predict
prioritise
prevent

TRESPASS

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

Deliverable 5.2.1

Currently established risk-assessment methods

Project:	TRE$_S$PASS
Project Number:	ICT-318003
Deliverable:	D5.2.1
Title:	Currently established risk-assessment methods
Version:	1.0
Confidentiality:	Public
Editor:	Ben Fetler, itrust consulting
Cont. Authors:	Carlo Harpes, Guillaume Schaff, Miguel Martins, Barbara Kordy, Rolando Trujillo, Dan Ionita
Date:	2014-10-31

Part of the Seventh Framework Programme
Funded by the EC-DG CONNECT

Members of the TRESPASS Consortium

1.	University of Twente	UT	The Netherlands
2.	Technical University of Denmark	DTU	Denmark
3.	Cybernetica	CYB	Estonia
4.	GMV Portugal	GMVP	Portugal
5.	GMV Spain	GMVS	Spain
6.	Royal Holloway University of London	RHUL	United Kingdom
7.	itrust consulting	ITR	Luxembourg
8.	Goethe University Frankfurt	GUF	Germany
9.	IBM Research	IBM	Switzerland
10.	Delft University of Technology	TUD	The Netherlands
11.	Hamburg University of Technology	TUHH	Germany
12.	University of Luxembourg	UL	Luxembourg
13.	Aalborg University	AAU	Denmark
14.	Consult Hyperion	CHYP	United Kingdom
15.	BizzDesign	BD	The Netherlands
16.	Deloitte	DELO	The Netherlands
17.	Lust	LUST	The Netherlands

Document History

Authors		
Partner	Name	Chapters
UT	Dan Ionita	1, 2, 3, Appendices
ITR	Carlo Harpes	2
ITR	Guillaume Schaff	2
ITR	Miguel Martins	Appendices
UL	Barbara Kordy	2
UL	Rolando Trujillo Rasua	2,3

Quality assurance		
Role	Name	Date
Editor	Ben Fetler, ITR	2014-03-13
Reviewer	Fatima Reis	2014-10-02
Reviewer	Trajce Dimkov	2014-10-14
WP leader	Jan Willemson	2014-10-31
Coordinator	Pieter Hartel	2014-10-31

Circulation	
Recipient	Date of submission
Project Partners	2014-06-02
European Commission	2014-10-31

***Acknowledgement**: The research leading to these results has received funding from the European Union Seventh Framework Programme (FP7/2007-2013) under grant agreement no. 318003 (TRESPASS). This publication reflects only the author's views and the Union is not liable for any use that may be made of the information contained herein.*

Contents

List of Figures

List of Tables

List of Acronyms

COBIT Control Objectives for Information and Related Technology

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

EBIOS Expression des Besoins et Identification des Objectifs de Sécurité

FAIR Factor Analysis of Information Risk

FRAP Facilitator-led Risk Assessment Process

MEHARI Methode Harmonisee d'Analyse de Risques

MSAT Microsoft Security Assessment Tool

MTM Microsoft Threat Model

IEC International Electrotechnical Commission

ISMS Information Security Management System

IS Information System

ISO International Standards Organization

OCTAVE Operationally Critical Threat, Asset, and Vulnerability Evaluation

OWASP Open Web Application Security Project

RA Risk Assessment

RM Risk Management

ROSI Return On Security Investment

SME Small or Medium Enterprise

TARA Threat Agent Risk Assessment

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

SRA Structured Risk Analysis

Management Summary

Key takeaways

- Information security standards and methodologies are reviewed based on a standardised template to allow for quick understanding and easy comparison based on several key aspects;
- For each methodology, the available software tools are briefly described. Third-party tools used by practitioners but unrelated to a particular methodology are described separately;
- Conceptual and procedural patterns are identified are identified across the reviewed methodologies;
- The TRE$_S$PASS approach is compared to the established methods and tools, both conceptually and procedurally.

In order to build upon existing knowledge, and advance the state-of-the-art, it is crucial that we first conduct a structured survey of the frameworks, standards, methodologies and tools that are currently used in practice. This is exactly what this Deliverable sets out to achieve: an in-depth review of current standardised Risk Assessment methodologies.

Relevant international Information Security standards are listed and described. However, the core of the document consists of descriptions of Risk Assessment methodologies, as well as any related tools. Owners, countries of origin, target organisations are also discussed for each individual method.

The document then attempts to map and compare the TRE$_S$PASS approach to Risk Assessment with that of established methodologies.

This is done firstly at a conceptual level, by distilling an *integrated conceptual model of Risk* — essentially an overview of the common concepts used by various methodologies to describe or discuss Risk — and then comparing this model with TRE$_S$PASS's own WP1 model — a modelling language used within the project to represent the targets of assessment and relevant elements. Secondly, the expected TRE$_S$PASS work-flow is compared to established methods for conducting Risk Assessment.

Conclusions are drawn with regard to the conceptual and methodological differences and similarities observed and indications are given as to how and why these set the TRE$_S$PASS approach apart from existing Risk Assessment techniques.

Namely, TRE$_S$PASS aims at obtaining a physical, digital, technical and social model of the organisation and then using pre-built, crowd-sourced knowledge on vulnerabilities, attack vectors and threat agents to semi-automatically output a ranked list of Risks that the

organisations if facing. Most established methodologies on the other hand, usually require some sort of manual or informal way of identifying and evaluating potentially unwanted events based on experience and/or vulnerability catalogues.

1 Introduction

1.1 TRESPASS

The TRESPASS project aims to develop a widely applicable and standardised security framework that enables risk assessment, attack models creation, and advice on countermeasures allowing organisations and their customers to make informed decisions about security investments and consequently reduce security incidents or the organisational impact of such, e.g., monetary loss or damage of brand reputation. This increases resilience of European businesses both large and small and is vital to safeguarding the social and economic prospects of Europe.

TRESPASS 's primary goals are complementary to the goals with respect to executing our research and development agenda to influence the risk management domain in multiple ways. On the one hand, we intend to get substantial visibility and influence in the academic research community based on our research results, on the other hand we want to get our results adopted in the organisational risk management practice. Thereby TRESPASS intends to contribute throughout the value chain of the risk management ecosystem, that is, in the full spectrum ranging from academic research to practical tools and methodologies.

Overall, we want to be perceived as the project being a thought leader in the field of socio-technical risk management and help space move forward towards having more effective, yet efficient, approaches to handling socio-technical risks related to IT.

1.2 Objectives

There exist several standardised methodologies for risk assessment and attack models creation. However, the current standards do not support the full range of socio-technical aspects of heterogeneous systems. For example, ISO 15408 (The Common Criteria) is concerned with evaluating security of IT products and IEC 61025 concentrates only on fault trees, which is a subset of concepts required for full risk assessment. A general framework for information security risk management is given by ISO/IEC 27005 for information security and ISO 31000 and 31004 on general risk management, but this framework remains on a very abstract level and does not give sufficient guidelines for building socio-technical models.

Another approach in standardised risk assessment methodology is taken by baseline security, for example the German BSI. Following this approach, the system is broken down

into standard components and a list of known threats is considered for each of them. However, the workflow is mostly manual and the standard threat catalogues are very hard to keep up to date, hence preventing any kind of model lifecycle.

The third previous approach taken by the international research community is building visual tools to aid security modelling and risk assessment. The most prominent example of such an approach is CORAS that has produced both tools and methodologies for building practical security models. However, even CORAS does not support full socio-technical modelling and lacks integration with existing quantitative analysis methods.

Hence, the main task of this document is mapping the needs identified in WP1 to existing standardised methodologies and identifying the gaps that are uncovered. This will not only help position the TRE$_S$PASS project within the application domain, emphasising its unique selling points, but also highlight the areas where further research is needed in order to advance the state-of-the art.

1.3 Foreground and background

As this document attempts to present an overview of the state-of-the art, its content is intrinsically "background". However, Section 3.1 do provide foreground information by describing the latest version of the TRE$_S$PASS model and method, distilling an integrated conceptual model of Risk based on some the methodologies and frameworks described throughout the document and comparing the two. Section 3.2 also provides limited foreground information by mapping the expectations of the TRE$_S$PASS project to capabilities of existing tools.

2 Overview of risk assessment methods & tools

The following section provides a non-exhaustive list of existing risk management / assessment methods and associated tools.

As starting point, we considered tools designed by the TRE$_S$PASS partners. Then we expanded the list with the methods and tools listed on the inventory of risk management / assessment methods managed by the European Network and Information Security Agency (ENISA) (2013a). Finally, two recent master thesis written by TRE$_S$PASS researchers which survey the state-of-the-art (Fetler, 2012; Ionita, 2013) were integrated. This method does not define its own inclusion and exclusion criteria but rather relies on the criteria used by each author individually. This selection method promotes completeness rather than repeatability.

An inventory summarising the analysed risk management / assessment approaches can be found in Appendix A - Inventory of risk assessment methods.

Appendix B - Inventory of risk assessment tools includes the full list of risk assessment tools and Appendix C - Comparison of risk assessment tools contains a comparison of risk assessment tools based on specific functionalities.

Each of the following sub-sections will describe a risk management / assessment methodology using a fixed structure. Due to the large number of methods available and the fact that most of them are commercial made in-depth analysis impossible. Furthermore, reliable third-party information about usage of each method is not available so time-lines (when created, used, fallen in disuse), popularity and geographical spread are unfortunately not discussed. The including following aspects are described for each method:

Owner : Name of the organisation/ institution that developed and/ or distributes the methodology;

Country of origin : Country in which the methodology was established;

Targeted organisations : List of targeted types of organisations that the methodology is adapted for (example: Government, agencies, large companies, SMEs);

Method description : Brief description including key aspects of the methodology;

Tool(s) : Identification of tools that are based on the methodology. Where possible, a description of the tool is also included. Unfortunately, some (commercial) proprietary tools do not provide sufficient publicly available documentation.

Chapter 2 will close with a list of additional risk assessment tools that are not developed with the aim of supporting a specific methodology but may be compatible with several best practices or international standards.

2.1 Standards

2.1.1 ISO 31000:2009

Owner :

- International Organisation for Standardisation.

Country of origin :

- International (place of business in Switzerland).

Targeted organisations :

- Usable by any organisation regardless of its size, activity or sector.

Standard description (ISO, Geneva, Switzerland, 2009):

ISO 31000 - *Risk management - Principles and guidelines* provides a framework and a generic process to manage risk in all part of any type of organisation. ISO 31000 cannot be used for certification purposes, however it provides guidance for internal or external audit programmes.

In general ISO 31000 establishes eleven principles that need to be satisfied. ISO/TR 31004:2013 provides guidance on how to apply the principles. The eleven principles are (ISO, Geneva, Switzerland, 2013):

1. Risk management creates and protects value.
   Risk management contributes to the demonstrable achievement of objectives and improvement of performance in, for example, human health and safety, security, legal and regulatory compliance, public acceptance, environmental protection, product quality, project management, efficiency in operations, governance and reputation.
2. Risk management is an integral part of all organisational processes.
   Risk management is not a stand-alone activity that is separate from the main activities and processes of the organisation. Risk management is part of the responsibilities of management and an integral part of all organisational processes, including strategic planning and all project and change management processes.
3. Risk management is part of decision making.
   Risk management helps decision makers make informed choices, prioritise actions and distinguish among alternative courses of action.

4. Risk management explicitly addresses uncertainty.
   Risk management explicitly takes account of uncertainty, the nature of that uncertainty, and how it can be addressed.
5. Risk management is systematic, structured and timely.
   A systematic, timely and structured approach to risk management contributes to efficiency and to consistent, comparable and reliable results.
6. Risk management is based on the best available information.
   The inputs to the process of managing risk are based on information sources such as historical data, experience, stakeholder feedback, observation, forecasts and expert judgement. However, decision makers should inform themselves of, and should take into account, any limitations of the data or modelling used or the possibility of divergence among experts.
7. Risk management is tailored.
   Risk management is aligned with the organisation's external and internal context and risk profile.
8. Risk management takes human and cultural factors into account.
   Risk management recognises the capabilities, perceptions and intentions of external and internal people that can facilitate or hinder achievement of the organisation's objectives.
9. Risk management is transparent and inclusive.
   Appropriate and timely involvement of stakeholders and, in particular, decision makers at all levels of the organisation, ensures that risk management remains relevant and up-to-date. Involvement also allows stakeholders to be properly represented and to have their views taken into account in determining risk criteria.
10. Risk management is dynamic, iterative and responsive to change.
    Risk management continually senses and responds to change. As external and internal events occur, context and knowledge change, monitoring and review of risks take place, new risks emerge, some change, and others disappear.
11. Risk management facilitates continual improvement of the organisation.
    Organisations should develop and implement strategies to improve their risk management maturity alongside all other aspects of their organisation.

Some related standards which help to implement and integrate ISO 31000 in an organisation's environment are listed in the following paragraph.

Related standards:

- ISO/TR 31004 - *Guidance for the implementation of ISO 31000* is a technical report that is intended to assist organisations to integrate risk management into the organisation's management processes.

- ISO/IEC 31010 - *Risk management – Risk assessment techniques* focuses on risk assessment concepts, processes and the selection of risk assessment techniques.

2.1.2 ISO/IEC 27005:2011

Owner :

- International Organisation for Standardisation.

Country of origin :

- International (place of business in Switzerland).

Targeted organisations :

- Government, agencies;
- Large companies;
- SME.

Standard description (ISO, Geneva, Switzerland, 2011):

ISO/IEC 27005:2011 provides an iterative process for risk management which advances to be the framework for several methodologies in the domain of risk management.

The risk management process, proposed by the standard, includes context establishment, risk assessment, risk treatment, risk communication, consultation, monitoring and review (see process in Figure 2.1).

The context establishment includes:

- Setting basic criteria such as the risk management approach, the risk evaluation criteria, the impact criteria and the risk acceptance criteria;
- Defining the scope and boundaries of the risk management;
- Defining the organisation and the responsibilities for information security risk management.

The risk assessment consists of:

- The risk identification which has the aim to find possible sources of potential loss:
  - The assets within the defined scope;
  - The threats and their sources;
  - Existing and planned controls;

  - Vulnerabilities that can be abused by threats having a negative impact to assets or to the organisation;
  - The consequences that a loss of confidentiality, integrity and availability may have on the assets.
  - Business processes
- The risk analysis/estimation which includes:
  - The selection of the risk analysis methodology which can be qualitative (using a scale of qualifying attributes, e.g. Low, Medium and High), quantitative (using a scale with numerical values) or depending on the situation a mixture of both;
  - Assessment of consequences and more precisely the business impact of a security incident with loss of confidentiality, integrity or availability of the assets;
  - Assessment of incident likelihood by evaluating threats and vulnerabilities;
  - Determination of the risk level for all relevant incident scenarios.
- The risk evaluation has the aim to compare the level of risk against the risk evaluation criteria and the risk acceptance criteria (defined in the context establishment).

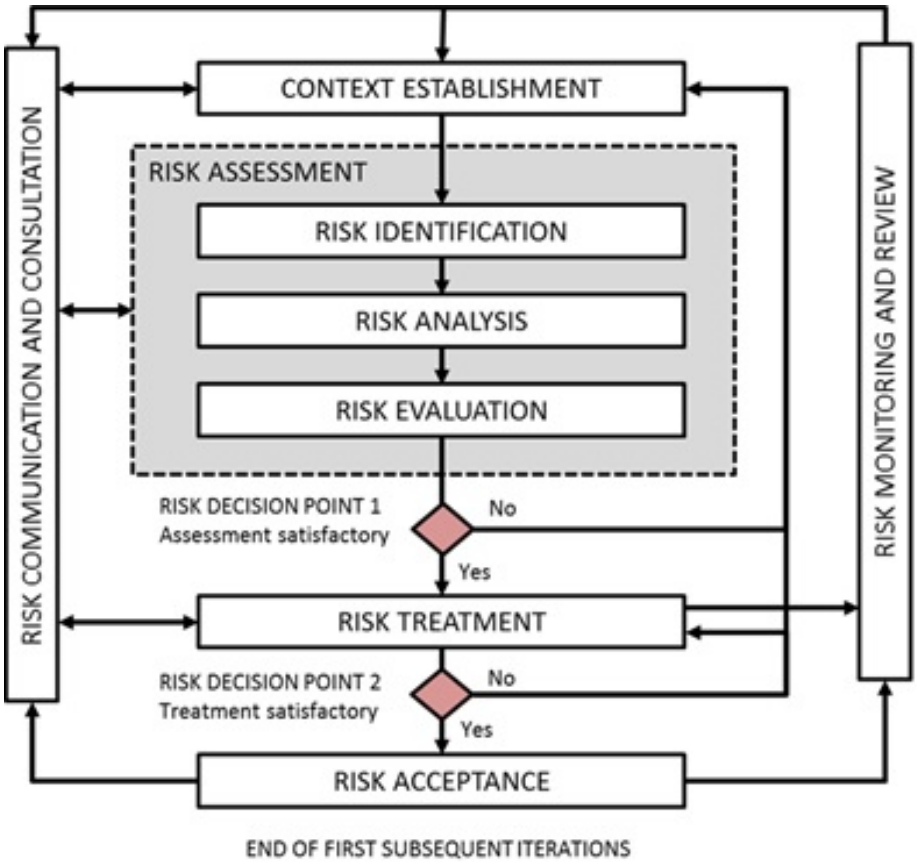

Figure 2.1: ISO/IEC 27005:2011 Information security risk management process

As shown in Figure 2.2, risk treatment will be done based on the results of the risk assessment. The risk treatment consists of four different options which should be selected by considering the outcome of the risk assessment, the expected cost for implementing these options and the expected benefits from these options. The different options are:

- Risk modification: Reducing risk by introducing, removing or altering appropriated security controls such that the residual risk becomes acceptable;
- Risk retention: Accepting the risk without further action;
- Risk avoidance: Abandon the activity or condition that represents the source of the risk;
- Risk sharing: Sharing the risk with another party that can handle the particular risk (e.g. insurance, subcontractors, etc.).

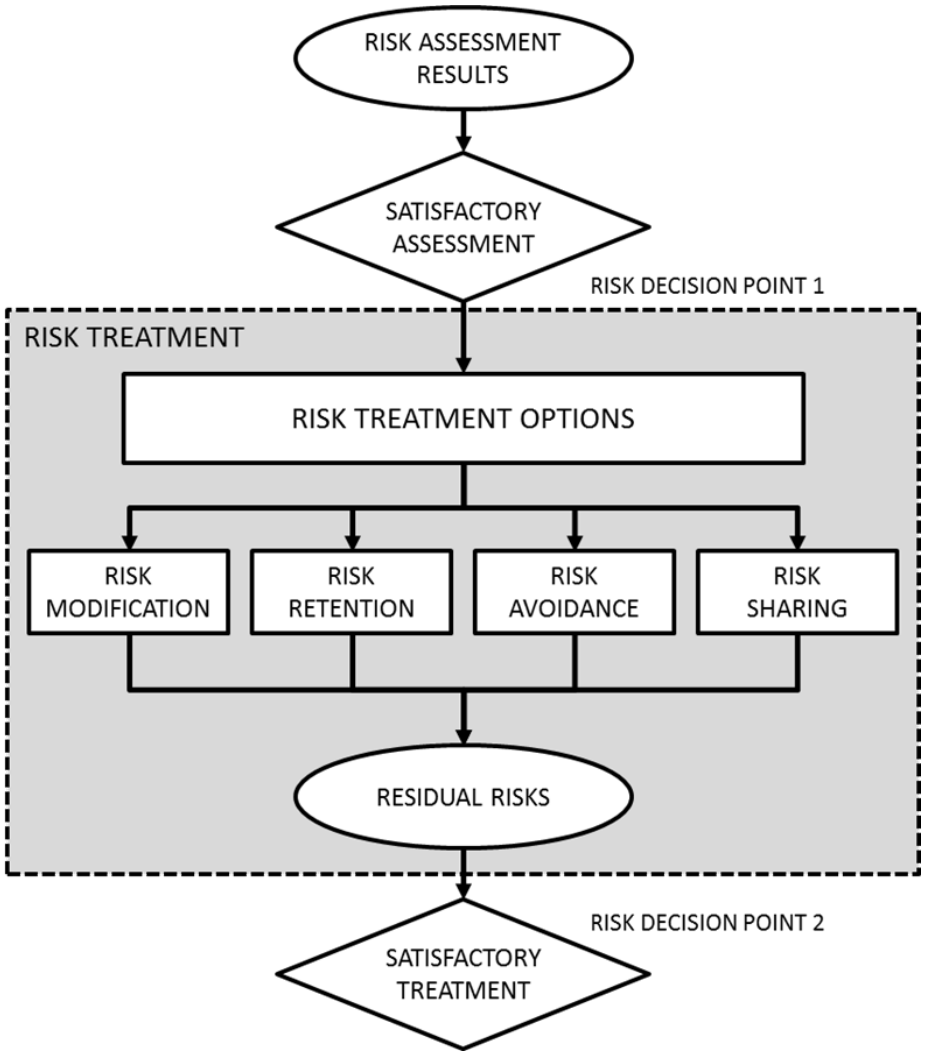

Figure 2.2: The risk treatment activity

After a satisfactory completion of the risk treatment, the residual risks have to be accepted by responsible managers. If accepted risks exceed the normal risk acceptance criteria there has to be a documented justification. The risk communication and consultation showed in the risk management process, represents the fact that information about the risks has to be shared between the decision-makers and other stakeholders. The communication of risks has to be done during the whole risk management process. Another important part of the risk management process is the Information security risk monitoring and review which consists in monitoring and reviewing the risks and their factors in order to identify changes and maintain an overview. This is important due to the fact that new threats, vulnerabilities or changes in likelihood or consequences can generate new risks or lead to a situation where an acceptable risk becomes unacceptable.

Tool(s) :

No tool

2.1.3 NIST Special Publication 800-39

Owner :

- National Institute for Standards and Technology (NIST).

Country of origin :

- USA.

Targeted organisations :

- Government, agencies;
- Large companies;
- SME.

Standard description (National Institute of Standards and Technology, 2011):

The NIST (National Institute for Standards and Technology) risk analysis document contains three chapters. The first one is an introductory chapter, the second chapter presents the fundamentals for risk management and the third chapter includes the risk management process.
The proposed risk management process consists of several steps which have inputs and preconditions, several activities with associated tasks and outputs with post-conditions.

1. Risk framing:
   a) Risk assumptions;
   b) Risk constraints;
   c) Risk tolerance;
   d) Priorities and Trade-offs.
2. Risk assessment:
   a) Threat and vulnerability identification;
   b) Risk determination.
3. Risk response:
   a) Risk response identification;
   b) Evaluation of alternatives;
   c) Risk response decision;
   d) Risk response implementation.

4. Risk monitoring:
    a) Risk monitoring strategy;
    b) Risk monitoring.

Tool(s) :

- MEHARI (described in Section 2.2.13
- Risicare (described in Section 2.2.13)

2.1.4 AS/NZS 4360 (superseded by AS/NZS ISO 3100:2009)

Owner :

- Standards Australia International and Standards New Zealand.

Country of origin :

- Australia/New Zealand.

Targeted organisations :

- Government, agencies;
- Large companies;
- SME.

Standard description :

The standard was introduced by Standards Australia International and Standards New Zealand in 1995, and revised in 2004. It has since been incorporated into the international standard AS/NZS ISO 3100:2009 - Principles and Guidelines.

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

The Australian/New Zealand Standard for Risk Management AS/NZS 4360:2004 provides a generic framework for the process of managing risks which divides the elements of the risk assessment process into several sub-processes: "Establish the context", "Identify Risks", "Analyse Risks", "Evaluate Risks" and "Treat Risks". The standard also describes two processes that should run in parallel with the risk assessment sessions as part of the Risk Management: "Monitoring and Review" and "Communicate and Consult". A flowchart describing this process can be found in Figure 2.3.

The standard also puts heavy emphasis on establishing the context - both external and internal. In 2009 it was integrated into the AS/NZS ISO 3100:2009 international

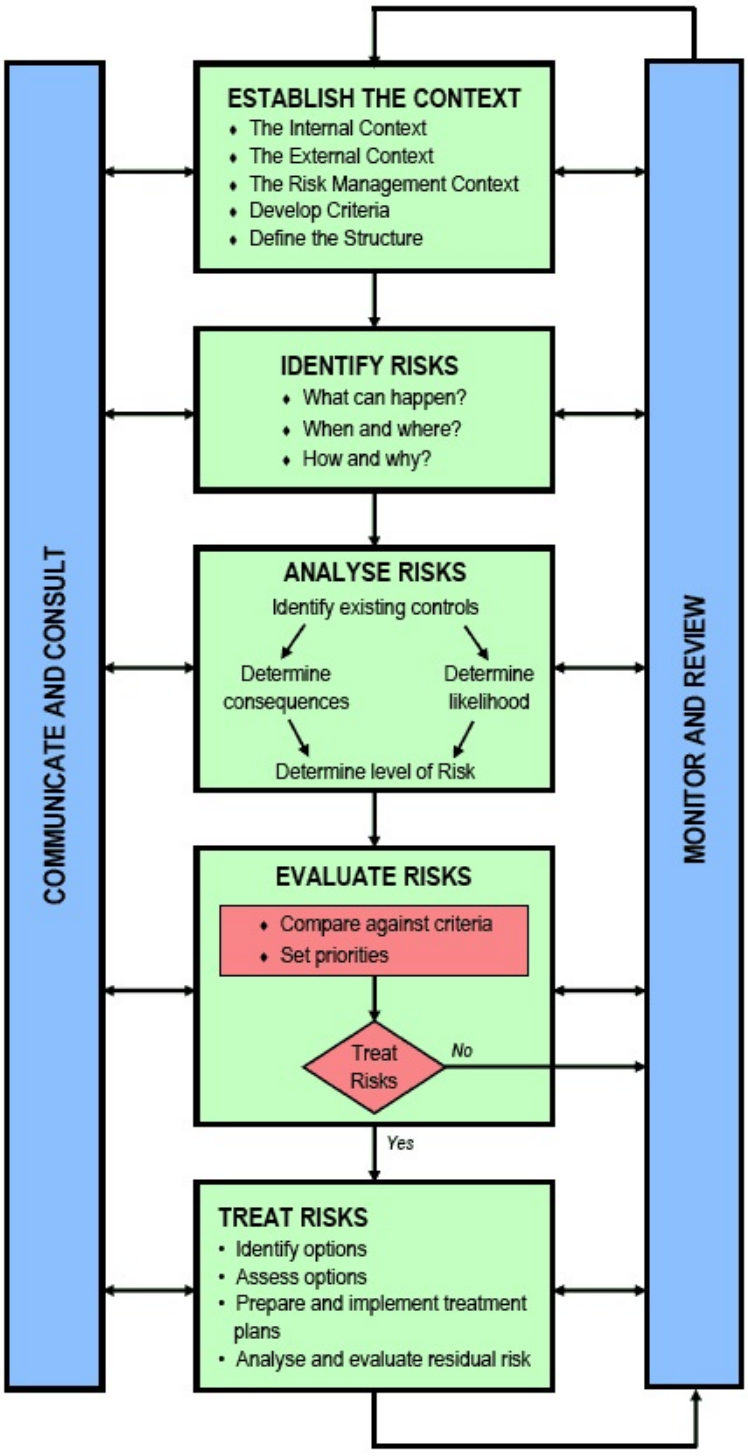

Figure 2.3: The AS/NZS 4360 Risk Management process

standard which introduces a new conceptualisation of Risk: from "chance or probability of loss" to "the effect of uncertainty on objectives". However, in this case, its strength can also be seen as a weakness. Due to its broad applicability, it offers almost no practical guidelines for its implementation and leaves that up to the actual assessor. For non-experts this can lead to ambiguities regarding certain subprocesses and their correct implementation.

2.2 Methods and related tools

2.2.1 Attack-Defence Trees

Owner :

- University of Luxembourg.

Country of origin :

- Luxembourg.

Targeted organisations :

- Government, agencies;
- Large companies;
- SME.

Method description :

Attack-defence trees (ADTrees) were developed at the University of Luxembourg in 2010 (Kordy, Mauw, Radomirović, & Schweitzer, 2011). They extend the well-known attack tree methodology (Schneier, 1999; Mauw & Oostdijk, 2005), by considering not only actions of an attacker, but also possible countermeasures of a defender. The improved formalism is able to capture evolutionary aspects of attack-defence scenarios and therefore allows for a more thorough and accurate security assessment process compared to attack trees, without, however, requiring additional computational power (Kordy, Pouly, & Schweitzer, 2012).

Attack-defence trees represent in a recursive, hierarchical way how an attacker may attack a given system or organisation and how a defender may protect against such an attack. In ADTrees, both types of nodes, attacks and defences, can be conjunctively as well as disjunctively refined. Furthermore, the formalism allows for each node to have one child of the opposite type. Children of opposite type represent countermeasures. These countermeasures can be refined and countered again. Two sets of formal definitions build the basis of ADTrees: a graph-based definition and an equivalent term-based definition. The graph-based definition ensures a visual and intuitive handling of ADTree models. The term-based representation allows

for formal reasoning about the models. The formalism is enriched through several semantics that define equivalent ADTree representations of a scenario (Kordy, Mauw, Radomirović, & Schweitzer, 2012).

Attack-defence trees allow for qualitative as well as quantitative analysis of security scenarios. The standard bottom-up algorithm, formalised for attack trees in Mauw and Oostdijk (2005) has been extended to ADTrees in Kordy, Mauw, et al. (2012). The formalism allows the user to quantify a variety of security relevant parameters, such as time of attack, probability of defence, scenario satisfiability and environmental costs.

Tool(s) :

The use of the attack-defence tree methodology is supported by a software tool, called ADTool, developed at the University of Luxembourg (Kordy, Kordy, Mauw, & Schweitzer, 2013).

ADTool is free, open source software assisting graphical modelling and quantitative analysis of security, using attack-defence trees. The main features of ADTool are easy creation, efficient editing, and automated bottom-up evaluation of security-relevant measures. The tool also supports the usage of attack trees, protection trees and defence trees, which are all particular instances of attack-defence trees.

The bottom-up algorithm for evaluation of attributes on ADTrees has been implemented in ADTool. Supported measures include: attributes based on real values (e.g., time, cost, probability), attributes based on levels (e.g., required skill level, reachability of the goal in less than k units of time), Boolean properties (e.g., satisfiability of a scenario). The implemented measures can be computed from the point of view of an attacker (e.g., the cost of an attack), of a defender (e.g., the cost of defending a system), or relate to both of them (e.g., overall maximum power consumption). Using different attribute domains allows us to distinguish between actions executed sequentially or in parallel.

Security assessment using ADTool is illustrated in Figure 2.4.

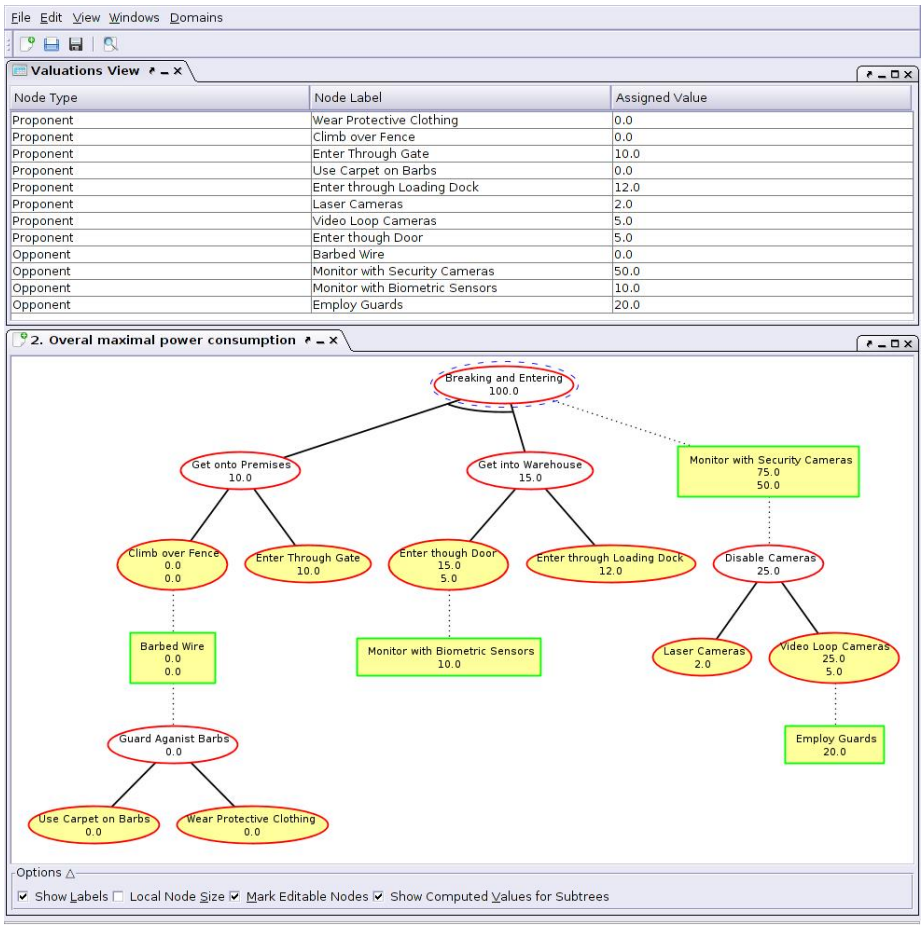

Figure 2.4: Security assessment using ADTool

ADTool runs on all common operating systems (Windows, Linux, Mac OS). The program is written in Java. It is available for download and as an online application at http://satoss.uni.lu/software/adtool.

2.2.2 Austrian IT Security Handbook

Owner :

- Austrian federal chancellery.

Country of origin :

- Austria.

Targeted organisations :

- Government, agencies;
- Large companies;

- SME.

Method description (Bundeskanzleramt Österreich, 2013):

The Austrian IT Security Handbook (V3.1.4) consists of 15 sections and several appendixes. The handbook is based on the international standards ISO/IEC 27001 and ISO/IEC 27002 and extends these standards with additional guidance and requirements related to Austrian regulations.

Section 1 is an introduction that describes on how to use the handbook and the basic subject.

Section 2 and 3 describe relevant requirements on how to establish, implement, operate, monitor, review, maintain and improve an Information Security Management System (following ISO/IEC 27001 Section 4, 5, 6, 7 and 8).

Section 4 to 15 defines the different security measures including the activities on how to implement and become compliant to them. The order and subject of the security measures follow the recommendations of ISO/IEC 27002 and the appendix of ISO/IEC 27001. In detail, some security measures may vary from the international standards in order to include specific requirements related to Austrian regulations and basic conditions.

The Appendixes includes amongst others agreement templates, instructions and references to standards, laws and related literature.

Tool(s) :

No specific tool available but an online version of the handbook allows: generating checklists and comments which can be locally stored; filtering by domains, industrial sectors, languages, roles and audience; browsing to related Austrian regulations (with the help of specific links); generating a selection of topics of interest which can be locally stored and loaded.

2.2.3 CORAS

Owner :

- EU-funded project (IST-2000-25031) January 2001 – June 2003.

Country of origin :

- Norway.

Targeted organisations :

- Academic organisation;
- Independent workers;
- SME.

Method description (CORAS, 2013):

CORAS, a method for conducting a risk analysis, is the result of a European funded project, lasting from January 2001 until September 2003 which had the goal to develop a tool-supported methodology for model-based risk analysis of security-critical systems.

CORAS is model-based and offers a customised language for threat and risk modelling and the corresponding guidelines on how to use the language.

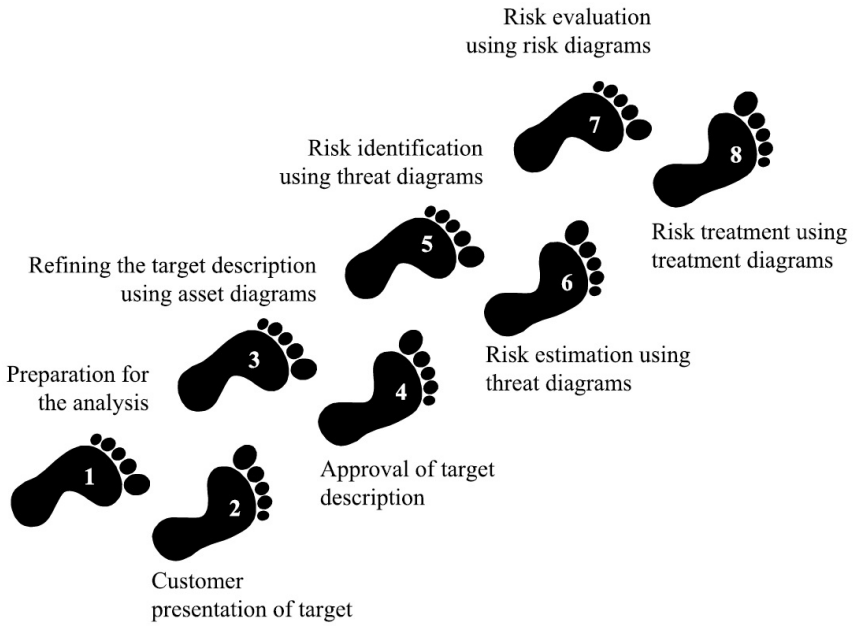

Figure 2.5: The 8 steps of CORAS security analysis method (CORAS, 2013)

The CORAS security risk analysis consists of eight different steps where the first four steps focus on context establishment and the last four steps are about risk identification, estimation, evaluation and possible risk treatments.

In the following, the eight steps will be briefly described (descriptions based on CORAS (2013) and Lund, Solhaug, and Stolen (2011):

Step 1 - Preparations for the risk analysis: In order to prepare the risk analysis, the main objectives of this step are to define the scope and to estimate the size of the project.

Step 2 - Customer presentation of the target: This step consists of an introductory meeting with the customer. The main item on the agenda is a presentation of the responsible persons of the customer, revealing their general objectives and expectations and the exact scope of the risk analysis. This has the aim to give a common understanding of the scope and to identify what the targeted organisation is worried about.

Step 3 - Refining the target description using asset diagrams: The goal of step 3 is to ensure a common understanding of the focus, the scope and the main assets. For this, the analysis team recapitulates the main results of the first meeting and from the readings of the company documents. For modelling the target of the analysis, CORAS uses the Unified Modelling Language (UML). Additionally the main assets to be protected are identified based on the interaction with the customer and a rough high-level analysis is conducted to identify major threat scenarios, vulnerabilities and enterprise risk levels.

Step 4 - Approval of the target description: Step 4 concludes the context establishment and includes as task the detailed description of the scope of the risk analysis by using a formal or semi-formal notation such as the UML. The description should be approved by the customer before moving on to the next step. Besides, the definition of the risk evaluation criteria for each asset is also done during this step.

Step 5 - Risk identification using threat diagrams: Step 5 includes the identification of possible risks by organising a brainstorm meeting with participants which have different competences in order to identify as much risks as possible. The risk identification includes the identification of threats, unwanted incidents, threat scenarios and vulnerabilities with reference to the identified assets. The results will be documented with the help of CORAS threat diagrams, part of the CORAS language.

Step 6 - Risk estimation using threat diagrams: Step 6 takes the results from step 5 in order to define the level of the risks. Step 6 is, similarly to step 5, also conducted as a brainstorming with participants having different competences in order to estimate the likelihoods and consequences of unwanted incidents.

Step 7 - Risk evaluation using risk diagrams: Step 7 consists in evaluating if the identified risks are acceptable or not. The evaluation is done by using the risk evaluation criteria, defined during the context establishment and the results of the risk estimation of step 6.

Step 8 - Risk treatment using treatment diagrams: The aim of step 8 is the identification of risk treatments for risks which are classified as not acceptable. The different risk treatments are chosen with respect to a cost-benefit analysis.

CORAS relies on its own modelling language which is an extension of UML. The methodology defines four kinds of diagrams (asset, threat, risk and treatment diagrams) as part of its “model-based” approach to support various visualisations in various steps of the process. These diagrams can be used in conjunction with the risk assessment to serve three purposes:

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

The method differentiates between direct and indirect assets (defined as entities that need to be protected). Furthermore, it classifies threats to these assets as:

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

The CORAS method is based on the ISO/IEC 17799 standard (now ISO/IEC 27002) and as such is also compatible with ISO/IEC 13335 (now 27005, described in Section 2.1.2) as well as the AS/NZS 4360 standard (described in Section 2.1).

Further, the CORAS method provides a computerised tool developed to be used together with the CORAS method described as follows:

Tool(s) :

"The CORAS method provides a computerised tool designed to support documenting, maintaining and reporting analysis results through risk modelling." (CORAS, 2013)

In summary, the CORAS tool is a diagram editor that is available for free which can be used to draw the different CORAS diagrams (asset diagrams, threat diagrams, risk diagrams and treatment diagrams).

Key functionality:

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

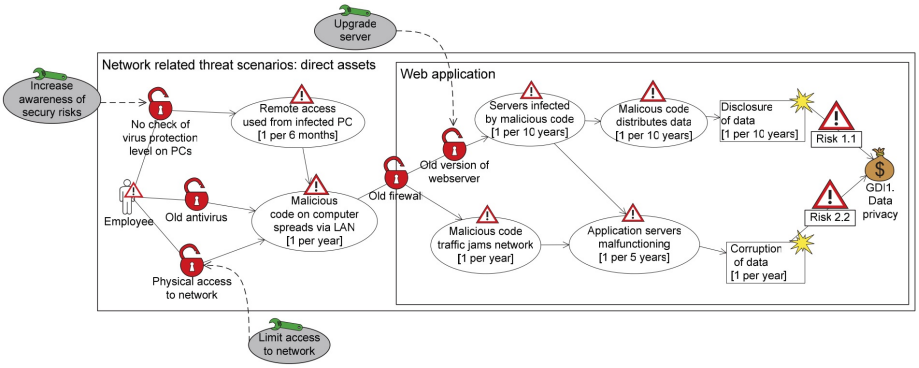

Figure 2.6: CORAS tool

2.2.4 CRAMM

Owner :

- Insight Consulting.

Country of origin :

- United Kingdom.

Targeted organisations :

- Government, agencies;
- Large companies.

Method description (Siemens, 2011; European Network and Information Security Agency, 2013a):

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

CRAMM can be used to justify security investments by demonstrating need for action at management level. Secondary applications can be benchmarking the security of an organisation or showing compliance to other standards (like the BS7799 - British standard for information security management).

The CCTA Risk Analysis and Management Method (CRAMM) offers an approach divided into three stages including technical and non-technical aspects of security:

Asset identification and valuation: Identification and valuation of the physical, software (valuation in terms of the replacement costs), data and location assets composing the information system under review. Valuation of physical assets by providing the replacement costs and valuation of software and data assets by providing the impact in case of an incident. This activity is supported by 10 pre-defined asset tables to aid in the identification and valuation of assets. Assets are classified into categories, each with a pre-defined set of known vulnerabilities and threats.

Threat and vulnerability assessment: Identification of occurrence likelihood of deliberate and accidental threats that may have an impact on the information systems. This stage identifies the likelihood that an incident occurs and calculates the level of the actual risk. CRAMM covers a full range of deliberate and accidental threats that may affect information. The output of this stage is the calculated level of the current risk.

Countermeasure selection and recommendation: CRAMM offers a countermeasure library including over 3000 countermeasures. Based on the risk measurements in the previous stage, CRAMM helps to identify if the computed risk level justifies the implementation of specific countermeasures. Further CRAMM includes backtracking, 'What If?', prioritisation functions and reporting tools to assist with the implementation of countermeasures and the management of the identified risks.

CRAMM is a very versatile method, allowing users to achieve various tasks at various levels of complexity. CRAMM describes a qualitative, asset-centric approach, which makes use of 10 predefined asset tables to aid in the identification and valuation of assets. Assets are classified into categories, each with a pre-defined set of known vulnerabilities and threats. Once assets have been identified and evaluated, and likely threats and vulnerabilities found, the dedicated tool automatically returns possible countermeasures. However, this means that the methodology itself is of little use without the software toolkit.

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

Tool(s) (Siemens, 2011):

CRAMM is also supported by a tool based on the CRAMM method which additionally is compliant with the BS7799: 2005 standard and offers support for ISO 27001.

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

Key functionality:

- Comprehensive tool that supports the entire RA process;
- Range of help functions and tools to help information security managers plan and manage security;
- Wizards to rapidly create pro-forma information security policies and other related documentation;
- 'Copy and Compare' feature allowing users to compare two reviews;
- Back tracking;
- "What if" analysis;
- Prioritisation functions;
- Reporting tools;
- A database of over 3000 security controls referenced to relevant risks and ranked by effectiveness and cost
- Various tools that support the key processes involved in business continuity management;
- Supports certification or compliance against ISO 27001.

2.2.5 EBIOS 2010

Owner :

- Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI).

Country of origin :

- France.

Targeted organisations :

- Government, agencies;
- Large companies;
- SME.

Method description (Agence national de la sécurité des systèmes d'information, 2010; European Network and Information Security Agency, 2013a):

EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité), published by ANSSI, the French Network and Information Security Agency, is an iterative and module-based risk management approach which complies with the security standards ISO/IEC 31000, ISO/IEC 27005 and ISO/IEC 27001. It is currently maintained by a private club of experts from various fields (i.e. Club EBIOS).

EBIOS includes 5 different iterative modules:

1. Context establishment: Defining and describing the relationship between the business context and the IS (contribution to business goals, boundary, decomposition);
2. Feared events analysis: Security requirements are determined based on the feared security events;
3. Vector (threat events) analysis: A risk study is conducted in order to identify and analyse threat scenarios;
4. Risk analysis: Information from previous modules is used to identify risks and describe the necessary and sufficient security goals relating to these risks;
5. Security controls analysis: The necessary security controls are determined, and any residual risk is made explicit

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

Every module includes several tasks which are described with the help of a standardised form. Every task of a module includes recommended actions for which guidelines are described to explain how to realise the actions.

EBIOS can be used either in the design stage or against existing systems. Instead of a scenario-based risk analysis, EBIOS goes for a more structured approach, allowing a more exhaustive analysis through the identification of various sub-components or causes of risk (e.g. entities, vulnerabilities, attack methods, threat agents, etc.). Its 5 phases can also be applied somewhat independently, allowing for only certain parts of the analysis to be (re)done (e.g. vulnerability analysis) (Kouns & Minoli, 2010). Furthermore, the method is compatible with all relevant ISO standards (13335, 15408, 17799, 31000, 27005, 27001).

Tool(s) (Agence national de la sécurité des systèmes d'information, 2010):

EBIOS 2010 comes together with a software tool (EBIOS) which is available for free. The tool supports the end-user by implementing the different modules of the method and offers the possibility to export the reports in unformatted comma-separated values (CSV) files. The tool is capable of matching a threat with relevant vulnerabilities and even building up risk scenarios automatically (European Network and Information Security Agency, 2013c).

Key functionality:

- Customisable knowledge bases including vulnerabilities, threats, metrics, security requirements, etc. (Task Group IST-049, 2008);
- Sample tutorial scenario (self-training module);
- Support for logging results and performing certain computations automatically;
- Capability of producing several types of reports and deliverables based on different templates.

2.2.6 FAIR

Owner :

- Risk Management Insight LLC.

Country of origin :

- USA.

Targeted organisations :

- Government, agencies;
- Large companies;
- SME.

Method description (Risk Management Insight LLC, 2006):

The FAIR (Factor Analysis of Information Risk) methodology is part of the FAIR framework, introduced by Risk Management Insight LLC. in 2005 under a Creative Commons Attribution-Noncommercial-Share Alike 2.5 License.

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

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

Stage 1 Identify scenario components:

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

Stage 2 Evaluate Loss Event Frequency (LEF):

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

Stage 3 Evaluate Probable Loss Magnitude (PLM):

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

Stage 4 Derive and articulate Risk:

10. Derive and articulate risk.

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

FAIR's Basic Risk Assessment process, as described in the "FAIR Basic Risk Assessment Guide", relies extensively on tables which need to be filled in with ordinal values of the type: "low-medium-high". The ordinal values are however, defined based on intervals, described in the guide. Operators are then defined on these factors by means of matrices. After step by step estimation and computation of the various factors driving risk, an evaluation of total Risk is obtained, also on a 4 level ordinal scale. This is similar to the approach undertaken in a Structured Risk Assessment (see Section 2.2.16). The key difference here is that a FAIR analysis focuses on single assets, while an SRA first decomposes the target of assessment into components and then evaluates risk individually for each one. Furthermore, the FAIR analysis evaluates the risk for one Threat Community at a time. However, the FAIR analysis takes many more factors into account and offers a more precise evaluation of each Asset - Threat Community pair. The Risk Assessment described above is intended for use in simple, single level risk analysis, not describing the additional steps required for a multilevel analysis. A slightly more complex analysis (looking at a number of assets, or various threat communities) can of course be achieved by simply running the Basic risk assessment multiple times, once for each Asset - Threat Community pair. Documentation of performing more complex Risk Assessments is not publicly available on-line, and knowledge and qualification to perform such assessments based on FAIR can only be obtained by following training courses.

The FAIR methodology is not in direct competition with the other methodologies. In fact, it is complementary to most other Risk Management methodologies and can be used in conjunction with NIST 800-30, ISO/IEC 27002, COBIT, ITIL or COSO Furthermore, it has been adopted as the basis for The Open Group's Risk Taxonomy and is referenced in ISACA's RiskIt framework (The Open Group, 2009a).

Tool(s) :

FAIRLite is an Excel application designed to enable simple and effective quantitative analysis of risk scenarios using the Factor Analysis of Information risk (FAIR) framework. FAIRLite is simple to use and yet flexible enough to perform powerful analyses on complex scenarios. FAIRLite leverages a widely used commercial Monte Carlo function specifically designed to analyse uncertain input data. Analysis results are then represented in both graphical and table forms that inform management of the most likely outcomes while also accurately reflecting the degree of uncertainty associated with the analysis and the

potential for "tail events". FAIRLite is primarily intended for use in analysing discrete risk issues – i.e., those risk issues that are distilled to a single scenario. Since the merge between Risk Management Insight LLC and CXOWARE, the FAIRLite tool has been made obsolete by the new FAIRiq tool (LLC, 2010).
Key functionality:

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

FAIRiq is a quantitative risk analysis application and decision analysis solution based on the FAIR methodology. It is implemented as a software-as-a-service cloud application. FAIRiq is built as the foundational decision-analysis application enabling an organisation to measure economic loss associated with information security & operational risk. The application is designed with flexible data export capability which makes it a nice compliment to the leading GRC applications on the market. Since the merge between Risk Management Insight LLC and CXOWARE, the FAIRiq tool has replaced the FAIRLite tool. According to the developers, FAIRiq helps decision-makers prioritise issues, evaluate threats, account for assets, and make sense of audit findings, all based on risk (LLC, 2010).
Key functionality:

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

2.2.7 FRAP

Owner :

- Peltier and Associates LLC.

Country of origin :

- USA.

Targeted organisations :

- SME.

Method description (Peltier, 2005; Kouns & Minoli, 2010; Coles-Kemp & Overill, 2007):

Application of the FRAP (Facilitated Risk Assessment Process) method was first described by Thomas R. Peltier in his book Information Security Risk Analysis, published in 2001, and further detailed in the second edition published in New York in 2005.

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

The RA process described by FRAP is divided into three phases:

1. A pre-FRAP session where the scope and definitions of the assessment as well as how threats are to be prioritised are agreed upon. In this method, the team is put together and a decision is made regarding the assets that are to be included in the analysis;
2. A FRAP session, the actual risk assessment takes place: risks are identified and risk levels are determined by taking into account the likelihood of the threat occurring;
3. A post-FRAP report generation: this report contains a summary of the risks as well as suggestions on how these can be diminished..

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

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

can be internal to the organisation and managers. The FRAP methodology is based on the assumption that security controls are not yet implemented and, as such, does not take into account the vulnerability caused by a lack of such controls. The impact of undesired events is evaluated based on how it affects business operations, not only based on the financial loss caused. There is also an extension of FRAP that allows for the estimation of residual risk (i.e. the risk level once a control has been selected and implemented).

Tools(s) :

No tool

2.2.8 ISAMM

Owner :

- Telindus N.V.

Country of origin :

- Belgium.

Targeted organisations :

- Government, agencies;
- Large companies;
- SME.

Method description (Kouns & Minoli, 2010):

ISAMM (Information Security Assessment & Monitoring Method), can be used to identify assets and threats, to assess the probability and impact of the threats, to represent the risks, to give a support in deciding if a risk is acceptable or not, a support for selecting security controls in order to treat non-acceptable risks and finally to support the risk communication process.

The ISAMM risk assessment consists of four parts:

- Scoping;
- Assessment – compliance and threats;
- Validation of compliance and threats;
- Result – Calculation and reporting.

ISAMM offers beside a pure qualitative approach also a quantitative risk management method which quantifies the risks with a monetary value calculated by the Annual Loss Expectancy (ALE). The Annual loss expectancy is the expected annual monetary loss due to the occurrence of threats on assets of the organisation.

ISAMM also establishes the risk treatment plan based on the Return On Security Investment (ROSI). Based on this it is possible to compare the implementation costs of a security measure with the costs saved due to the reduction of a risk by this security measure.

Tool(s) :

No tool

2.2.9 ISF Methods

Owner :

- Information Security Forum (ISF).

Country of origin :

- International ISF Members.

Targeted organisations :

- Government, agencies;
- Large companies.

Method description (Information Security Forum, 2013):

The Information Security Forum (ISF) elaborated several methodologies and tools addressing risk management / assessment:

- Information Risk Analysis Methodologies (IRAM): IRAM is elaborated by the ISF to analyse business information risk and select justified security controls to shrink identified risk;
- Fundamental Information Risk Management (FIRM): This methodology uses a scorecard approach to measure the extent to which the organisation is managing information risk across a wide range of information assets.

Further details on the ISF methodologies are not freely available without being Member of the ISF.

Tool(s) (available to ISF members only):

- Information Security Benchmark;
- Third Party Security Assessment Tool (TPSAT);
- Return on Security Investment (ROSI).

2.2.10 IT-Grundschutz

Owner :

- Federal Office for Information Security (BSI) .

Country of origin :

- Germany.

Targeted organisations :

- Government, agencies;
- Large companies;.
- SME.

Method description (BSI, 2013):

IT-Grundschutz is part of a series of standards published by the German Federal Office for Information Security (BSI) describing "methods, processes, procedures, approaches and measures relating to information security". Apart from a more general Information Security Management methodology, The “IT-Grundschutz” offers on the one hand a guideline for conducting a risk analysis and on the other hand the “IT-Grundschutz” Catalogue (actual version: “12. Ergänzungslieferung” - September 2011) which includes a great number of standardised security controls in order to set up a relatively high security level without performing a detailed risk analysis.

The goal of the IT-Grundschutz Risk Assessment methodology is to provide a qualitative method for identification, analysis and evaluation of security incidents that might be damaging to the business, that is also consistent and usable with the rest of the standard, and that can be applied efficiently. The standard describes a two-tier risk assessment: one is designed for reaching a "standard" level of security, while a second "supplementary risk analysis" can be undertaken by companies that desire an approach customised to their specific needs or sector or that have special security requirements.

The main body of the standard does not describe a specific Risk Assessment procedure, but instead gives suggestions for safeguards appropriate for typical business processes, applications and IT systems that have normal security requirements. For companies that only require implementing a "standard" Information Security Management System based on IT-Grundschutz, the Risk Assessment is done by using the IT-Grundschutz Catalogues. These contain repositories of common threat scenarios and standard security countermeasures applicable to most IT environments, and grouped by modules corresponding to various business environments and Information System components.

If IT systems with higher security requirements have to be secure, the “IT-Grundschutz” recommends following the guidelines of the BSI-Standard 100-3 including a risk

analysis method which complements the “IT-Grundschutz” Catalogue. This is a process called "Supplementary Risk Analysis" that is to be used in contexts that differ significantly from standard IT security application scenarios and requirements. It is the responsibility of the (IT) management to decide whether or not such a supplementary analysis is warranted and for which assets or components. In order to achieve this higher level of information security, a "supplementary risk analysis based on IT-Grundschutz" is to be performed by taking the following steps:

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

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

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

Tool(s) (based on BSI (2013)):

BSI GSTOOL: is used to support the use of the “IT-Grundschutz” method. The main goal of the software is to support preparation, administration and updating of IT security concepts according to the requirements of the IT-Grundschutz methodology. After collecting the information required, the users have a comprehensive reporting system at their disposal for carrying out structure analyses on all of their compiled data and for generating reports on paper or in electronic form. GSTOOL is a stand-alone application with database support. A trial version is available (European Network and Information Security Agency, 2013c).
Functionalities of the GSTOOL are:

- Capture and structural analysis of IT-Systems, applications, networks, etc.;
- Modelling and layer models in accordance with IT-Grundschutz;

- ISO 27001 certificate based on the “IT-Grundschutz”;
- Basis security check and implementation of security controls (baseline protection modelling);
- Risk analysis based on the “IT-Grundschutz”;
- Estimation of Cost, effort and residual risks;
- Security requirements analysis;
- Reporting;
- Review support;
- Encryption of user-specific data for exports;
- IT system recording / structural analysis;
- Assessing protection requirements;
- Reporting module.

HiSolutions AG -HiScout GRC Suite: is a comprehensive tool set for Governance, Risk and Compliance Management. Its modules cover: Business Continuity Management, Information Security Management, Operational Risk Management, Compliance Management, Quality Management and IT-Service Management. The most notable modules are of course, the Information Security Management and Risk Management modules. These allow Risk assessments to be carried out covering both operational and enterprise Risk, as well as support the implementation of a complete ISMS.
Main functionality includes:

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

- The module automatically calculates the overall security requirements for all company resources, and lets you use that information as the foundation for goal-oriented decisions.
- Modifiable templates for management reports and audit reports enable you to quickly demonstrate your findings.

RM Studio is a full-featured, customisable and dynamic solution that combines business continuity management software and risk management software into one simple to use platform. RM Studio guides users through the process of risk assessment, risk treatment and risk management. Standards are easy to embed and users can easily define their company own standards. RM Studio comes with a predefined asset category library and a predefined threat library with interconnection helping users to identify important threats and select the appropriate mitigating control. RM Studio is a holistic modular solution with the option to add a risk assessment and treatment module and a business continuity module. It assists users in embedding a culture of risk management throughout the organisation by combining risk management software and business continuity management software (European Network and Information Security Agency, 2013b).
Main functionality:

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

NFODAS GmbH - SAVe is a Database-supported tool that implements the IT-Grundschutz methodology, but can also be used to obtain ISO 27001 OR BSI 100-2 and 100-3 results. It is supported by an extensive "IT Security Database" that allows IT security concepts to be created, applied and updated in a manner consistent manner, compatible with the IT-Grundschutz methodology. It allows the user to analyse and model the IT architecture, identify security needs, perform basic security checks and surveys. Furthermore, it can be used to perform audits and certifications against the IT-Grundschutz and ISO/IEC 27001 standards. It can be adapted to various scenarios (e.g. military or security-critical infrastructures) by extending the security model. It also contains modules that allow things like

monitoring the costs of implementation, introducing custom measure and building blocks, mapping of e-business requirements, capturing of deadlines, roles and responsibilities, action planning and tracking, etc. Main functionality:

- Network-capable;
- Multi-user;
- Supports distributed development of part-concepts;
- Manages multiple security concepts and part-concepts;
- Flexible, role-based access control;
- Revision and tracking ability;
- Automatic data update for new IT-Grundschutz version;
- Data export for development in Office components;
- Import function to data inputs from the GSTOOL;
- Interactive creation of customised report formats;
- Open interface for the integration of additional modules.

Kronsoft e.K. - Secu-Max (Relevant documentation not publicly available)

F.-J. Lang IT-Security Consulting GmbH EISA-Project (Relevant documentation not publicly available)

Swiss Infosec AG - Baseline-Tool (Relevant documentation not publicly available)

2.2.11 MAGERIT V2 (2005)

Owner :

- Spanish Ministry for Public Administrations .

Country of origin :

- Spain.

Targeted organisations :

- Government, agencies;
- Large companies;
- SME.

Method description (Ministerio de Administraciones Publicas, 2006):

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

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

MAGERIT, supported by the Spanish Ministry for Public Administrations, consists of three books which are briefly described in the following.

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

The risk analysis consists of several steps which allow the estimation of possible impacts and risks:

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

Step 2: Threats – Determine the threats to which those assets are exposed. Threats are "things that happen." Of all the things that could happen, those that are of interest are those that could happen to our assets and cause damage.;

Step 3: Safeguards to be implemented – Determine what safeguards are available and how effective they are against the risk.;

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

Step 5: Determination of the risk – Estimate the risk, defined as the weighted impact on the rate of occurrence (or the expectation of appearance) of the threat. Risk is the measurement of the probable damage to the system. Knowing the impact of the threats to the assets, the risk can be derived directly simply by taking into account the frequency of occurrence. The risk increases with the impact and with the frequency. After completion of these steps, MAGERIT describes the additional tasks, namely the revision of step 4 to determine the residual impact and the revision of step 5 to determine the residual risk.

Book 2: Book 2 consists of a catalogue of elements providing guidelines for:

- Types of assets;
- Dimensions for evaluating assets;
- Criteria for evaluating assets;
- Typical threats to information systems;
- Safeguards to be considered for protecting information systems.

Book 2 additionally provides for each chapter extensible mark-up language (XML) notations with the aim that they can easily or even automatically be integrated in risk analysis and risk management tools.

Book 3: Book 3 contains techniques often used by risk analysis and management projects.
Techniques specific to risk analysis:

- Analysis using tables;
- Algorithmic analysis;
- Attack trees.

General techniques:

- Cost/benefit analysis;
- Data flow charts;
- Process charts;

- Graphical techniques;
- Project planning;
- Work sessions: interviews, meetings and presentations;
- Delphi evaluation.

Tool(s) (Mañas, 2012):

A.L.H. J. Mañas S.L. provides tools for risk analysis and management which support the MAGERIT methodology. It is designed to support the risk management process along long periods, providing incremental analysis as the safeguards improve. The tool is intuitive, provides fast calculations and generates a quantity of textual and graphical output.

The proprietary tools developed by the Spanish National Center for Cryptography are part of a family of tools named EAR (Environment for the Analysis of Risk):

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

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

Key functionality:

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

2.2.12 Marion 1998 (not maintained anymore)

Owner :

- CLUSIF (Club de la Sécurité de l'Information Français).

Country of origin :

- France.

Targeted organisations :

- Large companies.

Method description (European Network and Information Security Agency, 2013a):

MARION (Méthodologie d'Analyse des Risques Informatiques et d'Optimisation par Niveau – Methodology of Analysis of Computer Risks Directed by Levels) is an audit based methodology. It allows estimating the level of risks through weighted questionnaires relative to security.
The methodology includes 4 phases:

Preparation: Definition of the security objectives and the scope of the risk analysis.

Vulnerability audit: Based on a questionnaire provided by the methodology, the requirements are identified and the questionnaire is filled out. The questionnaire has the aim to assign to 27 indicators distributed in 6 large subjects (Organisational security, Physical security, Continuity of services, IT organisation, Logical security and exploitation, Security of applications) a grade between 0 and 4. The level 3 is the level to be reached to ensure a security considered as acceptable.

Risk analysis: The evaluation of the audit results allow to split the risks in major risks and minor risks and to identify the threats and vulnerabilities together with their likelihood and impact.

Elaboration of an action plan: Based on the previous findings the methodology allows now to take decisions on actions to be taken in order to reduce risks and to attend a general risk level of 3.

Remark: The CLUSIF does not sponsor this method anymore, as MARION is replaced by MEHARI. However, MARION is still used by various companies.

Tool(s) :

No tools

2.2.13 MEHARI

Owner :

- CLUSIF (Club de la Sécurité de l'Information Français) .

Country of origin :

- France.

Targeted organisations :

- Government, agencies;
- Medium to Large companies;

- Commercial companies;
- Non-profit: NGOs, education, health sector, public services, etc.

Method description (European Network and Information Security Agency, 2013a; CLUSIF, 2010):

MEHARI provides the possibility to evaluate and manage the risks attached to risk scenarios. MEHARI follows the ISO/IEC 27005 standard and includes the following key elements:

- Risks are described by risk scenarios that contain the following elements:
  - An identifier for the classification in the family of scenarios;
  - The type of primary asset;
  - The type of vulnerability (type of secondary asset considered, type of damage, criterion concerned (CIA or E));
  - The type of threat (type of the triggering event, possible circumstances of the trigger, type of possible actor);
  - A description of the scenario, in text form.
- Each risk scenario is quantitatively evaluated:
  - Impact of the risk scenario;
  - Likelihood of the scenario occurrence;
  - Risk reduction factors based on the security measures, which indicate the effect of a security measure on the impact and likelihood of risk scenarios;
  - The evaluation of risk scenarios enables to select appropriate security measures such that the risk coming from the risk scenarios can be decreased below an acceptable level.

Tool(s) :

MEHARI knowledge base – is a very basic tool, with limited functionality. It can be used, however, as a supporting document for a limited-purpose RA following the MEHARI methodology. The worksheet of the method contains multiple formulas allowing to display step by step the results of the RA and RM activities and to propose additional controls for risk reduction. It allows assessing the seriousness of individual risk scenarios based on impact and likelihood, selection of countermeasures.

Risicare – assists the information risk analysis and management actions in support of MEHARI. The functions of Risicare simulate real-world conditions and test multiple "what if" threat situations or scenarios. As a result, Risicare can be considered additionally as a risk modelling software. Moreover, Risicare allows the management of an ISMS and uses a set of control points which includes

those of ISO 27002.
Main functionality includes:

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

2.2.14 MIGRA

Owner :

- AMTEC/Elsag Datamat S.p.A.

Country of origin :

- Italy.

Targeted organisations :

- Government, agencies;
- Large companies;
- SME.

Method description (European Network and Information Security Agency, 2013a):

MIGRA (Metodologia Integrata per la Gestione del Rischio Aziendale) is a qualitative risk assessment and management methodology. The methodology provides an analysis framework based on assessed risk scenarios (the estimation of likelihood and impact).
MIGRA defines (European Network and Information Security Agency, 2013a):

- a security and risk taxonomy for information and tangible assets;
- a logical framework for generating a model of the security perimeter to be analysed;
- an algorithm (based on questionnaires) for assessing, on a four level qualitative scale (High, Medium, Low, Negligible/Not applicable), the value of both information and tangible assets relevant to the above perimeter;

- a scheme for performing threat and vulnerability analysis;
- a procedure for calculating (on a qualitative scale) risk;
- a mechanism to identify in every scenario a set of appropriate security measures;
- a procedure to perform gap and compliance analysis with reference to corporate security policies, norms, standards, guidelines and best practices. MIGRA puts in relationship threats, attacks, security measures and components of the security perimeter in order to ease the identification of security measures to implement.

Tool(s) : MIGRA tool (relevant English documentation not available)

2.2.15 OCTAVE

Owner :

- Carnegie Mellon University, SEI (Software Engineering Institute).

Country of origin :

- USA.

Targeted organisations :

- Large companies.

Method description (Alberts & Dorofee, 2001):

The OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) Method uses a three-phase approach where each phase consists of several processes. Prior to the risk assessment, some preparation has to be done (Alberts & Dorofee, 2001):

- Get senior management sponsorship – This is the most critical success factor. If senior managers support the process, people in the organisation will actively participate.
- Select the analysis team – Team members need to have sufficient skills to lead the evaluation. They also need to know how to go outside the team to augment their knowledge and skills.
- Scope OCTAVE – The evaluation should include important operational areas. If the scope is too big, it will be hard to analyse all of the data. If it is too small, the results may not be as meaningful.
- Select participants – Staff members from multiple organisational levels will contribute their knowledge. It is important for these people to understand their operational areas.

The three phases of the OCTAVE methodology are:

Phase 1: Build Asset-Based Threat Profiles – Identification of critical assets and current security measures implemented for their protection. The processes of Phase 1 are (Alberts & Dorofee, 2001):

- Process 1: Identify Senior Management Knowledge – Selected senior managers identify important assets, perceived threats, security requirements, current security practices, and organisational vulnerabilities.
- Process 2: Identify Operational Area Management Knowledge – Selected operational area managers identify important assets, perceived threats, security requirements, current security practices, and organisational vulnerabilities.
- Process 3: Identify Staff Knowledge – Selected general and IT staff members identify important assets, perceived threats, security requirements, current security practices, and organisational vulnerabilities.
- Process 4: Create Threat Profiles – The analysis team analyses the information from Processes 1 to 3, selects critical assets, refines the associated security requirements, and identifies threats to those assets, creating threat profiles.

Phase 2: Identify Infrastructure Vulnerabilities – Identification of key operational components and their vulnerabilities. The processes of Phase 2 are (Alberts & Dorofee, 2001):

- Process 5: Identify Key Components – The analysis team identifies key information technology systems and components for each critical asset. Specific instances are then selected for evaluation.
- Process 6: Evaluate Selected Components – The analysis team examines the key systems and components for technology weaknesses. Vulnerability tools (software, checklists, scripts) are used. The results are examined and summarised, looking for the relevance to the critical assets and their threat profiles.

Phase 3: Develop Security Strategy and Plans – Identification of risks related to the organisation's critical assets and definition of action plan. The processes of Phase 3 are (Alberts & Dorofee, 2001):

- Process 7: Conduct Risk Analysis – The analysis team identifies the impact of threats to critical assets, creates criteria to evaluate those risks, and evaluates the impacts based on those criteria. This produces a risk profile for each critical asset.
- Process 8: Develop Protection Strategy – The analysis team creates a protection strategy for the organisation and mitigation plans for critical assets, based upon an analysis of the information gathered. Senior managers then review, refine, and approve the strategy and plans.

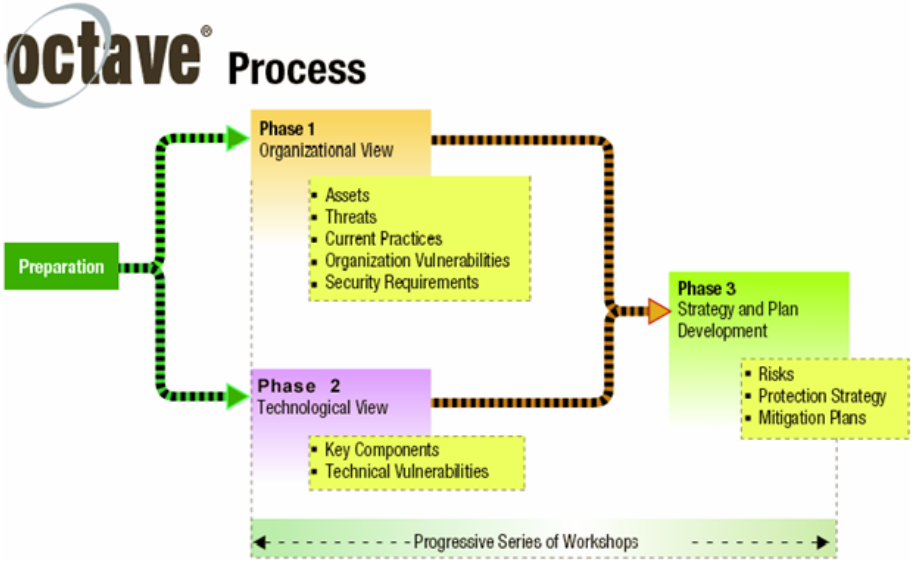

Figure 2.7: OCTAVE Method (Alberts & Dorofee, 2001)

An adapted version of OCTAVE called OCTAVE-S was developed for the needs of smaller organisations (about 100 people or less). The same criteria as the OCTAVE method is used but adapted to smaller organisations.

Tool(s) :

No tool

2.2.16 Structured Risk Analysis

Owner :

- Consult Hyperion.

Country of origin :

- United Kingdom.

Targeted organisations :

- SME.

Method description (McEvoy & Andrew, 2002):

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

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

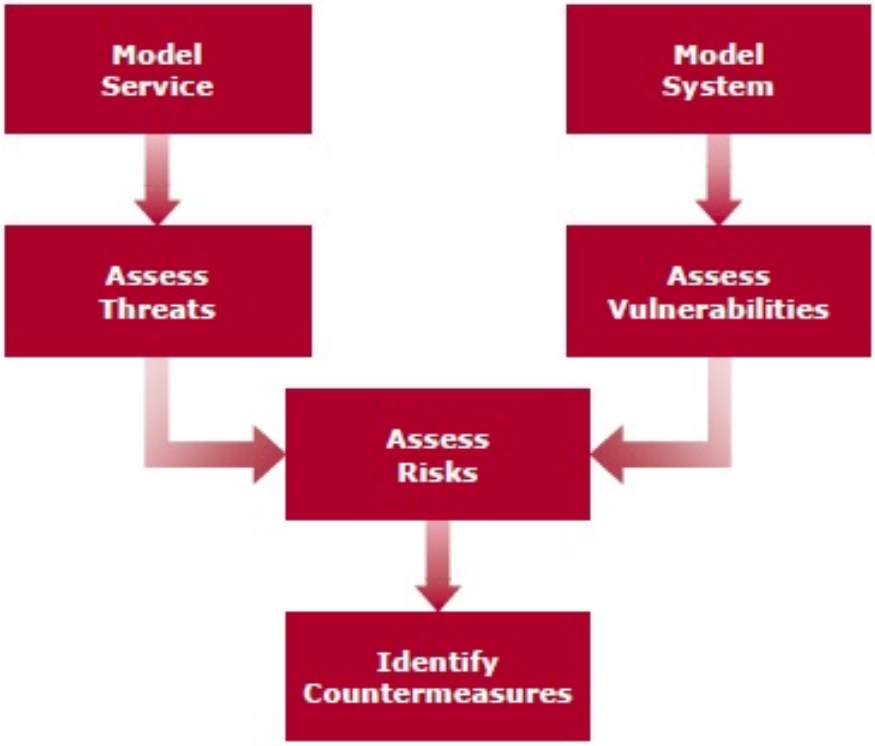

Figure 2.8: SRA process

The method is made up of a small number of steps. An overview of the process can be found in Figure 2.8 SRA process. In the Model Service step, all data entities are identified. Next, in the Assess Threats step for each data entity, the Damage for the customer and the Gain for an average attacker that a compromise in Confidentiality, Integrity or Availability might cause is estimated. The Model System step simply decomposes the physical architecture into sub-components and interfaces. The Assess vulnerabilities step estimated the difficulty (average cost and likelihood of capture) of an attack on each component or interface. In the Assess risks step, a cross-reference table is used to describe which data entities are stored, processed, or transmitted by each physical component or interface. Then, using some predefined operators, the overall risk (called Exposure) of each valid component-entity pair is automatically calculated. In the final, Identify countermeasures step, mitigations and treatments are manually identified for the highest risks.

The method is described in McEvoy and Andrew (2002). As the name suggests it offers an extremely structured way of identifying and ranking risks. Its main strength comes from the fact that it uses a table-based deconstruction of the system and

its physical and digital entities. After describing this decomposition, the pre-defined table structure allows for easy identification of risks. An (expert) evaluation of each component interaction is required, but thanks to the method's pre-defined operations on the input table, the output (i.e. a ranking of the most exposed risks) is easy to read and understand even by management users.

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

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

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

Tool(s) :

No tool

2.2.17 TRICK light

Owner :

- itrust consulting s.à r.l.

Country of origin :

- Luxembourg.

Targeted organisations :

- SME.

Method description (itrust consulting s. à r. l., 2013):

TRICK light is a risk analysis and treatment tool which is used in the context of Information security risk management. TRICK is acronym for “Tool for Risk management of an ISMS based on Central Knowledge base”. The extension “light” indicates that the tool does not provide until now a Central Knowledge base. The basic idea of TRICK light is the result of a European FP7 project proposal which had the aim to develop a software tool and a belonging methodology for counteracting risk management problems encountered by small and medium enterprises (SME). A prototype of the tool was developed by itrust consulting before a new extended version had been developed in the context of the project “Building security assurance in open infrastructures” (BUGYO) proposed by the Cooperation for a European sustained Leadership in Telecommunications (CELTIC).

The TRICK light allows to determine for an information system and his associated context (financial, administration,. . .) a list of security measures to be put in place in order to reduce losses caused by the occurrence of threats.

The analysis of TRICK light is based on two principles:

- The steps of risk management as proposed by the standard ISO 27005, mainly the risk identification and risk estimation of the risk assessment part.
- Profitability calculation which:
  - is based on the influence of the security measures on the losses caused by the occurrence of threats: this parameter is called Risk Reduction Factor (RRF) and needs to define the specificity of the risks;
  - is oriented towards the Return on Security Investment (ROSI) (Harpes, Adeslbach, Zatti, & Peccia, 2007) in the choice of the security measures to be implemented.

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

In order to have an indicator on the quality of the Information Security Management System in which the security measures will be implemented, TRICK light additionally offers the possibility to measure the maturity of the security environment of the targeted organisation. The maturity of the security environment is measured with the help of a 6 levelled maturity model and adjusts the estimated implementation rate according to the current reached maturity level. Figure 2.9 illustrates the different steps implemented in TRICK light.

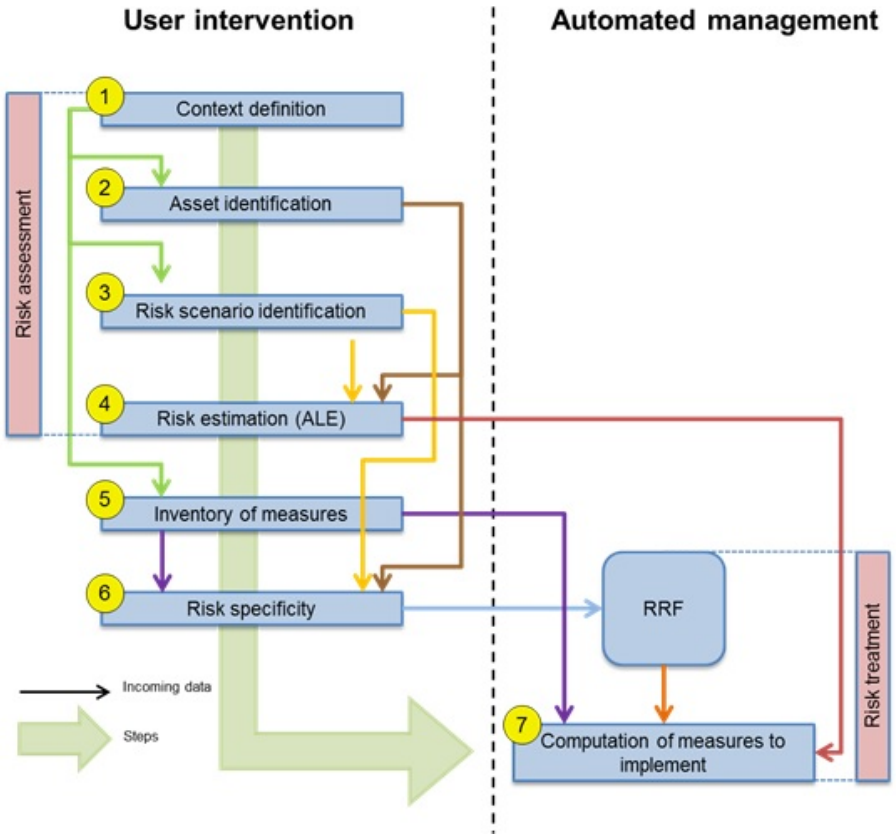

Figure 2.9: TRICK light steps

1. Context definition

The risk assessment starts with the definition of the context of the risk analysis. In this step, information about the type of the studied organisation and its main business processes gets collected. This information will be used in the following steps by the auditor in order to evaluate what are the most important assets regarding the sector of the organisation.

2. Asset identification

This sub step consists of creating an inventory of the organisation assets considered as important for the organisation business. The assets are identified by name and grouped by types. Other information that can be defined is the financial value of the assets and a justification on how this value has been generated.

3. Risk scenario identification

The risk identification is done by analysing the inventory of identified assets and by analysing an inventory of possible threats that could occur on the assets and cause losses. From the list of identified risks, a list of generic risk scenarios will be worked out for a quantitative risk assessment. TRICK light already proposes a predefined list of 8 generic risk scenarios as starting point. Additionally, for

each generic risk scenario the assessor can define the risk specificity (see below for description).

4. Risk estimation
This step allows quantifying possible losses by indicating for each asset/risk scenario the likelihood of occurrence and impact of each risk scenario on each asset. It follows for each asset/risk scenario an Annual Loss Expectancy (ALE). The sum of all ALE's corresponds to the total ALE of the analysed organisation.

5. Inventory of the measures
This step consists of defining for each security measure of the ISO 27002 norm its current implementation rate and the cost required in order to complete the implementation of the measure. This allows determining the security measures already completely implemented and consider only the remaining security measures for the risk treatment plan. It is also possible to exclude some measures which are not relevant regarding the context of the organisation or to consider some measures as mandatory in order to force them to appear at the beginning of the action plan.

6. Risk specificity
The objective of this step is to quantify the risk specificity for the generation of the RRF (Risk Reduction Factor). We apply risk specificity to three elements:

- For each risk scenario, we determine if it specifically relates to confidentiality, integrity or availability, if it is of intentional, accidental or environmental cause, etc.;
- For each security measure, we qualify their influences on every security criteria;
- For assets, we directly define the influence of each security measure on each asset.

The risk specificity step has partially already been performed by the auditors and the developers of the tools and specificity values are freely available for the security measures of the ISO 27001 and the ISO 27002, and the asset type, limited to 10 elements: Service, Information, Software, Hardware, Network, Staff, Immaterial, Business, Financial, and Compliance.

The only elements which require to be defined during a risk analysis are the risk specificity of risk scenarios added by the user and the risk specificity of customised security measures not covered by the ISO 27001 and the ISO 27002.

Risk Reduction Factors (RRF) All previously mentioned security criteria are now used to compute the Risk Reduction Factor (RRF) associated to each triple Asset / Risk-Scenario / Security-Measure. Concretely, by associating these criteria together using a weighted computing, TRICK light determines a global coefficient of the influence of the security measures on the ALE generated by the occurrence of a scenario on an asset.

An RRF is thus a coefficient representing the ALE reduction generated by complete implementation of the security measure.

Return on Security Investment (ROSI) The ROSI is based on the ROI concept, which consists of investing a sum and gaining at least the equivalent, the ideal being to pass the invest sum by a maximal margin.

$$ROI = Return - Investment$$

For example, for €4,000 invested and €10,000 of return, the ROSI would be of €10,000 – €4,000 = €6,000. The reasoning of the ROSI considers the investment made when implementing the security measure: by analogy with the ROI, the cost of the implementation of a measure corresponds to the invested sum and the ΔALE_M corresponds to the gains. Thus, we have the following formula:

$$ROSI_M = \Delta ALE_M - cost_M$$

Example: Considering a risk scenario "Deletion of data" which impacts the "know-how" of an organisation, it results in an ALE which can be estimated at €100,000. The whole implementation of a solution of "data backup" would enable a decrease of the ALE of €75,000 (ΔALE_M). Knowing that the cost of the implementation of this measure of backup is €5,000 ($cost_M$), we have a $ROSI_M$ of €70,000 ($\Delta ALE_M - cost_M$).

Tool(s) :

TRICK light (Tool for Risk management of an ISMS based on a Central Knowledge base) is a risk assessment & management software tool, developed in the VBA Excel environment. TRICK light enables to determine a list of security measures to implement in order to reduce the impact caused by the occurrence of possible incident scenarios.

TRICK light is designed based on three core principles:

- Risk management following the ISO/IEC 27005 standard;
- "Risk Reduction Factor" (RRF) determination which enables to quantify the influence of security measures on the losses caused by threats to assets;
- Cost-effectiveness of security controls; TRICK light considers the Return On Security Investment (ROSI) and derives a prioritised action plan.

Results/output of TRICK light:

- Risk treatment plan: Risk treatment plan, sorted by Phase and Return On Security Investment (ROSI).
- Statement of Applicability: TRICK light provides a documented statement describing the control objectives and controls that are relevant and applicable to the organisation's Information Security Management System.

- Indicators and management view of security status: Charts showing information on Annual Loss Expectancy by threats and by assets.
- Management view of implementation phases: Summary tables and diagrams providing information on the resources that are needed during the different implementation phases of the risk treatment plan and on the profitability of the security controls.
- ISO/IEC 27002 Compliance evolution with risk treatment plan: Chart showing compliance evolution with ISO/IEC 27002 after each implementation phase indicated during risk treatment plan establishment

TRICK service: Web service under development, allowing the same functionalities as the VBA Excel based version. Additional functionalities such as comparing several risk analysis and access to Central Knowledge Base will be included in order to allow a more mature analysis and evolution of information security.

2.2.18 TARA

Owner :

- Intel Corporation.

Country of origin :

- USA.

Targeted organisations :

- Large companies;
- SME.

Method description (Rosenquist, 2009):

TARA (i.e. Threat Agent Risk Assessment) was introduced by the Intel Corporation in 2010 in order to tackle the problem created by the very large number of possible attacks on any given infrastructure.

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

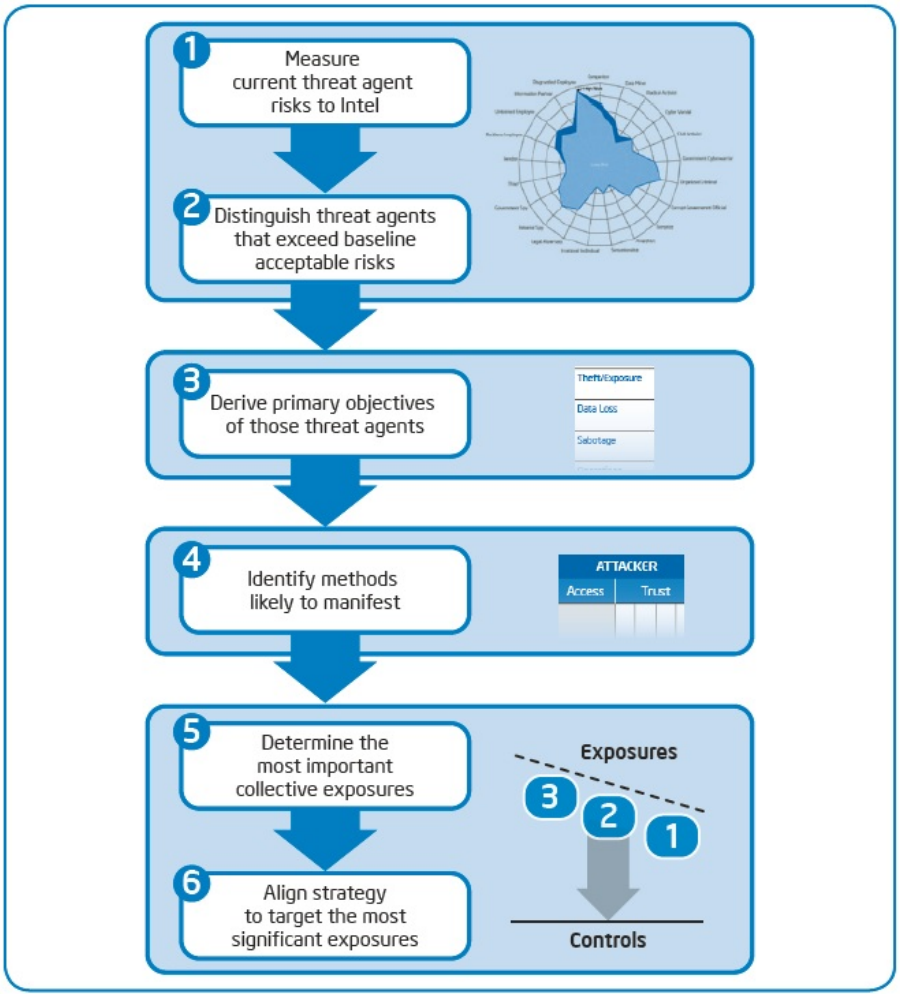

Figure 2.10: Overview of the TARA Risk Assessment process

TARA achieves its purpose by first looking at which attack vectors or methods are more likely for the specific project/infrastructure than the "default" risks. Then this information is cross-referenced with the existing controls in order to identify exposed areas. An overview of the TARA process can be seen in Figure 2.10. More details on the steps follow:

1. Measure current threat agent risks: by using the Threat Agent Library and experts;
2. Distinguish threat agents that exceed baseline acceptable risks: by using Threat Agent Library;
3. Derive primary objectives of those threat agents: using Methods and Objectives library;
4. Identify methods likely to manifest: using Methods and Objective library;

5. Determine the most important collective exposures: using Common Exposures Library;
6. Align strategy to target the most significant exposures: by using previous information to adapt security; strategy and allocation of security resources.

Its strong visualisation techniques enable awareness dissemination amongst stakeholders, and helps reach an acceptable level of residual risk with low resources (Violino, 2010). This makes it less applicable to security-critical systems, but more relevant to large enterprise scenarios, where multiple, diverse stakeholders are involved.

The method puts heavy emphasis on attacker profiles. These are defined in Intel's own Threat Agent Library and classified for simplicity in 22 "archetypes". The methodology also describes how to make use of vulnerability databases, or Common Exposure Libraries, a number of which are available online. Further, the method suggests using a Methods and Objectives Library which links the attacker profiles to common "modus operandi" and objectives. Finally, TARA is a qualitative method and is commonly used in conjunction with other enterprise risk analysis tools, applications or processes.

Tool(s) :

No tool

2.3 Tools not related to a specific risk assessment method

In the following section, we will present several risk assessment tools which do not explicitly support one specific methodology but support different best practices or international standards.

2.3.1 Acuity Stream

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

essential compliance and residual risk summary data (European Network and Information Security Agency, 2013c).
Key functionality:

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

2.3.2 Callio secura 17799

Callio Secura 17799 is a product from Callio technologies. It is a web based tool with database support that let the user implement and certify an information security management system (ISMS). It supports the ISO17799 and ISO 27001 (BS 7799-2) standards and can produce the documents that are needed for certification. Moreover it provides document Management functionality as well as customisation of tool's databases. A trial version is available for evaluation (European Network and Information Security Agency, 2013c).
Key functionality:

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

2.3.3 CCS Risk Manager

2.3.3.1 Description

Control Compliance Suite (CCS) Risk Manager enables security leaders to better understand and communicate risks to the business environment from their IT infrastructure. Risk Manager translates technical issues into risks relevant to business processes, delivers customised views of IT risk for different stakeholders, and helps prioritise remediation efforts based on business criticality rather than technical severity (European Network and Information Security Agency, 2013c).
Key functionality:

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

2.3.4 Countermeasures

CounterMeasures is a proven risk analysis solution that has been applied to address a wide range of risk disciplines including physical security and information security. The software is a scalable web-based program that is usually delivered as a pay-as-you-go web-service. The user standardises the evaluation criteria and using a “tailor-made” assessment checklist, the software provides objective evaluation criteria for determining security posture and/or compliance. CounterMeasures is available in both networked and desktop configurations and can be evaluated through a flash demonstration and a trial version (European Network and Information Security Agency, 2013c).
Key functionality:

- User interface upgrades with offer dynamic and interactive table and chart displays;
- Critical asset rating;

- Threat and hazard characterisation;
- Security control identification;
- Dynamic reports in Excel, PowerPoint, and Word with advanced graphics;
- Risk mitigation tracking;
- Customisable dashboards and views (not all versions).

2.3.5 GxSGSI

GxSGSI is a Risk Management tool, which allows the identification and evaluation of threats, vulnerabilities, and impacts, the calculation of intrinsic and residual risk, the adoption of countermeasures and controls necessary for certification of a Management System of Information Security (ISMS), under ISO 27001 and ISO 27002 (European Network and Information Security Agency, 2013c).
Key functionality:

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

2.3.6 Modulo Risk Manager

The Modulo Risk Manager (Risk Management Solutions, 2013) is a tool which aims to support the risk management process by using leading frameworks such as ISO 27001, COBIT, Sarbanes-Oxley Act, BASEL II, ITIL, and BS 25999.
The included process consists of four steps:

1. Inventory: Collecting organisational assets, business processes and threats;
2. Analyse: Risk analysis;
3. Evaluate: Includes risk evaluation;
4. Treat: Includes risk treatment.

Key characteristics:

- Assets view integrated in the organisation's business processes;
- Integrated analysis of technology, processes, physical environments and people;
- Centralised information on risk analysis, compliance and business continuity;
- Automated generation of reports, graphics and statistics;
- More than 4,000 automatic collectors for a variety of technological assets;

- Knowledge Bases with more than 11,000 controls;
- Access control, audit and encrypted database protection;
- Automatic versioning and knowledge base update;
- Centralised repository of assets;
- Allows risks to be viewed in different ways, as assets, parameters, business components, threats, and others;
- Customisation of parameters, adapting them to the organisation's specific situation;
- Allows the user to produce a score and set of reports for any of the contained standards;
- Live Up-date: feature to download the latest controls, standards and automatic collectors. Modulo's Security Research Lab updates this approximately every two weeks
- Business Continuity Plan: BCP Module integrated in Risk Manager Solution;
- WEB Interview: For remote usage;
- Geo-referenced risk: Risk map with Google Earth;
- PDA use: Use of PDA to remote interview.

2.3.7 MSAT

MSAT (Microsoft Corporation, 2013) is a high level security assessment tool developed by Microsoft which is available for free. It is designed to provide information and recommendations regarding best practices for security within IT infrastructures of SMEs (50-500 employees) and is available for free. MSAT includes 200 questions covering four categories (infrastructure, applications, operations, and people). The questions, answers and recommendations of MSAT come from different sources (ISO/IEC 17799, NIST-800.x, recommendations and prescriptive guidance from the Microsoft Trustworthy Computing Group, etc.).
The procedure of the tool is:

1. Define profile of organisation by answering questions about basic information, infrastructure security, application security, operations security, people security and environment;
2. Create Risk assessment by answering questions about security controls in place;
3. MSAT computes reports based on the given answers. MSAT computes a report summary, a complete report (including a business risk profile and an index based on the security measures in place) and a comparison report in order to compare the results of the assessment with a previous assessment or with assessments realised by other companies in the same sector.

MSAT also calculates a security maturity of the organisation. At the lower-end few security defences are employed and actions are reactive. At the high-end, established and proven processes allow a company to be more proactive, and to respond more efficiently and consistently when needed.

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

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

2.3.8 Proteus

Proteus (Information Security Forum, 2013) is a tool developed for IT Governance, Risk management and Compliance.

Proteus is Web based and scalable so that components of the tool can be disabled or enabled depending on the needs of the organisation.

Supported standards are ISO/IEC 27001, BS 25999 (ISO 22301), ISO 9001, ISO 14001, ISO 20000, BS 10012 and PCI DSS.
Main functionality:

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

- Risk Matrix plotting Risk vs. Business Impact;
- Large number of Graphs, charts, pictures and reports can be customised and published.

2.3.9 RA2 art of risk

RA2 (European Network and Information Security Agency, 2013a) art of risk is a risk assessment tool in accordance with the requirements of the ISO/IEC 27001/BS7799-2 norm. The tool includes the security controls of the ISO/IEC 27002 norm and questionnaires which guarantee the compliance with the standards. RA2 art of risk comes together with the RA2 Information Collection Device which can be installed on places in the organisation where information has to be collected. The collected information can afterwards be imported in the RA2 art of risk. RA2 art of risk can create an archive to store the result of a risk assessment. The stored results can then be used as basis for a next risk assessment.

2.3.10 Real ISMS

Real ISMS (European Network and Information Security Agency, 2013a) is a tool dedicated to support the implementation of the ISO/IEC 27001 norm. The tool also includes, beside other features, risk management comprising risk identification and estimation. The tool can choose by itself appropriate security controls. The tool is able to produce reports such as a risk treatment plan, a risk report, a list of assets by area or process, a list of risks by controls and an efficiency follow-up report.

2.3.11 Resolver Ballot

2.3.11.1 Description

Typically used in a small meeting with a board of directors, audit committee, or with department heads, Resolver Ballot is a group risk assessment application which allows meeting participants to anonymously voice their opinion on the impact and likelihood of risks to their organisation. According to the developer: "Resolver Ballot is an anonymous risk workshop assessment tool that enables groups to make better decisions in less time, with less arguing." As no two risk methodologies are identical Resolver Ballot can easily be configured to use local language, terminology, and criteria scales. Vote results are displayed on-screen real-time analysis providing rare access to all viewpoints on a topic. (European Network and Information Security Agency, 2013c). Although the tool is not dedicated to analysing Information Security Risk, its support for group discussion on Risk Assessment topics makes it useful for any methodology which involves brainstorming meetings.
Main functionality:

- (Remote) anonymous voting on impact, likelihood or any other criteria for each risk (from wireless keypad, mobile phone, or computer);
- Assess control effectiveness;
- In-room or web based voting via computer;
- Focus and facilitate discussions on topics without agreement to share viewpoints and re-vote after discussion to see the change;
- Generation of standard or custom heat maps (e.g. inherent vs. residual risk or Year 1 vs. Year 2);
- Relationship Modelling: identifies and explains relationships between risks: how each key risk impacts others;
- Generates over 15 different commonly used Risk Management and Decision making reports.

2.3.12 RiskSafe Assessment

The RiskSafe Assessment tool (Platinum Squared, 2014) is a cloud-based Software as a Service (SaaS) risk-assessment tool compliant with ISO 27001.
RiskSafe adopts a three-stage approach:

- Asset identification and valuation: Identification of relevant assets, their relation to other assets, their location and the people who support them. The assets are valued in terms of the impact that would result if the they were unavailable, destroyed, disclosed or modified.
- Threat and vulnerability assessment: This stage identifies the likelihood of threats to occur and the vulnerability level of the organisation towards this threat. The tool covers a range of deliberate and accidental threats that may affect information systems. Likelihood of threats is assessed on a five-point scale ranging from "Very low" to "Very high" and levels of vulnerabilities are assessed as "Low", "Medium" or "High". This stage results in computing the level of risk. It determines the level of risk by combining the levels of threat and vulnerability with impact levels determined during the asset valuation stage to produce a qualitative assessment of the risk on a scale between 1 and 7.
- Countermeasure selection and recommendation: The tools includes a countermeasure library of over 2000 countermeasures organised into more than 90 logical groups. RiskSafe Assessment uses the measures of risks determined during the previous stages and compares them against the security level (a threshold level associated with each countermeasure) in order to identify if the risks are sufficiently great to justify the installation of a particular countermeasure. If the risks are sufficiently high, the countermeasure will be recommended. In addition to recording the status of controls, RiskSafe Assessment also allows the resources used to deliver the controls and any required security improvement actions to be recorded.

RiskSafe enables the creation of predefined reports which are generated as spreadsheets.

2.3.13 Riskwatch

RiskWatch for Information Systems & ISO 17799 is a IS Risk Management solution. The tool conducts automated risk analysis and vulnerability assessments of information systems. The knowledge databases that are provided along with the product are completely customisable by the user, including the ability to create new asset categories, threat categories, vulnerability categories, safeguards, question categories, and question sets. The tool includes controls from the ISO 17799 and US-NIST 800-26 standards. RiskWatch provides an online demonstration of the product (European Network and Information Security Agency, 2013c). It is one of the most comprehensive (and expensive) RA tools available.
Main functionality:

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

2.3.14 verinice

Verenice (SerNet Gmbh., 2013) is an open source ISMS tool which can be freely downloaded. verinice is compliant with several standards like ISO/IEC 27001, IT-Grundschutz and Information Security Assessment of the German automotive association VDA (German Association of the Automotive Industry – German: "Verband der Atomobilindustrie"). verinice is a java application based on Eclipse which provides as special feature a maturity model in order to ensure the quality of the management system. There is also a paid version: verinice.PRO. It is an additional application server for the verinice client. This server module collaborates with the client to give you a complete three-tier architecture. The verinice.PRO server acts as a central IS repository in your network, allowing you to work collaboratively on your ISMS or audits. You can assign tasks, use email notifications and a web-frontend to get feedback on completed tasks, create a central storage for policies

and other documents and much more.
Key functionality:

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

2.3.15 vsRisk

vsRisk (Vigilant Software, 2013) is an ISO/IEC 27001:2005 compliant qualitative risk assessment tool. Besides this, the tool also supports ISO/IEC 27002, ISO/IEC 27005 and NIST SP 800-30, complies with BS7799-3:2006 and UK's Risk Assessment Standard and conforms to ISO/IEC TR 13335-3:1998 and NIST SP 800-30.
Key features of the tool are:

- Capturing information security policy, objectives and ISMS scope;
- Assessing attributes on Confidentiality, Integrity, and Availability, in relation to Business, Legal, Contractual;
- Built-in Audit Trail and comparative history;
- Reporting;
- Wizard-based approach to simplify and accelerate the RA process;
- Asset-by-asset identification of threats, vulnerabilities ;
- Specific process for identification and assistance in the implementation of ISO/IEC 27001 controls as well as the ability to import additional controls;
- Constantly updated threat and vulnerability databases;
- Customisable risk acceptance criteria and management scales;
- Helps define scope and business requirements, policy, objectives and asset inventory of the ISMS;
- Gap analysis versus ISO/IEC standards;
- Import and export of asset information.

3 Mapping TRESPASS to established methods

In this chapter, the TRESPASS approach will be compared to the established Risk Assessment methodologies covered in the previous sections. This comparison will include a contrasting of concepts traditionally involved in Risk Assessment to the way these concepts are defined within TRESPASS as well as as a comparison of the expected TRESPASS workflow to established Risk Assessment methods.

3.1 Conceptual mapping

The following section presents the current state of the Security model being designed within the TRESPASS project while attempting to distil an overview of common conceptual models described or implied by established Risk Assessment methodologies and framework. It then outlines a mapping of the elements of the model developed in Work Package 1 to core elements found in these other frameworks. Further, model properties that cannot be mapped will be discussed.

3.1.1 The TRESPASS Information Security conceptual model

The TRESPASS modelling formalism - developed as part of Work Package 1 - is under continuous improvement throughout the duration of the project. As such, we base the discussion in this section on the most recent snapshot of this model, as described in Deliverable D1.3.1: Initial prototype of the social-technical security model (The TRESPASS Project, D1.3.1, 2013).

The WP1 model currently represents an organisation's infrastructure in the form of a directed graph. Nodes represent locations of interest: rooms, access control points, and others. Edges are used to represent connected locations, which can belong to different domains such as building or network. These domains limit where actors can move and where processes can take place: human actors are restricted to room nodes, computer processes are restricted to network nodes.

For reference, the main concepts defined in D1.3.1 are included below and their interrelationships are showcased in Figure 3.1:

Actors are represented by process nodes, which model all entities that execute a process and may move in the infrastructure. Each actor has an individually defined behaviour, or belongs to a class with a shared behaviour. Actors can share roles, that can be used in policies.

Assets are represented by nodes that can be attached to locations or to actors. Assets attached to actors move around with the actor. Assets model any kind of data that is relevant in the modelled organisation. Assets can be annotated with a value and with a metric that, e.g., could represent how likely it is to lose the data.

Actions are performed by actors or applied to actors. Actions have a target they are performed on. Actions can be logged or unlogged.

Policies are used in the TRE$_S$PASS model in a rather broad sense; they represent both regulation of access to locations and data, and the behaviour as expected by an organisation from its employees. Policies consist of required credentials and enabled actions, representing what an actor needs to provide in order to enable the actions in a policy, and what actions are enabled if an actor provides the required credentials, respectively. Each policy can consist of several pairs of this kind. Credentials can be a location the actor needs to be at, an identity the actor needs to have, or data the actor needs to possess. Each enabled action in a policy can have some (optional) metric attached. Metrics are discussed in the following section.

Locations describe the physical and digital infrastructure of an organisation. They are drawn as nodes in the model and can represent physical containers (such as buildings or rooms), digital containers (such as networks or servers) or access control points (such as doors or terminals). Locations can fall in different domains, such as physical or network. Domains are used to limit where processes can move; human actors are restricted to physical nodes, computer processes are restricted to network nodes.

3.1.2 Existing Information Security conceptual models

Since it would be unreasonable to compare the (initial) TRE$_S$PASS WP1 model to every method described in this deliverable, we attempt to distil an "integrated" conceptual model of Risk that encompasses the most well-known Risk Assessment frameworks.

This was achieved by first selecting a subset of Risk Assessment frameworks and standards that at least one of the methods and/or tools described in this Deliverable are compatible with. Furthermore, only frameworks that explicitly define and decompose Risk, as well as suggest either a taxonomy of factors or a formula for computing Risk based on these factors are selected. Finally, the subset is further trimmed for mutual diversity. The selection and analysis process is based on Chapter 3 of the Master Thesis by Ionita (2013).

The selected frameworks are:

- FAIR (Jones, 2005) & The Open Group Risk Taxonomy (The Open Group, 2009b);

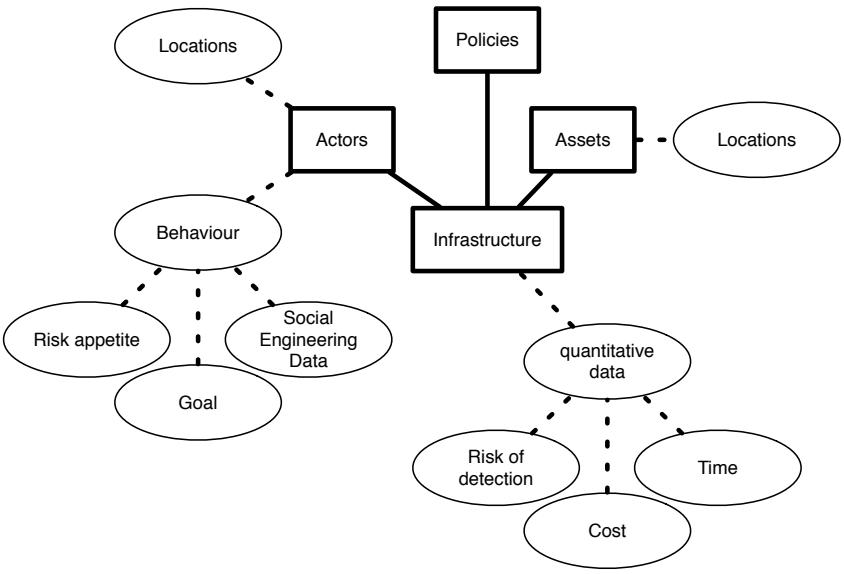

Figure 3.1: The structure of the first version of the TRE$_S$PASS model. The boxes represent the main components, the ovals properties of the components. The most noteworthy parts are the explicit behaviour component and the quantitative data, that extend the core consisting of infrastructure, assets, policies, and actors. Each actor has a separate behaviour that is queried whenever the analysis or simulation needs to perform an action. The data associated with the behaviour then determine, which action will be performed. The *goal* describes, which mode the actor is in, *e.g.*, minimising risk of detection or time for actions. Both actors and assets are associated with locations that describe where they are located in the model.

- ISO 13335-1 (*Information technology – Security techniques – Management of information and communications technology security – Part 1: Concepts and models for information and communications technology security management*, 2001);
- Structured Risk Assessment (McEvoy & Andrew, 2002);
- Microsoft Threat Model (Meier et al., 2010);
- OWASP Risk Rating Methodology (The Open Web Application Security Project Foundation, 2008, Chapter 5).

Across all the methodologies and tools discussed in this Deliverable, a few fundamental concepts are reoccurring. All RA/RM frameworks seem to include the concepts of a Threat (be-it an agent/attacker, an environmental factor, or simply something that can go wrong), Asset (as a possible target for attacks, that provides value either for the organisation or attackers), Vulnerability (as either as missing controls, a weakness of the system or an attack path) and of course the actual Attack (which is often results from a combination of the previous three) (Ionita, 2013).

Variations in naming are common, as can be seen in Table 4 (found in Annex3.3). Slight differences also exist in how the causal relationships between risk factors are defined and in the formulas used to compute Risk. Despite these differences, the following definitions can be assumed to be consistent with the five frameworks discussed in this Chapter (Ionita, 2013):

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

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

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

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

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

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

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

- It is usually classified into multiple *Types* by various methodologies (see 6th row in Table 4). There are also "multi-step attacks" possible, comprised of multiple attacks, each with its own attributes.
- Another variable usually associated with this entity are the *Threat Capability* (sometimes referred to as TCap) which reflects the skills and resources that the Threat has available for each Attack. It is sometimes regarded as a variable of the Threat

- Most taxonomies usually discuss the *Defense Strength* which is usually related to the existing controls and security policy. The same discussion applies here: while it may be intuitive to see Defence Strength as an attribute of the Asset, it is also an attribute of Attack as each Asset can have different security controls against various attack vectors and threats or multiple controls that mitigate different vulnerabilities.
- The *Frequency* of the attack usually refers to the number of attacks estimated to be attempted by the Threat in a given time-frame.
- The *Loss Type* and *Loss Magnitude* are variables usually included in the estimation of the impact or consequences that a successful attack might have on an organisation and are present in all reviewed Risk taxonomies. They are also attributes of the Attack entity as the amount and type of damage that a compromise of a certain asset can bring about is dependent on the type of attack and the goals of the threat. For example, an attacker (i.e., threat) reading some private employee accounts in order to send them spam has a considerably lower impact than a hacker who launches a Denial of Service against the same records causing employees to lose access to their accounts and leading to significant drops in productivity and maybe even reputation.

Figure 3.2 shows these core entities, the relationships between them and possible attributes. Furthermore, the occurrence rate of each attribute across the selected sub-set of 5 frameworks is shown by color-codes. We will refer to the Entity Relationship diagram below an *"Integrated model" of Risk*.

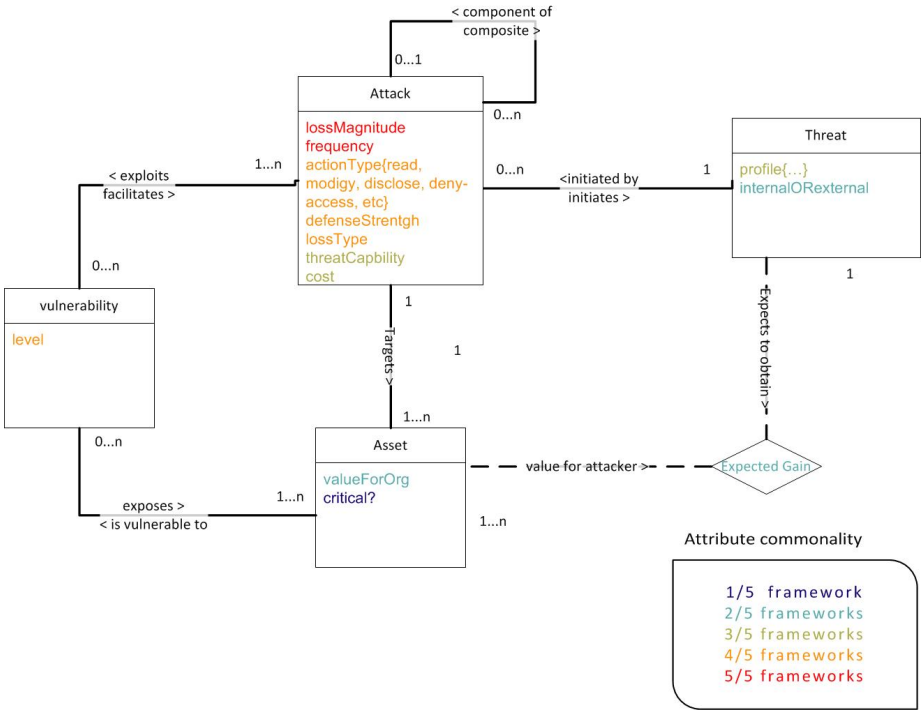

Figure 3.2: Common concepts in established Risk Assessment frameworks

3.1.3 Mapping of concepts

This sub-section maps elements of the TRE$_S$PASS model to elements of existing, established risk assessment methods.

Actors(TRE$_S$PASS) vs. Threats(established) While most Risk Assessment frameworks only discuss malicious actors, the TRE$_S$PASS model makes use of a much broader scope of actors. These can be humans (employees, users and even external persons of interest) and also processes that represent, for example, computer viruses.

Similar to previous RA methodologies, TRE$_S$PASS considers a threat or an attacker to have a *profile* that describes its distinctive features. A profile normally defines a group of attackers with similar goals and capabilities. TRE$_S$PASS is, therefore, agnostic with respect to whether an attacker is external or internal (outsider or insider) to the organisation.

Assets(TRE$_S$PASS) vs. Assets(established) There is no significant difference in the way the TRE$_S$PASS model sees assets and how other established frameworks and standards define them. They can be physical, digital or abstract (e.g., knowledge).

Assets can be also decorated with attribute values such as impact and reward. This values are expected to be used in TRE$_S$PASS by quantification methods in order to rank attacks and countermeasures. For example, if the cost of the attack is higher than the reward, that attack might be considered impractical. Similarly, if the monetary impact is significantly lower than the cost of a countermeasure, that countermeasure can be discarded.

Actions(TRE$_S$PASS) vs. Attacks(established) Again, the TRE$_S$PASS model refers to a much broader range of possible actions, whereas traditional Risk models only discuss malicious or potentially damaging ones. Attacks are actions which are either break an organisational or access policy, actions which are damaging to the organisation or actions that are conducted with one of these two goals in mind. This is related to the fact that TRE$_S$PASS models also include non-malicious actors (such as employees, users or customers) which may perform a multitude of non-damaging or even desire-able of actions or activities.

Vulnerability(TRE$_S$PASS) vs. Vulnerability(established) A vulnerability in TRE$_S$PASS, as in other RA methodologies, is a weakness in the system that can be exploited by an attacker. TRE$_S$PASS will contain a built-in database of known attack patterns that is hidden from the user during the modelling phase. These attack patterns contain implicit knowledge of technical, digital, social and even hybrid vulnerabilities and it is only taken into consideration by the software tool when the model is executed in order to generate the attack vectors. As such, the concept of a vulnerability is not explicitly included in the model, or even visible to the users. This is indeed one of the innovative features of the TRE$_S$PASS approach: complete separation of aspects related to the organisation (assets, actors, infrastructure and policies) from elements describing risks (vulnerabilities, threat agents, attacks). The two disjoint

sets of concepts and their relevant parameters are taken combined only when the analysis is ran within the software tool.

TRESPASS, however, does not only rely on known vulnerabilities, it also aims at discovering new and unknown vulnerabilities. This is achieved in TRESPASS by means of policy invalidation (Kammüller & Probst, 2013).

Policies (TRESPASS), are not commonly encountered in other Risk Assessment frameworks. Some methodologies do describe policies but in a much more restricted sense. Since actors can be both in the social and in the digital domain, policies can be used in the TRESPASS model to represent expected behaviour as well as access rights. This is a novel addition and, while it does introduce some ambiguity to the term, it also greatly enhances the flexibility and capabilities of the language.

3.2 Methods mapping

This sub-section shortly compares established Risk Assessment methods with the expectations of the TRESPASS project.

As detailed in Section 2, most risk assessment methods and frameworks, such as Standards New Zealand (2009); Jones (2005); Peltier (2000); BSI (2013), consist of high-level guidelines to be executed by security experts. These approaches, named *rule-based* by Houmb (2007), make use of brainstorming and regular meeting with stakeholders in order to move through the different stages of the risk assessment process. For example, four out of eight steps in the CORAS method (2013) are simply devoted to defining and reaching consensus among all stakeholders regarding the target, context and goals of the assessment.

Amongst the risk assessment methods studied, rule-based methods require less time to come up with a conclusive result, which makes them particularly useful for auditing and certification. For instance, performing risk analysis with the FRAP method (Peltier, 2000) is expected to take roughly 4 hours and no more that 15 people in most organisations (Ionita, 2013). Due to lack of low-level technical details, rule-based methods are normally suitable to be adopted by standards, such as the ISO/IEC 27002:2005 and the ISO 27005, and thus they reach a broader audience.

However, rule-base methods may fall short in the analysis of complex organisations and critical systems. Given that their processes are mostly based on human intervention, they just overlook those attacks that none of the security experts could imagine. Moreover, the process needs to be restarted from scratch whenever the organisation changes or new attacks appear, which is expensive and time consuming for large organisations.

The TRESPASS project aims at extending established rule-based methods with an analytical approach to predict, prioritise, and prevent complex attacks. In this sense, the TRESPASS method falls in the category of risk-based methods according to Houmb (2007). TRESPASS will thus be integrated into established standards and methodologies, such as (CORAS, 2013), adding powerful analytic capabilities in which vulnerabilities and countermeasures can be analysed across different attack scenarios.

There already exist methodologies with analytic capabilities, though. For example, CRAMM (Siemens, 2011) attempts a qualitative, asset-centric approach, making use of 10 predefined asset tables and a database with over 3000 ranked security controls. A dedicated tool provided automatically returns possible countermeasures given identified assets, and likely threats and vulnerabilities. A similar methodology, based on risk knowledge base, was designed in France and named the “Methode Harmonisee d’Analyse de Risques” (MEHARI).

The TRE$_S$PASS method also makes use of databases of common vulnerabilities and threats so as to assist security experts and refine results. In particular, a preliminary design of an Attack Pattern Library (APL) has been proposed in the deliverable (The TRE$_S$PASS Project, D5.3.1, 2013). The APL contains those meaningful attacks, threats, and vulnerabilities, that cannot be explicitly represented in the WP1 model. In this way, the WP1 model focuses on modelling the physical and socio-technical aspects of an organisation, and links to the APL in order to automatically generate detailed attacks (The TRE$_S$PASS Project, D1.3.1, 2013; Kammuller & Probst, 2013).

The automatic generation of attacks is, indeed, an improvement of the TRE$_S$PASS method with respect to previous methodologies. It allows a proactive security assessment by predicting how changes to the model impact on the attack attributes, such as likelihood and cost. An analogy that helps to understand the advantages of a model-based approach, such as TRE$_S$PASS, over table-based approaches, such as SRA (McEvoy & Andrew, 2002), is the boom of Cartography in the current society realised by, for example, Google Maps and Waze. Creating and maintaining good maps is cumbersome, yet it has been proven to be fully rewarding.

3.3 Discussion

Most conceptual differences between the "Integrated model" and the WP1 model can be traced back to the slightly wider scope of the TRE$_S$PASS project: it aims at modelling entire organisations, together will all relevant factors that might facilitate, influence or give an indication of potential Risks; the conceptual models found in most RA frameworks however, are designed to only support reasoning about the Risks themselves and their decomposition or quantification. As such, the "Integrated Model" (and all conceptual models it incorporates) is a model of Risk, while the WP1 model is an organisational model.

All in all, despite the slightly different scope of the two conceptual models, many parallels could be drawn. All concepts and factors commonly used to analyse Risk in established methodologies, tools, standards and frameworks are also found in the TRE$_S$PASS approach. Even more so, it seems that most established conceptual models of Risk can be viewed as sub-sets of the TRE$_S$PASS WP1 model. This reveals, on the one hand, the ambitious nature of the project and on the other hand, an increase in the quantity and quality of factors that need to be taken into consideration when discussing Information Security Risk.

From a process point of view, TRE$_S$PASS is therefore designed to overcome shortcomings presented in previous methodologies, such as CORAS, where the models (based on UML) are troublesome to maintain and not well-suited for discovering unknown attacks. Furthermore, the project extends traditional rule-based methodologies with analytic capabilities in order to achieve automatic generation of attacks based on several (crowd-sourced) knowledge bases so as to also allow proactive security. Finally, and similar to Threat Agent Risk Assessment (TARA) methodology, TRE$_S$PASS aims to provide strong visualisation techniques enabling awareness dissemination amongst stakeholders, and helping to reach acceptable level of risk with low resources.

References

Agence national de la sécurité des systèmes d'information. (2010). *Expression des besoins et identification des objectifs de sécurité* (Tech. Rep.). Paris.

Alberts, C., & Dorofee, A. (2001). *Octave method implementation guide version 2.0 - volume 1: Introduction* (Tech. Rep.). Pittsburgh: Software Engineering Institute (SEI).

BSI, G. (2013). *Bsi standards 100-1, 100-2, 100-3, 100-4.* https://www.bsi.bund.de/EN/Publications/BSIStandards/standards.html.

Bundeskanzleramt Österreich. (2013). *Österreichisches Informationssicherheitshandbuch* (Tech. Rep.). Wien.

CLUSIF. (2010). *Mehari 2010 - risk analysis and treatment guide* (Tech. Rep.). Paris.

Coles-Kemp, L., & Overill, R. E. (2007). On the role of the facilitator in information security risk assessment. *Journal in Computer Virology*, 143-148.

CORAS. (2013, July). *The coras method.* http://coras.sourceforge.net/.

European Network and Information Security Agency. (2013a, February). *Inventory of risk management / risk assessment methods.* http://rm-inv.enisa.europa.eu/methods.

European Network and Information Security Agency. (2013b, February). *Inventory of risk management / risk assessment methods.* http://rm-inv.enisa.europa.eu/methods.

European Network and Information Security Agency. (2013c, February). *Inventory of risk management / risk assessment tools.* http://rm-inv.enisa.europa.eu/tools.

Fetler, B. (2012). *Security maturity, uncertainty estimation and performance measurement for the risk management tool trick light*. Unpublished master's thesis, Reutlingen University, Reutlingen.

Harpes, C., Adeslbach, A., Zatti, S., & Peccia, N. (2007). Quantitative assessment with isamm on esa's operations data system. *The 4th ESA International Work-shop on Tracking*.

Houmb, S. (2007). *Decision support for choice of security solution: The aspect-oriented risk driven development (AORDD) framework*. Unpublished doctoral dissertation, Norwegian University of Science and Technology, Trondheim. Retrieved from http://doc.utwente.nl/67423/

Information Security Forum. (2013, June). *Isf tools and methodologies.* https://www.securityforum.org/tools/.

Information technology – Security techniques – Management of information and communications technology security – Part 1: Concepts and models for information and communications technology security management (Norm No. ISO 13335-1:2004). (2001). ISO, Geneva, Switzerland.

Ionita, D. (2013). *Current established risk assessment methodologies and tools*. Unpublished master's thesis, Twente University, Enschede.

ISO, Geneva, Switzerland. (2009). *Risk management – Principles and guidelines* (Standard No. ISO 31000:2009).

ISO, Geneva, Switzerland. (2011). *Information technology – Security techniques – Information security risk management* (Standard No. ISO 27005:2011).

ISO, Geneva, Switzerland. (2013). *Risk management – Guidance for the implementation of ISO 31000* (Standard No. ISO 31004:2013).

itrust consulting s. à r. l. (2013). *Trick light - user guide* (Tech. Rep.). Niederanven.

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

Kammüller, F., & Probst, C. W. (2013). Invalidating policies using structural information. In *IEEE Symposium on Security and Privacy Workshops* (p. 76-81).

Kammuller, F., & Probst, C. W. (2013). Invalidating policies using structural information. *2013 IEEE Security and Privacy Workshops*, *0*, 76-81. doi: http://doi.ieeecomputersociety.org/10.1109/SPW.2013.36

Kordy, B., Kordy, P., Mauw, S., & Schweitzer, P. (2013). Adtool: Security analysis with attack–defense trees. In K. Joshi, M. Siegle, M. Stoelinga, & P. D'Argenio (Eds.), *Quantitative Evaluation of Systems* (Vol. 8054, p. 173-176). Springer Berlin Heidelberg. Retrieved from http://dx.doi.org/10.1007/978-3-642-40196-1_15 doi: 10.1007/978-3-642-40196-1_15

Kordy, B., Mauw, S., Radomirović, S., & Schweitzer, P. (2011). Foundations of attack–defense trees. In P. Degano, S. Etalle, & J. Guttman (Eds.), *Formal Aspects of Security and Trust* (Vol. 6561, p. 80-95). Springer Berlin Heidelberg. Retrieved from http://dx.doi.org/10.1007/978-3-642-19751-2_6 doi: 10.1007/978-3-642-19751-2_6

Kordy, B., Mauw, S., Radomirović, S., & Schweitzer, P. (2012). Attack-defense trees. *Journal of Logic and Computation*, exs029.

Kordy, B., Pouly, M., & Schweitzer, P. (2012). Computational aspects of attack–defense trees. In P. Bouvry, M. Kłopotek, F. Leprévost, M. Marciniak, A. Mykowiecka, & H. Rybiński (Eds.), *Security and Intelligent Information Systems* (Vol. 7053, p. 103-116). Springer Berlin Heidelberg. Retrieved from http://dx.doi.org/10.1007/978-3-642-25261-7_8 doi: 10.1007/978-3-642-25261-7_8

Kouns, J., & Minoli, D. (2010). *Information technology risk management in enterprise environments*. New Jersey: Wiley.

LLC, R. M. I. (2010). *Fairlite high-level description*. Author. http://riskmanagementinsight.com/wp-content/uploads/2010/09/FAIRLite-Description-v2.pdf.

Lund, M. S., Solhaug, B., & Stolen, K. (2011). *Model driven risk analysis - the CORAS approach*. Heidelberg: Springer-Verlag.

Mañas, D. J. A. (2012). *EAR / PILAR Environment for the Analysis of Risk.* http://www.pilar-tools.com/en/index.html.

Mauw, S., & Oostdijk, M. (2005). Foundations of attack trees. In (p. 186-198). LNCS, vol. 3935, Springer.

McEvoy, N. A., & Andrew, W. (2002). Structured risk analysis. In (p. 88-103). London: Springer-Verlag.

Meier, J., Mackman, A., Dunner, M., Vasireddy, S., Escamilla, R., & Murukan, A. (2010). *Improving web application security: Threats and countermeasures.* http://msdn.microsoft.com/en-us/library/ff649874.aspx. Microsoft Corporation.

Microsoft Corporation. (2013). *Microsoft security assessment tool.* http://www.microsoft.com/fr-fr/download/details.aspx?id=12273.

Ministerio de Administraciones Publicas. (2006). *Magerit - version 2 - methodology for information systems risk analysis and management* (Tech. Rep.). Madrid.

National Institute of Standards and Technology. (2011). *Managing information security risk - oganization, mission, and information system view* (Tech. Rep.). Gaithersburg.

Peltier, T. R. (2000). Facilitated risk analysis process (frap). In A. Publications (Ed.), *80 data security management.* New York: CRC Press LLC.

Peltier, T. R. (2005). *Information security risk analysis*. New York: Taylor & Francis.

Platinum Squared. (2014). *Risksafe assessment.* http://www.risksafe.co.uk.

Risk Management Insight LLC. (2006). *FAIR (factor analysis of information risk) basic risk assessment guide*. Risk Management Insight LLC. http://www.riskmanagementinsight.com/media/docs/FAIR_brag.pdf.

Risk Management Solutions. (2013). *Modulo - solutions for GRC.* http://www.modulo.com/risk-management.

Rosenquist, M. (2009, December). *Prioritizing information security risks with threat agent risk assessment.* "http://www.communities.intel.com/servlet/JiveServlet/download/4693-1-3205/Prioritizing_Info_Security_Risks_with_TARA.pdf". Intel Corporation.

Schneier, B. (1999). Attack trees. *Dr. Dobb's Journal of Software Tools 24(12)*, 21-29.

SerNet Gmbh. (2013). *Verinice.* http://www.verinice.org/.

Siemens. (2011). *Cramm - the total information security toolkit.* http://www.cramm.com.

Standards New Zealand. (2009). *Risk management - principles and guidelines* (AS/NZS 31000:2009 ed.). Standards Australia International and Standards New Zealand. Retrieved from http://sherq.org/31000.pdf

Task Group IST-049. (2008, September). *Improving common security risk analysis* (Tech. Rep. No. RTO-TR-IST-049). NATO Science and Technology Organization. Retrieved from http://citeseerx.ist.psu.edu/viewdoc/download?rep=rep1&type=pdf&doi=10.1.1.215.1106

The Open Group. (2009a). *Technical standard to risk taxonomy* (Tech. Rep.).

The Open Group. (2009b). *Technical Standard to Risk Taxonomy* (No. C081). http://pubs.opengroup.org/onlinepubs/9699919899/toc.pdf, accessed on 16.03.2013.

The Open Web Application Security Project Foundation. (2008, November). *Owasp testing guide v3.* https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology, accessed on 9.06.2013.

The TRE$_S$PASS Project, D1.3.1. (2013). *Initial prototype of the socio-technical security model.* (Deliverable D1.3.1)

The TRE$_S$PASS Project, D5.3.1. (2013). *Abstraction levels for model sharing.* (Deliverable D5.3.1)

Vigilant Software. (2013). *Vigilant software.* http://www.vigilantsoftware.co.uk/.

Violino, B. (2010, May). *It risk assessment frameworks: real-world experience.* http://www.csoonline.com/article/592525/it-risk-assessment-frameworks-real-world-experience. CXO Media Inc.

Appendix A - Inventory of risk assessment methods

Method name	Owner	Country of origin	Target organisations
AS/NZ 4360	Standards Australia International and Standards New Zealand	Australia/New Zealand	Government agencies, Large companies, SME
AU IT Security Handbook (V.2.3, April 2007)	Austrian federal chancellery http://www.digitales.oesterreich.gv.at/site/5261/default.aspx#o19389	Austria	Government agencies, Large companies, SME
CORAS	EU-funded project (IST-2000-25031) January 2001 – June 2003 http://coras.sourceforge.net/	Norway	
CRAMM	Insight Consulting http://www.cramm.com	United Kingdom	Government agencies, Large companies
Dutch A&K Analysis	Dutch Ministry of Internal Affairs	Netherlands	Government agencies, Large companies, SME
EBIOS 2010 (25 January 2010)	Agence nationale de la Sécurité des Systèmes d'Information (ANSSI) http://www.ssi.gouv.fr/ebios	France	Government agencies, Large companies, SME
FAIR	Risk Management Insight LLC http://www.riskmanagementinsight.com/media/docs/FAIR_brag.pdf	USA	Government agencies, Large companies, SME
FRAP	Peltier and Associates LLC http://www.ittoday.info/AIMS/DSM/85-01-21.pdf	USA	SME

Continues on the next page...

Method name	Owner	Country of origin	Target organisations
ISAMM	Telindus N.V. http://rm-inv.enisa.europa.eu/methods_tools/t_isamm.html	Belgium	Government agencies, Large companies, SME
ISF	Methods Information Security Forum (ISF) https://www.securityforum.org/whatwedo/publictools/	International ISF Members	Government agencies, Large companies
ISO/IEC 27005 (2011)	International Organisation for Standardisation http://www.iso.org/	International (place of business in Switzerland)	
IT Grundschutz	Federal Office for Information Security (BSI) http://www.bsi.de/gshb/	Germany	Government agencies, Large companies, SME
MAGERIT V2 (2005)	Spanish Ministry for Public Administrations http://administracionelectronica.gob.es/?_nfpb=true&_pageLabel=PAE_PG_CTT_Area_Descargas&langPae=es&iniciativa=184	Spain	Government agencies, Large companies, SME
MARION 1998 (not maintained anymore)	CLUSIF	France	Large companies
MEHARI (2010)	CLUSIF https://www.clusif.asso.fr/	France	Government agencies, Medium to Large companies, Commercial companies Non-profit: NGOs, education, health sector, public services, etc.
MIGRA	AMTEC/Elsag Datamat S.p.A.	Italy	Government agencies, Large companies

Continues on the next page...

Method name	Owner	Country of origin	Target organisations
NIST Special Publication 800-30 Revision 1 (September 2011) DRAFT	National Institute for Standards and Technology (NIST) http://csrc.nist.gov/publications/drafts/800-30-rev1/SP800-30-Rev1-ipd.pdf	USA	Government agencies, Large companies, SME
NIST Special Publication 800-39 (March 2011)	National Institute for Standards and Technology (NIST) http://csrc.nist.gov/publications/nistpubs/800-39/SP800-39-final.pdf	USA	Government agencies, Large companies, SME
OCTAVE (Version 2.0, January 2005)	Carnegie Mellon University, SEI (Software Engineering Institute) http://www.cert.org/octave/octavemethod.html	USA	Large companies
Structured Risk Analysis	Consult Hyperion http://www.chyp.com	United Kingdom	SME
TARA	Intel Corporation https://communities.intel.com/docs/DOC-4693	USA	Large companies, SME
TRICK light	itrust consulting s.à r.l. http://www.itrust.lu	Luxembourg	SME

Table 1: Inventory of Risk Assessment methods

Appendix B - Inventory of risk assessment tools

Product name	Owner	Country of origin	Target organisations
Acuity Stream	Acuity Risk Management LLP http://www.acuityrm.com/	United Kingdom	Government agencies, Large scale companies, SME
CALLIO SECURA (V.2.10)	Callio technologies http://www.callio.com/secura.php	Canada	Government agencies, Large scale companies, SME
Cobra (Under redevelopment)	C&A Systems Security http://www.riskworld.net/	United Kingdom	SME
CORAS tool	EU-funded project (IST-2000-25031) http://coras.sourceforge.net/	No information	No information
Countermeasures	Alion http://www.countermeasures.com/	USA	Government agencies, Large scale companies
CRAMM (V.5.2)	Siemens Enterprise Communications Limited http://www.cramm.com	United Kingdom	Government agencies, Large scale companies SME
EAR / PILAR (V.5)	A.L.H. J. Mañas http://www.ar-tools.com/en/index.html	Spain	Government agencies, Large scale companies, SME
EBIOS 2010 (25 January 2010)	Central Information Systems Security Division http://www.ssi.gouv.fr/ebios	France	Government agencies, Large scale companies, SME

Continues on the next page...

Product name	Owner	Country of origin	Target organisations
EasyRisk Manager	Det Norske Veritas (DNV) http://www.easyrisk.no	Norway	No information
GSTOOL (V.4.7 - December 2009)	Federal Office for Information Security (BSI) http://www.bsi.bund.de/gstool	Germany	Government agencies, Large scale companies, SME
GxSGSI	SIGEA http://www.sigea.es/articulos/57-the-project/114-gxsgsi.html	Spain	Government agencies, Large scale companies, SME
ISAMM tool	Telindus N.V.	Belgium	No information
Mehari 2010 basic tool	CLUSIF http://www.clusif.asso.fr/	France	Government agencies, Large scale companies
MIGRA Tool	AMTEC/Elsag Datamat S.p.A	Italy	Government agencies, Large scale companies
Modulo Risk Manager (V.7.2)	Modulo Security http://www.modulo.com/risk-manager	Brazil	Government agencies, Large scale companies, SME
MSAT	Microsoft http://technet.microsoft.com/en-us/security/cc185712	USA	SME
Octave Tools	Security Risk Solutions Inc http://www.securityrisksolutions.com/OCTAVE_tools.htm	USA	Government agencies, Large scale companies, SME
opus i ISO 27001 ISMS	kronsoft e.K. http://www.kronsoft.de/	Germany	No information
Proteus	Infogov (Information Governance Limited) http://www.infogov.co.uk/solutions/proteus	United Kingdom	Government agencies, Large scale companies, SME

Continues on the next page...

Product name	Owner	Country of origin	Target organisations
Real ISMS	Realiso http://www.realiso.com/en/index_isms.html	Brazil	Government agencies, Large scale companies, SME
Resolver Ballot	Resolver http://www.bpsresolver.com/applications/resolver_ballot/	Canada	Government agencies, Large scale companies, SME
Risicare (V.2010)	BUC S.A. http://www.risicare.fr/	France	Governmental and regional agencies, Large scale companies
RiskWatch for Information Systems & ISO 17799	RiskWatch http://www.riskwatch.com/index.php/information-systems	USA	Government agencies, Large scale companies, SME
Risk Management Studio (V.4.0.1 – 10 February 2012)	Stiki – Information Security http://www.riskmanagementstudio.com/	Iceland	Government agencies, Large scale companies, SME
TRICK light	itrust consulting s.à r.l. http://www.itrust.lu	Luxembourg	SME
verinice (1.5.0)	SerNet GmbH http://www.verinice.org/	Germany	Government agencies, Large scale companies, SME
vsRisk	Vigilant Software http://www.vigilantsoftware.co.uk/	United Kingdom	No information

Table 2: Inventory of Risk Assessment tools

Appendix C - Comparison of risk assessment tools

Tool	Integrated methods and standards	Risk methodology	Report generation	Comparison of two risk assessments possible	Risk management supported (Assessment, Treatment, Acceptance)	Risk analysis supported (Identification, Analysis, Evaluation)	Cost
CORAS tool	CORAS	Qualitative	No	No	Yes	Yes	Free
CRAMM tool	BS 7799 ISO 27001 CRAMM	Qualitative	Yes	Yes	Yes	Yes	2000€(Basic) 4400€(Expert)
EAR/PILAR	ISO 27002 SP800-53 MAGERIT	Quantitative & Qualitative	Yes	/	Yes	Yes	1500€
EBIOS 2010	EBIOS ISO 31000 ISO 27001 ISO 27002 ISO 27005	Qualitative	Yes	/	Yes	Yes	Free
GSTOOL	IT-Grundschutz ISO 27001	Qualitative	Yes	/	Yes	Yes	900€

Continues on the next page...

Tool	Integrated methods and standards	Risk methodology	Report generation	Comparison of two risk assessments possible	Risk management supported (Assessment, Treatment, Acceptance)	Risk analysis supported (Identification, Analysis, Evaluation)	Cost
Modulo Risk	ISO 27001 COBIT Sarbanes-Oxley Act BASEL II ITIL BS 25999 PCI HIPAA GLBA FISMA	Quantitative & Qualitative	Yes	/	Yes	Yes	On request
MSAT	ISO 17799 NIST-800.x	/	Yes	/	Yes	Yes	Free
Proteus	ISO 27001 BS 25999 (ISO 22301) ISO 9001 ISO 14001 ISO 20000 BS 10012 PCI DSS	Quantitative & Qualitative	Yes	/	Yes	Yes	700€
Real ISMS	ISO 27001	Qualitative	Yes	/	Yes	Yes	700€
TRICK light	ISO 27001 ISO 27002 ISO 27005 ISAMM MAGERIT	Quantitative	Yes	No	Yes	Yes	Included in consulting services only

Continues on the next page...

Tool	Integrated methods and standards	Risk methodology	Report generation	Comparison of two risk assessments possible	Risk management supported (Assessment, Treatment, Acceptance)	Risk analysis supported (Identification, Analysis, Evaluation)	Cost
verinice	IT-Grundschutz ISO 27001 VDA ISA-Assessments	Qualitative	Yes	/	Yes	Yes	Free
vsRisk	ISO 27001 ISO 27002 ISO 27005 BS7799-3 ISO TR 13335-3 NIST SP 800-30	Qualitative	Yes	/	Yes	Yes	1350€

Table 3: Basic functionality of Risk Assessment tools

Appendix D - Variations in naming across RA/RM frameworks

Integrated Model	FAIR & Open Group	ISO 13335-1	SRA	Microsoft Threat Model	OWASP Risk Rating Methodology
Threat	Threat Agent	Threat Agent	Attacker	N/A	Treat Agent
Threat.internal OR external	Threat Loss Factors: internal vs. external	Threat: source	N/A	N/A	N/A
Threat.profile	Threat Community	Threat: group	N/A	N/A	Threat Agent Factors
Attack	Threat Event	Attack	Attack	Threat	Attack
Attack.actionType	Threat Loss Factors: action type	threat: numberOfAssets + threat.Severity	Attack: ThreatType {confidentiality, integrity, availability}	Threat.STRIDE {spoofing, tampering, repudiation, disclosure, DoS, elevationOfPrivilege}	Attack
Attack.threat Capability	Vulnerability: TCap	N/A	N/A	N/A	Threat Agent Skill Level + Opportunity + Size
Attack.defense Strentgh	Vulnerability: DefenseStrentgh	Asset: Safeguards	Likelihood of Capture	N/A	Intrusion Detection
Attack.frequency	Threat Event Frequency	Threat: frequency	Attack.Probability	Reproductibility + Discover-ability	Likelihood

Continues on the next page...

Integrated Model	FAIR & Open Group	ISO 13335-1	SRA	Microsoft Threat Model	OWASP Risk Rating Methodology
Attack.lossType	Loss form	Impact: consequences	Vulnerability: Type {Confidentiality, Integrity, Availability}	N/A	Technical Impact + Business Impact
Attack.loss Magnitude	Probable Loss magnitude	Impact	Damage	DamagePotential + Affected users	Impact
Attack.cost	Asset: level of effort	N/A	Cost of attack	N/A	Opportunity
Asset	Asset	Asset	Information entity	Asset	Asset
Asset.valueforOrg	Asset Loss Factors: Value	Asset: value	N/A	N/A	N/A
Asset.critical?	N/A	Asset: sensitivity	N/A	N/A	N/A
Expected gain	Asset value	Threat: motivation	Gain	N/A	Threat Agent Motive
Vulnerability	Vulnerability	Vulnerability	Vulnerability	Vulnerability	Vulnerability
Vulnerability.level	TCap - Control Strentgh	N/A	1 - Cost of attack	Exploitability	Vulnerability Factors

Table 4: Naming variations between Information Security Conceptual Models