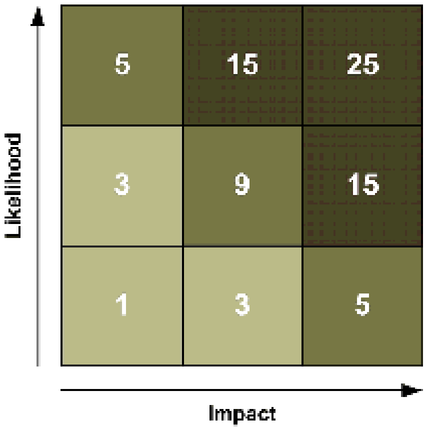


Figure G.1: SPARK: Risk as formed by impact and likelihood

Table G.2: SPARK: list of threats and vulnerabilities

Threats	Vulnerabilities
• User error • Confidentiality of information exchange • Integrity of information exchange • Unauthorized disclosure of information • System malfunction • Abuse of information (fraud) • Viruses • Access to network by unauthorized people • Integrity of information exchange • ...	• Segregation of duties mismanaged • Failing change management • Sharing of passwords • New and unknown employees (not screened) • Non-functional security zones • Usage of real patient data for testing purposes • Too much security or non-practical security • Not working compliant to Troy's laws • Not locking workstations • 'Laissez faire' culture • ...

G.3 Phase 3: Output

In phase 3, controls are mapped to threats and vulnerabilities for systems with a medium or high risk ranking. In SPARK this means a mapping to specific controls from ISO/IEC 17799-2005 and ISO/IEC 27001-2005 as shown in Table G.3 .

Table G.3: SPARK: System specific findings (5. Apollo)

5. Apollo					
Nr.	**Threat or Vulnerability**	**Impact**	**Likelihood**	**Risk**	**Control(s)**
C1	Unauthorized disclosure of information	H	H	25	None
C2	Abuse of information, fraud	H	L	5	None
C4	Segregation of duties mismanaged	H	H	25	Segregation of duties (10.1.3)
C6	Confidentiality of information exchange	H	H	25	Addressing security when dealing with customers (6.2.2), Information classification (7.2), Physical media in transit (10.8.3), Electronic messaging (10.8.4), Business information systems (10.8.5), Electronic commerce (10.9.1), User authentication for external communication (11.4.2), Network routing control (11.4.7)
I1	User error	H	M	15	Management responsibilities (8.2.1), Information security awareness, education and training (8.2.2), Documented operating procedures (10.1.1), Input data validation (12.2.1), Control of internal processing (12.2.2), Output data validation (12.2.4), Change control procedures (12.5.1)
I4	Integrity of information exchange	H	M	15	None
I7	Failing change management	H	M	15	Change management (10.1.2)
I11	Virus	H	L	5	Controls against malicious code (10.4.1), Controls against mobile code (10.4.2)
A1	Serious calamity	L	L	1	None
A2	Failing continuity controls	L	L	1	None
A4	System malfunction	L	M	3	Supporting utilities (9.2.2), Equipment maintenance (9.2.4), Security of equipment off-premises (9.2.5), Change management (10.1.2), Separation of development, test and operational facilities (10.1.4), System acceptance (10.3.2), Segregation in networks (11.4.5), Input data validation (12.2.1), Control of operational software (12.4.1)
A6	Theft of equipment	L	M	3	External parties (6.2), Terms and conditions of employment (8.1.3), Physical security perimeter (9.1.1), Physical entry controls (9.1.2), Securing offices, rooms, and facilities (9.1.3), Protecting against external and environmental threats (9.1.4), Unattended user equipment (11.3.2), Mobile computing and communications (11.7.1)
...	...	...	...	...	...

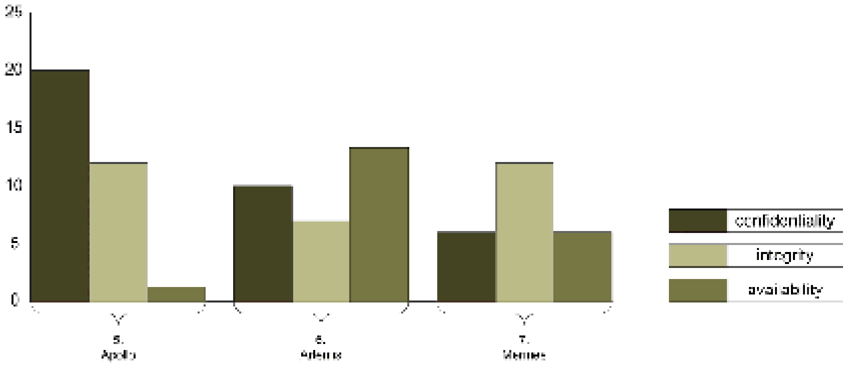


Figure G.2: SPARK: Risk per aspect per information system

APPENDIX H

Workflow Implementation

Introduction

The workflow of the implementation of the quantitative model is given form in this chapter using activity diagrams conform the UML 2.1.1 specification [37]. The UML specification has also been accepted as an ISO specification as ISO/IEC 19501. "Activity diagrams are flowchart-like notations with constructs to express sequence, choice and parallel execution of activities" [14].

The UML activity diagram is used for the workflow of implementing the quantitative addition to an existing methodology. A formal representation of the workflow is desirable for the possibility of model checking. Tools exist for the verification of performance properties and functional properties of workflow models. Since the activity diagrams in this chapter are a representation of a specific quantitative model, it is logical to assume that different situations ask for a somewhat different approach. This underlines the desirable property of model validation.

Processes are chains of activities to reach a certain goal. Our workflow implementation process is no different. The four activity diagrams represent the four steps of the Shewhart/Deming Cycle [13, 47]. This four stage iterative process improvement cycle knows the phases “Plan”, “Do”, “Act” and “Check”. These phases, although very general, can be found in a large amount of process and quality management theories (e.g. balanced scorecards (Kaizen) [27, 18], Six Sigma [40] and TQM [41]) [33].

Step 1: Plan

In this phase, the current situation is analysed for the availability of the necessary components for the computational method. The process is started with a check of the availability of a methodology flowchart. Based on this flowcharts checks are made on business processes, business applications, threats, vulnerabilities, information criteria, acceptable risk level and loss amount calculation. If the components are existent in the flowchart, it is assumed that the building blocks are present and the method can be implemented.

Step 2: Do

The implementation process of the computational method is started in this phase. The flowchart shows the steps that have to be taken to form a quantitative branch in the current methodology flowchart. This includes the definition of the variables in order to be able to do the calculations.

Step 3: Check

In this phase, the implementation steps are reviewed for suitability and usability. Checks are made on system components to identify points of improvement.

Step 4: Act

The points of improvement from the previous steps are incorporated in the model in this fourth step. The variables can be adjusted to improve the results of the model (e.g. enhance the predictive quality of the threat and vulnerability type indicators). After this step, the entire process is iterated, for continuous improvement.

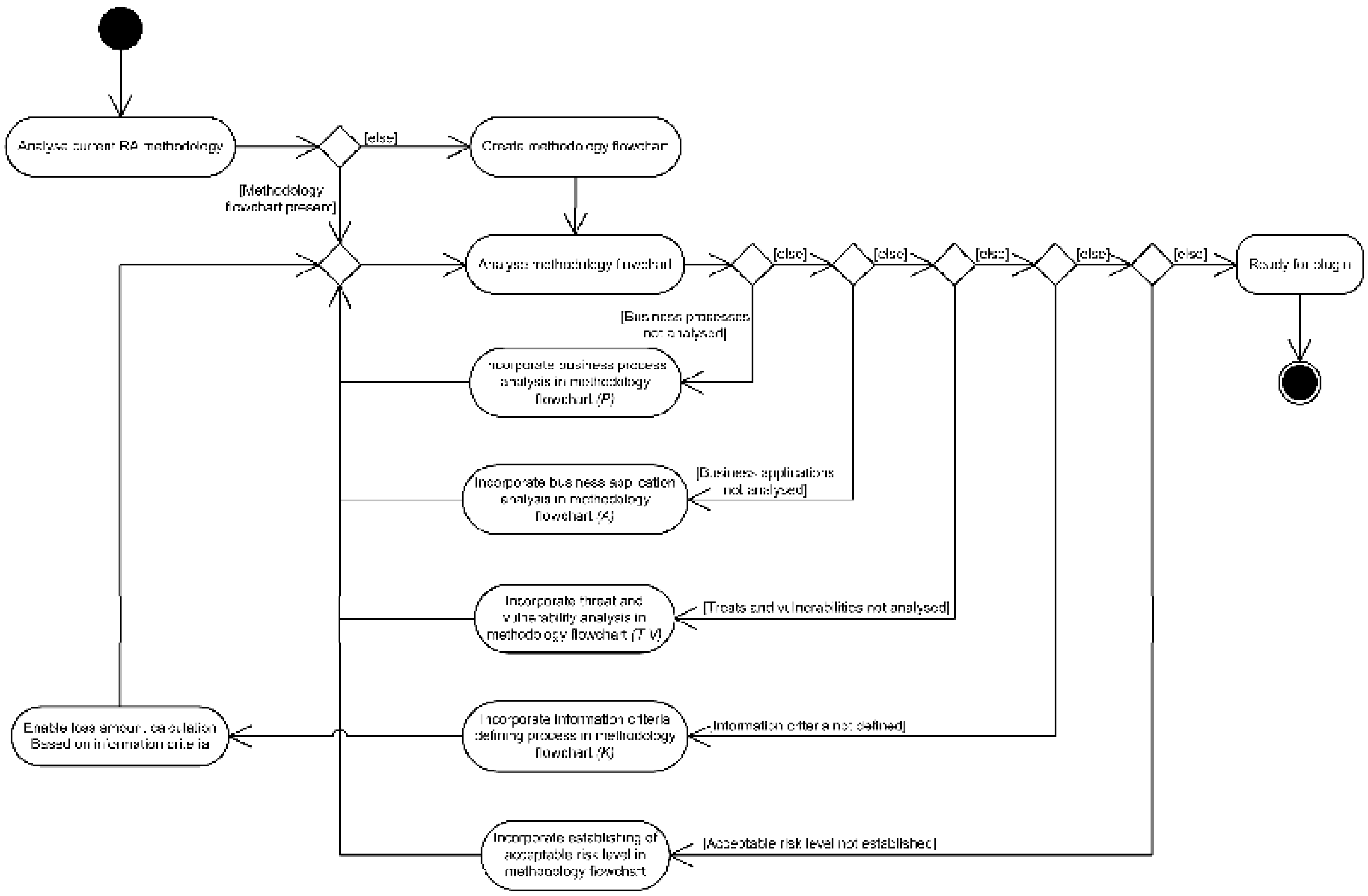

Analyse current RA methodology
[else]
Create methodology flowchart
[Methodology flowchart present]
Analyse methodology flowchart
[else]
[else]
[else]
[else]
[else]
Ready for plugin
[Business processes not analysed]
Incorporate business process analysis in methodology flowchart (P)
[Business applications not analysed]
Incorporate business application analysis in methodology flowchart (A)
[Treats and vulnerabilities not analysed]
Incorporate threat and vulnerability analysis in methodology flowchart (T,V)
[Information criteria not defined]
Incorporate Information criteria defining process in methodology flowchart (K)
Enable loss amount calculation Based on information criteria
[Acceptable risk level not established]
Incorporate establishing of acceptable risk level in methodology flowchart

Figure 11.1: Implementation workflow step 1: Plan

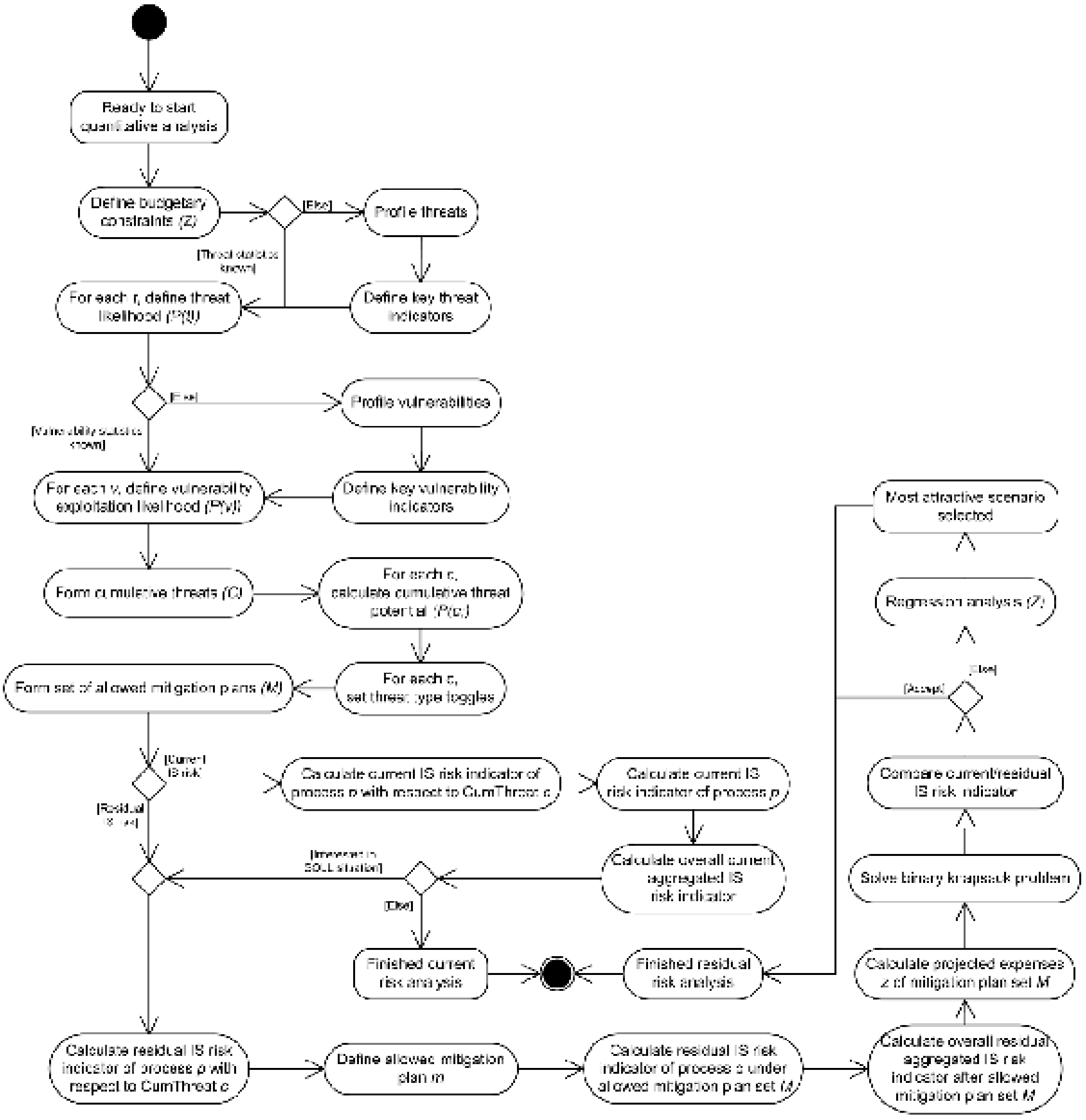

Ready to start quantitative analysis
Define budgetary constraints (Z)
[Else]
Profile threats
[Threat statistics known]
Define key threat indicators
For each r, define threat likelihood (P(t))
[Else]
Profile vulnerabilities
[Vulnerability statistics known]
Define key vulnerability indicators
For each v, define vulnerability exploitation likelihood (P(v))
Form cumulative threats (C)
For each c, calculate cumulative threat potential (P(c))
For each c, set threat type toggles
Form set of allowed mitigation plans (M)
[Current IS risk]
[Residual IS risk]
Calculate current IS risk indicator of process p with respect to CumThreat c
Calculate current IS risk indicator of process p
Calculate overall current aggregated IS risk indicator
[Interested in SOLL situation]
[Else]
Finished current risk analysis
Finished residual risk analysis
Calculate residual IS risk indicator of process p with respect to CumThreat c
Define allowed mitigation plan m
Calculate residual IS risk indicator of process p under allowed mitigation plan set M
Calculate overall residual aggregated IS risk indicator after allowed mitigation plan set M
Calculate projected expenses z of mitigation plan set M
Solve binary knapsack problem
Compare current/residual IS risk indicator
[Accept]
[Else]
Regression analysis (Z)
Most attractive scenario selected

Figure H.2: Implementation workflow step 2: Do

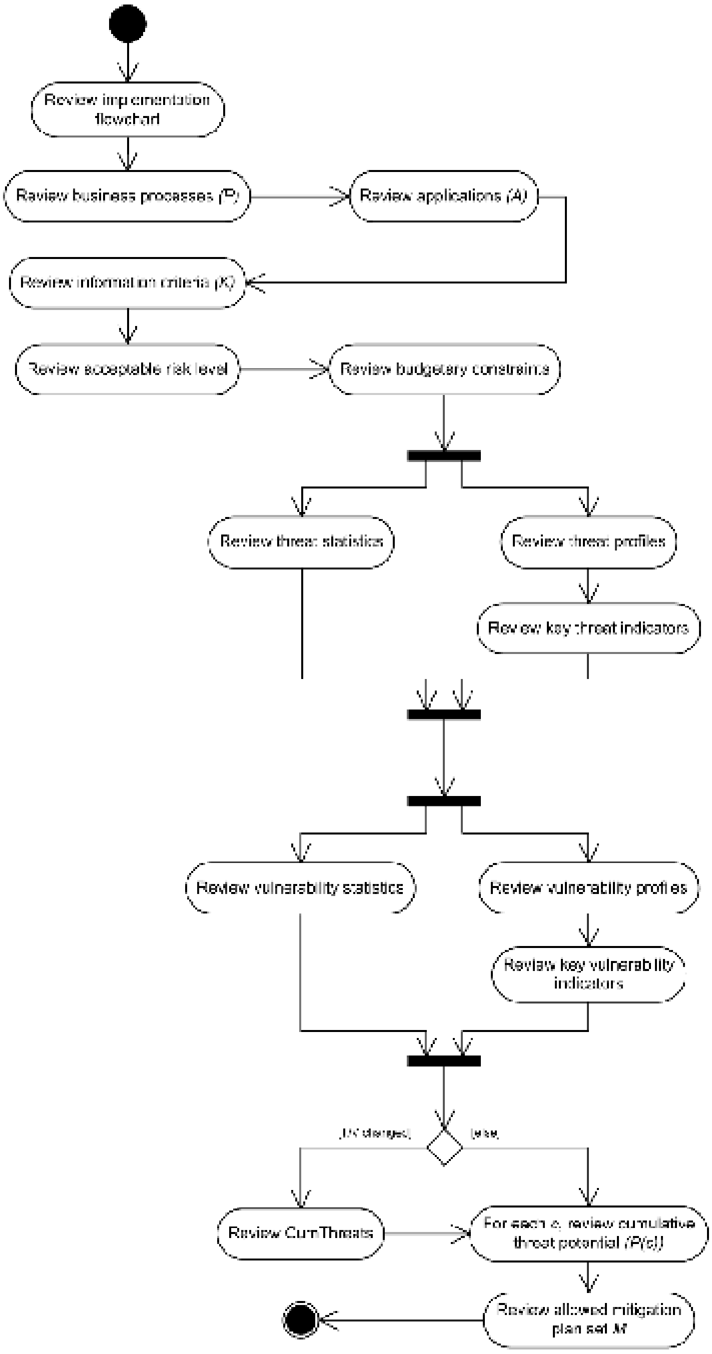

Review implementation flowchart
Review business processes (P)
Review applications (A)
Review information criteria (X)
Review acceptable risk level
Review budgetary constraints
Review threat statistics
Review threat profiles
Review key threat indicators
Review vulnerability statistics
Review vulnerability profiles
Review key vulnerability indicators
[X changed]
[else]
Review CumThreats
For each c, review cumulative threat potential (P(c))
Review allowed mitigation plan set M

Figure H.3: Implementation workflow step 2: Check

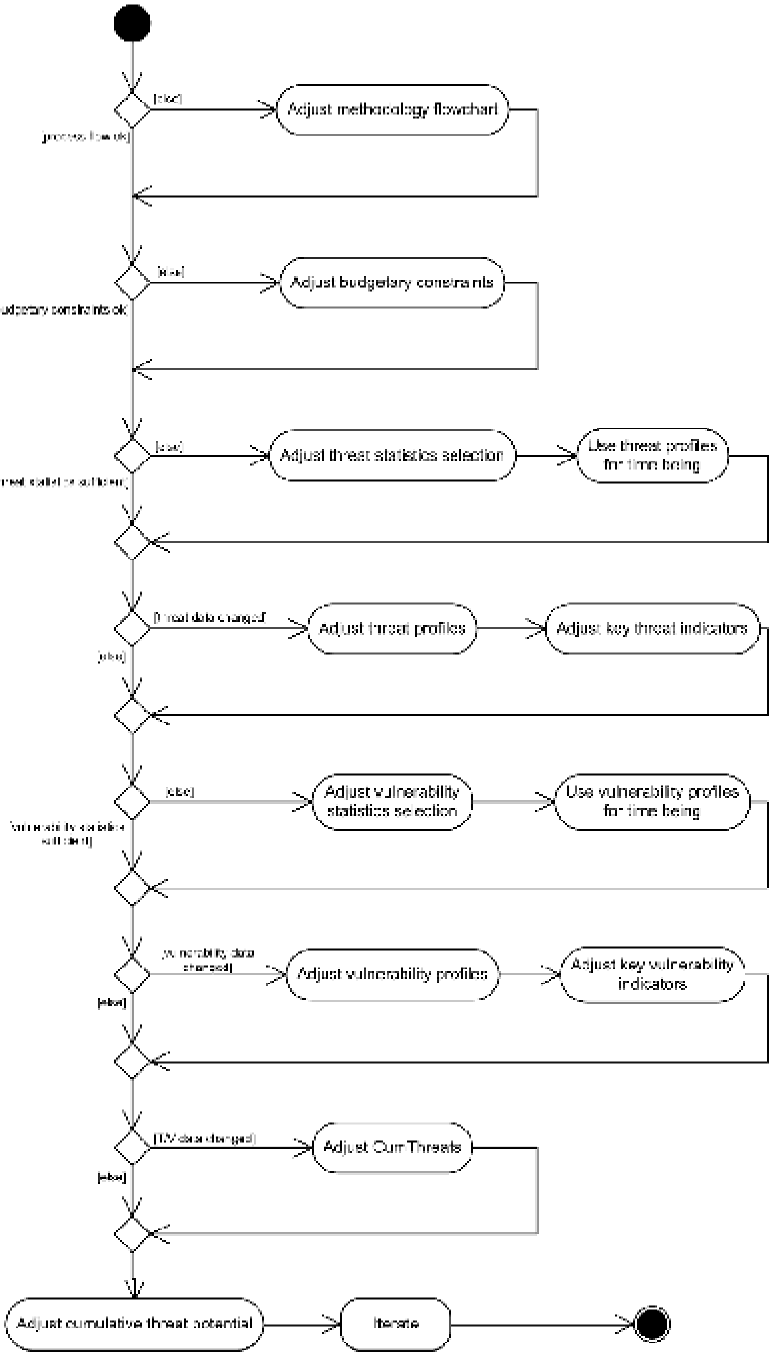

[else]
Adjust methodology flowchart
[process flow ok]
[else]
Adjust budgetary constraints
[budgetary constraints ok]
[else]
Adjust threat statistics selection
Use threat profiles for time being
[threat statistics sufficient]
[threat data changed]
Adjust threat profiles
Adjust key threat indicators
[else]
[else]
Adjust vulnerability statistics selection
Use vulnerability profiles for time being
[vulnerability statistics sufficient]
[vulnerability data changed]
Adjust vulnerability profiles
Adjust key vulnerability indicators
[else]
[T/V data changed]
Adjust Curr Threats
[else]
Adjust cumulative threat potential
Iterate

Figure H.4: Implementation workflow step 4: Act

BIBLIOGRAPHY

[1] 3-Angle Software & Services BV. Handleiding CRAMM 5.0, Nederlands Profiel, December 2003.

[2] C. Acosta and N. Siu. Dynamic event trees in accident sequence analysis: Application to steam generator tube rupture. *Reliability Engineering and System Safety*, 41:135–154, 1993.

[3] C. Alberts, A. Dorofee, J. Stevens, and C Woody. Introduction to the OCTAVE® approach. Technical report, Carnegie Mellon, Software Engineering Institute, August 2003.

[4] J.P. Balkenende. Besluit voorschrift informatiebeveiliging rijksdienst 2007. *Staatscourant*, 122, June 2007.

[5] W.G. Bornman and L. Labuschagne. A comparative framework for evaluating information security risk management methods. Technical report, Standard Bank Academy for Information Technology, Rand Afrikaans University, April 1994.

[6] F. den Braber, T. Dimitrakos, B.A. Gran, M.S. Lund, K. Stølen, and J.Ø. Aagedal. *The CORAS methodology: model-based risk management using UML and UP*, pages 332–357. IRM Press, 2003.

[7] BSI. *BS ISO/IEC 17799:2005 BS 7799-2005, Information Technology - Security Techniques - Code of Practice for Information Security Management.* BSI British Standards, 2005.

[8] J.M. Carroll. *Computer Security.* Butterworth-Heinemann, April 1996. ISBN 0750696001.

[9] P. Clarke and S. Young. Reliability-centered maintenance and HAZOP, is there a need for both? The Asset Partnership Pty Ltd., 2006.

[10] P.L. Clemens. Cause-consequence analysis. JACOBS presentation, February 2002.

[11] F.L. Crespo, M.A.A. Gómez, J. Candau, and J.S. Mañas. MAGERIT, Methodology for Information Systems Risk Analysis and Management, Book I, The Method. Ministerio de Administraciones Públicas, June 2006.

[12] T. Davenport. *Process Innovation: Reengineering work through Information Technology.* Harvard Business School Press, November 1992. ISBN 0875843662.

[13] W.E. Deming. *Out of the Crisis.* MIT Press, February 1982. ISBN 0911379010.

[14] R. Eshuis and R. Wieringa. Tool support for verifying UML activity diagrams. *IEEE Transactions on Software Engineering*, 20(7), July 2004.

[15] R.E. Freeman and J. McVea. A stakeholder approach to strategic management. Technical report, Darden Graduate School of Business Administration, 2001.

[16] R. Frei, J. Kingston, F. Koornneef, and P. Schallier. *MORT User's Manual: for use with the Management Oversight and Risk Tree Analytical Logic Diagram.* The Noordwijk Risk Initiative Foundation, 2002. ISBN 90-77284-01-X.

[17] P. Herzog. *OSSTMM 2.2.* ISECOM, December 2006.

[18] M. Imai. *Kaizen: The Key To Japan's Competitive Success.* McGraw-Hill/Irwin, November 1986. ISBN 0075543329.

[19] Information Security Forum. Fundamental information risk management: Implementation guide, March 2000.

[20] Information Security Forum. Fundamental information risk management: Supporting material, March 2000.

[21] Information Security Forum. Iram: Understanding and using the isf's information risk management tools, October 2003.

[22] Information Security Forum. Business impact assessment, June 2004.

[23] Istituto Superiore delle Comunicazioni e delle Tecnologie dell' Informazione. *Risk Analysis Approfondimenti.* Ministero delle Comunicazioni, September 2006.

[24] W.G. Johnson. *The Management Oversight and Risk Tree - MORT: Including Systems Developed by the Idaho Operations Office and Aerojet Nuclear Company.* United States Atomic Energy Commission, February 1973.

[25] Joint Technical Committee OB-007. *Risk management, AS/NZS 4360:2004, Third edition.* Standards Australia/Standards New Zealand, 2004. ISBN 0-7337-5904-1.

[26] J.P. Jouas and J.L. Roule. *MEHARI 2007, Overview.* Club de la Sécurité de l'Information Français (CLUSIF), 2007.

[27] R. Kaplan and D. Norton. The balanced scorecard: Measures that drive performance. *Harvard Business Review,* January 1992.

[28] P.K. Ketrick. Business transformation agency leverages dod acquisition decision making, testing the enterprise risk assessment model. *Defense AT&L,* September-October 2006.

[29] KPMG EDP Auditors N.V. SPARK: Risicoanalyse. Technical report, KPMG ITA, 2007.

[30] KPMG ITA. ITRMB talkbook. Tool introduction presentation, 2006.

[31] C.E. Landwehr. *Computer Security.* Springer-Verlag, July 2001.

[32] A. Leccadito, S.O. Lozza, and E. Russo. Portfolio selection and risk management with markov chains. *International Journal of Computer Science and Network Security,* 7(6):116–123, June 2007.

[33] S. Macey. An integrated model for performance management based on ISO 9000 and business excellence models. Master's thesis, Dalhousie University, Halifax, Nova Scotia, August 2001.

[34] S. Malik. *Network Security Principles and Practices (CCIE Professional Development).* Cisco Press, November 2002. ISBN 1587050250.

[35] J. Marnewick. In praise of FIRM: The measure of a good methodology. Presentation, November 2003.

[36] netSurity. iQSM, Total Risk Management. iQSM Datasheet, 2007.

[37] OMG. Unified modeling language: Superstructure. Technical report, Object Management Group, Inc., 2007.

[38] P. Overbeek, R. Joosten, A. Jochem, R. Kuiper, A. Moens, J. Popping, P. Ruijgrok, and J. Voeten. Return on security investment (rosi): Hoe te komen tot een bedrijfseconomische onderbouwing van uitgaven op het gebied van informatiebeveiliging?, 2006.

[39] Premier Ministre, Secrétariat général de la défense nationale, Direction centrale de la sécurité des systèmes d'information, Sous-direction des opérations, Bureau conseil. *EBIOS®, Section 1, Introduction.* DCSSI Advisory Office (SCDN / DCSSI / SDO / BCS) in collaboration with the EBIOS Club, February 2004.

[40] T. Pyzdek. *The Six Sigma Handbook: The Complete Guide for Greenbelts, Blackbelts, and Managers at All Levels.* McGraw-Hill, March 2003. ISBN 0071410155.

[41] H.K. Rampersad. *Total Quality Management: een strategie voor voortdurende verbetering.* Kluwer, 2000. ISBN 9026731280.

[42] Random House Webster. *Unabridged Dictionary.* Random House Reference, September 2001. ISBN 0375425667.

[43] E.P. Rutkens, H. Bouthoorn, and L.P.F. Tushuizen. Risicoanalyse gemakkelijk gemaakt. *Compact,* 1, 2004.

[44] P. Saitta, B. Larcom, and M. Eddington. Trike v.1 methodology document. Working Paper, July 2005.

[45] W.R. Scott. *Institutions and Organizations*. Sage Publications, Inc., 2001. ISBN 0761920013.

[46] W.G. Shenkier and P.L. Walker. Implementing enterprise risk management. Technical report, Institute of Management Accountants, 2006.

[47] W.A. Shewhart. *Statistical Method for the Viewpoint of Quality Control*. Dover Publications, December 1986. ISBN 0486652327.

[48] N. Siu. Risk assessment for dynamic systems : An overview. *Reliability Engineering and System Safety*, 43:43–73, 1994.

[49] M. Spruit. Waardevol maakt kwetsbaar, het belang van informatiebeveiliging. Oration, De Haagse Hogeschool, December 2003.

[50] M. Stamatelatos. *Probabilistic Risk Assessment: What is it and why is it worth performing it?* NASA Office of Safety and Mission Assurance, May 2000.

[51] G. Stoneburner, A. Goguen, and A. Feringa. Risk management guide for information technology systems. Special publication 800-30, National Institute of Standards and Technology, 2002.

[52] J. Suokas and V. Rouhiainen. *Quality Management of Safety and Risk Analysis*. Elsevier Science Publishers B.V., 1993.

[53] The European Security Forum. Simple to apply risk analysis for information systems, May 1993.

[54] The European Security Forum. Sprint, risk analysis for information systems - user guide, January 1997.

[55] The Financial Services Authority. *The FSA's Risk-Assessment Framework*. FSA, August 2006.

[56] The Institute of Risk Management. A risk management standard. Technical report, AIRMIC, ALARM, IRM, 2002.

[57] The International Organization for Standardization and The International Electrotechnical Commission. ISO/IEC Guide 73:2002, risk management - vocabulary - guidelines for use in standards. Technical report, ISO/IEC, 2002.

[58] The International Organization for Standardization and The International Electrotechnical Commission. International standard ISO/IEC 27001, information technology - security techniques - information security management systems - requirements. Technical report, ISO/IEC, 2005.

[59] The International Organization for Standardization and The International Electrotechnical Commission. ISO/IEC TR 13335-1, information technology - concepts and models for it security. Technical report, ISO/IEC, 1996.

[60] The Security Officers Management and Analysis Project. *The SOMAP.org Open Information Security Risk Management Handbook*. SOMAP.org, June 2006.

[61] J.K. Tudor. *Information Security Architecture, An Integrated Approach to Security in the Organization*. Auerbach Publishers Inc., September 2000. ISBN 0849399882.

[62] W.E. Vesely, F.F. Goldverg, N.H. Roberts, and D.F. Haasl. *Fault Tree Handbook*. United States Nuclear Regulatory Commission, January 1981.

[63] R.J.J. Wieringa. *Design methods for reactive systems. Yourdon, Statemate and the UML*. Elsevier Science & Technology Books, January 2002. ISBN 1558607552.

[64] J.A. Zachman. Enterprise architecture: The issie of the century. *Database Programming and Design Magazine*, March 1997.

Glossary

A

A en K Analyse 90

Afhankelijkheid en Kwetsbaarheid Analyse (Dependability and Vulnerability Analysis)

AITTTMS 89

Amenaza IT Threat Tree Modeling System, a risk assessment methodology

ALE 24

Annual Loss Expectancy.

ARiES 89

Aerospace Risk Evaluation System, a risk assessment methodology

ARO 27

Annual Rate of Occurrence.

ARROW 97

Advanced, Risk-Responsive Operating FrameWork

Arthur Andersen 14

One of the 'Big Five' accounting firms.

AS/NZS 4360:2004 13

Australian/New Zealand standard on Risk Management, Risk Management Framework.

Asset 23

Anything of value to the organisation.

Authenticity 20

Validity, conformance and genuineness of information.

Availability 18

Usability of information for a purpose.

B

BIA 90

Business Impact Assessment

Business Process 77

A structured set of activities designed to produce a specified output for a particular customer or market.

C

CCA 90

Cause-Consequence Analysis

CCTA 91

Central Computer and Telecommunications Agency

CEO 17

Chief Executive Officer

CIA Triad 16
Confidentiality, Integrity, Availability. See Fig. 3.4 .

CIO 17
Chief Information Officer.

CISO 95
Chief Information Security Officer

CobiT 15
Control Objectives for Information and related Technology. A Risk Assessment Framework.

COBRA 89
Consultative Objective & Bi-functional Risk Analysis, a risk assessment methodology

Concerns 76
Considerations about a system. Usually entail aspects like confidentiality, integrity and availability.

Confidentiality 17
Limited observation and disclosure of knowledge.

Control 78
See: Countermeasure.

CORAS 91
A Platform for Risk Analysis of Security Critical Systems

COSO 13
Risk Management Framework from The Committee of Sponsoring Organizations of the Treadway Commission

Countermeasure 78
Means of managing risk, including policies, procedures, guidelines, practices or organisational structures, which can be of administrative, technical, management, or legal nature.

CRAMM 91
CCTA Risk Analysis and Management Method

D

DAGs 37
Directed Acyclic Graphs. For example, a Bayesian network)

Data Integrity 18
The need to retain or preserve the information from source to destination.

DELAM 91
Dynamic Event Logic Analytical Methodology

Deloitte Touche Tohmatsu 14
One of the 'Big Four' accounting firms.

DETAM 91
Dynamic Event Tree Analysis Method

DFM 93
Double Failure Matrix

DoD 92
Department of Defense

DoDD 92
Department of Defense Directive

DREAD 92
Damage Potential, Reproducibility, Exploitablity, Affected Users, Discoverability

E

EBIOS 92
Expression des Besoins des Objectifs de Sécurité

Enron Corporation 14
An American energy company that went bankrupt in late 2001.

Enterprise (Security) Architecture 76
Helps to create an understanding what threats there are to information assets are and how to allocate resources to combat these threats.

ERAM 92
Enterprise Risk Assessment Methodology

ERM 2
Enterprise Risk Management.

Ernst and Young 14
One of the 'Big Four' accounting firms.

ETA 93
Event Tree Analysis

F

FHA 93
Fault Hazard Analysis

FIPS 27
Federal Information Processing Standard.

FIRM 93
Fundamental Information Risk Management developed by the ISF

FMEA 93
Failure Model and Effect Analysis

FMECA 93
Failure Mode Effect and Criticality Analysis

FSA 97
Financial Services Authority

FTA 93
Fault Tree Analysis

H

HAZOP 94
Hazard and Operability Studies

I

Information assurance 13
The practice of managing information-related.

Integrity 18
Completeness, wholeness and readability of information and quality of being unchanged form a previous state.

IRAM 94
Information Security Analysis Methodologies

IRR 29
Internal Rate of Return.

IS 66
Information Security

ISF 93
Information Security Forum, formerly known as European Security Forum. Independent authority on information security.

ISMS 91
Information Security Management System

ISO/IEC 15408:2005 15
Information technology; Security techniques and Evaluation criteria for IT security. A Risk Assessment Framework.

ISO/IEC 27001:2005 15
The Information Security Management System (ISMS) requirements standard specification, against which organisations are formally certified compliant. A Risk Assessment Framework.

ITA 2
KPMG IT Advisory department.

ITIL 15
Information Technology Infrastructure Library. A Risk Assessment Framework.

ITRMB 94
Information Technology Risk Management Benchmark

K

King II Report 98
The King Report on Corporate Governance for South Africa assumes risk management as an integral part of corporate governance

KPMG 14
One of the 'Big Four' accounting firms.

M

MAGERIT 95
Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información

Management Of Risk 13
Also known as M_O_R, Risk Management Framework from the OGC.

MARION 89
Méthodologie d'Analyse des Risques Informatiques et d'Optimisation par Niveau

Markov 95
A probability method

MEHARI 95
Méthode Harmonisée d'analyse des risques

Mitigation Plan 78
A plan that describes controls or countermeasures to influence an organisation's vulnerabilities and thus risk exposure.

MORT 95
Management Oversight Risk Tree

N

NIST 99
National Institute for Standards and Technology

NORA 96
Network Oriented Risk Analysis Methodology

NP-hard 54
Non-deterministic polynomial-time hard. A class of problems as least as hard as the hardest problems in NP

NPV 29
Net Present Value.

O

OCTAVE 96
Operationally Critical Threat, Asset and Vulnerability Evaluation

OCTAVE-S 96
Operationally Critical Threat, Asset and Vulnerability Evaluation for Smaller organisations

OGC 13
Office of Government Commerce, known for their ITIL, PRINCE2, M O R and MSP products.

Organisation 76
A distinctive type of social form in which professionals share in the determination of goals and standards.

OSSTMM 96
Open Source Security Testing Methodology Manual

OSSTMM-RAV 97
Open Source Security Testing Methodology Manual - Risk Assessment Values

P

Parkerian Hexad 19
An alternative to the CIA model developed by Donn B. Parker.

PHA 93
Preliminary Hazard Analysis

Possession 19
Holding, controlling and having the ability to use information.

PricewaterhouseCoopers 14
One of the 'Big Four' accounting firms.

PV 29
Present Value.

Q

QSM Security Expert 97
Quality Security Management - Security Expert

R

RAF 97
Risk Assessment Framework

Risk 78
The potential that a given threat will exploit a vulnerability exposing assets to harm.

ROI 28
Return On Investment.

ROISI 98
Return On Information Security Investments

ROSI 97
Return On Security Investments

S

Safeguard 23
A practice, procedure or mechanism that reduces risk.

SARA 98
Simple to Apply Risk Analysis for information systems developed by the ISF

Security Principles 76
Fundamental, primary, or general law or truth concerning security, from which others are derived.

Skimming 20
Obtaining bank- and/or credit card information in an illegal way.

SLE 27
Single Loss Expectancy.

SME 105
Small or Medium sized Enterprise

SMORT 98
Safety Management Organisation Review Technique

SOMAP 99
Security Officers Management and Analysis Project

Source Integrity 18
The verification process that is involved in ensuring that the data comes from the correct source rather than from an imposter.

SOX 2
Sarbanes-Oxley Act of 2002. Specifically, section 404 defines guidelines for the management of the assessment of internal controls [127].

SP800-30 99
Risk Management Guide for Information Technology Systems supported by NIST

SPARK 99
Simplified Process for Analyzing Risk by KPMG

SPRINT 99
Simplified Process for Risk Identification developed by the ISF

Stakeholders 76
Any group or individual who is affected by or can affect the achievement of an organisation's objectives.

STIR 89
Simple Technique for Illustrating Risk, a risk assessment methodology

STRIDE 100
Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, Elevation of privilege

T

The 'Big Five' 14
Arthur Andersen, Ernst & Young, Deloitte Touche Tohmatsu, KPMG, PricewaterhouseCoopers.

The 'Big Four' 14
Ernst & Young, Deloitte Touche Tohmatsu, KPMG, PricewaterhouseCoopers.

Threat 77

A potential cause of an unwanted incident or event which may result in harm to a system or organisation.

Threat Agent 77

A person or phenomenon that can make a threat manifest.

Threat likelihood 27

The probability that a threat, once present, successfully manifests itself.

TRIKE 100

A Conceptual Framework for Threat Modelling

Turnbull Report 98

Report assuming that the company's board uses a risk-based approach to internal control

U

UML 91

Unified Modeling Language

Utility 20

Usefulness of information for a purpose.

V

Value at Risk 31

Quantifies the maximal amount that may be lost in a portfolio over a given period of time, at a certain confidence level.

VaR 31

See: Value at Risk.

Vulnerability 78

A weakness of an asset or group of assets, which can be exploited by a threat. If risk is viewed as a positive scenario, 'vulnerability' can be replaced with 'opportunity'.