FAKULTÄT
FÜR !NFORMATIK

Faculty of Informatics

Software-based automation of risk assessment

DIPLOMARBEIT

zur Erlangung des akademischen Grades

Diplom-Ingenieur/in

im Rahmen des Studiums

Software Engineering and Internet Computing

eingereicht von

Alexander Duggleby
Matrikelnummer 0426744

an der
Fakultät für Informatik der Technischen Universität Wien

Betreuung
o.Univ.Prof. Dr. A Min Tjoa
PD Dr. Edgar Weippl

Wien, 01.07.2010

(Unterschrift Verfasser/in)

(Unterschrift Betreuer/in)

Alexander Duggleby
Wallensteinstrasse 54/15
1200 Wien
Österreich

„Hiermit erkläre ich, dass ich diese Arbeit selbständig verfasst habe, dass ich die verwendeten Quellen und Hilfsmittel vollständig angegeben habe und dass ich die Stellen der Arbeit – einschließlich Tabellen, Karten und Abbildungen –,die anderen Werken oder dem Internet im Wortlaut oder dem Sinn nach entnommen sind, auf jeden Fall unter Angabe der Quelle als Entlehnung kenntlich gemacht habe."

Wien, 01.07.2010,

SOFTWARE-BASED AUTOMATION OF RISK ASSESSMENT

AN APPROACH TO REDUCING COSTS OF RISK ASSESSMENT PROCESSES

BY MEANS OF MULTI DIMENSIONAL AGGREGATION SYSTEMS

by Alexander Duggleby

Kurzfassung

Wir leben in einer komplexen Welt, in der es nicht mehr möglich ist, sämtliche Zusammenhänge und Auswirkungen unserer Entscheidungen zu überblicken. Im Alltag haben wir gelernt, diese Ungewissheit zu akzeptieren und mit ihr zu leben. Besondere Vorsicht ist allerdings geboten, sobald Dritte von unseren Handlungen betroffen sind.

Die Forschung spricht hier von Risiko-Management. Dieses jahrzehntealte Themengebiet hat mittlerweile viele Methoden hervorgebracht, die einer systematischen Behandlung von Risiken ermöglichen. Da allerdings einheitliche Begriffsdefinitionen und vergleichbare Bestimmungsmethoden fehlen, führen die meisten dieser Ansätze zu höchst subjektiv interpretierbaren Resultaten. Weiter verursacht eine fehlende Unterstützung in der praktischen Integration dieser Methoden dazu, dass in Unternehmen nur minimal Risikomanagement eingesetzt wird.

Innerhalb des Risikomanagements ist die Risikobeurteilung mit dem größten Aufwand verbunden. Es erfordert das Spezialwissen von Experten, die regelmäßig mit den zu untersuchenden Objekten und Prozessen arbeiten. Diese werden für gewöhnlich persönlich befragt, was einen großen Teil der Risikomanagement-Kosten pro Objekt bedingt.

In der vorliegenden Arbeit wird der Versuch unternommen, den Prozess der Risikobeurteilung mittels Softwarelösungen weitestgehend zu automatisieren. Ziel ist es, mit Hilfe einer durchdachten Anwendung die Kosten pro Betrachtungsobjekt zu reduzieren und auf lange Sicht den Wirkunsgrad von Risikomanagement zu maximieren.

Das Automatisierungskonzept baut auf eine schematische Erfassung von Ist-Zuständen und einer hierarchischen Aggregation der daraus resultierenden Risikowerte auf. Bereits existierende Risikomanagement-Methoden werden auf ihre Gemeinsamkeiten hin untersucht, um einen generischen Ansatz zu definieren. In Folge wird ein logisches Datenmodell entwickelt, das zur Abbildung spezifischer, auf diesem Modell aufbauender neuer Ansätze dient. Das so abgeleitete technische Datenmodell wurde als Software-Prototyp umgesetzt und anhand einer gebräuchlichen Risikomanagement-Methode getestet.

Zu folgenden Ergebnissen kommt diese Arbeit: ein generischer Risikobeurteilungsprozess, der Entwurf eines technischen Datenmodells sowie eine prototypische Softwareanwendung zur Durchführung von Risikobeurteilung (auf Basis von besagtem Datenmodell).

Abstract

Due to the complex world we live the outcome and consequences of the decisions we make cannot be fully understood. We have evolved to cope with this uncertainty in our daily lives. It becomes a challenge when multiple stakeholders are involved and we are held responsible by others for our actions.

The field of risk research has occupied researches for decades and produced numerous methods for managing these risks. Even so they are often incompatible with each other and the results are highly subjective causing low adoption rates by organisations.

These methods seldom define details in process implementation and a lack of tooling support makes the actual risk assessment phase very cost intensive. The expert sources required are often interviewed personally and the data processed by hand. This ultimately leads to less assets being surveyed.

This thesis attempts to automate large parts of the aforementioned process with the help of software tools. The cost of the whole process can be reduced by designing an integrated and automated software solution for risk assessment which in turn allows more assets to be assessed.

The basis for the automation is a systematic assessment of the assets state and hierarchical aggregation of the resulting risk levels. Common risk management methodologies were examined, commonalities identified and a generic risk assessment approach defined.

A data model was developed to describe processes based on this approach. A software prototype based on the derived technical data model was used to test the validity and aggregation capabilities of the concept based upon a common risk management methodology for IT security.

The main results of this work are the generic risk assessment process, the design of a technical model for describing and documenting it and the software prototype application that supports it.

Content

Kurzfassung iii

Abstract v

Content vii

Figures xi

Tables xiii

1 Introduction 1

1.1 Problem statement and motivation 2

1.2 Research method 3

2 Fundamentals 5

2.1 Basic terms 5

2.1.1 Organisation 5

2.1.2 Asset 5

2.1.3 Value 5

2.1.4 Threat / Opportunity 6

2.1.5 Incident 6

2.1.6 Inherent Risk 6

2.1.7 Controls 6

2.1.8 Residual risk 6

2.2 Risk management process 6

2.3 Risk analysis 7

2.3.1 Qualitative analysis 7

2.3.2 Semi-quantitative analysis 7

2.3.3 Quantitative analysis 7

2.4 Risk aggregation 8

2.5 Options to manage risks 8

2.6 Enterprise risk management 9

3 Related work 11
3.1 Risk Analysis Methodologies 11
3.1.1 US-Military Standard 882-D 11
3.1.2 SUVA 13
3.1.3 DIN 25424 14
3.1.4 Facilitated Risk Analysis and Assessment Process 15
3.1.5 Austrian IT Security Handbook 16
3.1.6 EBIOS 16
3.1.7 MAGERIT 17
3.1.8 MEHARI 18
3.2 Case Study: Major International Oil Company 19
3.2.1 Structure 20
3.2.2 Risk assessment 21
3.3 Industry tools 23
3.3.1 Archer Risk Management 23
3.3.2 Achiever Plus 23
3.3.3 Enablon RM 23
3.3.4 AgenaRisk 24
3.3.5 Centerprise Enterprise Oprisk Center 24
3.4 Observations 24
4 Analysis 26
4.1 Definition 26
4.1.1 Assets 26
4.1.2 Threats 28
4.1.3 Risks 29
4.1.4 Strategies 31
4.2 Opportunities 31

4.2.1 Assets ... 31

4.2.2 Threats ... 32

4.2.3 Risks ... 34

4.2.4 Strategies ... 35

4.2.5 Conclusion ... 36

5 Concept ... 38

5.1 Inputs and Outputs ... 38

5.2 Conceptual data model ... 41

5.2.1 Asset hierarchies ... 41

5.2.2 Threats and Risks ... 41

5.2.3 Impact Valuation ... 43

5.2.4 General risk states ... 44

5.2.5 Risk level probabilities ... 45

5.3 Technical data model ... 46

5.3.1 Aggregation dimensions ... 48

5.3.2 Asset dimension ... 49

5.3.3 Question dimension ... 49

5.3.4 Value objects for aggregation ... 50

5.4 Aggregation Process ... 53

5.4.1 Tree ordering ... 56

5.5 Assessment Markup Language ... 59

5.5.1 Organisational Structures ... 59

5.5.2 Process Structures ... 61

5.5.3 Results ... 66

6 Prototype ... 68

6.1 Architecture ... 68

6.2 MEHARI ... 69

6.2.1 Process ... 69

6.2.2 Knowledge Base ... 71

6.3 Conversion ... 74

6.3.1 Process ... 74

6.3.2 Knowledge base ... 75

7 Conclusion and Future Work ... 79

8 Bibliography ... 81

Figures

Figure 1: Example decision tree ... 14

Figure 2: Example fault tree ... 15

Figure 3: EBIOS global approach [CIS05] ... 17

Figure 4: The Risk Analysis Process, and MEHARI aids and assistance [Clu07]... 19

Figure 5: Asset Hierarchy of Interviewed Oil Company ... 20

Figure 6: High Level Matrices for Risk Level Determination ... 22

Figure 7: MuDRA Concept: Assets ... 41

Figure 8: MuDRA Concept - Asset, Threat, Risk Schema ... 43

Figure 9: MuDRA Concept - Question Schema... 43

Figure 10: MuDRA Concept - Impact Schema ... 44

Figure 11: MuDRA Concept - Composite Asset Schema ... 45

Figure 12: MuDRA Concept - Incident Schema ... 45

Figure 13: MuDRA Technical Conversion - Master Data ... 47

Figure 14: MuDRA Technical Conversion - Threats to Questions... 48

Figure 15: MuDRA Dimensions ... 49

Figure 16: MuDRA Technical Data Model - Asset Hierarchies ... 49

Figure 17: MuDRA Technical Data Model - Questions ... 50

Figure 18: MuDRA Technical Data Model - Value Objects ... 51

Figure 19: MuDRA Technical Data Model - Value Propagation ... 52

Figure 20: MuDRA Technical Data Model - Assessment Answer Instances ... 53

Figure 21: MuDRA Technical Data Model and Concrete Aggregation Model ... 53

Figure 22: MuDRA Technical Data Model - Aggregator Objects... 54

Figure 23: MuDRA Aggregation - Node and Value Conversion... 54

Figure 24: MuDRA Aggregation - User Supplied Answers ... 55

Figure 25: MuDRA Aggregation - IAggregatable and IAnswerable ... 56

Figure 26: MuDRA Aggregation - Tree to Set Conversion ... 59

Figure 27: MuDRA Prototype Architecture 69

Figure 28: MEHARI 2007 phases [Clu07] 70

Figure 29: MEHARI 2007 Knowledge Base [Clu07] 71

Figure 30: MEHARI 2007 Evaluation Grids [Clu07] 73

Figure 31: MEHARI 2007 - Conversion to MuDRA AML 74

Figure 32: MEHARI 2007 Conversion - Questions 75

Figure 33: MEHARI 2007 Conversion - Formula and Propagation 78

Tables

Table 1: Example mishap risk assessment values from MIL-STD-882D [Dod00]. 11

Table 2: Suggested mishap severity categories [Dod00] 12

Table 3: Example mishap risk categories and mishap risk acceptance levels [Dod00] 13

Table 4:SUVA probability mapping [Suv09] 14

Table 5: Excerpt from MEHARI 2007 Knowledge Base [Clu07] 19

Table 6: Risk level probability 39

Table 7: Current impact level probability 40

Table 8: AML - Clients 60

Table 9: AML - Assets 60

Table 10: AML - Virtual Assets.. 61

Table 11: AML - Security 61

Table 12: AML - Values 62

Table 13: AML - Questions 63

Table 14: AML - Question Groups 64

Table 15: AML - Formulas 65

Table 16: AML - Processes... 66

Table 17: AML - Reports.. 67

Table 18: Base Scenario Columns [Clu07] 72

Table 19: MEHARI 2007 Impact and Probability Matrix [Clu07] 73

1 Introduction

"Be wary of the man who urges an action in which he himself incurs no risk."

Seneca the Elder, Roman Rhetorician

Risk is ubiquitous. Every decision we make, we make it under uncertainty. Interactions, implications and interference in the complex world we live in are and probably never will be completely understandable. Naturally this has become a major part, maybe even the foundation, of our modern economy.

Taking risk is taking responsibility for both positive outcomes and negative consequences. The question to be asked is by whom will we be held responsible for the actions we take? What happens if we take risks that affect others? Society has created legislation which governs our interactions and is designed to protect the innocent. This encompasses life, safety and security in our homes and at work. The risk management within these governmental structures are gradually expanding to also permeate all aspects of our environment as an integral part of life.

Responsibility in business is directly associated with liability which is the primary means by which legislation can be used to redress the damages suffered by third parties. However, our market economy is also built upon the principle of free decision making. Regulations must be designed to avoid running the risk of paralyzing economic forces. Unfortunately this can lead to large areas of our daily activities not being covered by law. These must rely solely on responsibility:

- Responsibility to our shareholders for strategic decisions we make.
- Responsibility to our managers for the outcomes of projects we undertake.
- Responsibility to our children for damages to their environment.

Our conscience acts as a risk meter, highlighting what actions we should take. Therefore all of these responsibilities ultimately boil down to our own conscience to do what is right. Have we considered enough alternatives, asked the right questions and talked to the right people? If we can honestly claim to ourselves that we did everything in our reach to achieve the best results possible then justifying our actions becomes easier.

Achieving this goal in business is the essence of effective risk management. Justifying decisions systematically requires a continuous monitoring and recalculation of exposure to risk and intervention with decisive actions when decisions turn out to be suboptimal. The latter can take courage and requires reliable information. In particular this information must be delivered in a timely manner for corrective measures to have maximum effect. Effective management of risk depends upon a systematic approach to identifying possible threats and opportunities, applying controls and measures to identify them early and taking actions to control their occurrence or mitigate any negative impact once they occur. As always in business there is another side of the coin. The costs for these processes must be balanced against the potential losses. The former must not outweigh the latter in order to create a net benefit.

Today governments strive to influence the risk management process as a means of preventing damages from poor business controls. This has been increasingly visible for publicly owned companies, for example German law was one of the first to require a corporate risk management[1]. These laws generally require a monitoring system that identifies potentially damaging developments at an early stage [**Brü03**].

1.1 Problem statement and motivation

The current recession and economic crisis remind us that there is no such thing as a certain bet. All our daily and long running decisions are exposed to risks. These risks may be hidden behind the activities of those we consider to be experts or knowledgeable advisors but nevertheless they remain. Safeguards are claimed to be in place, but how effective are they? The past months have shown that they have failed to react fast enough or effectively and the result can be seen in the media today. However, even here "all risks are not equal": Postponing a project may be less of a risk to you personally than postponing a visit to the dentist. On the other hand the owner of the business whose livelihood depends on the project will certainly have a different view of the relative priorities. Being able to express the reasoning behind your decisions is important, but risk is a highly subjective matter and an explanation which is satisfactory to one party may not be considered an adequate justification by another.

Attempting to systemize the management of risk undoubtedly requires risk evaluation. Personal implications can be tragic enough if they are self inflicted, but do we all understand the impact our financial service organisations are taking on our behalf?

Clearly the risks arising from high volume transactions which affect external stakeholders need to be managed. Fortunately considerable research and information is available on the topic of risk understanding, analysis and management. Many governmental, academic and other institutions have published risk management guidelines, the adoption of which are

[1] KonTraG [**Bun98**]

required in order to gain certification or governmental supplier status (e.g. Financial Service Providers).

Despite these guidelines the economy still managed to deteriorate into its current “financial crisis” state. Therefore these processes are not adequately implemented. To avoid similar situations in the future we must understand the reasons for this. There is a trade off between the costs of risk management and the benefit it brings. Finding the right balance proves to be the real challenge. So how can we improve the management of risk? There are two variables that we can change. First by increasing their efficiency the cost of implementing and executing risk management processes can be reduced. This will allow more risk controls to be put in place for a given price. Secondly the effectiveness of the management of individual risks can be improved. The latter is at the core of risk management research and outside the scope of this work. This thesis looks at opportunities for improving efficiency and reducing cost through software automation of processes commonly found in risk management.

A preliminary analysis of the software tools which support risk management has shown only a few solutions that can support generic risk management in an enterprise scenario. Many available solutions currently focus on one specific methodology. Also there is no industry standard for exchanging data between these systems. This ultimately leads to a vendor lock-in for any organisation wishing to implement these tool based risk processes. These dependencies represent hidden long term costs and are therefore an inherent disadvantage of the use of these solutions.

Therefore this work focuses on defining a generic risk management process that employs commonalities from different standards and best practices. An attempt is then made to find opportunities for automating parts of this process using software systems. Once identified a modelling schema for the assessment of data is defined. This is subsequently used in a risk assessment software prototype and tested using a risk management process, the contents of which are publically available.

1.2 Research method

This thesis starts by analysing common risk management methodologies to find commonalities. The recommendations of ENISA, the European Network and Information

Security Agency[2], are taken as a starting point for further research. A list of generic features is compiled to enable an evaluation of process components.

This is followed by a short review of available software systems that support these processes. The focus will be on the unique differences of each product or solution.

Based upon these findings a generic high-level risk assessment approach is documented and examined to find opportunities for improvement through software automation. Areas with large impact will be used to devise a risk management data model. This model will be implemented as an interexchange format capable of describing multiple risk assessment standards including the methods described by ENISA.

The data model will then be implemented as a software prototype which can execute assessments. The models will be tested on a chosen ENISA method. A converter will be developed to convert the chosen process' data format to the generic format defined in this work. This format will then be imported into the working prototype to run the risk assessment based on this process. The definition of the generic format, the prototype and the converter are the main results of this thesis.

[2] ENISA - The European Network and Information Security Agency maintains an information portal for risk management and risk assessment. There is an ongoing effort to maintain a repository of risk management methods with comparable properties.

2 Fundamentals

The field of risk management research is at least 30 years old and more recent developments have attempted to standardize terms and methods. They have only partly succeeded resulting in varying definitions. For the scope of this work a set of definitions will be applied and described in the following chapter.

2.1 Basic terms

2.1.1 Organisation

The term is used to describe a structure for interactions between people. Frequently it is synonymous with companies. For the purposes of this work the only characteristic required from an organisation is the ability to introduce processes to control the interactions. The shape or style of these processes can be formal or informal and do not necessarily require the strict hierarchies normally found in companies.

2.1.2 Asset

Any object of any value to the organisation it belongs to. The object can be tangible, such as a building or desk, or intangible like reputation, data or intellectual property. The value of such an asset consists of the monetary accounting value and includes any strategic elements, such as the value of a unique selling proposition. Assets can be composed of and depend on other assets that further alter the value.

In contrast to McCumber [**McC05**] an asset is herein not restricted to an object that requires protection. This would reduce the analysis of assets to negative events and excludes positive opportunities by definition. With regard to information as an asset he correctly mentions that it is not the information as such which is valuable to the organisation but rather having access to it. Data must be differentiated from information. The latter is data put in context and analyzed for future consumption of the results.

2.1.3 Value

The value of an asset is the maximum loss that can occur if the asset is completely destroyed. This includes the loss of material, the loss of functionality and potential implications to related assets. This usually includes the accounting valuation as a basis. It must be carefully considered if depreciation is taken into account. For example the only company printer that has been completely depreciated should certainly be valued at the cost of replacing it with a comparable model to ensure no interruption is caused. If there are multiple compatible printers then the value of a single printer is negligible and depreciation can be taken into account.

Intangible assets can be difficult to value. Public image is often only subjectively perceived and cannot be defined as a monetary value. Some approaches therefore will determine values on a discrete scale which portraits relative value instead of absolute values which simplifies this process.

2.1.4 Threat / Opportunity

These terms are used to describe an event that causes an asset to lose or gain value. The change in value it creates is called the impact and is directed at one or more assets. Each asset can have a different impact value. Frequently only threats, i.e. a loss in value, are considered in risk management. Solutions provided herein will predominantly concentrate on threats.

2.1.5 Incident

This denotes an event where a threat (or multiple threats) have occurred and had an impact on one or more assets. The impact of a threat can by definition only be smaller than the asset's value. Thus a difference exists between the impact value of the threat (the maximum loss) and the probable impact value of the risk as defined below.

2.1.6 Inherent Risk

The occurrence of a threat is uncertain and is subject to a probability. The inherent risk is an indicator for the impact under consideration of its probability. The inherent risk of an asset is the sum of the inherent risks of each threat that can affect it.

2.1.7 Controls

The goal is to reduce the impact of the threat on an asset's value. This can be achieved by reducing the probability or reducing the potential impact. The term control is used for all measures and processes put in place that attempt to achieve this task.

2.1.8 Residual risk

Once controls have been applied to an asset the threat properties have changed and the residual risk now reflects the new probability and impact.

2.2 Risk management process

Generally speaking the risk management process consists of a periodic risk analysis and ongoing risk management decisions and monitoring. The former assesses which assets are affected by threats and decides what actions are to be taken. The latter will continuously monitor the correct implementation and effectiveness of these actions. The reaction to incidents is outside the scope of this work and is embedded in crisis management processes.

2.3 Risk analysis

Risk analysis is a phase within the total risk management process which identifies threats, their nature and impact. It takes into consideration the controls already in place and recommends suitable additions. Any number of calculations can be used to determine a risk level from the given threat properties, but these should be defined once and used throughout the risk management process. Consistency over time is important because it ensures comparability of results and eases the detection of change.

Sources for threat properties can be past data, statistics, experiments, models or even expert advice. The type of data determines the risk analysis approach used. Commonly there are three classes of analysis and many hybrid forms involving aspects of each class.

2.3.1 Qualitative analysis

When data on threat properties is not readily available or too costly to gather, the qualitative approach can be used. The information gathered is largely based on expert opinion and focuses rather on the magnitude of threat properties, i.e. small or large, than on the exact figures.

The techniques used in the assessment itself can range from interviews to brainstorming sessions where different domain experts figure out what the appropriate risk level is. The method of determining this level must be consistent throughout the process and therefore well documented and communicated.

2.3.2 Semi-quantitative analysis

This approach takes the qualitative magnitude scales and assigns a number of values to the ranges. For example the organisation defines five risk levels ranging from a loss smaller than €10000 up to a loss of over €10 Million. Similarly a scale could range from one day of production outage to a month. This attempts to objectivise the results (not the analysis itself) and reduces the margin for interpretation error.

2.3.3 Quantitative analysis

If data is available or can be derived from different sources then threat properties can be assigned numeric values directly. These provide the most meaningful results if data is accurate enough. Precaution must be taken to not interpret too much into the results of this type of analysis. An exact figure is just as prone to error as the scales used in qualitative analysis. Often techniques from statistics are used such as Monte Carlo simulations that will disclose the distribution these values have. Some of these methods may have a margin of error themselves which will have an effect on the risk analysis.

2.4 Risk aggregation

Depending on the risk analysis technique in use it may be possible to form a relationship between the risks of a parent and its children. The act of calculating risks using composition or relationships is called risk aggregation.

Bontempi [**Bon03**] notes that risk aggregation can be differentiated hierarchically in multiple stages. Apart from the risk assessment performed on a single asset, for example a project, he "superimposes the total risks of the individual projects to the total operative risk". He further considers the possibility of aggregating total asset risk to a corporate risk level.

2.5 Options to manage risks

The purpose of risk analysis is to identify threats and opportunities and determine the appropriate value at risk for each of them. The task of the larger risk management process is to successfully manage these. Vose [**Vos08**] proposes nine options that can be used alone and in combination with each other:

- Acceptance: Although risk is ubiquitous not all risk events are highly likely to occur. Therefore in some cases it is the best choice to accept the risk thus taking the chance of a loss if it occurs. For example low impact combined with low probability risks are a candidate for this action. Sometimes the cost of controlling the risk is higher than the potential loss and therefore financially not viable.
- Increase or adjust: Risk analysis must be an ongoing exercise to identify risks that have decreased in probability. The existing controls for these risks can be removed and the operating costs be reinvested in controls for higher risks.
- Avoidance (Elimination): If risks cannot be successfully managed using controls and their impact is unacceptable then often the only choice is to eliminate the risk from the venture at hand. This results in a change of assets and may introduce new assets requiring the risk analysis to be reconsidered.
- Reduction (Mitigation): The most common action used in risk management is reduction of risk parameters. This implies either reducing the probability of occurrence, e.g. technological improvements, more testing, or a reduction of impact if the threat does happen, e.g. redundant systems, early warning systems.
- Contingency planning: Regardless of any preventative action taken threats can occur and the speed of detecting and handling their occurrence is often directly connected to the impact they have on the business. Contingency plans include warning signals and details about what actions to take and who must take them.

- Risk reserve: A buffer is included in the management plan to compensate for any impact the threat has. This action is often implied by management without explicitly mentioning it as a chosen strategy leading to funds being used for other matters instead of the designated use as a reserve, e.g. overhead costs in projects used for additional project goals instead of improving the processes managing the project.
- Insurance: In the case that management regards their exposure to a certain threat to be higher than the industry average taking an insurance to cover the impact can be the most cost effective decision.
- Risk transfer: A contractual option that penalizes one partner if an incident occurs that should have been mitigated or managed.

The last option presented by Vose it to get more information. Risk is uncertainty. Therefore reducing the gap in knowledge about a certain threat can lead to better risk estimation and to better choices for control implementation. But waiting for the data needed to improve the decision could leave an asset at risk during the gathering process.

2.6 Enterprise risk management

The European Network and Information Security Agency defines Enterprise Risk Management as an "integrated business process that incorporates all of the Risk Management processes, activities, methodologies and policies adopted and carried out in an organization. [It] is usually released by the executive management of an organization [and] consists of two processes, one setting the framework for the entire Risk Management and the other setting the communication channels in the organization" [**Eni09**].

Risk management must not be seen as an isolated discipline but rather an integral part of management practices. To date even though some national laws require risk management to be in place there are multiple standards and "best" practices as well as many internally developed systems for managing risk. The lack of standard terminology leads to incompatibilities between approaches and results. Nevertheless most large firms have introduced the Risk Manager as an official position whose responsibility lies in assessing risk, making recommendations and as a vital part of the management process ensuring that those recommendations are implemented and monitored.

Often it is common sense and a certain ability to abstract and look at problems from a different point of view that is required to fill the position. But tools and methods ensure a certain level of traceability and documentation required in a corporate environment. The larger the organisation is the greater the need for large teams in risk management which consequently leads to internal standards to cope with the increased complexity.

Brühweiler [**Brü03**] emphasizes that a management system needs "checks and balances”. It is important to have synchronized processes in risk management and the general management of the organisation. “Management by chaos” or “...under time pressure” will provide a breeding ground for risks.

Therefore an efficient software based approach to enterprise risk could in itself reduce the overall risk level of the organisation by providing structures, discipline and transparency leading to less chaotic environments. If designed appropriately such systems can integrate transparently into the day to day operations promoting proactive risk management and reducing the need to constantly react to events under time pressure.

3 Related work

3.1 Risk Analysis Methodologies

The following chapter will describe some of the most common risk management practices. The focus of the analysis will lie in differences in the risk assessment approach.

3.1.1 US-Military Standard 882-D

The American Department of Defence has and continues to play an important role [**Brü03**] in the development of risk management practices. Threats to the economy, the environment and human life are considered. The primary focus lies in technical assets. These are regarded as part of a lifecycle from creation to destruction. The risk management process described follows the definition from the previous chapter. With regard to risk assessment the prioritization of risks is based on discrete impact (severity) and probability scales. These two dimensions are projected onto a single risk level using the matrix show below.

Severity Probability	*Catastrophic*	*Critical*	*Marginal*	*Negligible*
Frequent	1	3	7	13
Probable	2	5	9	16
Occasional	4	6	11	18
Remote	8	10	14	19
Improbable	12	15	17	20

Table 1: Example mishap risk assessment values from MIL-STD-882D [Dod00**].**

The severity can be applied to different threats or different scenarios. They could have multiple impacts on different domains, such as loss of human life, monetary or even ecological impact. Therefore a system of severity buckets is specified that allow the maximum impact to be associated with a severity level.

Severity level	Criteria
Catastrophic	Could result in death, permanent total disability, loss exceeding $1M, or irreversible severe environmental damage that violates law or regulation.
Critical	Could result in permanent partial disability, injuries or occupational illness that may result in hospitalization of at least three personnel, loss exceeding $200K but less than $1M, or reversible environmental damage causing a violation of law or regulation.
Marginal	Could result in injury or occupational illness resulting in one or more lost work days(s), loss exceeding $10K but less than $200K, or mitigatable environmental damage without violation of law or regulation where restoration activities can be accomplished.
Negligible	Could result in injury or illness not resulting in a lost work day, loss exceeding $2K but less than $10K, or minimal environmental damage not violating law or regulation.

Table 2: Suggested mishap severity categories [Dod00**]**

The risk categories are then used to generate specific actions. The military chain of command requires acceptance of these actions by a certain hierarchy level.

Mishap Risk Assessment Value	Mishap Risk Category	Mishap Risk Acceptance Level
1 – 5	High	Component Acquisition Executive
6 – 9	Serious	Program Executive Officer
10 – 17	Medium	Program Manager
18 – 20	Low	As directed

Table 3: Example mishap risk categories and mishap risk acceptance levels [Dod00**]**

3.1.2 SUVA

The Swiss Accident Insurance Body developed the SUVA methodology based on principles found in the US-MIL-882-D standard. The process was reduced to five levels:

1. Define scope
2. Determine threats
3. Determine risks
4. Evaluate risks
5. Mitigate risks

At the core of the assessment phase a brainstorming session is held that uses a list of thirteen threat classes as a starting point for identifying threats. The qualitative risk assessment used in SUVA proposes two different types of probability calculation for threats. The first is used to determine a probability of a threat occurring in an industry sector. It uses a five point scale and incident statistics provided by the insurance body as a reference measure. Secondly the process defines a calculation for determining probability in individual cases such as single buildings or a personal work space. The formula used is based on the European Norm EN1050 [**Bak09**]. The resulting value is then mapped to a probability using a mapping table.

$$\mathbf{W = e + 2w + v}$$

e Exposition to the threat, ranging from 40 (e=5) to 2 hours per week (e=1).
w Probability of the threat occurring on a scale from 1 (rare) to 5 (expected)
v Possibility of mitigating the threat on a scale from 1 (possible) to 5 (not possible)

Level	Definition	Value of W
A	Frequent	19, 20
B	Regularly	17, 18
C	Rate	14, 15, 16
D	Improbable	11, 12, 13
E	Close to impossible	< 11

Table 4:SUVA probability mapping [Suv09**]**

3.1.3 DIN 25424

This norm was developed by the German Institute for Standardization and formalizes a technique for deriving incident probability from causes (bottom up) or impact from cause aggregation (top to bottom). Fault trees continuously decompose threats into the required conditions for an incident to happen. These are again threats for the next iteration. This is done until atomic conditions are reached where there is a known probability for their occurrence.

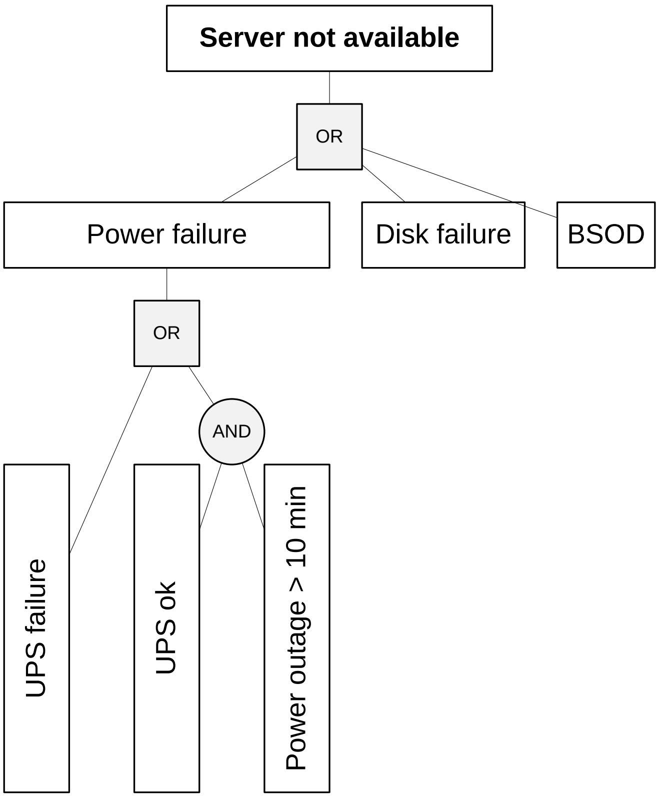


Figure 1: Example decision tree

Decision trees will examine threats under different conditions that may occur. For each set of conditions a possible impact and a probability is determined.

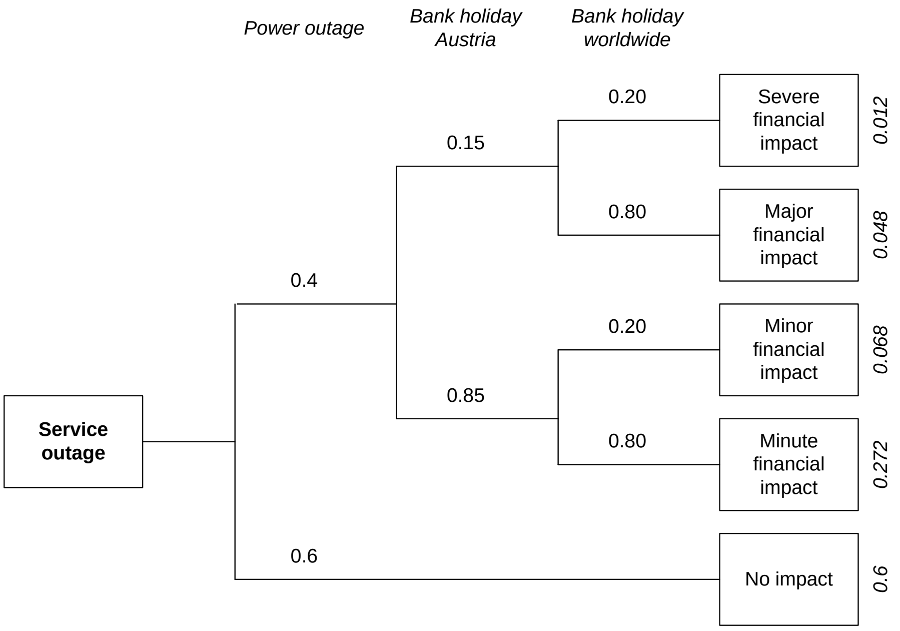


Figure 2: Example fault tree

3.1.4 Facilitated Risk Analysis and Assessment Process

FRAP (Facilitated Risk Analysis Process) is a qualitative approach described by Peltier [**Pel01**] in 2001 and was later revised and renamed to include Assessment. It consists of a three step analytical process to generate and evaluate risks to a specific target asset and the dependent business processes. The results are recommendations for the business owner. It is commonly used in information security domains due to its easy implementation. First the hour long pre-FRAAP meeting is conducted and includes the business sponsor. It creates a visual representation of the scope of the analysis including the target asset and the composition. Secondly a facilitator will call in the designated team consisting of business and technical staff to the FRAAP meeting to brainstorm on risks to the asset that may result in negative impacts on confidentiality, integrity and availability. Next the implications on business operations are considered. It is important to note that unless data is readily available the quantification of impact values is considered costly. It is not unusual that this detailed process leads to bloated documentation. More often than not the exact data is not required for determining if a control is necessary. The expertise of the FRAAP team based on national or internal incident statistics is sufficient to formulate a sound recommendation for the business owner. Their starting point is a set of twenty-five common controls.

Finally the post-FRAAP phase creates the final report including control measures and accepted risks. This is signed by the business owner as an indication of passing on of responsibility and retained by records management.

3.1.5 Austrian IT Security Handbook

The Austrian IT Security Handbook (AT-ITSH) recommends three approaches towards risk aggregation. First a detailed risk analysis is described in which every IT asset is analysed. Controls are then identified to ascertain an acceptable level of risk. This process is cost intensive and will take some time to implement and execute. This may lead to certain assets that are exposed to high risk to operate for some time without controls in place to mitigate the risk. The second approach generally assumes that all systems are equally threatened and implements a set of baseline security controls to ensure an enterprise wide level of security. The downside to this method is that this level may be too high or even too low for some assets.

A combination of both is taken in the third approach. A high level risk analysis is conducted to classify assets into low, medium and high risk assets. Detailed risk analysis is conducted in order of priority (high to low) and an appropriate set of baseline controls are implemented for low to medium assets. This ensures immediate action is taken for high risk assets whilst ensuring a minimum level of security for the remaining assets.

Risk aggregation in the AT-ITSH includes four asset classes:

- physical objects, e.g. buildings, infrastructure
- logical objects, e.g. software, data
- people
- immaterial goods, e.g. public image, trust

It is assumed that relationships between assets exist and are considered complex. Therefore these are dealt with in a separate process step.

3.1.6 EBIOS

The French Central Information Systems Security Division defines standards for information security with a focus on assessment and certification of information systems. In 2000 the second version of EBIOS (French acronym for Expression of Needs and Identification of Security Objectives) was developed. It represents an ISO 17799[3]

[3] An international standard for implementing information security management in an organisation.

compatible and thus common criteria compliant method for assessing and treating Information Security risks.

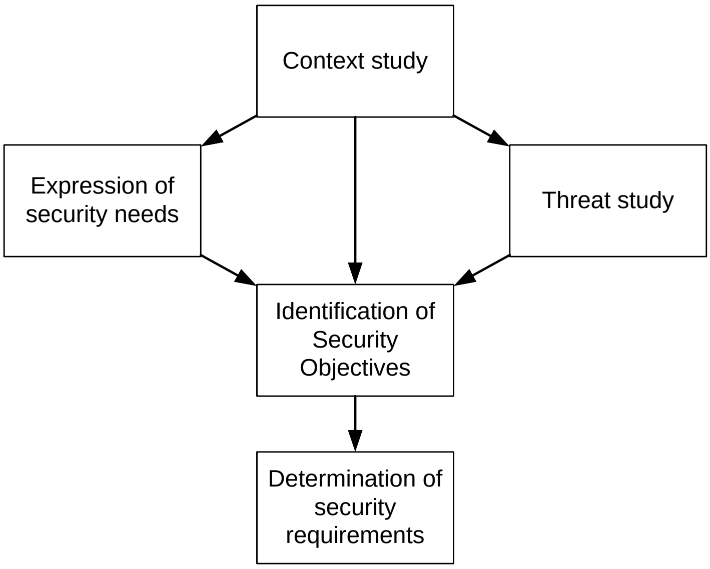

Context study
Expression of security needs
Threat study
Identification of Security Objectives
Determination of security requirements

Figure 3: EBIOS global approach [CIS05**]**

A unique characteristic in this five step approach is the expression of security needs at an early stage.

"The expression of security needs results from the operational requirements of the system, independently of any technical solution. It is based on the preparation and use of a scale of needs and the detection of impacts that are unacceptable for the organisation." [**Cis04**]

This explicit separation of needs and threats can lead to measures that do not incur as a result of a threat but should rather be understood as a mode of recommended operation.

3.1.7 MAGERIT

Introduced in 1997 by the Spanish Ministry for Public Administrations MAGERIT (Spanish abbreviation for Methodology for Information Systems Risk Analysis and Management) is used throughout public administration in Spain for managing risk. The current version 2.0 was published in 2005.

During the impact valuation phase the methodology raises the question how time dependent threats, e.g. production outage, are to be valued. For example availability is commonly a function of impact per time interval. Here two factors must be considered. Firstly is there an acceptable time frame where non availability is tolerated and secondly what is the time frame where “it could be said that the organisation has lost its operating capacity: it is dead.” [**Spa06**]

The values provided as a function are gathered using methods from business continuity management and outside the scope of this work, but the results of this work must cope with possibly complex definitions as formulas that results from them.

The MAGERIT documentation describes two different types of impact:

- **Accumulated impact**: the value loss a threat imposes on an asset and the accumulated value loss by this threat on assets that depend on it.
- **Deflected impact**: the value loss a threat imposes on an asset and the value loss by this threat on assets that it depends on.

The risk is calculated for both classes using the threat probability.

3.1.8 MEHARI

As a successor to the French MARION risk management approach the MEHARI process was developed and the last revision published in April 2007. It is the newest of the models surveyed in this work. It was developed by CLUSIF, a non profit organisation for professionals dealing with information security.

The risk analysis covered in MEHARI is heavily automated through the use of quantitative aggregation of qualitative scales. For a number of threat scenarios, questionnaires are available with assigned aggregation formulas that determine overall risk.

The aggregation model consists of multiple factors. These include intrinsic impact, natural exposure, potentiality but also a control specific distinction between values for dissuasion and prevention.

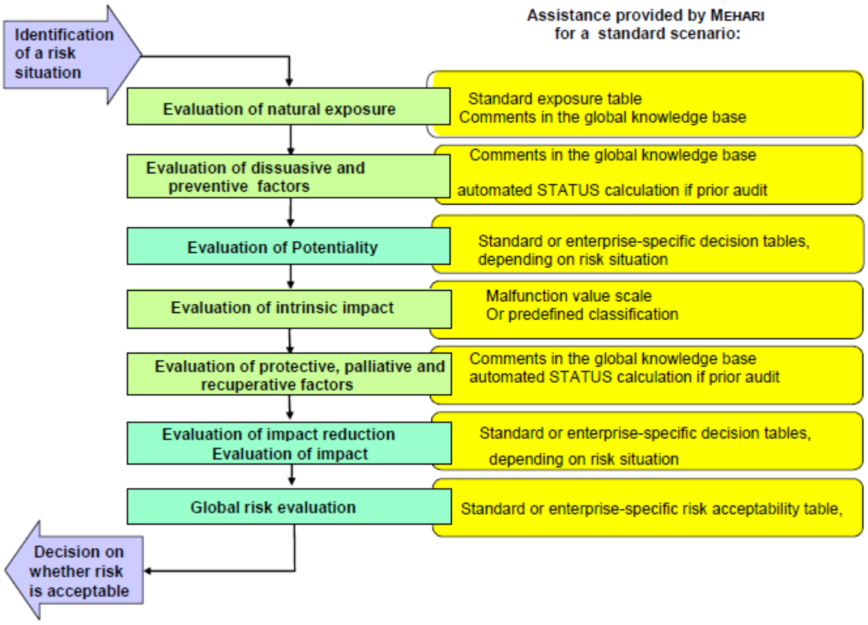

Identification of a risk situation
Assistance provided by MEHARI for a standard scenario:
Evaluation of natural exposure
Standard exposure table
Comments in the global knowledge base
Evaluation of dissuasive and preventive factors
Comments in the global knowledge base
automated STATUS calculation if prior audit
Evaluation of Potentiality
Standard or enterprise-specific decision tables, depending on risk situation
Evaluation of intrinsic impact
Malfunction value scale
Or predefined classification
Evaluation of protective, palliative and recuperative factors
Comments in the global knowledge base
automated STATUS calculation if prior audit
Evaluation of impact reduction
Evaluation of impact
Standard or enterprise-specific decision tables, depending on risk situation
Global risk evaluation
Standard or enterprise-specific risk acceptability table,
Decision on whether risk is acceptable

Figure 4: The Risk Analysis Process, and MEHARI aids and assistance [Clu07]

The calculation consists of basic mathematical formulas as shown in the following example. The references, e.g. 07C02 are references to numeric values assigned to specific answers given in the questionnaire.

	Dissuasive effect	Preventive effect
Control number	MAX(MIN(07C02;08E02);08C01)	08A02

Table 5: Excerpt from MEHARI 2007 Knowledge Base [Clu07]

MEHARI includes a comprehensive knowledge base for assessing information security, including questionnaires, the aggregation model and lookup tables for specific model values that can be modified to suit the organisation's needs.

3.2 Case Study: Major International Oil Company

On 25th April an interview was conducted with a senior risk manager at a major international oil company to understand the strategies and processes used by large enterprises to manage risk.

The processes used for managing risks have been developed internally over the years with the help of several external consultants. The core elements are implemented throughout the business and risk management is considered to be part of the company's culture. Concepts found in the previously mentioned methodologies are encountered in the industrial environment albeit in an adapted version which suits the organisation's structure and its individual business needs.

3.2.1 Structure

There are two levels at which risk analysis is conducted. At the group level audits are carried out to ensure controls are in place and operating to protect assets against major risk exposures. This uses a top to bottom approach. The risks in the global asset tree are audited centrally. Each of the leaves in the global asset trees themselves represent a local asset tree, managed by a local operations team. The company policy requires these teams to pursue a bottom-up approach for aggregating and determining risk levels. These risks together with their mitigation plans are fed into the global system through the annual planning process.

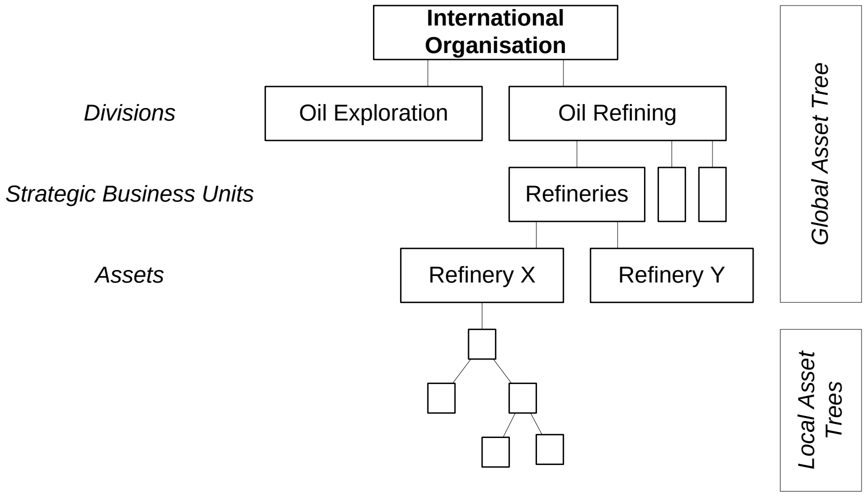


Figure 5: Asset Hierarchy of Interviewed Oil Company

The Company's global asset hierarchy consists of a rather flat but very wide tree. The international divisions are areas of operation, i.e. "oil exploration", "oil refining" and "chemicals". These are divided into strategic business units which group the leaf assets into similar or related classes.

Each new global venture, for example a new oil platform, is an asset which may not have been included in the earlier risk assessments used to build up the global asset risk tree. Therefore, for such new assets, risk identification must be conducted at the beginning of the investment planning process to ensure controls to potential risks are adequately considered.

In terms of risk aggregation the composition of each parent asset is based on the potential impact value of its children using a standardised impact valuation system. Therefore weighting of children relative to each other is unnecessary and the absolute values are aggregated. The local asset trees commonly consist of more granular asset hierarchies which are used to define the individual risk exposure composition and identify local controls.

3.2.2 Risk assessment

The current process for risk assessment is based on local quantification of monetary or reputational impact which is converted using an Enterprise Risk Management template to facilitate global risk assessment. Assessment audits are conducted on global assets in cycles which are prioritized based on asset value and the perceived level of risk. The company culture focuses heavily on managing risks and a number of baseline security controls exist to ensure that asset security is maintained outside of these audit cycles. For example, automated checks within the controlling IT infrastructure check compliance with global company policies.

3.2.2.1 Threat identification

The Oil Company recommends that each local asset maintains its own risk database to identify risks with a material impact in terms of value or reputation. These risks are used in brainstorming sessions to design impact/probability vectors of risks which then feed into the business planning process for global aggregation.

At the global level threats are reviewed when each asset is assessed. The auditing department checks these threats and the effectiveness of the controls using internal benchmarks, procedures and guidelines together with data derived from comparable ventures and the experience of subject matter experts.

3.2.2.2 Threat mitigation

Mitigation of threats is considered a two step process. Firstly an attempt is made to reduce the probability of occurrence of the risk and secondly the level of impact is controlled. The choice of controls for either step is part of each local risk assessment process. The threat databases and company policies provide a set of common controls that can be adapted to fit specific situations. Controls are then chosen by their effectiveness on both steps in relation to their implementation cost.

In the case of new threats arising or controls becoming ineffective the auditing teams may refer to similar internal or external cases and recommend controlling measures based on these.

The assessment process focuses on design effectiveness and operational effectiveness of the controls, i.e. does the control address the actual risk and is it working as intended. The methods used to gather the required information differ based on the domain under inspection.

For highly standardized domains, e.g. IT operations, the company uses standard questionnaires to assess the correct implementation and effectiveness of these controls. This is the desirable method for assessment in terms of costs and efficiency but cannot be applied to all scenarios. Therefore the audit teams need to also conduct interviews with asset personnel to determine the effectiveness of the controls in place for specialized scenarios.

These manual processes are documented and preserved in evidence databases and collected in a central repository. The repository also stores the plan used to test the controls used by individual assets. These capture the kind of assessment used to evaluate the control and what led to the final conclusion regarding its effectiveness.

3.2.2.3 Risk level determination

Local quantitative risk assessments result in overview matrices for significant threats which are then aggregated as part of the global planning process. Each high level matrix can be drilled down to view aggregations performed for each threat.

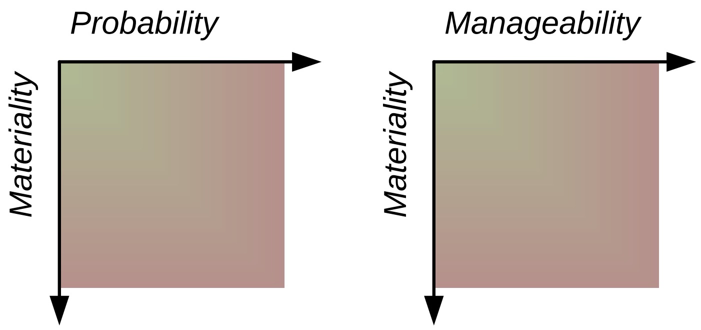


Figure 6: High Level Matrices for Risk Level Determination

Neither matrix shows a direct risk level for inherent or residual risk, but both values can be derived from the values provided.

The term materiality refers to a scale of impact levels that are analogous to the mishap severity categories used in US Military Standard 882D (but with different interpretations for each level’s financial value). This allows their use in different scenarios. The manageability dimension could be interpreted similarly to the MEHARI impact reduction value. Using the projection methods found in both standards these matrices can be projected onto linear scales for risk levels, though currently the materiality scale is the main ranking attribute.

3.3 Industry tools

In this chapter an attempt is made to identify a common set of features found in generic risk assessment tools and to point out some of their special characteristics.

3.3.1 Archer Risk Management

This product is part of a larger Archer GRC (governance, risk management and compliance) solution. The risk management module allows risk managers to define campaigns for assessing specific assets. These campaigns generate questionnaires from a library of questions in the system. These questions can be imported in various formats and Archer provides question packs based on common standards such as the Payment Card Industry Data Security Standard.

Each question can be linked to a number of standards providing answers for multiple assessments. The question need therefore only be asked once. Groups of questions can be shown or hidden based on rules defined by the model.

Assets are provided in this approach by an accompanying asset management module. This allows assets to be centrally collected and prioritized for the risk assessment process. The asset manager can define simple relationships and dependencies that are used to enable drill-down functionality in the reporting features of the solution. An archive of assessments is used to report on changes over time.

http://www.archer.com/solutions/

3.3.2 Achiever Plus

This solution specializes in automating periodic re-assessments of assets. This ensures an up to date database of risk levels and control efficiencies. Actions taken based on assessments are recorded and automatically inform the asset manager. The compliance with these recommendations can be monitored by the risk manager and escalated using a configurable engine.

http://www.achieverplus.com/

3.3.3 Enablon RM

Risk appetite is a term used in this solution to identify thresholds that companies have defined at which they accept certain risks. These can then be used to automate the mitigation process to the extent that certain risks are automatically reported as accepted.

http://enablon.com/

3.3.4 AgenaRisk

This risk assessment solution is more flexible in its underlying models. It includes the possibility of risk maps based on a Bayesian network for modelling causal relationships. These relationships can be quantified using aggregate expressions. A large number of values in the model can be simulated using techniques from pure quantitative analysis.

http://www.agenarisk.com

3.3.5 Centerprise Enterprise Oprisk Center

As part of data collection for future risk assessments this product helps manage loss events. Past incidents are recorded as they happen, can be linked to a threat and ultimately lead to probability and impact estimations. The data can similarly be used to estimate the control efficiency if controls are in place and incidents continue to occur.

http://www.centerprise.com/

3.4 Observations

Each example in this selection of risk management products addresses risk assessment and fulfils its individual promise. There are differences in each product that imply its unique selling proposition.

In terms of generic solutions the AgenaRisk product has the most flexible model definitions but continues to lack full control over the aggregation process by means of formula definition.

Even though many solution providers supply prepared packages for common standards these usually only include questionnaires and threat lists. Models such as MEHARI with a highly automated aggregation approach cannot be imported because the product's underlying technical data models do not support them.

It was also observed that asset hierarchies are commonly only defined in terms of simple relationships or dependencies. These compositions lack information for automatic aggregation of risks.

The types of questions provided in questionnaire based products commonly had two answer types (yes and no). A support for a set of values, multi-valued answers or even open text or numeric answers could not be identified.

None of the products surveyed published a standard rich format for importing or exporting data from their systems. Each question pack was tailored for their specific product.

4 Analysis

The previous chapter has given a general understanding of commonalities and differences between risk management methodologies and supporting software systems. The emphasis of this thesis lies in finding software support opportunities for these processes. So far the reviews have shown that there is no gold standard in risk management, even though many make references to certification standards or national governance regulations. Hence it does not pose any restrictions on which processes are used and the goal within is to strive to construct a software design that can support a wide range of processes. Peltier notes: “The organizations that are most satisfied with their risk analyses process are those that have defined a relatively simple process that can be adapted”. Therefore in the following chapter an attempt is made at defining a generic process for assessing organisational risk with a minimum of constraints regarding its use and implementation.

4.1 Definition

In general risk management includes four areas of operations: Assets, Threats, Risks and Strategies. The first includes an in-depth analysis of the organisation’s asset structure and its value to the business. The highest valued assets will undergo a threat modelling to identify losses that could occur through threats if certain environmental attributes change. These changes can in turn be compensated by other environmental or asset properties thus reducing the risk of the threat to the asset. Once the remaining threats and their corresponding risks have been found the organisation can attempt to come up with mitigation strategies or explicitly accept the remaining risk.

4.1.1 Assets

The term asset is used widely in business to describe important parts of an organisation. Common definitions are:

- an item of value owned [**Mer09**]
- a useful or valuable quality, person, or thing; an advantage or resource [**Far09**]
- a useful and desirable thing or quality [**Dic09**]

The notion of ownership and value play a large role for an asset. It is important to ask not only what the value of an asset is but also for whom. An organisation in the sense used throughout this document usually implies an owner of some sort. A company has its shareholders and a project has a project owner.

Next we consider which assets are at a potential risk of losing value. The only asset that is not at risk of losing any value is an asset that has no value at all. All other assets with a value greater than zero could ideally be locked away in a theoretically perfectly safe container. But they would still lose value through depreciation over time. If the owner gives the asset a value of zero, then and only then can we exclude these assets from our list. Taking into account that the term value is quite broad and includes monetary, emotional and environmental value, it is hard to imagine any assets being excluded.

Clearly assessing risk for low value items such as a chair is not in the best interest of the owner. Therefore it is practicable to introduce a value threshold to prioritize the assets. Nevertheless a chair for a sole proprietor may well be a very important asset. The height of this threshold largely depends on a trade-off between the process costs of assessing the risks involved and the potential loss. The attempt to simplify parts of the assessment process within this thesis will without doubt have an impact on lowering the cost of the assessment per asset allowing risk managers to reduce this threshold and cover more assets.

So far examples for assets were tangible physical assets such as buildings or pencils, but in order to compile a complete list of assets the process must consider three classes of assets.

Physical assets are tangible and usually identifiable through the organisations accounting structures. This source also helps in determining a value for these assets. The accounting value is the current value of the asset including factors such as depreciation. Even though using this value directly may not be applicable in every case it can certainly be taken as a basis for an evaluation.

Logical assets are usually synonymous with intellectual property. Generally speaking this class consists of intangible objects such as information, human resources and their knowledge or reputation. In this class it is harder to find a monetary amount that represents the value of the asset. More commonly a sense of subjective value can be found. This must be objectivised as much as possible to reduce subjectivism.

The last class covers composition of assets and these are named virtual (or composite) assets. Business processes are a common example for this class. They are composed of multiple tangible and intangible assets and their value is an aggregation of the value of their atomic assets. This value is the intrinsic value. A certain group of assets within this class may have a larger value than just the sum of the assets they consist of. The composition itself has its own imputed value.

The value of fire evacuation infrastructure is not solely the sum of the evacuation signs and alarms. The composition of them creating a large connected intervention system increases their values. If all the signs were removed from the walls and put on a large pile the composition has changed, the value of the infrastructure is reduced to just the sum of its parts.

This must not be confused with tangible assets that have undergone an external manufacturing process. The pencil certainly has a higher value than the wood and graphite it is made of but it was purchased as one item. Therefore only the single imputed value is considered.

4.1.2 Threats

Once a common definition for asset and a list of high priority assets have been determined it is commonly suggested to cluster these assets into groups of similar assets, e.g. server systems, office buildings, patents. This simplifies the next step: threat identification.

Experts in the domain can conduct a brainstorming session and identify all major threats. The result is largely dependent on the expertise, the concentration and size of the subject. There are numerous brainstorming techniques that can be used to help creativity during these sessions. A commonly used concept are prompt lists [**Vos08**]. They provide a set of categories of risks that are pertinent to the scenario at hand. They can help the risk management team to think about possible risks and improve the chance for uncovering all major threats. These lists can be very specific to the domain they were designed for. Organisations can and should define detailed checklists for common scenarios.

The threats identified must be documented extensively including actors, pre and post conditions and environmental factors. A threat database can help to reduce the cost of re-identifying risks for the next assessment by providing search and access to the already identified threats.

We can build on our definition of asset and define a threat as any process which will reduce the value of the asset it is applied to. The impact a threat can have is the absolute loss in value that occurs. A common mnemonic used in impact valuation is DREAD. This model was introduced by Microsoft to improve threat ratings and is similar to the prompt lists and has since been used more broadly [**Wik09**].

The five categories to be taken into consideration when giving a threat an impact value are:

- Damage – Direct loss in value of the asset
- Reliability – Number of factors required for the threat to occur
- Exploitability – Possibility of occurrence
- Affected users – Network effect of the threat
- Discoverability – How fast can countermeasures be applied

The mitigation effects of countermeasures mentioned in the last category are not considered when determining maximum impact value of threats. These are implemented as controls and can reduce the impact of the threat or alleviate them completely. But the correct implementation must be verified and is done at a later stage of this process. Including existing controls at this stage would distort the view on threats and could lead to them not being assessed because their importance is interpreted too low.

At this point the threat list can be shortened by removing threats with impact values below a certain threshold. But this threshold must be carefully determined because probability has not been included. One runs the risk of losing important threats that may have a low impact but high probability for a higher ranked high impact but low probability threat. Generally this reduction should only affect miniscule impact threats, to remove only insignificant threats from further analysis.

For specific asset classes the analyst can resort to existing lists of common threats and adapt them to suit specific needs. More specialized asset classes may require a technique for threat discovery. The domain of software development has recently seen developments in the area of threat modelling. Tools such as Trike [**Lar09**] analyse software systems, their dependencies and can guide the process of determining what threats could pose a risk to the asset.

The identified threats for each class are applied to each asset contained within. It can be necessary to add additional threats to specific assets if the classes exist that include marginally disparate assets. A common example is a server class in a small business. This can include a public web server that is threatened by external threats whereas internal servers in the same class may not be.

4.1.3 Risks

The list of threats that could affect an asset does not include any information about the probability that the threat is going to occur. It is merely an indicator for a common threat. The next step is to qualify the risk the threat imposes by including the notion of frequency.

Reducing the list and so reducing the cost for analysis is the primary task in this phase. A preliminary risk level based on probability and impact is used to exclude low risk threats.

Domain experts within the organisation assign coarse risk levels to the threats identified. A qualitative approach using a scale of three levels (high, medium, low) is considered an exception and a method of last resort, only used for edge cases such as loss of reputation where quantification is difficult. If applied to multiple units of an organisation it must be communicated that the risk level is in proportion to the scope of the organisation not of the unit. A high risk threat for the facility management is most certainly not equal to a high risk investment threat by another strategic business unit.

The use of semi quantitative scales to assign an interval representing different risk levels reduces the chance of misinterpretation. Even in the case mentioned above reputation loss could be measured on a semi quantitative scale using the percentage of people in a public survey that confirm a loss in reputation if a certain action happened.

This first step provides a list of high-risk assets that can be further analysed. A list of common threats with high impact can be compiled and used for implementing a set of baseline security controls to ensure a general level of security.

The detailed analysis of high-risk assets will also use techniques introduced above but will go into more detail. The importance of comparable results over time increases in this step. Therefore it is stressed again that qualitative analysis must be carefully considered as it is hard to achieve those kinds of results with that approach.

Often elements of quantitative analysis will be used to come up with more exact estimates for risk levels. If reliable historical data exists for impact and probability then quantitative analysis is generally the preferred method for risk level evaluation. Caution is advised when using these data sources. They must not be blindly trusted as past threat occurrences may have had external causes that were not recorded and therefore impacting the causality. The data could be distorted and hide other causes and reasons if it was collected after the threat occurred.

Commonly systematic approaches to assessment rely on a set of structured questionnaires that determine the risk level. This reduces the subjectivity factor by providing a path from simple questions about the efficiency level of certain controls and the resulting risk level. For example one asset operator may consider username and password a fully adequate means of securing a server from the threat of unwanted access. Another may see a moderate risk and imply that only smart card authentication reduces risk to a minimum. Using the same questionnaire and paths to derive these values throughout the organisation reduces the ambiguity of the risk scale and improves comparability. For specific asset classes questionnaires may be readily available on the market.

The properties of the risk level of each threat itself must be determined from the set of answers given to the questions. This can include impact, frequency and other more detailed factors. Each answer is given a numeric scale value and a formula computes the resulting threat values. Once each threat has been evaluated the assets overall risk is determined through analysis of each assigned threat. This can be done by manual analysis if the number of threats and assets is small. For larger assessments and to improve comparability it is suggested to again use a formula to generate the assets risk level.

Once all logical and physical assets have been evaluated the virtual assets can be calculated using simple weighted aggregation functions and taking child asset percentages into account. Use of the minimum function throughout this aggregation process is recommended because the weakest link poses the largest threat. This is compensated for by the percentages in composite assets to avoid low value assets with high risk bringing down the organisation's overall risk level.

4.1.4 Strategies

After completing an aggregated assessment the organisation can analyze the information, identify high risk assets and consider measures to reduce the area of exposure to threat. These strategies can include the implementation of additional controls to assets with high risk and cause additional costs that must be compared with the potential losses to ensure a positive outcome.

The combination of the structured questionnaire with an automatic risk determination and aggregation makes it easier to choose the correct controls by simulating the impact of each implementation alternative. For each variation an assessment could be executed and the resulting risk determined.

The result of the threats phase is an assessment of the overall organisational risk at one moment in time. Therefore it is reasonable to conduct these assessments in periodic cycles. Risk levels determined in one single assessment represent acute threats and should be managed quickly. But changes to risk over time may help to predict dangerous developments such as aging methods or invalid strategies.

4.2 Opportunities

In line with the problem statement each phase is analysed to identify opportunities for software automation. For each phase possible data sources and formats are identified and methods for extraction and interpretation described.

4.2.1 Assets

The main factors involved in this phase are asset valuation and determining of composition. As mentioned, values for physical assets can commonly be derived from an organisation's accounting system. These systems have mature methods for evaluating assets that comply with international standards. Therefore this data source can be considered to be reasonably reliable and unambiguous.

Values determined for logical assets are more subjective and therefore open to misinterpretation. Estimation techniques such as Wide-band Delphi [**Wik09b**] can help improve the result. In some cases external factors are decisive and public surveys are the best option. For example the value of a database may be determined by the amount of customers who are willing to pay different amounts for access to the data it contains.

The focus for composite assets shifts from valuation to composition. Here one finds different levels of maturity in the documentation available depending upon the domain under consideration. The composition of a data centre is well understood and can be easily looked up in the inventory catalogue which should include references to business processes depending on the infrastructure contained within them allowing these values to be considered. Similarly processes in the health sector tend to be well documented. Due to the constant pressure to cut costs, detailed information on most elements of these processes has been calculated and is available.

Although some domains may have existing documentation for their composite assets there is a lack of a standardized format. Very few domains have been built using open standards such as UML or the data centre infrastructure formats in development by Microsoft [**Mic09**].

The valuation of composite assets is normally a matter of calculating the weighted sum of their component assets' values.

In this phase there are only few improvement opportunities using software automation:

- The surveying of valuations is well understood in the field of statistics and supported by a rich tool set for execution and interpretation.
- A schema to standardize the documentation of composition holds little value if the underlying process providing the data does not exist.

4.2.2 Threats

Initially an attempt is made to reduce the list of assets by clustering them into classes of similar properties. Once these classes have been identified an attempt to identify threats to these classes can be made.

For clustering to work in a meaningful way a set of properties must be created for each asset. These properties can be found in technical documentation where they can be extracted into a simple key value set. Some domains may make use of inventory systems that hold information which is more easily extractable. To foster single interpretations of these values the organisation can define a discrete set of possible values. Clustering techniques, e.g. Self-organizing maps, can then be applied to group the assets.

Identifying threats should be a two phase process. The first determines a generic list of common threats for the asset classes. The second identifies specific threats to each class or to individual assets within the class. Sources for the initial threat gathering can be open databases such as OWASP [**Owa07**] that identify relevant threats to specific classes. Internal statistics or freely available data from insurance or other institutions can identify the most prominent threats.

Depending on the maturity of the domain under assessment there may not be enough data available for this phase and techniques of threat identification must be developed to analyse assets, decompose them, find relationships and dependencies and then infer possible threats. Naturally this is error prone because threat discovery is subject to the expertise of the analyst involved and the results are highly subjective. The process that led to the list of threats and the identification of the threat itself must be well documented to ensure traceability in future analysis.

A lot of research has already been undertaken into finding and developing opportunities in this phase:

- Some domains such as IT have developed inventory systems that automate the analysis of systems within their scope. They produce sets of properties for each asset that can be used for further analysis [**Mic09b**].
- Finding groups of similar assets is a common problem in the data mining field. Methods applied there can be used for asset clustering. Property sets can be interpreted as vectors in multidimensional space. Therefore well known clustering algorithms such as self-organizing maps with respective visualization techniques lead to the required result. An example of this from the field of risk management in the biodiversity domain is BioMatch [**Dug08**].
- Mature domains with incident management systems may be able to record exact costs for incidents, including man-power, material costs and loss in revenue. This opportunity applies more to the insurance domain.
- An organisation’s information policy may collect and provide data about incident frequencies which in turn can be used for assessing future risk. These databases do not pose a technical challenge but depend heavily on processes being diligently followed.

- The challenge with threat modelling is domain specific. There are formal techniques with tooling support developed for software systems [**Lar09**] and guidance provided in directives of the European Union [**Wik09c**].

4.2.3 Risks

The lists of assets under assessment in this phase will normally have been reduced to a manageable amount. However, a reliable estimation of threat properties will still require a large number of domain experts. These will process the information gathered and produce a risk level. The results of this step have a consistent format and can be easily processed.

The interpretation of the data depends on the technique used. In qualitative and semi quantitative analysis the data provided is often biased which can lead to incomparable results. The quantitative approach is only applicable to very mature domains that have large sets of data on numerous events, properties and processes.

The approach using a structured questionnaire to answer questions about measures in place can counterbalance the subjectivity. Many risk assessment methods that are domain specific supply a set of controls and corresponding questions that help with the implementation of this phase. Generally the role of the domain expert shifts from answering each question, which may be done by operations personnel, to the defining of a path from the answer provided to the resulting risk level. This is complex and requires intimate understanding of the threat and the controls but needs only be determined once for each threat type. This allows this method to scale up and enables rapid execution and re-execution. In some cases it may even be possible to check the correct implementation of a control via automation, e.g. an installed virus scanner using a virus scan test file such as the EICAR-Test-File.

Data formats in this phase can include paper forms, spreadsheets and enterprise databases. Automated processing requires a standard format that must be used throughout the process. Even within the enterprise databases data exportability is commonly a missing feature and therefore organisations are locked into their original vendor. This can be a major constraint on the process of deciding which software tool to use in this process.

Aggregation of data relating to the assets represents a one-time cost of defining the appropriate aggregation clauses. The interpretation of data is related to the specific scope of the organisation and can therefore be comparable for multiple assessments.

This chosen approach with semi quantitative elements and a structured questionnaire to determine the risk levels poses a large opportunity for software automation. The potentially large amount of data sources, the large number of domain experts required for assessment, and the use of simple questionnaires create a scenario of data presentation and input which lends itself well to a software based assessment solution.

Defining data and aggregation structures creates two opportunities. A common format to structure assessment data and their corresponding calculations is required as a basis for tools to execute the assessment. Secondly a modelling tool to simplify data entry in this format would reduce the time-to-implementation for these processes.

In addition the issue of reporting is an area that can be assisted by existing visualisation techniques. However, considering the diversity of the formats involved a visually effective report may pose a challenge.

This phase certainly represents the area of greatest opportunity through standardization in combination with software automation.

4.2.4 Strategies

Once aggregated values are available their interpretation is the focus of the strategies phase. The risk analyst will work from top to bottom trying to identify hotspots of high risk that need to be tackled. This process can be tedious if the information from the risks stage is not readily available in a format that allows easy navigation through the asset hierarchies, questions and answers. A manual pre-processing of results into an electronic report with hyperlinks should be considered to reduce time spent on risk analysis and reduce the error margin of incorrectly interpreted data.

Reporting generally plays a vital role in this phase. It must allow quick identification of causes for high risk levels on assets, for example, supporting a drill-down to the control that was tested and where the implementation failed. If a control was implemented at all it should be possible to trace how efficient or effective it was or identify the root cause for its failure. The choice for additional controls or improvements to existing controls will be determined by the analyst. To help in this decision making process it should be possible to re-execute assessments using different parameters. Without software automation in the risks phase this task is unlikely to be cost-effective.

The goal of the assessor is to produce a list of controls and predicted changes in risk levels after successfully implementing them. It may be further required to provide a cost for each control implementation. This aspect of the phase is outside the scope of this work.

Once controls have been implemented the assessment should be re-executed to verify that the results align with the predictions. Risk assessment is not a linear but rather an iterative process that repeats in regular cycles to assess changes in risk levels.

Opportunities:

- The pre-processing phase mentioned above is easily automated by the tool used to gather and aggregate data for the assessment. A software application could use visualisation techniques, possibly even multiple dimensions to let the risk assessor navigate through the available data.
- The organisation and its processes will evolve. Therefore the risk assessment approach may change and the tooling or specifics may have to adapt to this change. Any approach suggested here should be as generic as possible to cater for this evolution.
- Depending on the quality of the model the detection of unsuitable, ineffective or missing controls could be automatically derived from the answers to a specific assessment in conjunction with the solutions designed for the asset under assessment. The optimal set of controls across a set of assets can be calculated based on mathematical optimization.

4.2.5 Conclusion

The analysis of the generic risk assessment process has helped to identify a lot of minor and some major opportunities for software automation to improve the process execution. The goal of a domain independent risk assessment approach has led to fewer opportunities than expected due to very domain specific data sources in the assets and threats phases. Nevertheless the risks phase offers the greatest opportunity for automation through software systems without setting constraints on the domain to which it is applied.

Some minor opportunities identified are already the subject of research or under development. Impacts of these developments on the software tool must be considered. Some could be seen as an extension of this proposed tool and may therefore be considered for inclusion. Others may be able to make use of supplied interfaces.

The iterative nature of risk management requires comparability. Aggregation in risk assessment will benefit this goal. Faber notes: "Indeed the aggregation of risks may be seen as the ultimate goal of establishing a uniform basis for assessing risks; only if risks are assessed in a comparable way it will be possible to aggregate them" [**Fab08**]. Naturally risk aggregation leads to better designed risk distribution strategies and improved calculations of realistic values for monetary buffers in case of incidents.

Two types of aggregation are of interest for this work. First, the aggregated risk model can disclose horizontal sensitivities. This is the effect different threats can have on one asset. Secondly it can disclose vertical sensitivity by identifying how threats can impact higher level assets and processes. In addition recording aggregated losses will provide a source of information for determining the impact values of future threats.

Aggregation can not only be applied to physical asset hierarchies, (pencils and desks up to equipment and buildings), but is also applicable to a multitude of other factors like geographical distribution, threat categories or incident duration.

In aggregating risk values a distinction in direct and indirect threats can be made. This separation allows the calculation of a robustness factor using risk levels for direct threat (R_{AD}) and indirect threat (R_{AID}) expressed as [**Fab08**]:

$$I_{AR} = \frac{R_{AD}}{R_{AD} + R_{AID}}$$

To sum up, the use of a software system to automate and support risk aggregation offers considerable potential and is therefore the rest of this work will focus on this opportunity.

5 Concept

The following chapter describes the design of data models for objects identified using the generic risk management process but will focus on the risk aggregation phase. Attention will be given so that it is applicable to multiple domains thereby allowing flexible usage.

The model must cater for the calculation of multiple values at different levels. The chosen approach will be multi dimensional in order to facilitate any level of aggregation that may be encountered. The calculation and modelling modules of these systems must be capable of working with existing risk assessment models. These implementations can be based on standards, adaptations of standards or customized models to ensure a perfect fit to the organisation. A highly generic approach must therefore be taken.

In the following chapter MuDRA, the multi dimensional risk assessment process developed as a part of this thesis will be described and explained.

5.1 Inputs and Outputs

The first consideration in the development of this risk aggregation model is to define available inputs and required outputs. The former includes data from the first phase of the previously described process:

- Asset hierarchies are the identified assets that are valuable to the organisation, together with their dependencies, relationships and any composition information. These assets will be grouped into clusters with similar attributes. For example server systems in the demilitarized zone with connections to the Internet can be grouped into a “web server” cluster. Each asset has been given a value representing the maximum loss that can occur if the asset is completely destroyed.
- Security requirements for each asset or asset class have been defined and potential threats identified. These threats have been documented and prioritized by the maximum impact they can inflict on the asset. Threats can fall into different categories depending on the origin of the threat, e.g. confidentiality, integrity or availability.

Within the risk management system the aggregation process must deliver the following outputs for the succeeding phases.

- First and foremost a general sense of the health of the organization as a whole (being the primary asset) must be delivered from the aggregation phase. This will typically be a traffic light based indicator. Red representing a highly acute criticality, yellow means the current maximum impact value has surpassed a policy threshold and green ensuring risk measures comply with organizational standards.

- These indicators are usually semi quantitative scales scored on the basis of quantitative aggregation. Monetary values are important at this level to gain a fast overview of the materiality of any hotspots that were identified. Therefore the following values should be included as outputs for this phase.
    - The probable monetary impact this year: Based on the probability of an incident occurring in the respective risk level this year, multiplied by the number of deficient assets, multiplied by the average maximum impact of each asset in this category. This results in a scalar value for expected losses in this relevant risk level category.
    - Percent of maximum monetary impact this year: Sum of all maximum impact values of each asset at this level as a percentage of the sum of maximum impact at all risk levels . This value will help to disclose high value assets which are at high risk levels.

Risk level	Average incidents per year	Probability of occurrence per year
1	3	0,8%
2	11	3,1%
3	23	6,5%
4	35	9,8%
5	55	15,4%
Total	127	36,7%

Table 6: Risk level probability[4]

[4] Each row depicts how many incidents occurred that could have been completely mitigated by measures that are in place in this risk category. The values given are examples.

Risk level	Assets at this level	Probable number of deficient assets	Probable monetary impact (in 1000 EUR)	*Maximum monetary impact (in 1000 EUR)*	Maximum monetary impact in this risk level as a percentage of the sum of total maximum monetary impact in all risk levels:
1	1024	8	354	*1780*	73%
2	512	16	34	*66*	2,8%
3	256	17	35	*300*	12,4%
4	50	5	134	*20*	0,8%
5	5	1	455	*260*	10,8%

Table 7: Current impact level probability[5]

These outputs are sufficient when the risk levels meet organisational approval. More often than not they will uncover areas of improvement that need to be further investigated. For this the model developed must be able to provide a means of navigating from calculated values to the corresponding sources. The following information is required for such a drill-down analysis:

- An asset hierarchy with links to allow navigation through asset compositions showing individual properties and cluster membership.
- For each asset; the aggregated risk level, any corresponding threats or associated threats resulting from other assets and any threat values such as impact or probability.

[5] Each row depicts how many incidents occurred that could have been completely mitigated by measures that are in place in this risk category.

- A decomposable risk level aggregation identifying separate criteria for each control and the questions that prompted the answers for these properties.

5.2 Conceptual data model

The goal of the aggregation subsystem is to generate the outputs from the inputs provided. Therefore relationships and processing logic are now defined between these elements.

5.2.1 Asset hierarchies

The organisation consists of one main asset hierarchy, comprised of all physical and logical assets. The model is defined by composition, each parent specifying what percentage of its own value the child's value represents. Each asset is therefore comprised of its own value and the weighted sum of its children's values.

The concept of virtual assets allows there to be a number of virtual hierarchies of assets that represent intangible concepts such as processes. For example certain business processes may be audited separately. These virtual hierarchies are composed in the same way as the main asset hierarchy.

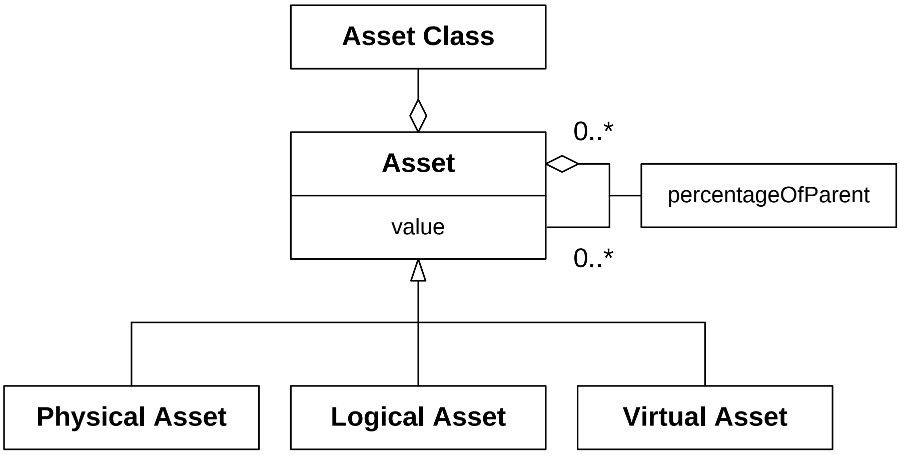


Figure 7: MuDRA Concept: Assets

5.2.2 Threats and Risks

Identified threats can impact assets (or asset classes where each asset is impacted) which denotes a risk. For each asset a risk level can be defined. This level consists of the probability that the threat will occur, and if it does, identify what value the asset could lose. This level should always err in the favour of a higher value to ensure visibility.

Risk is defined based on the threat scenario. For example the threat "Manipulation of data files by an unauthorized person usurping an authorized user's authority" may have the following risk level definitions. These inherent risk levels describe an exemplary environment expected at this level.

1. Very Low risk: Camera surveillance, physical access checks
2. Low risk: Physical access on premise required
3. Medium risk: Access to physical object required, but remote access to data
4. High risk: Remote access manipulation possible based solely on virtual objects
5. Very high risk: authentication and authorization mechanism vulnerable

The implementation of controls, e.g. the camera surveillance mentioned above, can partly mitigate threats and therefore change the risk for an asset.

Determining this residual risk level can be very complex. It includes multiple parameters about the controls in place (e.g. implementation status, efficiency, coverage), possible interactions between different controls and organisational policies. The large amount of possibilities requires a flexible calculation mechanism at this level. The MuDRA model caters for this by allowing multiple values and freely definable formulas.

This model can also handle controls that ensure maximum or minimum risk levels, via these formulas. In the example provided above, physically isolated (disconnected) server systems always ensure a maximum risk level of two using the definitions above because physical access to the server rooms is required. In this case the model would be defined so that:

$$c_1 \ldots\ control\colon physically\ isolated\ system$$

$$c_x \ldots\ all\ controls\ applied\ to\ asset, i\ \{1..n\}$$

$$n \ldots number\ of\ controls$$

$$t \ldots threat\ mitigated\ by\ c_x$$

$$risk_{max}(c_1, a) = \begin{cases} impl(c_1, a)\colon 2 \\ undefined \end{cases}$$

$$risk(c_1, a) = \ calculated\ risk\ level\ value\ based\ on\ parameters$$

$$risk(t, a) = \min\left(\boldsymbol{risk_{max}}(\boldsymbol{c_1}, \boldsymbol{a}), avg\left(risk(c_x, a)\right)\right)$$

This will reduce any risk level calculated by other controls to at least the maximum of control c_1. The analogue approach is taken for certain controls that imply a minimum level of risk. For example systems using username and password based authentication can never reach a risk level below three, because this credential type relies solely on access to virtual objects.

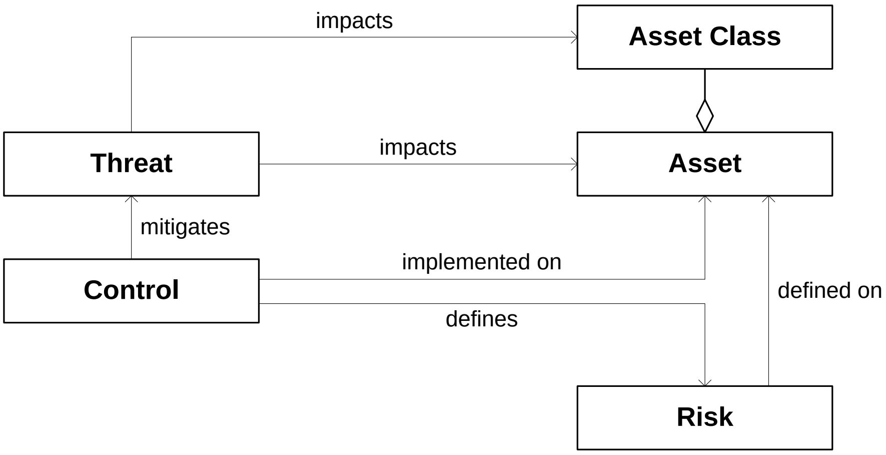


Figure 8: MuDRA Concept - Asset, Threat, Risk Schema

The formulas for risk level calculation can require a lot of information. The concept herein uses a questionnaire type approach to gather this information which is later processed and aggregated. The risk assessor defines the aggregation formula and dependant questions. A specialist for the asset, i.e. operating personnel, will then provide answers to these questions to assess the asset's current state. This separation of concerns leads to a systematic - risk levels are determined consistently - and a scalable - the complex formula definition needs only to be done once - approach. The assessment of status becomes a simplified and easily automated risk assessment process.

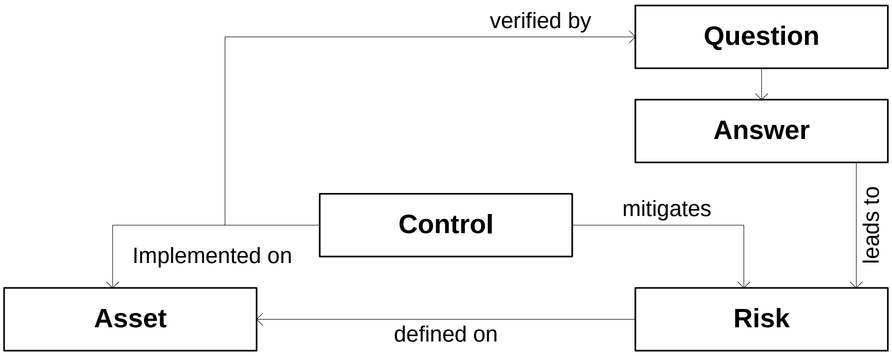


Figure 9: MuDRA Concept - Question Schema

5.2.3 Impact Valuation

The impact of a threat may have different types of impacts with differing value losses for the asset.

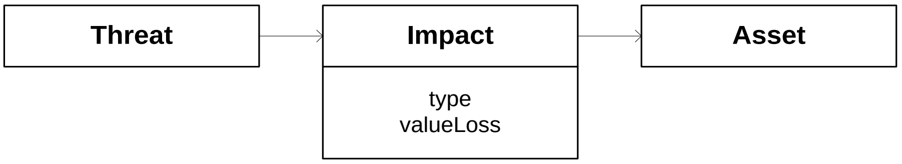


Figure 10: MuDRA Concept - Impact Schema

The values chosen represent a best guess case. This is referred to as single-point or deterministic modelling [**Vos08**]. In the grand picture of a large model these best guess values can lead to a false sense of accuracy. It can be useful to vary these values based on a probability distribution. These distributions will take the best guess value as the centre of an interval and provide probabilities that the values deviate from this value. Common distributions are the Gaussian distribution [**Wik09d**] for continuous values or the Bernoulli distribution [**Wik09f**] for discrete values. Models that have been populated with best guess values can be run through simulations based on these probability distributions to generate a set of combinations for what-if Analysis. A particular combination of inputs may lead to a spike in risk levels. These could be used to implement special controls for just these high-risk scenarios and in risk monitoring phases to identify potential catastrophes that may occur. This concept of adapting the model values is frequently used in Monte Carlo simulations of quantitative analysis. This approach can also be applicable for qualitative analysis if the correct distributions are chosen. The data model presented here could be used for these scenarios.

5.2.4 General risk states

Aggregation of risk levels requires a risk hierarchy based on the respective asset tree. The asset's own risk (based on atomic threats) and the children's risk levels (which are indirect threats for the parent asset) can be transformed to result in the deflected risk level for the asset. The composition function (cf) takes the asset weights into account to determine a realistic overall risk level for the parent asset. To determine a child's overall risk its composition function is used. This process is continued in each child until a leaf asset is reached that does not have any child assets. There the composition function is reduced to returning the asset's direct risk levels without transformation.

The traffic light thresholds are a property of each asset. These values may not vary within asset classes and could therefore be deduced from the corresponding class.

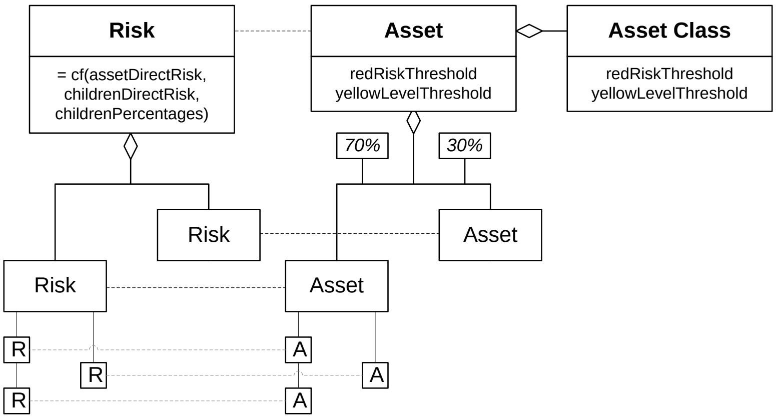


Figure 11: MuDRA Concept - Composite Asset Schema

5.2.5 Risk level probabilities

The model must include a record of incidents that have happened in the past including a monetary value of losses incurred by the asset through this incident. A history of risk levels from previous assessments is vital to reconstruct the risk level that was prevailing at the time of the incident. Ideally at the moment of the incident discovery a risk assessment should be undertaken as part of the forensic process to establish the most current risk level and capture any changes since the last general risk assessment. These form the basis for the following indicator values.

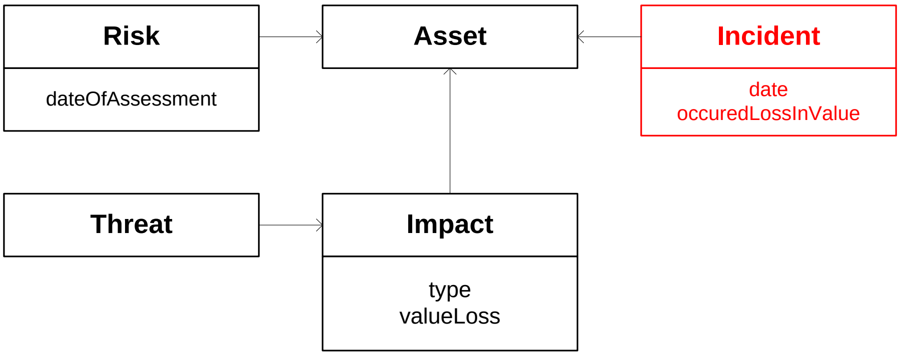


Figure 12: MuDRA Concept - Incident Schema

The number of probable asset deficiencies can be calculated as follows:

$$\text{def}_{\text{risk}} = \text{assets}_{\text{risk}} * (\text{incidents}_{\text{risk}} / \sum \text{incidents})$$

$\text{assets}_{\text{risk}}$	Number of assets currently at this risk level.
$\text{incidents}_{\text{risk}}$	Number of average past incidents occurred to assets at this risk level.

Most probable and maximum monetary impact per year can then be defined as:

$$\text{avg\_imp}_{\text{risk}} = \text{def}_{\text{risk}} * \text{avg\_valueloss}_{\text{risk}}$$

$$\text{max\_imp}_{\text{risk}} = \text{def}_{\text{risk}} * \text{max\_valueloss}_{\text{risk}} / \text{total\_max\_valueloss}$$

$\text{avg\_valueloss}_{\text{risk}}$	Average of value lost by impacts that affect assets at this risk level.
$\text{max\_valueloss}_{\text{risk}}$	Maximum of value lost by all impacts that affect assets at this risk level.
total_max_valueloss	Total of all value lost by all possible impacts.

5.3 Technical data model

So far the constraints imposed by the MuDRA model have been minimal. It is required that the model is implemented in a generic fashion thereby allowing properties of any object to be modelled as required. Therefore the technical model reduces the domain model to a simple set of objects with assigned values. This also ensures a common pattern for defining values and their calculations.

For example asset classes are properties of the asset and modelled as specific value objects (a). The same applies for thresholds properties (b). The goal of controls in the model is to determine their operational efficiency. They are modelled as question groups (c). The control properties are gathered through questions and answers and define properties for the risk level (d). The risk level uses a formula to calculate the resulting risk level which is stored in the value of the question group (e) and receives its input values from the selected answer's value objects (f).

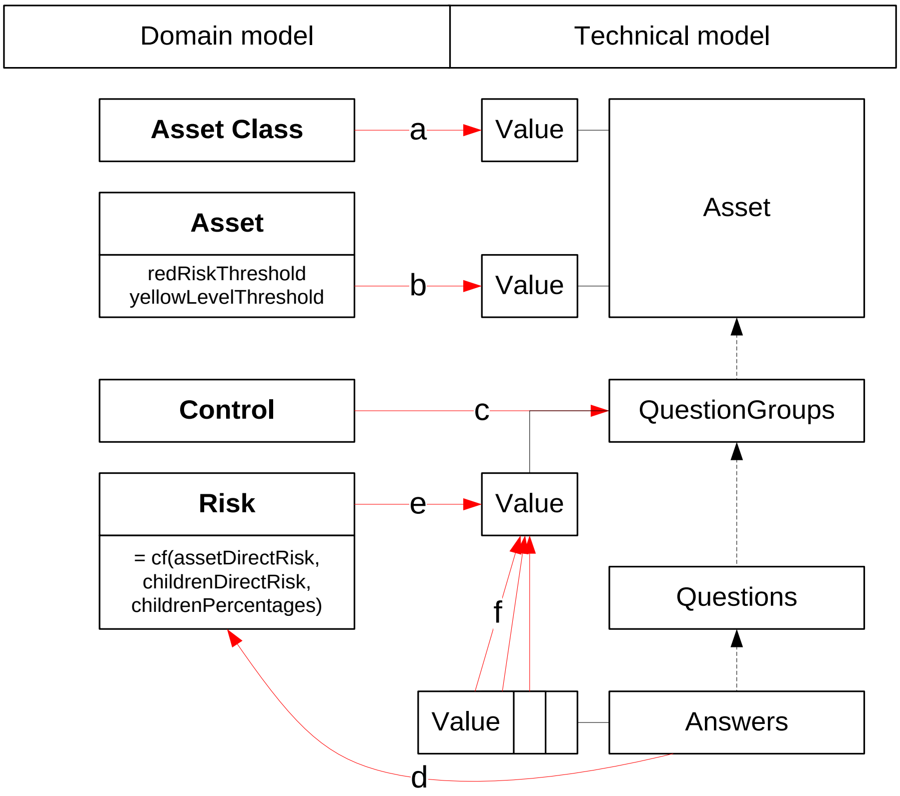


Figure 13: MuDRA Technical Conversion - Master Data

The concept of threats and risks is shown below and modelled such that each threat becomes a question (a). The question asks if the threat is relevant for the asset and if so what value loss is to be expected. The selected answer's value object contains the impact type, the user given value loss and other threat properties. These are transported to the asset (b) by the aggregation. Therefore the impact is implied in the value properties of the asset (c).

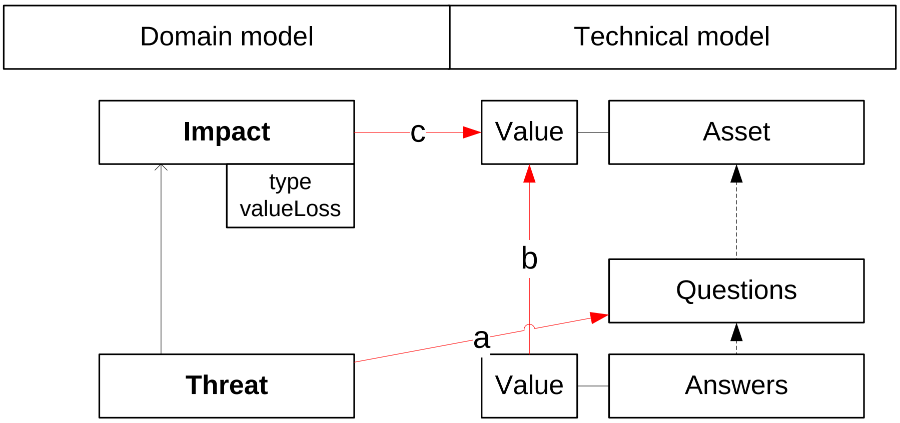


Figure 14: MuDRA Technical Conversion - Threats to Questions

This simplification results in a highly generic technical model for the assessment approach, described above, which in itself was already very generic. This supports the concept of using of MuDRA for a number of different domain scenarios.

5.3.1 Aggregation dimensions

As described above the MuDRA concept requires aggregation at different levels (in order) to incorporate the proposed generic assessment approach. The concept interprets different levels of aggregation as dimensions. The primary dimension is the timeline. In deciding which strategy provides the most efficient implementation, assessments can be simulated using MuDRA. Therefore the timeline is not strictly linear but may contain branches to reflect these simulations.

The second dimension incorporates the primary asset tree and any virtual asset trees. These trees are unordered, weighted, labelled trees. Each asset spans a question dimension based upon threats identified for the asset. Questions can activate further questions leading to a logical tree construct for this dimension. Answers to questions can include single and multi-valued answers. The latter can lead to a fourth dimension of sub questions that are posed for each answer given in a multi-valued answer set.

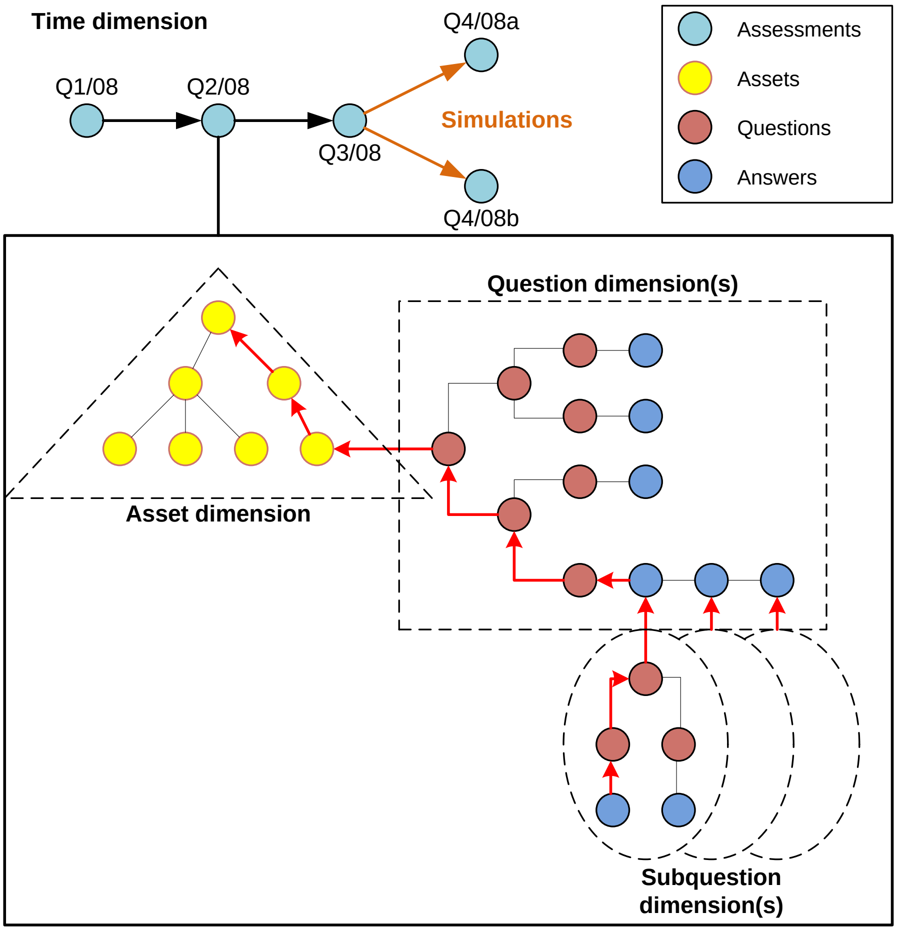


Figure 15: MuDRA Dimensions

5.3.2 Asset dimension

Primary asset trees are defined through simple references from the child asset to its parent. Each asset can be represented by a virtual asset in a number of virtual asset trees. Separate objects were introduced to maximize flexibility of the virtual tree aggregation dimension. The virtual assets are linked to each other with linking objects that specify weight and ordering.

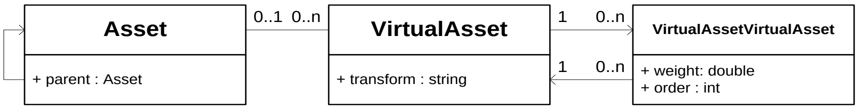


Figure 16: MuDRA Technical Data Model - Asset Hierarchies

5.3.3 Question dimension

MuDRA supports multi-stage risk aggregation processes. Stages are ordered and consist of a number of weighted question groups. Each question group is composed of further weighted question groups or questions. Each answer consists of multiple answers that can activate question groups which then must be answered. Question groups without activating answers are considered automatically activated and form the initial starting point for the risk assessment questionnaire.

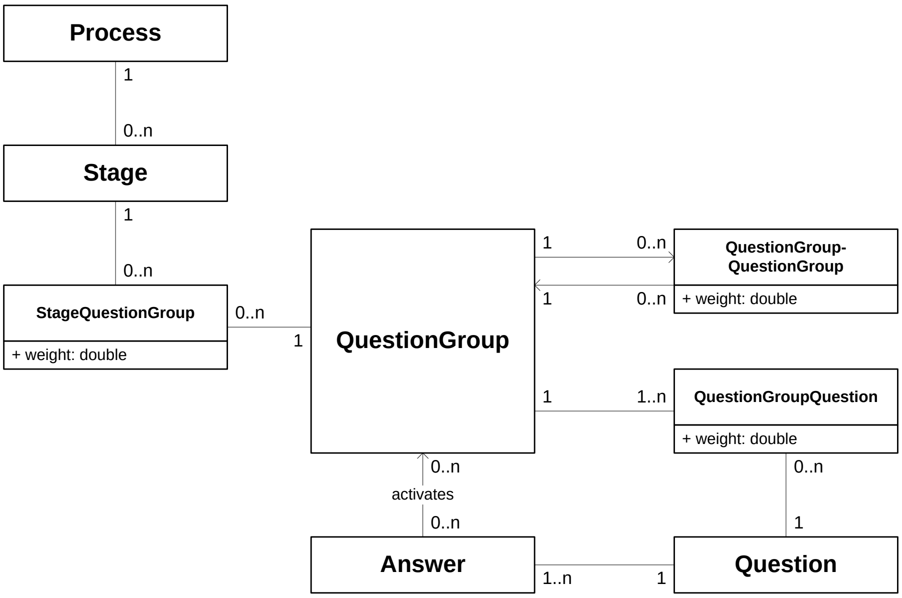


Figure 17: MuDRA Technical Data Model - Questions

A common feature found during the analysis was the utilisation of the same question groups to multiple processes. This way question groups for specific controls can be reused in different assessment situations. For example controls such as fire extinguishers in the server rooms are common to multiple risk assessment frameworks and share similar questions to determine control implementation.

5.3.4 Value objects for aggregation

Value objects are used during aggregation for data storage, transformation and flow throughout the tree. Values constructed at any level can contain data such as integer, string and multi valued items. This data is held in the transform property and can consist of three types of data:

- Atomic values contain a piece of data (e.g. “4.5”).
- Reference values refer to the data from another value object. This can be a node in the same collection of the parent’s value objects or a value supplied by another branch in one of the predecessor dimensions (e.g. “#REFA#”). See the chapter on tree ordering for further information.

- Composite values that contain a formula for calculating a new value from a mix of atomic and reference values (e.g. “MAX(4.5,#REFA#)”).

If placed at a non-leaf node it is expected that the transform property contains a transformation property defining the aggregation of child values. Currently any aggregation function with multiple inputs (e.g. average, maximum, minimum or sum) is supported and can be supplied with the child values or weighted child values (if supported) (e.g. “AVG(#WEIGHTEDCHILDREN#)”).

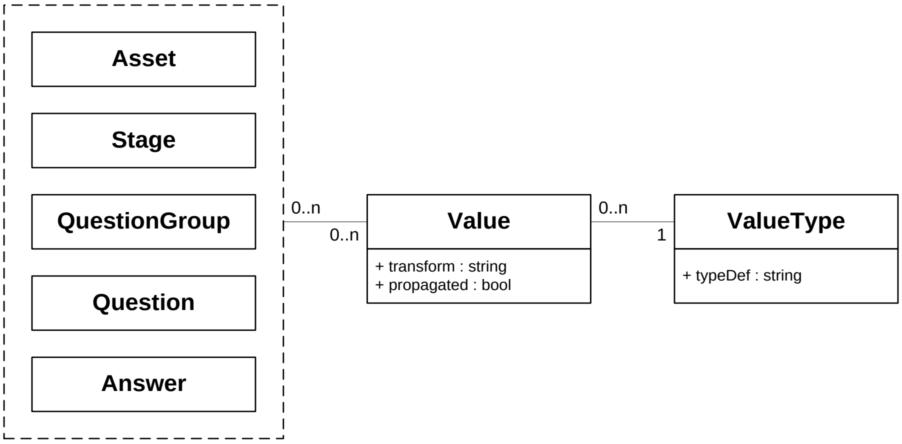


Figure 18: MuDRA Technical Data Model - Value Objects

This generic data flows through the aggregation tree bottom to top if the data flow is activated. This activation is defined top to bottom. Data only flows along the path of a chain of values of the same value type. In the following figure two values have been defined on the asset. Both have the propagate setting set to true. Therefore during aggregation the parent creates a value object for each child until it encounters a child that also defines a value for the corresponding value type. If this happens propagation is halted and the new value type adopts control of the propagation. In the left case (see diagram below) propagation is halted and no data is transferred to the asset. The right case constructs a chain of equal value objects and the data flows from the answer object to the asset.

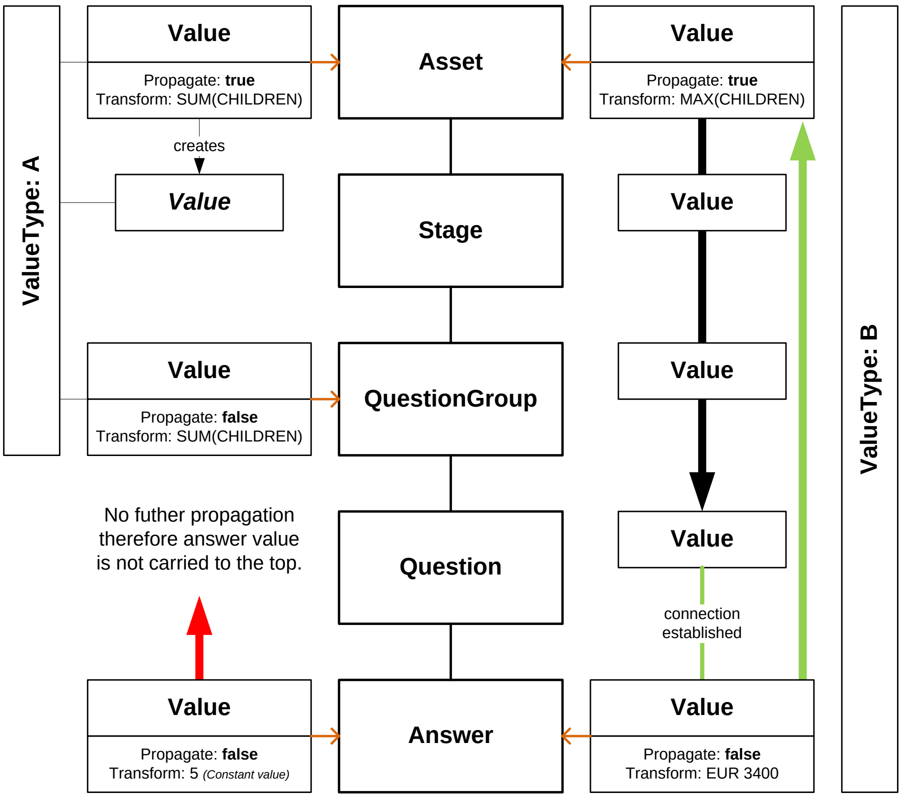


Figure 19: MuDRA Technical Data Model - Value Propagation

Assessments are carried out in cycles. The assessment cycle object allows creation of a template for an assessment including a specific process and the asset to assess. The risk assessor can choose an assessment cycle to execute, which creates a running assessment based on the corresponding process and asset. All domain objects mentioned before are considered master data that is shared between all assessments. The answers given for each assessment are recorded in answer instance objects that apply to a specific answer for a question and the currently executed assessment.

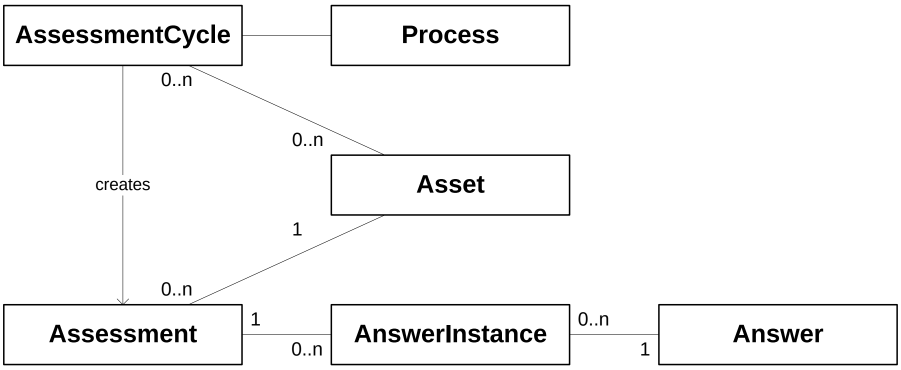


Figure 20: MuDRA Technical Data Model - Assessment Answer Instances

5.4 Aggregation Process

The multiple dimensions in the technical data model (TDM) support modelling of the aggregation domain. When calculating the aggregation, the TDM exposes unneeded complexity. Therefore it is projected into a concrete aggregation model (CAM) representing a large totally ordered rooted tree.

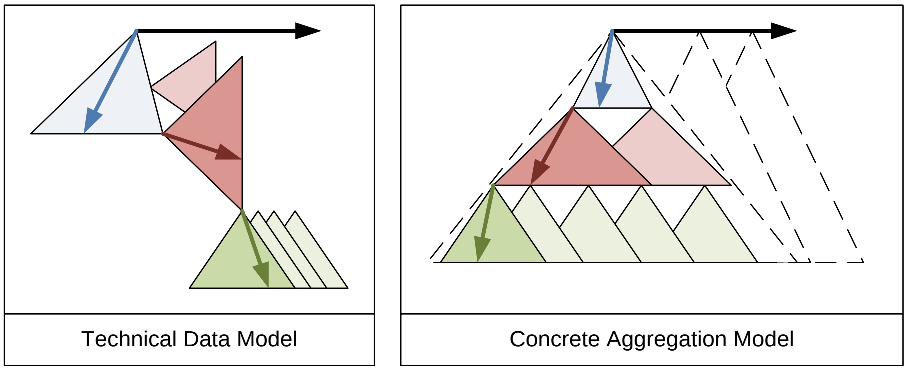


Figure 21: MuDRA Technical Data Model and Concrete Aggregation Model

The time dimension remains unaffected. The asset, question and sub question dimensions are projected into aggregation specific objects. More specifically an aggregator node object represents an object in the CAM that implements an interface called IAggregatable and thus supplies information common to all aggregation nodes

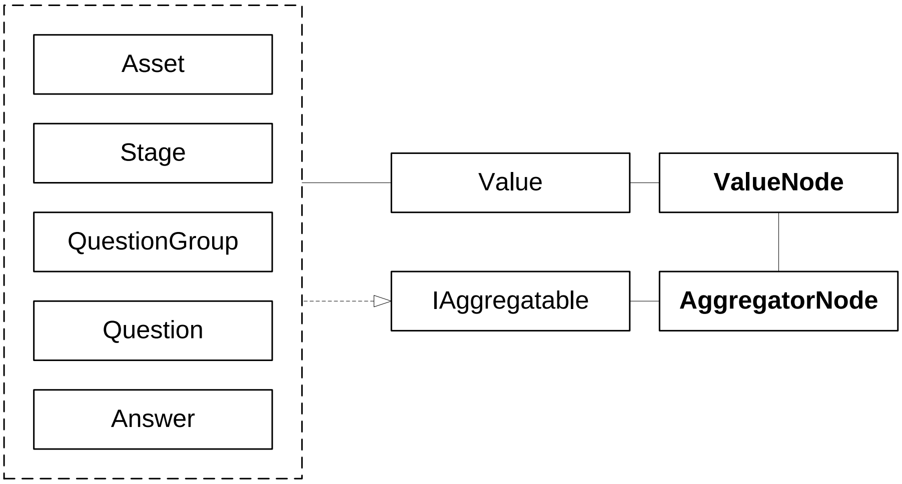


Figure 22: MuDRA Technical Data Model - Aggregator Objects

These nodes contain value node objects for each value represented by the original TDM object. During the projection the TDM is flattened, meaning propagation is carried out and a value node object created for each propagated value node. Each aggregator node creates its child nodes. The resulting tree represents the full calculation schema for the aggregation.

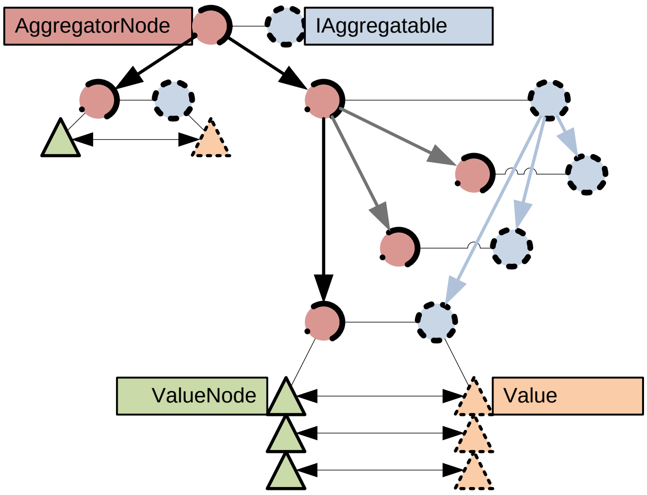


Figure 23: MuDRA Aggregation - Node and Value Conversion

The CAM can now proceed to gather a snapshot of data from the current assessment. Each aggregation is a snapshot view on the assessment's status and must therefore run in complete isolation of any changes that might occur due to a running assessment. Therefore each node in the CAM copies data required for calculation, including selected answers and provided answer values. In doing so it is also possible to retrace resulting aggregation values to their source values even if the actual assessment answers change over time. This feature allows MuDRA to create intermediate aggregation snapshots before an assessment is fully completed.

Each value object contains data in the transform property which is copied. If the owning IAggregatable object also implements the interface IAnswerable this denotes an open question where there is not a discrete set of answers to choose from, but rather a numeric or textual answer is supplied by the user. In this case the value node object in the CAM will replace the transform property with the supplied answer value. Traceability is still honoured because the corresponding domain value must have an atomic transform property with the value "$ANSWER". Compositions on the provided values are only possible in a secondary value object attached to the TDM node that references the provided value.

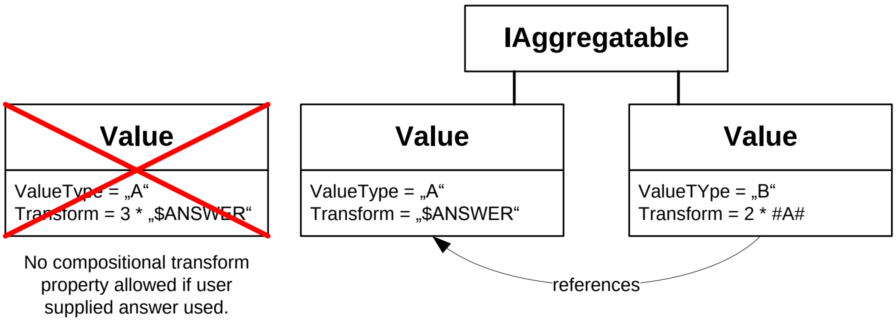


Figure 24: MuDRA Aggregation - User Supplied Answers

Additionally the transform property is parsed for references to other values to prepare for subsequent steps of the aggregation process.

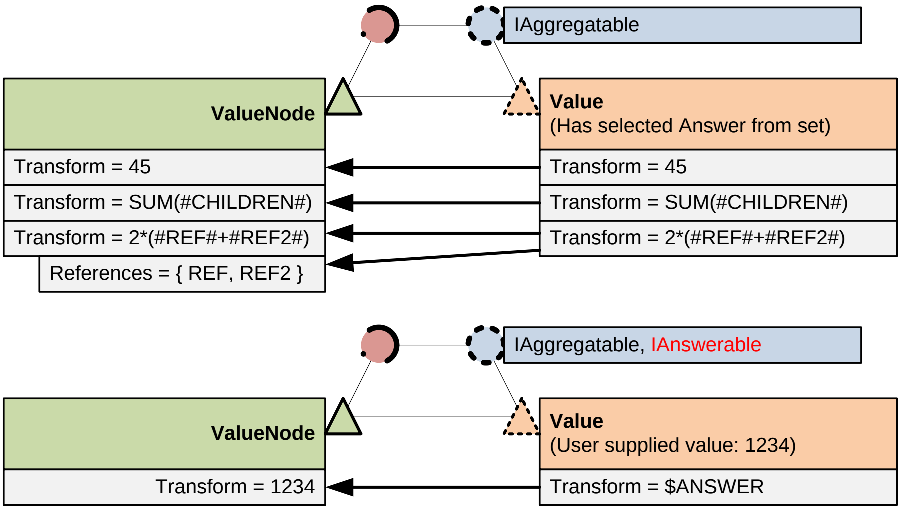

IAggregatable
ValueNode
Value
(Has selected Answer from set)
Transform = 45
Transform = SUM(#CHILDREN#)
Transform = 2*(#REF#+#REF2#)
References = { REF, REF2 }
Transform = 45
Transform = SUM(#CHILDREN#)
Transform = 2*(#REF#+#REF2#)
IAggregatable, IAnswerable
ValueNode
Value
(User supplied value: 1234)
Transform = 1234
Transform = $ANSWER

Figure 25: MuDRA Aggregation - IAggregatable and IAnswerable

5.4.1 Tree ordering

The aggregation tree provides a total ordering. This can be proven as follows.

Let $f_a(x)$ return the position of an aggregator node in the final ordered set and let $f_v(x)$ return the position of the value node within a collection of value nodes of the parent aggregator node. Additional functions are defined as follows:

The function S(x) will return a list of names that are calculated by the value nodes of x directly. In the above example S(J) = {A,B,C} and S(B) = {G}. The function C(x) will return all direct children of the aggregator node. Again in our example C(E) = {D} and C(I) = {K,L}. The function R(x) returns all references that a direct value node of the aggregator node x has in its transform property.

The function alpha(x,y) returns the alphabetical order of the names of the aggregator nodes x and y as minus one if x's name is alphabetically smaller then y's name and vice versa. If both names are identical the function returns zero.

The following functions and the main order function are now defined. The order function is undefined for nodes that contain circular references, as this is not allowed. The supplies function returns a set of names of calculated values by the sub tree with x as its root. The refs function similarly returns a set of all transitively referenced values in this sub tree.

```
supplies(aggregatornode x)
{
    set X = S(x)
    for each (c ∈ C(x))
        X = X ∪ supplies(c)
    return X;
}

refs(aggregatornode x)
{
    set X = R(x)
    for each (c ∈ C(x))
        X = X ∪ refs(c)
    for each (r ∈ R(x))
        X = X ∪ refs(r) /* transitive */

    return X;
}

order(aggregatornode x, aggregatornode y)
{
    /* intersect each reference list with the other supply list */
    set XRefInY = refs(x) ∩ supplies(y)
    set YRefInX = refs(y) ∩ supplies (x)

    if (|XRefInY| > 0 & |YRefInX| > 0) return undefined
    if (|XRefInY| = 0 & |YRefInX| = 0) return alpha(x,y)
    if (|XRefInY| > 0) return 1
    if (|YRefInX| > 0) return -1
}
```

To sum up the function order will return:

x < y: order(x,y) = -1
x > y: order(x,y) = 1
x = y: order(x,y) = 0

To achieve the aforementioned total ordering the following statements must hold true:

Totality: a<=b or b<=a

All paths of the order function return a value not equal to 0 except for when it falls back on alphabetical ordering. In the latter case the alphabetical ordering is totally ordered. Therefore under the precondition of non circular references the totality requirement is fulfilled.

Anti-symmetry: $a <= b$ and $b <= a$ ➔ $a = b$

Case 1: No references, alphabetical ordering:

In the case that a and b have no references to each other’s supplied values the alphabetical ordering provides total ordering for all cases of a and b except for two nodes with identical names, which is prohibited throughout the tree.

Case 2: References between a and b:

We split the condition into four possible cases.

1) $a < b$ & $b = a$: $[(\text{refs}(b) \cap \text{supplies}(a)) > 0 \;\&\; (\text{refs}(a) \cap \text{supplies}(b)) = 0] \;\&\; [(\text{refs}(a) \cap \text{supplies}(b) = 0 \;\&\; \text{refs}(b) \cap \text{supplies}(a)) = 0]$
2) $a = b$ & $b < a$: $[(\text{refs}(b) \cap \text{supplies}(a)) = 0 \;\&\; (\text{refs}(a) \cap \text{supplies}(b)) = 0] \;\&\; [(\text{refs}(a) \cap \text{supplies}(b) > 0 \;\&\; \text{refs}(b) \cap \text{supplies}(a)) = 0]$
3) $a < b$ & $b < a$: $[(\text{refs}(b) \cap \text{supplies}(a)) > 0 \;\&\; (\text{refs}(a) \cap \text{supplies}(b)) = 0] \;\&\; [(\text{refs}(a) \cap \text{supplies}(b) > 0 \;\&\; \text{refs}(b) \cap \text{supplies}(a)) = 0]$

Cases 1-3 all lead to contradictions in the sense that sets cannot be empty and not empty at the same time, leading to only one valid possibility:

4) $a=b$ & $b=a$. Thereby $a<=b$ & $b<=a$

This demonstrates $a=b$ and the anti-symmetry is proven.

Transitivity: $a <= b$ and $b <= c$ ➔ $a <= c$

If $a = b$ and $b < c$ then $a < c$ follows and vice versa for $b = c$.

If $a < b$ and $b < c$ then $\text{refs}(b) \cap s(a) > 0$ and refs(c) contains all elements of refs(b) based on the definition of the refs formula. Therefore $\text{refs}(c) \cap s(a) > 0$ must be valid and $c > a$ follows.

Due to this total ordering the nodes of the aggregation tree can be flattened to a single chain of nodes. References between nodes are resolved and the resulting chain can be processed from smallest to largest node in order to complete the aggregation.

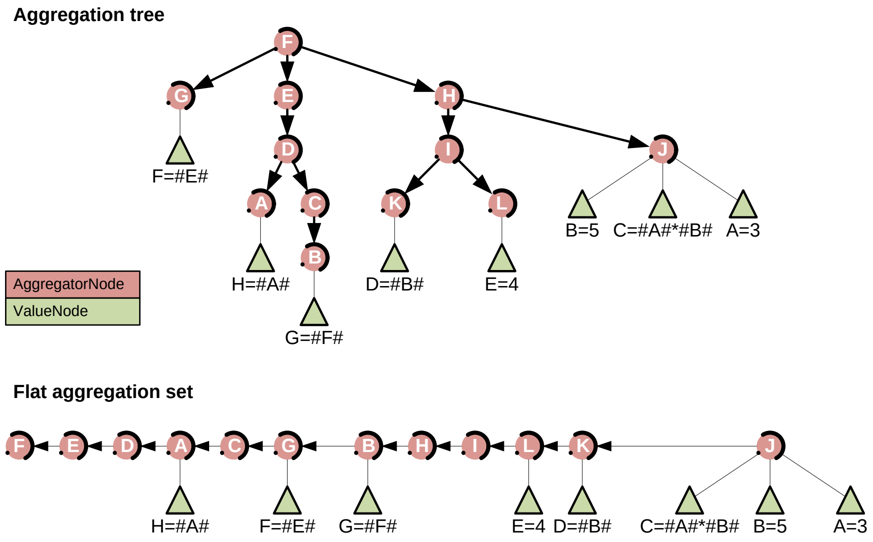


Figure 26: MuDRA Aggregation - Tree to Set Conversion

5.5 Assessment Markup Language

The inputs and outputs of the data model may be generated by other information systems. Therefore a generic format for exchanging data with a MuDRA system is defined. The Assessment Markup Language is an xml based format for three classes of data: organisational structures, process structures and results.

All AML documents must start with a root name called MuDRA. Beneath the root node any number of fragments representing model elements can be included.

5.5.1 Organisational Structures

This section defines organisation specific structures such as asset hierarchies, users, roles and clients.

A MuDRA system may potentially support multiple clients even within one organisation. Users are imported as part of a client.

`<Clients>`	
`    <`**`Client`**	
`        Spec="CLIENT1"`	A short name for referencing this item.
`        Name="Demo"`	A human identifier for the client.
`        Owner="PER-ORGADMIN">`	A reference to a person that manages this client’s persons.
`        <`**`Person`**	
`            Spec="PER-`	A short name for referencing this item.

ORGADMIN"	
Name="John Doe"/>	A human identifier for the person.
</Client>	
</Clients>	

Table 8: AML - Clients

The assets node contains a hierarchy of asset nodes representing the main asset tree.

<Assets>	
<**Asset**	
Spec="ORG"	A short name for referencing this item.
Name="Organisation"	A human identifier for the asset.
Owner="PER-ORGADMIN"	Reference to a person that manages this asset.
Client=”CLIENT1”	Reference to a client that this asset belongs to.
Percentage=”100”	Percentage of the parent’s value this child asset represents.
<Asset... />	Child assets.
</Asset>	
</Assets>	

Table 9: AML - Assets

Virtual assets and asset trees can be defined in the same format, except that child assets are only referenced by their spec attribute.

<Assets>	
<**VirtualAsset**	
Spec="ORG"	A short name for referencing this item.
Name="Organisation"	A human identifier for the asset.
Owner="PER-ORGADMIN"	Reference to a person that manages this asset.
Client=”CLIENT1”	Reference to a client that this asset belongs to.
Percentage=”100”	Percentage of the parent’s value this child asset represents.

`<Asset Spec=”A1” />`	Child assets.
`<VirtualAsset ... />`	Child virtual assets.
`</VirtualAsset>`	
`</Assets>`	

Table 10: AML - Virtual Assets

The security node underneath the root accepts a list of access nodes. These specify users’ roles for a specific asset.

`<`**`Security`**`>`	
`<`**`Access`**	
`Role="ADMIN"`	Specifies a role identifier. This value depends on the roles available in the importing system. By default two roles must be accepted: - ADMIN: has full control over all data in the system. - ASSESSOR: can change aggregation data for this specific asset. - OPERATOR: can answer questions for this asset during the assessment.
`Person="PER-ORGADMIN"`	This references the spec value of a person in the system and assigns the role.
`Asset="ORG" />`	This references the spec value of an asset in the system that the role applies to.
`</Security>`	

Table 11: AML - Security

5.5.2 Process Structures

This section includes elements required to represent a specific process such as process stages, value schemas, questions and formulas.

Value types used in AML must be defined in the values section.

`<`**`Values`**`>`	

<**Value**	
Spec="X01_CONF"	A short name for referencing this item.
Name="X01 Confidentiality"	A human identifier for the value.
Type="Double " />	The data type this value represents. Currently the only valid values are: - Double: a single value numeric node - Bag: a multi value node
</Values>	

Table 12: AML - Values

Questions used during the assessment are specified in the questions node.

<**Questions**>	
<**Question**	
Spec="X01_CONF"	A short name for referencing this item.
Title="X01 Confidentiality"	The question’s title.
Type="INTEGER"	The data type this value represents. Currently the only valid values are: - INTEGER: a single numeric must be specified as answer to this question. This value will be written the value type object specified by AnswerValue. - CHOICE: a set of answers is provided for the user to choose from.
AnswerValue=”X01_CONF” />	References a value type to write the answer to.
<Description>...</Description>	A descriptive text asking the question to the user.
<**Answers**>	The collection of answers. Only for question type CHOICE.

<**Answer**	The first possible answer.
Value=”YES”	The answer’s title presented to the user.
ActivatesQuestionGroup =”QG1,QG2” >	If this answer is selected the question groups referenced here are activate and must be answered during the assessment.
<**Value**	A value object that is created if this answer is selected.
Spec=”X01CONF”	The value type reference to create.
Transform=”43”/>	The data to write to the value created.
<**Value**	
Spec=”X02CONF”	
Transform= ”2*#X01CONF#”/>	Data written to the value created is two times the referenced value of another value object.
</Answer>	
<Answer>...</Answer>	Further answers for this question.
</Answers>	
</Question>	
</Questions >	

Table 13: AML - Questions

Questions are grouped into question groups for easier management and referencing.

<**QuestionGroups**>	
<**QuestionGroup**	
Spec="QG1"	A short name for referencing this item.
Name="Confidentialities"	A human identifier for the value.
<**QuestionGroup />**	Sub question groups
<**Question**	
Spec=”D01_CONF”	References a question to include in this question group.
Weight=”5” />	A weight for this question in the group. Used for the transform value

	#WEIGHTEDCHILDREN#. Defaults to 1.
</Question>	
<**Value**	A value object that is created for this group.
Spec=”D01_CONF”	The value type reference to create.
Transform= ”Max(#CHILDREN#)” />	Data written to the value created is the maximum of the values of the child objects (questions and question groups).
</QuestionGroup>	
</QuestionGroups>	

Table 14: AML - Question Groups

Risk assessment processes frequently use a matrix to transform a number of input values into a new output value. To facilitate this during aggregation AML allows the definition of formula elements. In this example a function with three input parameters is defined. The example shows only one result for the input parameters, i.e. FORMULAX(1,4,3) = 5

<Formulas>	
<**Formula**	
Spec="FORMULAX"	A short name for referencing this item.
Dimensions="3"	The number of input dimensions.
InputType=”System.Double”	The type for the formula input values.
OutputType=”System.Double”	The type for the formula output value.
QuestionGroupSpec="...">	A reference to a question group that this formula is loaded for.
<**Dim** Value="1"	The input value for the first dimension.
<**Dim** Value=”4”	The input value for the second dimension.

<**Dim** Value=”3”	The input value for the third dimension.
<**Result**	
Value=”5”/>	The result for the specified input parameters.
</Dim>	
</Dim>	
</Dim>	
<Dim ... />	
</Formula>	
</Formulas>	

Table 15: AML - Formulas

The elements defined so far can be composed to complete process structures using the process element. Here it is possible to create sequential stages and defined question groups to be asked. The first question group – the node with the greatest depth – is activated by default. Any other question groups must be activated by an answer.

<Process	
Spec=”MEHARI”	
Name=”Mehari 2007”	
Client=”CLIENT1”>	
<**Stage**	
Name="Last stage">	Name of the stage.
<Value	A value object created for this stage.
Spec=”X02CONF”	The value type reference to create.
Transform= ”...”/>	The data transformation string for this value object.
PropagateTransform =”True”>	Is this value propagated to all children (stages, question groups, questions).
<**Stage**	
Name=”Second stage”	
<**Stage**	
Name= ”First stage”>	
</Stage>	

```
             </Dim>
             <Dim ... />
       </Formula>
</Process>
```

Table 16: AML - Processes

The transform property of a value node can consist of the following values:

- A constant numeric value
- An aggregate function MAX, MIN, AVG, SUM, ROUND specifying either #CHILDREN# or #WEIGHTEDCHILDREN# as input where the values of child objects that correspond to the same value type as this value node are aggregated. In the latter case the inputs are weighted by the weight attribute provided.
- References to other value types whose values are copied. These values can include local value objects of this type or values of this type created by a different branch in the assessment tree (stages, question groups, questions). If there are two providers of this value type, then the local value wins first, followed by the last branch to have calculated the value. See the chapter on tree ordering.

5.5.3 Results

Results of assessments have the following format.

```
<Report>
       <Asset Spec="A01">
         <Asset Spec="A02">
           <Stage Name="Assessment">
             <QuestionGroup Spec="QG01">
                    <Question Spec="Q01">
                      <Answer Spec="A01">      The selected answer.
                        <Value                 The final calculated value at this node.
                          Spec="V01"
                          Value="6"/>
                      </Answer>
                      <Value                   The final calculated value at this node.
```

Spec="V01"	
Value="5"/>	
</Question>	
<**Value**	The final calculated value at this node.
Spec="V01"	
Value="4"/>	
</QuestionGroup>	
<**Value**	The final calculated value at this node.
Spec="V01"	
Value="3" />	
</Stage>	
<**Value** Spec="V01" Value="2"/>	The final calculated value at this node.
<**Stage** Name="Impact" />	
</Asset>	
<**Value** Spec="V01" Value="1"/>	The final calculated value at this node.
</Asset>	
<**VirtualAsset** Spec="V01">	
<Asset Spec="B01">...</Asset>	
</VirtualAsset>	
</Report>	

Table 17: AML - Reports

6 Prototype

The MuDRA concept was implemented as a software prototype and the model was tested with the French MEHARI IT-security risk assessment model.

6.1 Architecture

The development of a prototype to support the generic approach devised was undertaken on the Microsoft .NET framework.

> "The Microsoft .NET Framework is a software framework available with several Microsoft Windows operating systems. It includes a large library of coded solutions to prevent common programming problems and a virtual machine that manages the execution of programs written specifically for the framework.
>
> Programs written for the .NET Framework execute in a software environment that manages the program's runtime requirements. Also part of the .NET Framework, this runtime environment is known as the Common Language Runtime (CLR). The CLR provides the appearance of an application virtual machine so that programmers need not consider the capabilities of the specific CPU that will execute the program. The CLR also provides other important services such as security, memory management, and exception handling. The class library and the CLR together comprise the .NET Framework." [**Wik09g**]

The application architecture is a three layered approach often chosen for enterprise applications. Access to the data layer, in this case a Microsoft SQL Server 2008 database, is provided through a service layer incorporating the business logic. The user interface components use these services by means of the Windows Communication Foundation. This technology was introduced to the .NET Platform in 2006 to provide a uniform basis for all existing and future remote communication technologies.

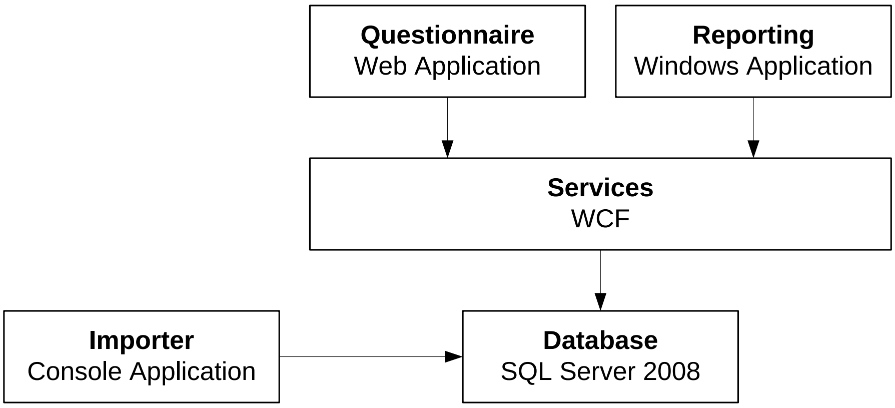


Figure 27: MuDRA Prototype Architecture

The benefit of this approach is that each layer is easily exchangeable with a different implementation. This is particularly important for future work in the proposed areas of user interfaces for input and output. New clients for modelling or reporting can be developed and use the same service infrastructure provided by the prototype. Similarly the database layer uses NHibernate [**Red09**] as a persistence abstraction layer making a change of database vendor possible if this is required later on.

6.2 MEHARI

MEHARI was chosen as a test case because a comprehensive knowledge database is available that includes questions and aggregation schemas. The data is available as an Excel sheet from CLUSIF [**Clu07**] and was converted into the AML format.

6.2.1 Process

MEHARI follows a common risk management process comprising of three phases.

The first phase includes security policies, company values and security objectives to create a security strategic plan (SSP). This plan lays out the companies joint objectives that act as guide throughout the assessment and thereafter. It is the reference for security decisions and must include participation by the company’s top and middle management.

The SSP includes a map of the company’s sensitive processes. For each process an impact criterion is chosen, e.g. drop in profit margin or drop in share price, and a discrete scale of value levels, e.g. ranging from one day to one month of production outage on a five part scale.

Next a set of resources is identified that these processes depend on. The assessment team then determines whether each resource is affected by a loss of confidentiality, integrity or availability (CIA) and if so what the maximum impact would be.

The last vital part of the SSP is the management charter which documents the contractual rights and obligations the company and its personnel have and the sanctions to be expected in case of non-compliance. This ensures a necessary level of commitment from top to bottom and vice versa.

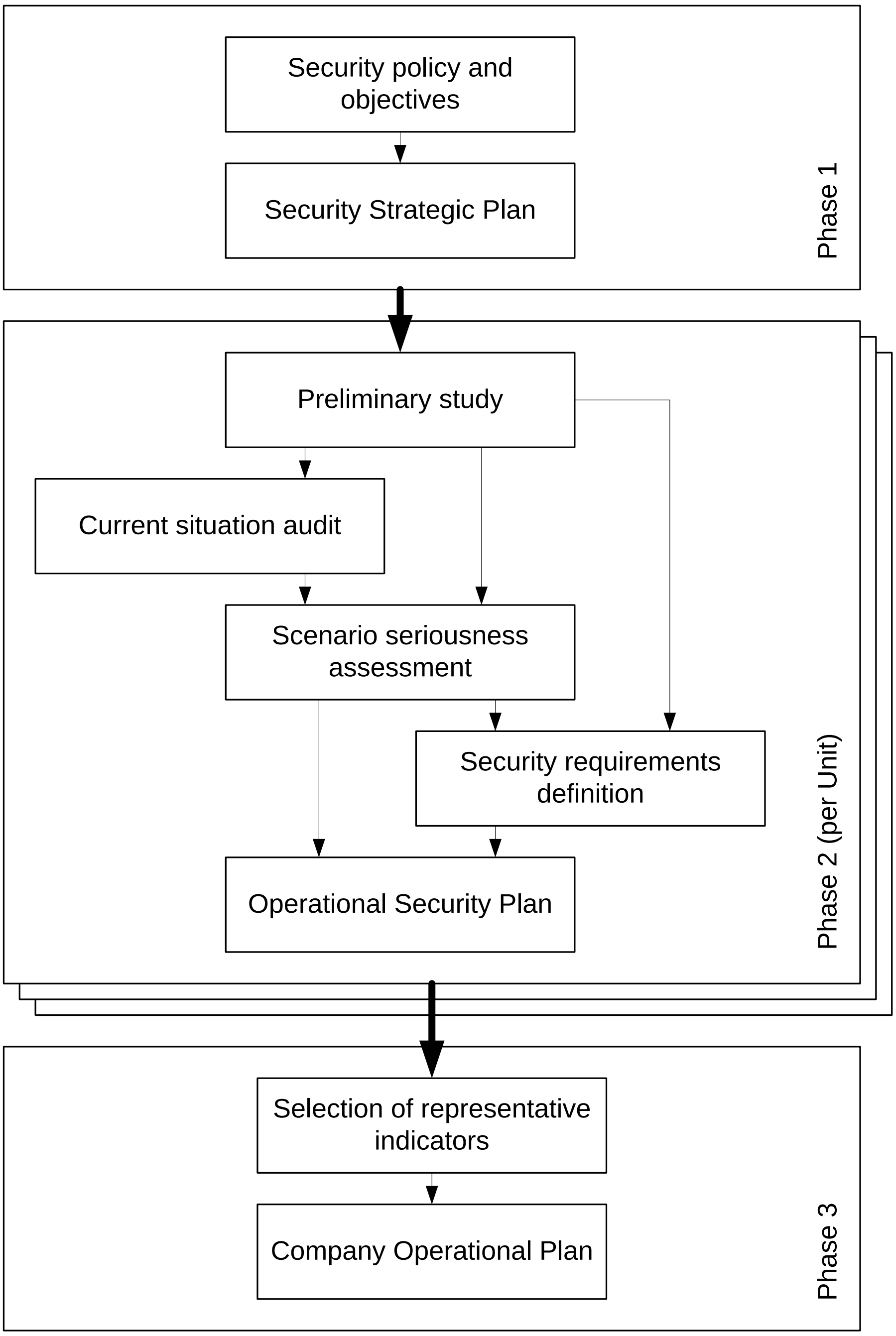

Security policy and objectives
Security Strategic Plan
Phase 1
Preliminary study
Current situation audit
Scenario seriousness assessment
Security requirements definition
Operational Security Plan
Phase 2 (per Unit)
Selection of representative indicators
Company Operational Plan
Phase 3

Figure 28: MEHARI 2007 phases [Clu07**]**

The second phase consists of assessing the risk per unit which incorporates a preliminary study of the unit and its assets, an audit of the current situation and an evaluation of scenario seriousness. This results in a definition of security requirements that form the operational security plan.

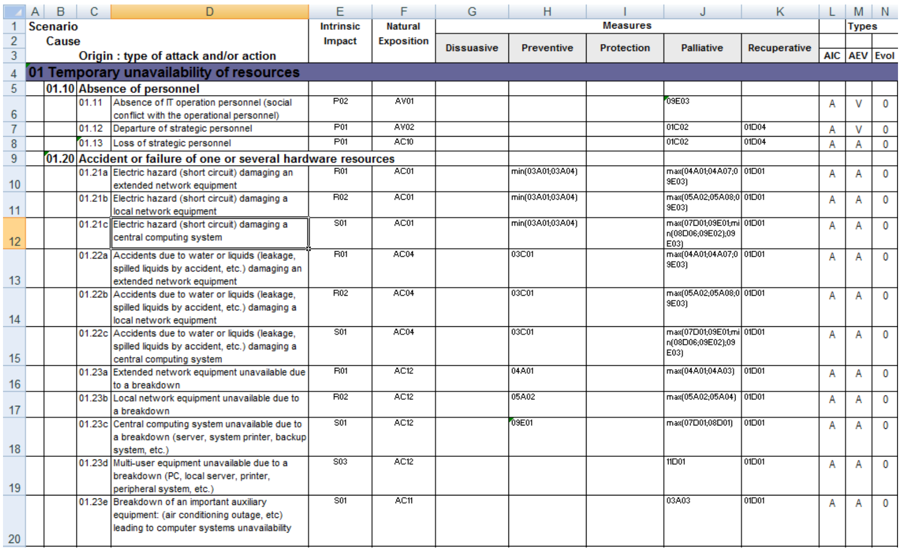
The MEHARI questionnaire may be asked multiple times inside the organisational unit under evaluation. Each question may not be applicable to each resource, but some scenarios will produce multiple answers for the same question. It is the task of the auditor to determine the most appropriate answer.

Based on these answers the calculation framework provided by MEHARI is executed and the resulting risk levels for each unit are determined.

The final phase incorporates the security plans for each unit, selects representative indicators and defines the company operational plan to mitigate the residual risks.

6.2.2 Knowledge Base

CLUSIF provides a complete set of scenarios and questions that can be used manually to produce an immediate assessment of an organisation’s risk. The data is provided in spreadsheet form.



	A	B	C	D	E	F	G	H	I	J	K	L	M	N
1	Scenario				Intrinsic Impact	Natural Exposition	Measures						Types	
2		Cause					Dissuasive	Preventive	Protection	Palliative	Recuperative			
3			Origin : type of attack and/or action									AIC	AEV	Evol
4	01 Temporary unavailability of resources													
5		01.10	Absence of personnel											
6			01.11	Absence of IT operation personnel (social conflict with the operational personnel)	P02	AV01				09E03		A	V	0
7			01.12	Departure of strategic personnel	P01	AV02				01C02	01D04	A	V	0
8			01.13	Loss of strategic personnel	P01	AC10				01C02	01D04	A	A	0
9		01.20	Accident or failure of one or several hardware resources											
10			01.21a	Electric hazard (short circuit) damaging an extended network equipment	R01	AC01		min(03A01;03A04)		max(04A01;04A07;09E03)	01D01	A	A	0
11			01.21b	Electric hazard (short circuit) damaging a local network equipment	R02	AC01		min(03A01;03A04)		max(05A02;05A08;09E03)	01D01	A	A	0
12			01.21c	Electric hazard (short circuit) damaging a central computing system	S01	AC01		min(03A01;03A04)		max(07D01;09E01;min(08D06;09E02);09E03)	01D01	A	A	0
13			01.22a	Accidents due to water or liquids (leakage, spilled liquids by accident, etc.) damaging an extended network equipment	R01	AC04		03C01		max(04A01;04A07;09E03)	01D01	A	A	0
14			01.22b	Accidents due to water or liquids (leakage, spilled liquids by accident, etc.) damaging a local network equipment	R02	AC04		03C01		max(05A02;05A08;09E03)	01D01	A	A	0
15			01.22c	Accidents due to water or liquids (leakage, spilled liquids by accident, etc.) damaging a central computing system	S01	AC04		03C01		max(07D01;09E01;min(08D06;09E02);09E03)	01D01	A	A	0
16			01.23a	Extended network equipment unavailable due to a breakdown	R01	AC12		04A01		max(04A01;04A03)	01D01	A	A	0
17			01.23b	Local network equipment unavailable due to a breakdown	R02	AC12		05A02		max(05A02;05A04)	01D01	A	A	0
18			01.23c	Central computing system unavailable due to a breakdown (server, system printer, backup system, etc.)	S01	AC12		09E01		max(07D01;08D01)	01D01	A	A	0
19			01.23d	Multi-user equipment unavailable due to a breakdown (PC, local server, printer, peripheral system, etc.)	S03	AC12				11D01	01D01	A	A	0
20			01.23e	Breakdown of an important auxiliary equipment: (air conditioning outage, etc) leading to computer systems unavailability	S01	AC11				03A03	01D01	A	A	0

Figure 29: MEHARI 2007 Knowledge Base [Clu07**]**

The base scenario sheet is the central point where calculation takes place. Each row constitutes a scenario, a cause or the origin. The origin rows are leaf rows that must be calculated first based on the columns provided.

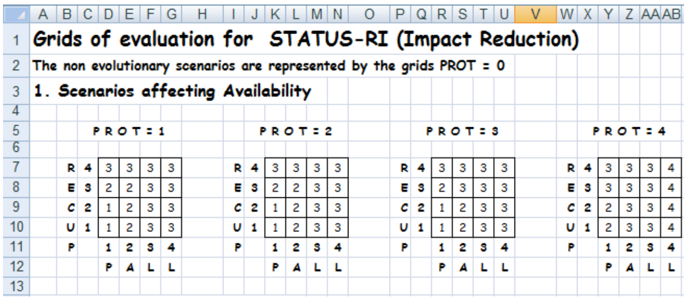
Intrinsic Impact	This is the deflected impact value caused by this threat from this origin to the asset. The value can be found in the classification sheet. The row is specified by the value in this cell and the column, i.e. C, I or A, is found in the origin row in the AIC column.
Natural Exposition	This is more commonly referred to as the probability of this threat occurring under this origin. The value can be found in the exposition sheet. The row is specific by the value in this cell and the value is in the column “Status-Expo”.
Dissuasive Measures	The measures reduce the probability of the threat occurring at all. The value for each measure can be calculated as follows. The value 01A02 corresponds to sheet 01 question group 01A02. The value is gained by weighting answers given to questions in the group taking minimum (once this question is answered with “yes”) and maximum (if the question is answered with “no”) values of the corresponding question into account.
Preventive Measures	The measures reduce the probability of the threat occurring at all.
Protection Measures	These measures reduce the impact of the threat when it happens.
Palliative Measures	These measures reduce the impact of the threat after is has been detected.
Recuperative Measures	These measures help to recover the asset to its original state once a threat has occurred.
AIC	Which class does this threat origin belong to (Confidentiality, Availability, or Integrity).
AEV	Accident, error or voluntary action. These are used by the grids described below.
Evol	Denotes if the scenario is a non-evolutive[6] scenario.

Table 18: Base Scenario Columns [Clu07**]**

[6] Certain scenarios, which are not fixed in time and space, can be such that potential protective measures have no effect on the intrinsic impact. They should then be considered non-evolutive, and treated as such.

The sheet “I_P grids” supplies transformation matrices to present reductions in impact and probability values. These values are calculated once the base scenario sheet has been aggregated and values for the effectiveness of different measures are available. These are rounded using Asymmetric Arithmetic Rounding to become the status of these measures.

Status values are then used as input values for these transformations.



Grids of evaluation for STATUS-RI (Impact Reduction)

The non evolutionary scenarios are represented by the grids PROT = 0

1. Scenarios affecting Availability

		PROT=1						PROT=2						PROT=3						PROT=4			
R	4	3	3	3	3	R	4	3	3	3	3	R	4	3	3	3	3	R	4	3	3	3	4
E	3	2	2	3	3	E	3	2	2	3	3	E	3	2	3	3	3	E	3	3	3	3	4
C	2	1	2	3	3	C	2	1	2	3	3	C	2	1	2	3	3	C	2	2	3	3	4
U	1	1	2	3	3	U	1	1	2	3	3	U	1	1	2	3	3	U	1	2	3	3	4
P		1	2	3	4	P		1	2	3	4	P		1	2	3	4	P		1	2	3	4
		P	A	L	L			P	A	L	L			P	A	L	L			P	A	L	L

Figure 30: MEHARI 2007 Evaluation Grids [Clu07**]**

The impact reduction and potentiality values are then mapped to a risk level for each threat using the following matrix.

Impact	***4***	2	3	4	4
	3	2	3	3	4
	2	1	2	2	3
	1	1	1	1	2
		1	***2***	***3***	***4***
		Potentiality			

Table 19: MEHARI 2007 Impact and Probability Matrix [Clu07**]**

6.3 Conversion

6.3.1 Process

The objects used in the MEHARI process are mapped to the MuDRA concept objects.

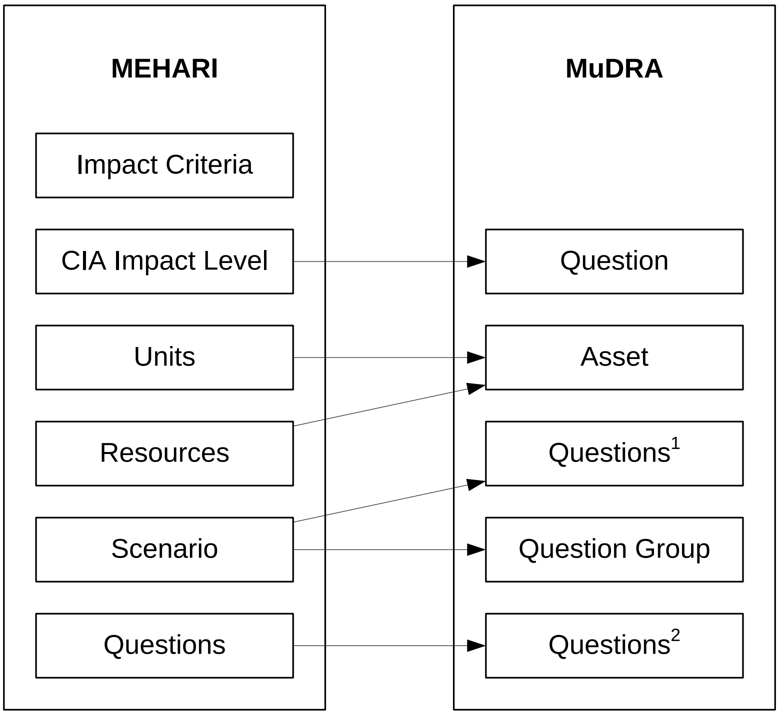


Figure 31: MEHARI 2007 - Conversion to MuDRA AML

The impact criteria definition is a pre-processing step and does not carry any direct value for the assessment. It is eliminated from the resulting MuDRA model. The impact values based on the CIA criteria are converted into numeric questions and the value stored in the question's value object.

Viewed from an abstract level units and resources are both assets and modelled as a hierarchy of equally weighted elements. These weights could be adapted based on the usage scenario.

A MEHARI scenario is fundamentally a threat as defined above. Threats need to be activated per asset therefore each scenario is mapped to a corresponding question. Once the question has been answered with yes, the threat is relevant for the asset and an associated question group is activated which poses questions on the activated scenario.

The questions themselves are converted into single choice yes/no questions in MuDRA.

The risk assessment phase is executed on a unit level. Therefore MuDRA will run assessments for a single asset. It is possible to use the MEHARI risk levels for each asset to construct a risk level for an asset hierarchy as described above. However, these are outside the scope of the MEHARI approach.

6.3.2 Knowledge base

The converter creates a process object for MEHARI consisting of three stages. The “scenarios” stage contains a single question group with questions for each threat row in the knowledge base.

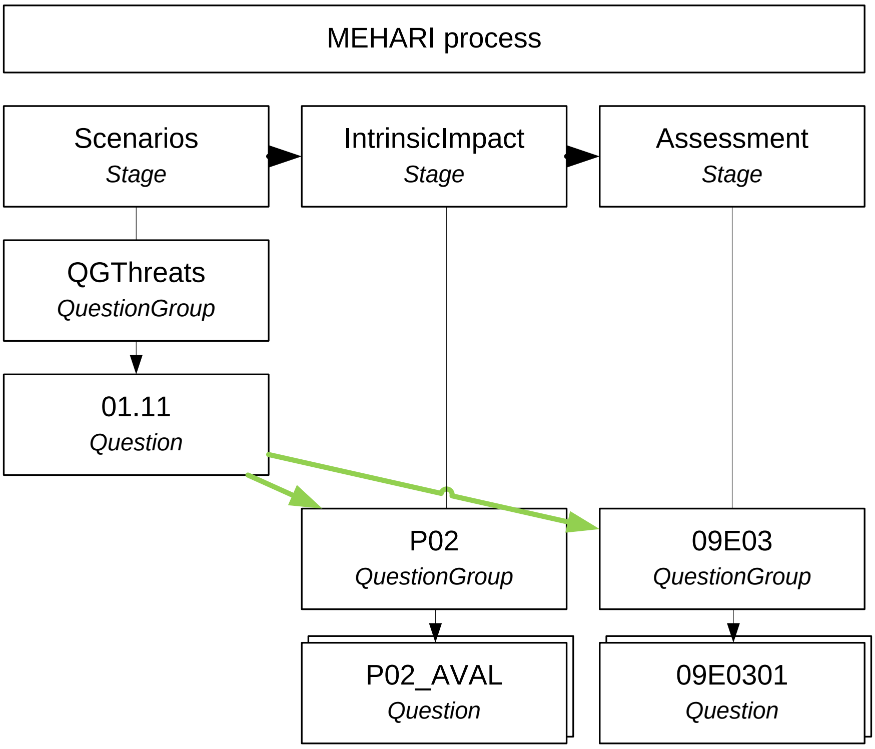


Figure 32: MEHARI 2007 Conversion - Questions

The question asks if the asset being assessed is threatened by this particular scenario. If the user chooses yes two types of question groups are activated for the user to answer. The first class (in this example P02) is the intrinsic impact question group. The second class (in this example 09E03) are the question groups related to controls in this scenario.

```
<Question Spec="01.11" Title="" Type="CHOICE" Weight="1">
      <Description>Is the asset threatened by “...”?</Description>
      <Answers>
        <Answer Value="YES" ActivatesQuestionGroup="P02,09E03 ">
          <Value Spec="PALL" Transform="#09E03#" />
          <Value Spec="EXPO" Transform="2" />
          <Value Spec="EVOL" Transform="0" />
          <Value Spec="STATUS-DISS" Transform="1" />
          <Value Spec="STATUS-PREV" Transform="1" />
          <Value Spec="STATUS-PROT" Transform="1" />
          <Value Spec="STATUS-RECUP" Transform="1" />

          <Value Spec="STATUS-PALL" Transform="ROUND(#PALL#)" />
          <Value Spec="STATUS-EXPO" Transform="ROUND(#EXPO#)" />
          <Value Spec="STATUS-EVOL" Transform="ROUND(#EVOL#)" />

          <Value Spec="IMPACT" Transform="#P02_AVAL#" />
          <Value Spec="STATUS-RI" Transform="
                  STATUS-RI-AVAL(
                        #EVOL#*#STATUS-PROT#,
                        #STATUS-RECUP#,
                        #STATUS-PALL#)" />
          <Value Spec="STATUS-P" Transform="
                  STATUS-P-VOL(
                        #STATUS-EXPO#,
                        #STATUS-DISS#,
                        #STATUS-PREV#)" />

          <Value  Spec="STATUS-I"  Transform="MIN(#IMPACT#,5-#STATUS-
RI#)" />
          <Value   Spec="RISK"   Transform="RISK(#STATUS-I#,#STATUS-
P#)" />
        </Answer>
        <Answer Value="NO" />
      </Answers>
</Question>
```

The intrinsic impact question group contains at most three questions and is asked during the second stage. One for each impact criteria class: confidentiality, integrity and availability. The questions ask for a numeric impact value.

```
<Question  Spec="P02_AVAL"
            Title="..."
            Type="INTEGER"
            AnswerValue="P02_AVAL">
      <Description>IT operation personnel</Description>
</Question>
```

The control question group is populated with the weighted questions and the transformation formula for calculating the real value taking maximum and minimum into account if they are available. This group is asked during the third and last stage.

```
<QuestionGroup Spec="09E03" Name="...">
      <Value Spec="09E03" Transform="
                  Max(#09E03_MAX#?,
                        Min(#09E03_MIN#?,
                              Sum(#WEIGHTEDCHILDREN#)))" />

      <Value Spec="09E03_MIN" Transform="Max(#CHILDREN#)" />
      <Value Spec="09E03_MAX" Transform="Min(#CHILDREN#)" />

      <Question Spec="09E0301" Weight="2" />
      <Question Spec="09E0302" Weight="2" />
      <Question Spec="09E0303" Weight="2" />
      <Question Spec="09E0304" Weight="2" />
      <Question Spec="09E0305" Weight="2" />

</QuestionGroup>
```

The questions themselves are simple choices and supply value options for the question together with any maxima or minima.

```
<Question Spec="09E0301" Title="09E0301" Type="CHOICE">
      <Description>...</Description>
      <Answers>
        <Answer Value="YES">
          <Value Spec="09E03" Transform="1" />
          <Value Spec="09E03_MIN" Transform="0" />
        </Answer>
        <Answer Value="NO">
          <Value Spec="09E03" Transform="0" />
          <Value Spec="09E03_MAX" Transform="4" />
        </Answer>
      </Answers>
</Question>
```

The MEHARI aggregation path is converted into a chain of MuDRA calculations. These are executed on the question object corresponding to the threat. Values are provided by associated question groups into the value types: Impact, Dissuasive, Preventive, Protection, Palliative and Recuperative. The evolutive property is supplied by the question itself. The diagram shows the paths that lead to impact (orange) and probability (blue) input factors for the risk function.

The STATUS-RI-AVAL/INTG/CONF formula is chosen based on the impact criteria class in use and uses the evolutive parameter with any protective, palliative and recuperative measures to calculate a value for reducing the risk impact. The impact parameter for the risk function is then determined using the original risk and the reduction factor.

The STATUS-P-VOL/ERR/ACC formula is chosen based on the type of action, i.e. accident, error or voluntary, and calculates the probability for the risk function using the dissuasive and preventive control values.

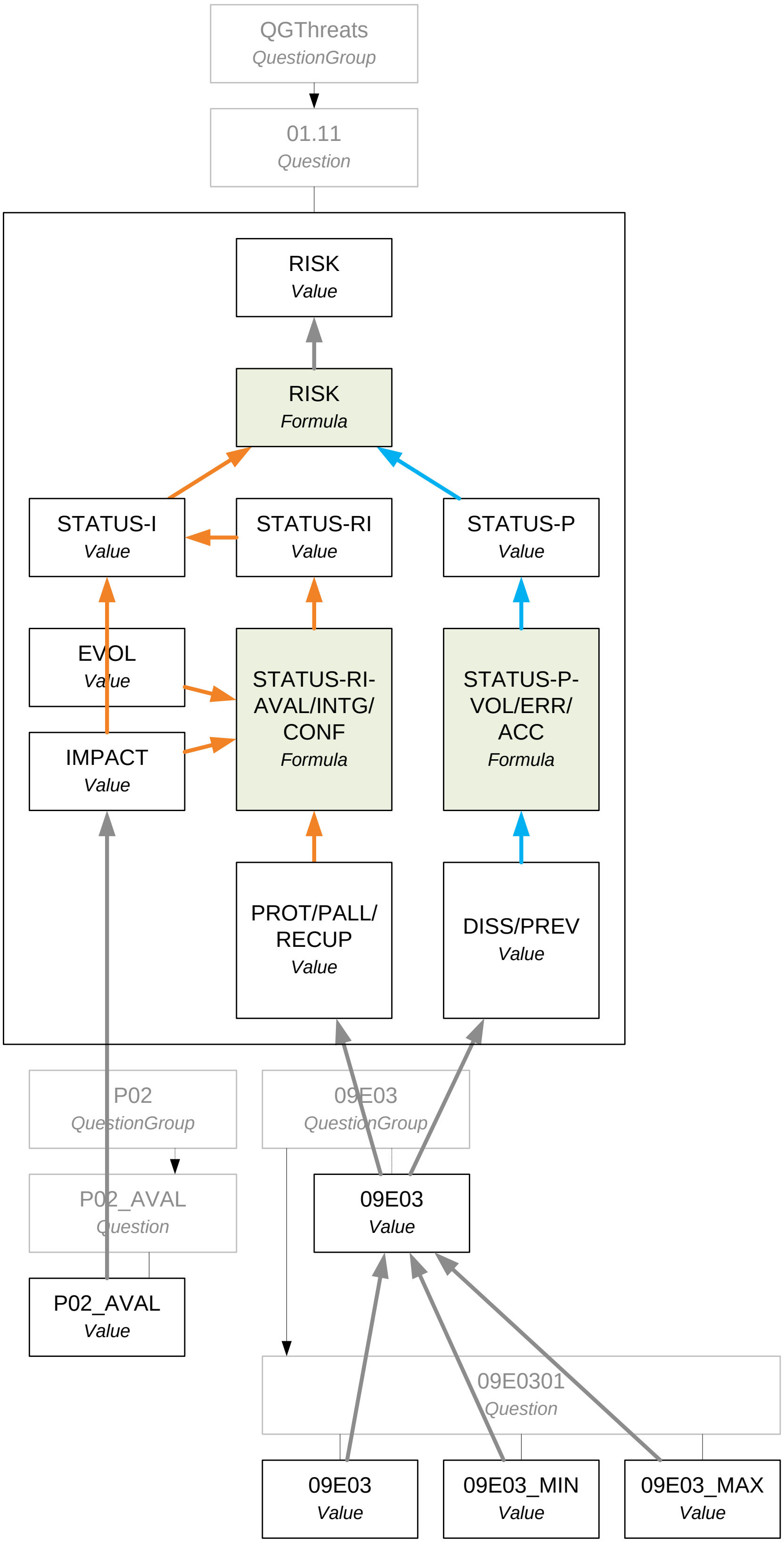


Figure 33: MEHARI 2007 Conversion - Formula and Propagation

7 Conclusion and Future Work

The MuDRA concept has been developed based on multiple risk assessment approaches and existing software systems built to support them. The identified patterns can be projected into a MuDRA compatible assessment model. The model supports qualitative, semi- and quantitative risk analysis and introduces a separation of concerns, i.e. determination of state by the operations personnel and definition of risk based on this state by the risk analyst, during the asset level assessment to ensure scalability. The ability to automatically aggregate on several levels and test configurations using simulated assessments scenarios bears the potential to greatly improve the risk assessment process. Some of the concepts introduced can be considered as starting points for further work.

The validity of the generic applicability of the MuDRA concept could be further tested by converting other existing models and developing aggregation systems using the concept. As the concept concentrates on risk assessment the problem lies in gaining access to standards that specify details of the models they use for assessing risks, e.g. threat lists, control definitions, questions and aggregation systems. During this analysis very few models were encountered that had knowledge bases which were openly available that could therefore be converted. Specifically the questionnaires were usually developed by organisations providing services in the regulatory governance and auditing field. This intellectual property is not publically available and not readily shared with third parties. This fact in itself causes problems for long-term assessment comparisons because of inherent differences in the implementation details.

The data models defined and the serialization in Assessment Markup Language encompasses a vast amount of possible scenarios, ranging from national standards to custom environments. The former may have sufficient access to technical staff to describe the process in AML based on existing documentation. The latter may base their implementation on an existing available model but hesitate to invest resources into understanding and adapting the complex structures of an AML model. Therefore future work would be required to provide a visual environment for modelling and adapting AML models. This would ease the burden of making changes to models. Each dimension in MuDRA represents a tree. Visualisation techniques for such structures are readily available in the software design industry and can be reutilized for this application. The aggregation tree which represents a different view covering all dimensions poses a challenge that a solution needs to be found for.

The current prototype will produce a simple report allowing the traversal of the aggregation tree with all calculated values and their respective sources. This is sufficient for the risk assessor with knowledge about the domain and the model used. For risk management to be successful it needs to become part of the organisational culture and information about risk assessments need to be published in a transparent format which facilitates understanding and interpretation by those who need it. This aspect still requires more development work. Traffic lights can be easily generated from the aggregation data, but management reports require more sophisticated forms of visualisation. The approach suggested here would be to automate the generation of the report based on a generic addition to the MuDRA concept which allows projection of results onto charts. Once defined both running and completed assessments could then be automatically reported to a wide audience so that improvements or the deteriorations in the risk exposure profile can be easily identified.

8 Bibliography

[Bak09] David Baker. Risk Assessment for Machinery. [Online]. http://www.riskman.info/en_1050.htm

[Bon03] Franco Bontempi, *System-based vision for strategic and creative design*, 1st ed.: A. A. Balkema, 2003, p. 351.

[Brü03] B Brühwiler, *Risk Management als Führungsaufgabe - Methoden und Prozesse der Risikobewältigung für Unternehmen, Organisationen, Produkte und Projekte*. Bern, Switzerland: Haupt Berne, 2003, pp. 25, 32.

[Bun98] Bundestag der Bundesrepublik Deutschland. (1998, April) Bundesgesetzblatt Jahrgang 1998 Teil 1 Nr. 24, ausgegeben zu Bonn am. 30 April 1998.

[CIS05] Central Information Systems Security Division. (2005, July) EBIOS – Expression of Needs and Identification of Security Objectives. [Online]. http://www.ssi.gouv.fr/en/confidence/ebiospresentation.html

[Cis04] Central Information Systems Security Division. (2004, February) Expression des Besoins et Identification des Objectifs de Sécurité. [Online]. http://www.ssi.gouv.fr/en/confidence/documents/methods/ebiosv2-section2-demarche-2004-02-05_en.pdf

[Clu07] Club de la Securite de l'Information Francais. (2007) Mehari 2007 Overview. [Online]. https://www.clusif.asso.fr/fr/production/ouvrages/pdf/MEHARI-2007-Overview_2007.pdf

[Dic09] Dictionary.com LLC. Dictionary.com. [Online]. http://dictionary.reference.com/

[Dug08] Alexander Duggleby. (2008) BioMatch. [Online]. http://www.biomatch.at

[Eni09] ENISA, European Network and Information Security Agency. Corporate Risk Management Strategy. [Online]. http://www.enisa.europa.eu/rmra/rm_process_01.html

[Fab08] Michael Havbro Faber, "Risk Assessment in Engineering, Principles, System Representation & Risk Criteria," JCSS Joint Committee on Structural Safety, 2008.

[Far09] Farlex, Inc. TheFreeDictionary.com. [Online]. http://www.thefreedictionary.com/

[Lar09] Brenda Larcom, Eleanor Saitta, Michael Eddington, and Stephanie Smith. (2009, April) Trike. [Online]. http://www.octotrike.org/

[McC05] John McCumber, *Assessing and managing security risk in IT systems: a structured methodology*. Florida, USA: Auerbach Publications, 2005, p. 4.

[Mer09] Merriam-Webster Online. [Online]. http://www.merriam-webster.com

[Mic09b] Microsoft Corporation. (2009) Microsoft Software Inventory Analyzer. [Online]. http://www.microsoft.com/resources/sam/msia.mspx

[Mic09] Microsoft Corporation. (2009, May) Overview of Logical Datacenter Designer. [Online]. http://msdn.microsoft.com/en-us/library/ms181931.aspx

[Pel01] Thomas R Peltier, *Information security risk analysis*. Florida, USA: Auerbach Publications, 2001.

[Red09] Red Hat Middleware, LLC. (2009) NHibernate for.NET. [Online]. https://www.hibernate.org/343.html

[Suv09] Schweizer Unfall- und Versicherungsanstalt. (2009, May) Methode Suva zur Beurteilung von Risiken an Arbeitsplätzen und bei Arbeitsabläufen. [Online]. https://wwwsapp1.suva.ch/sap/public/bc/its/mimes/zwaswo/99/pdf/66099_d.pdf

[Spa06] Spanish Ministry for Public Administrations, "Book 1 - The Method," in *MAGERIT Version 2 - Methodology for Information Systems Risk Analysis and Management*. Spain, 2006, p. 20.

[Owa07] The Open Web Application Security Project. (2007, Mar.) Comprehensive list of Threats to Authentication Procedures and Data. [Online]. http://www.owasp.org/index.php/Comprehensive_list_of_Threats_to_Authentication_Procedures_and_Data

[Dod00] United States of America Department of Defense. (2000, February) US Military Standard 882D (MIL-STD-882D). Document. [Online]. MIL-STD-882D

[Vos08] David Vose, *Risk analysis: a quantitative guide*, 3rd ed. Chichester, England: John Wiley & Sons. Ltd., 2008, pp. 6,7.

[Wik09] Wikipedia contributors. (2009, March) Wikipedia, The Free Encyclopedia. [Online]. http://en.wikipedia.org/wiki/DREAD:_Risk_assessment_model

[Wik09b] Wikipedia contributors. (2009, February) Wikipedia, The Free Encyclopedia. [Online]. http://en.wikipedia.org/wiki/Wideband_delphi

[Wik09c] Wikipedia contributors. (2009, Jan.) Wikipedia, The Free Encyclopedia. [Online]. http://en.wikipedia.org/wiki/Strategic_Environmental_Assessment

[Wik09d] Wikipedia contributors. (2009, May) Wikipedia, The Free Encyclopedia. [Online]. http://en.wikipedia.org/wiki/Normal_distribution

[Wik09f] Wikipedia contributors. (2009, May) Wikipedia, The Free Encyclopedia. [Online]. http://en.wikipedia.org/wiki/Bernoulli_distribution

[Wik09g] Wikipedia contributors. (2009, May) Wikipedia, The Free Encyclopedia. [Online]. http://en.wikipedia.org/wiki/.NET_Framework