Models for Assessing Information Security Risk

Filipe Neto Rodeia Macedo, nº 55352

Dissertação para obtenção do Grau de Mestre em
Engenharia Informática e de Computadores

Júri
Presidente: Prof. José Manuel Tribolet
Orientador: Prof. Miguel Mira da Silva
Vogal: Prof. José Delgado

Outubro de 2009
ACKNOWLEDGEMENTS

I would like to acknowledge and extend my heartfelt gratitude to the following persons who have made the completion of this thesis possible:

My supervisor, Prof. Dr. Miguel Mira da Silva, for his significant help in thinking up and reviewing this work.

Eng. Tiago Reis, my other supervisor, for taking out time from his busy schedule in order to guide me. For the constant reminders and much needed motivation. His expertise, patience and encouragement were a fundamental part of this work.

Eng. Gonçalo Carvalho for his understanding and assistance.

All KPMG staff.

I would also like to thank my family and friends for their unconditional support, help and advice. Despite seeming irrelevant in the context of this work, this indirect help was a major contribution to this thesis.
ABSTRACT

There are numerous risk assessment models nowadays and many more emerging every day. They all have the same basic goal, but try to achieve it through very different perspectives and addressing problems differently. Some of them can be applied to all kinds of risk, other are specific for particular risks. A particularly hazardous risk in today’s global economy is Information Security. Information is a critical asset for organizations making information security risk very important.

This study compares a choice of methods that allow an organization to assess their information security risk. The initial models went through two selection iterations before we end up with the final three fully studied models. The main purpose of the study is to compare and clarify the different activities, inputs and outputs required by each information security risk assessment models and also analyze which ones address information security risk effectively. The resulting information helps evaluating the models’ applicability to an organization and their specific needs.

In order to verify and validate the conclusions taken from the theoretical study of the three final models, a practical experience was put into practice in a real organization.

KEYWORDS

RESUMO

Existem actualmente inúmeros modelos de avaliação de risco e muitos mais a aparecerem cada dia. Todos eles têm o mesmo objetivo base, mas tentam alcançá-lo com diferentes perspetivas e abordando os problemas de forma diferente. Alguns deles podem ser aplicados transversalmente a qualquer tipo de risco, outros são específicos para determinados riscos. Um risco particularmente perigoso na economia global de hoje é o Risco de Segurança de Informação. A informação é um activo fundamental para as organizações, tornando o Risco de Segurança de Informação muito importante.

Este estudo compara métodos que permitam a uma organização avaliar os seus riscos de segurança da informação. Os modelos iniciais passaram por dois processos de selecção antes de se chegar aos últimos três modelos que foram estudados em maior detalhe.

O principal objectivo deste estudo é o de clarificar e comparar as diferentes actividades, informação e esforço que cada modelo de avaliação de risco de segurança da informação exige, bem como analisar quais dos modelos endereçam o risco de segurança de informação eficazmente. A informação resultante contribui para avaliar a aplicabilidade dos modelos em organizações reais tendo em conta as necessidades específicas da mesma.

A fim de verificar e validar as conclusões da parte mais teórica deste estudo comparativo de três modelos de avaliação de risco, foi posto em prática um caso de estudo numa organização real.

PALAVRAS-CHAVE

Modelos de Avaliação de Risco, Risco de Segurança de Informação, Avaliação de Risco de Segurança de Informação, Comparação de Modelos de Avaliação de Risco
# Table of Contents

Acknowledgements........................................................................................................... i
Abstract ............................................................................................................................... 2
Resumo ................................................................................................................................. 3
Table of Contents ............................................................................................................... 4
List of figures ...................................................................................................................... 7
List of tables ...................................................................................................................... 8

1. Introduction .................................................................................................................. 1
   1.1 Risk Management ..................................................................................................... 1
   1.2 Essential Terminology ............................................................................................ 1
   1.3 Motivation ................................................................................................................ 2
      1.3.1 Compliance ........................................................................................................ 2
      1.3.2 Information and information systems dependence ............................................. 2
      1.3.3 Change in organizations .................................................................................... 3
      1.3.4 Exposure and boundaries ................................................................................... 3
      1.3.5 Gap between business and information security ............................................... 3
      1.3.6 Summary ............................................................................................................ 4
   1.4 Problem Statement ................................................................................................... 4
      1.4.1 Information security risk is different ................................................................. 4
      1.4.2 Variety of assessment models ............................................................................. 5
   1.5 Contribution ............................................................................................................. 6
   1.6 Summary .................................................................................................................. 6

2. Risk and Risk Management ......................................................................................... 8
   2.1 Establishing the Context ......................................................................................... 8
   2.2 Risk Categories ....................................................................................................... 9
      2.1.1 Financial Risk ......................................................................................................
      2.1.2 Operational Risk ..............................................................................................
      2.1.3 Strategic Risk ....................................................................................................
      2.1.4 Reputation Risk ..............................................................................................
      2.1.5 Legal & Regulatory Compliance Risk ..............................................................
      2.1.6 Information Systems Risk ............................................................................... 13
   2.3 Risk Management .................................................................................................... 13
<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.2.1</td>
<td>Definition</td>
<td>13</td>
</tr>
<tr>
<td>2.2.2</td>
<td>Motivation</td>
<td>13</td>
</tr>
<tr>
<td>2.2.3</td>
<td>Risk Management Cycle</td>
<td>14</td>
</tr>
<tr>
<td>2.4</td>
<td>Summary</td>
<td>18</td>
</tr>
<tr>
<td>3.1</td>
<td>Information Security Risk</td>
<td>20</td>
</tr>
<tr>
<td>3.2</td>
<td>Information Security Risk Assessment</td>
<td>22</td>
</tr>
<tr>
<td>3.3</td>
<td>Information Security Risk Assessment Models</td>
<td>24</td>
</tr>
<tr>
<td>3.3.1</td>
<td>Qualitative vs. Quantitative Models</td>
<td>24</td>
</tr>
<tr>
<td>3.4</td>
<td>Summary</td>
<td>25</td>
</tr>
<tr>
<td>4.1</td>
<td>Introduction</td>
<td>27</td>
</tr>
<tr>
<td>4.2</td>
<td>Objectives</td>
<td>27</td>
</tr>
<tr>
<td>4.3</td>
<td>Process</td>
<td>28</td>
</tr>
<tr>
<td>4.4</td>
<td>Summary</td>
<td>28</td>
</tr>
<tr>
<td>5.1</td>
<td>Introduction</td>
<td>29</td>
</tr>
<tr>
<td>5.2</td>
<td>Model selection</td>
<td>29</td>
</tr>
<tr>
<td>5.2.1</td>
<td>Identified Models</td>
<td>30</td>
</tr>
<tr>
<td>5.2.2</td>
<td>First iteration selection criteria</td>
<td>30</td>
</tr>
<tr>
<td>5.2.3</td>
<td>Criteria applied to each model</td>
<td>31</td>
</tr>
<tr>
<td>5.2.4</td>
<td>Chosen models</td>
<td>33</td>
</tr>
<tr>
<td>5.2.5</td>
<td>Second iteration selection criteria</td>
<td>33</td>
</tr>
<tr>
<td>5.2.6</td>
<td>Criteria applied to each 2nd iteration model</td>
<td>34</td>
</tr>
<tr>
<td>5.2.7</td>
<td>Selection summary</td>
<td>35</td>
</tr>
<tr>
<td>5.3</td>
<td>Comparative Study</td>
<td>36</td>
</tr>
<tr>
<td>5.3.1</td>
<td>Comparison criteria</td>
<td>36</td>
</tr>
<tr>
<td>5.3.2</td>
<td>Comparing concept definitions of the three models</td>
<td>38</td>
</tr>
<tr>
<td>5.3.3</td>
<td>Approaches</td>
<td>39</td>
</tr>
<tr>
<td>5.3.4</td>
<td>Results and Output</td>
<td>41</td>
</tr>
<tr>
<td>5.3.5</td>
<td>Complexity</td>
<td>42</td>
</tr>
<tr>
<td>5.3.6</td>
<td>Supporting tools brief analysis</td>
<td>44</td>
</tr>
</tbody>
</table>
Appendix C – Practical Experience: Information Assets Profiles .................................................. 89
Appendix D – Practical Experience: Business Impact Table ....................................................... 92
Appendix E – Practical Experience: Threat’s description ............................................................. 94

LIST OF FIGURES

Figure 1 - Risk Management Drivers ......................................................................................... 2
Figure 2 – Risk Management Cycle ........................................................................................... 14
Figure 3 - Information Security ..................................................................................................... 20
Figure 4 – Information Security Risk Analysis ........................................................................... 23
LIST OF TABLES

Table 1 - Qualitative vs. Quantitative .............................................................................................................. 25
Table 2 – First iteration criteria applied to each model....................................................................................... 33
Table 3 – Criteria applied to each of the second iteration model ................................................................. 35
Table 4 – HCIS Impact Ratings ....................................................................................................................... 51
Table 5 – SONHO Impact Ratings ..................................................................................................................... 52
Table 6 – Security Level (IRAM and OCTAVE) ............................................................................................. 55
Table 7 – Security Level (IT-Grundshutz) ........................................................................................................ 55
Table 8 – Risk ratings and score ....................................................................................................................... 58
Table 9 – HCIS Security Requirements ............................................................................................................. 58
Table 10 – SONHO Security Requirements ..................................................................................................... 58
Table 11 – Critical Risks according to OCTAVE .............................................................................................. 58
Table 12 - Critical Risks according to IRAM ..................................................................................................... 59
Table 13 - Critical Risks according to IT-Grundschutz ...................................................................................... 59
Table 14 – Evaluation of the top priority risks .................................................................................................. 60
1. **INTRODUCTION**

1.1 **RISK MANAGEMENT**

Risk management is becoming one of the most prevalent business issues in our days and many companies regard it as a critical but challenging endeavour. It’s, however, a very broad concept that embraces several types of risk. Risk can be everywhere, in business, finance, people, buildings, information technology and even in getting out of bed in the morning. Some of these risks have already been addressed and studied extensively but others only briefly.

Organizations have always been aware of risk in doing business, so risk isn’t a very recent area of study. Nevertheless, professionals nowadays should be especially aware of risk in emerging areas. One area that’s particularly hazardous in today’s global economy is **Information Security Risk**.

The purpose of this study includes a wide understanding of risk management as well as a detailed study of information security risk assessment models. The result of the study will be a comparative and critic analysis of those models, and their significant concepts. The model comparison should be sustained by wide-ranging criteria.

The study also includes a brief analysis of tools that support the information security risk assessment process and the analysis of the adequacy of each tool with each model.

This work is currently being developed in collaboration with KPMG Portugal, mostly due to their great knowledge on this specific matter.

1.2 **ESSENTIAL TERMINOLOGY**

Before we can move on to study information risk management in more detail, we shall look at some of the key definitions. The essence of this section is to introduce the reader to the basic concepts and to adopt a standard terminology through the manuscript.

- **Asset** – Something valuable to the organization;
- **Threat** – An action or event that might prejudice security. A threat is a potential violation of security;
- **Vulnerability** – Existence of a weakness, design, or implementation error that can lead to an unexpected, undesirable event compromising the security of the system;
- **Impact** - Consequences of a security incident on business;
- **Risk** - A function of the probability/likelihood of a threat materialising through a vulnerability, and the impact of that event;
- **Control** - Countermeasure to manage and mitigate risks.
1.3 MOTIVATION

One of the motivations to study the risk management area, and more particularly the information security risk assessment part of it, is the growing need to properly manage information security risks in organizations as part of their overall risk management processes. The main factors driving this growing need are described below and summarized in Figure 1:

![Figure 1 - Risk Management Drivers](image)

1.3.1 COMPLIANCE

A great number of the laws and regulations created recently in reaction to corporate scandals address the information security issue and pressure organizations to effectively assess information security risk and/or to implement security measures. Compliance is mandatory for most of these regulations.

But note that compliance isn’t the same as security. Securing information may make you compliant, but being compliant doesn’t necessarily make you secure. If your controls satisfy your regulatory requirements, but don’t mitigate risk, then they are not adequate.

The implications of non-compliance are also growing, with the potential for what could be called catastrophic consequences ranging from significant fines and irrevocable damage of company brand and reputation to jail time for executives.

1.3.2 INFORMATION AND INFORMATION SYSTEMS DEPENDENCE

As you may know, information and the systems that handle it are critical to the operation of virtually all organizations. Access to reliable information has become an indispensable component of conducting business, indeed, in a growing number of organizations, information is the business. The livelihood of an organization is, therefore, linked to how well the availability, integrity, and confidentiality (the three main vectors of security) of the information is managed. This means that disruption of the systems that handle information would cause a much greater loss to the organization.
On the other hand, the higher expectations concerning information systems integration, performance and availability are creating a degree of process and system complexity that is difficult to effectively manage. Mission success in these complex environments requires excellent corporate and IT governance as well as effective risk management.

### 1.3.3 Change in Organizations

There are certain factors that induce change in organizations. Factors like the pressure to innovate and introduce new products and services in order to become competitive, the pressure to cut costs, the implementation of new technologies to make business processes more efficient and to reduce time to market. All these factors create new risks that need to be assessed and also change the information security risk context thus should be taken into consideration.

### 1.3.4 Exposure and Boundaries

Responsibility for completing a mission and the resources needed to pursue it were traditionally aligned with organizational boundaries. However, key drivers in the business environment, such as the globalization of business and the fast pace of technological change, have led to growing connectivity with clients, and increased outsourcing and partnering among organizations, causing greater exterior exposure and more ambiguous boundaries. This ambiguity creates multiple security contexts thus bringing greater risks to information.

### 1.3.5 Gap between Business and Information Security

Information security is a type of risk that intersects IT risk as well as business risk. But most companies have not yet effectively aligned IT risk management with their organization's overall risk-management strategy. For that reason, information security risk tends to underestimated or even disregarded. While boards usually look at business strategy and strategic risks, few boards have focused on information systems and security, despite the fact that it involves large investments and huge risks. Why is that? Among the reasons:

- Senior management does not view governance of information as a strategic issue;
- Few business managers have a complete understanding of the ever widening range of things that can go wrong with modern information systems; they don't really understand the amount of IT-related exposure. In some cases, top management doesn't even comprehend the impact IT has on business and the role it plays in generating revenue. Consequently management can't know how IT creates risks and opportunities, neither how to effectively address and manage information;
- On the other hand, IT staff, who know how vulnerable information systems are to disruption, are often not in a position to fully understand the impact that disruptive events can have on the business; They should be the ones to explain managers the risk exposure and the possibility of losing billions if it is not adequately addressed.
But most technical staff isn't well enough in tune with the business to be able to articulate a business case like that.

These disconnect between IT and business can be enormously destructive, as we could see in the Société Générale case. SG lost $7.2 billion in early 2008, and brought to the fore the fact that business risk can be directly exposed through IT. This, and other incidents like it, is encouraging other companies to talk about risk management and IT controls inside their businesses.

1.3.6 SUMMARY

We've seen that compliance with regulatory requirements, dependency on information processing, organizational change, exterior exposure and the gap between business and information security are strong drivers for addressing risk management in a new perspective, especially for managing information security risk. Disregarding any of these factors can affect the organization’s income, reputation, customer confidence, public image and brand.

It’s also clear that information security risk needs to be met and managed regardless of ROI (Return on Investment). This means that nowadays it’s not just about profitability, in our globally competitive marketplace it’s all about the intangible assets (information and reputation) that are at risk.

1.4 PROBLEM STATEMENT

Last section clearly exposed various drivers to study information security risk assessment. This section describes the particular set of problems and difficulties, related to information security risk assessment, that are going to be addressed in this work. So why is information security risk assessment so hard to achieve effectively? Here are two main reasons:

1.4.1 INFORMATION SECURITY RISK IS DIFFERENT

The main information security risk assessment problem is that information security risk is different from traditional risks. Information is one of the most challenging categories of critical assets for an organization to understand and define. Therefore, identifying information security risk can be a quite difficult task, since few organizations have a comprehensive understanding of their information assets, threat vectors and security capabilities.

Additionally, traditional risk assessment does not provide a method to accurately assess information security risks facing an ever changing, dynamic environment, it can only provide a snapshot of those risks. Current risk assessment practices were inherited from other fields such as insurance, medicine and finance but traditional risks are far easier to comprehend than information security risk.

So it’s clear that our old-world risk assessment model cannot keep up with permanent change of information security risks and that, therefore, it is not very useful in determining an overall
Information security strategy. Identification and evaluation of information security risks is a complicated, multi-dimensional process that involves the analysis of multiple technologies, people, processes and how they interoperate.

**1.4.2 Variety of Assessment Models**

All the drivers referred above are turning risk assessment into a rapidly developing discipline with varied views and descriptions of what it involves how it should be conducted and what it is for. Subsequently, many risk assessment methods are emerging as well. The goal is basically the same, and every method basically tries to do the same thing but in different ways, through different perspectives or addressing different aspects of risk.

There are general risk assessment methods, applicable to most kinds of risk, but also specific risk assessment methods, like information security risk assessment models, that address specific risks. These models have been developed by both academic researchers and practitioners, including quantitative methods such as expected value analysis, stochastic dominance approach, qualitative methods such as scenario analysis, questionnaire, fuzzy metrics, and popular practical toolkits such as IRAM and CRAMM.

A wide range of these risk assessment techniques can be applied to information security. Many suffer from being excessively complex, too time-consuming to apply, or from not addressing the full range of business and security issues that need to be considered or even from failing to involve business personnel in the risk assessment process. As a result, business managers have been inhibited from using information security risk assessment because most available techniques are hard to understand, produce results of uncertain value and require experienced risk assessment practitioners – who are in short supply – to apply them.

Due to this variety of existent models to assess information security risks and also due to the growing need to manage those risks, it’s often hard for a company to determine which model best fits their specific needs. Because so many models exist, it is often difficult to determine which one best applies to the organization. Companies don’t know which methodology to follow. Generic models offer the most comprehensive view, but these often require security measures that are inappropriate in one or another industry, or are often incomplete, not covering all risks. They fail to take into account the context.

The information security risk management process is furthermore complicated, since companies turn to standards and frameworks as solutions rather than as methods for organizing and communicating their risk postures. From Cobit and COSO to ISO/IEC 27002 and more, standard models are often inappropriately embraced as the key to managing information security risk. They do represent an effective baseline for risk governance. However, these guidelines often provide only part of the risk management solution. Usually they are useful to identify the current state of risk and security maturity.

Some of the companies also feel that there is no common risk language that is broadly accepted and understood by all the standards and models.
1.5 **CONTRIBUTION**

The studied models, standards and best practices are not workless solutions for the information security risk assessment problem as they may seem. Instead, they are more helpful for organizing and communicating organizations’ risk posture. Therefore this work seeks to study and compare in detail different models to assess information security, identify what each model has to offer, what topics it addresses, and it’s main up and downsides. By clarifying what each model has best (their main advantages relatively to the other models) it will be easier to choose between them.

Hopefully, as a result of this work, the assessment of information security risks, within a specific organization, will be made easier through fair and transparent visibility into the existing information security risk assessment models.

1.6 **SUMMARY**

In this first chapter the main topic of this work was presented and the basic terminology and concepts were introduced. The motivation driving this work is also clarified, showing clearly that information security risk needs to be met and managed.

The chapter also states the specific problem that is going to be addressed throughout the work, by identifying the two main reasons for the difficulty in assessing information security risk correctly.

Finally it is made clear how this work is going to contribute to help solving the stated problem(s).

This work is structured in the following order: first a brief review of risk and risk management that helps to establish the context and exposes the main concepts and ideas. Second the state-of-the-art in information security risk assessment and respective models. Then the proposal and objectives or the work are explained. The following chapters are part of the presented proposal and start with the selection of information security risk assessment models to study in detail. Then the actual comparative study is presented (comparing concepts, approaches, outputs, and tools). The final part of the work is the evaluation of the research done, a practical application of the models in a real organization and respective results.

The chosen research methodology for this research work can be classified as a qualitative research methodology. It involves observation and fieldwork, interviews and questionnaires, and researcher’s impressions and notes. The first phase of the research it’s purely theoretical, it consists in identifying, analysing and comparing information security models using only documentation and other studies. The second phase is much more practical, it involves field work. In this phase the studied models are applied in a real organization, and the final results of
this practical application are then compared against the results of the first phase of the research.

The motivation for doing qualitative research, as opposed to quantitative research, comes from the observation that the information security risk management topic is a very subjective topic.
2. Risk and Risk Management

2.1 Establishing the Context

There has been a revolution and renewed interest in the corporate governance practices of modern corporations. Particularly due to the high-profile business scandals and organizational failures of the past decade where stakeholders suffered tremendous loss (e.g. AOL Time Warner, Tyco, Bear Stearns among others). In response to those corporate collapses, industry groups and regulators recently created a complex array of additional new laws and regulations designed to force improvement in corporate governance and on risk management. The best example of those regulations is the USA Sarbanes-Oxley Act and the EU 8th directive:

- **Sarbanes-Oxley** (or SOX), was enacted in response to the flood of headline-dominating financial transgressions by companies such as Enron, Arthur Andersen, and WorldCom that led not only to their downfall but to a serious decline in stock markets and the economic health of the United States. In a nutshell, it was too easy for a company to “cook the books” and for executives to line their pockets at the expense of shareholders while claiming ignorance. SOX greatly tightened restrictions on methods companies can use for maintaining and reporting financial data and on their financial processes generally. What Sarbanes-Oxley did was make best business practices mandatory instead of optional. SOX compliance is a major issue for virtually any publicly traded firm.

- **European Union 8th Directive**: The EU is taking steps similar to the United States, issuing a proposal that broadens the scope of the 8th Council Directive on Company Law, which primarily pertains to the approval of statutory auditors in EU member states. The expanded directive, which will impact the 25 EU member countries, is expected to be adopted very soon. The proposal strives to improve cooperation between EU oversight bodies and provides for effective and balanced international regulatory cooperation with oversight bodies outside the EU regulatory infrastructure (e.g., the U.S. Public Company Accounting Oversight Board).

But there are also other regulations that require improvement on risk management like:

- **Basel II** framework sets up rigorous risk and capital management requirements designed to ensure that a bank holds capital reserves appropriate to the risk the bank exposes itself to through its lending and investment practices. It seeks to improve on the existing rules by aligning regulatory capital requirements more closely to the underlying risks that banks face. In addition, the Basel II Framework is intended to promote a more forward-looking approach to capital supervision, one that encourages banks to identify the risks they may face today and in the future.
and to develop or improve their ability to manage those risks. As a result, it is intended to be more flexible and better able to evolve with advances in markets and risk management practices.

- **Solvency II** is a fundamental review of the capital adequacy regime for all European insurers and reinsurers that aims to establish a revised set of EU-wide capital requirements and risk management standards that will replace the current Solvency 1 requirements. Often called “Basel for insurers,” Solvency II is somewhat similar to the banking regulations of Basel II. Solvency 2 will require firms to value their assets and liabilities on a market-consistent basis and that more risk-sensitive capital requirements will address asset as well as liability risks. The aim of a solvency regime is to ensure the financial soundness of insurance undertakings, and in particular to ensure that they can survive difficult periods. This is to protect policyholders (consumers, businesses) and the stability of the financial system as a whole.

But in fact these regulators are only stipulating commonsense best practices and are asking organizations to do the right thing, which they should have been doing anyway. These governance requirements have primarily been driven by the need for transparency of enterprise risks and the protection of shareholder value. Instilling corporate accountability hopefully will restore public confidence in corporate governance.

The acceptance of corporate governance rules defined by an external entity is called **compliance**. This usually means conformance with legislative and industry mandates.

Risk management is extremely important in the compliance process because it will help determine what regulations require full compliance, what's most important in terms of the company's definition of its own risk profile and where to focus corporate efforts in the expanding compliance universe. And curiously, compliance with most of these regulations also requires effective risk management. So risk management importance is undeniable in our present days.

As we’ve seen, governance, risk management and compliance are related activities emerging as some of today’s most prevalent business issues. There’s even an increasingly recognized term (“GRC”) that reflects a new way in which organizations can adopt an integrated approach to these three areas. However, despite intersections in some points, they have different goals and they solve different problems for different sets of constituents of an organization.

### 2.2 Risk Categories

Organizations are exposed to various types of business risk. These risks can be categorized in a number of ways. One approach is to consider the source of the risk, examples being investment, legal, operational and market risks. Another is to consider the nature of the asset which is at risk, examples being people, property and information. A further approach is to
consider the consequence of a risk in respect of its implications for the long, medium and short-term activities of the business, examples being strategic, tactical and operational risks.

In this work, the various risk categories are divided according to the purpose of the study. However, other people or entities have their own division (in most cases influenced by their business area). For example the Basel II framework divides risk management merely into credit, market and operational risk management. Another division is made by the Portuguese Central Bank in their risk assessment model. It first separates financial from non-financial risks. Financial risks include credit and market risks (like Basel II) and exchange and interest rates risk as well. Non-financial risks incorporate operational, information systems, strategy, compliance and reputation risks.

But despite the categorization of risks, organizations should be capable of dealing with all kinds of risks, irrespective of the way in which they are classified.

### 2.1.1 Financial Risk

In finance, risk is not an abstract uncertainty or possibility of failure or variability of the outcome. It’s the probability that an investment’s actual return will be different than expected. This includes the possibility of gaining or losing some or all of the original investment. The fundamental idea is the relationship between risk and return. The greater the amount of risk that an investor is willing to take on, the greater the potential return. The reason for this is that investors need to be compensated for taking on additional risk. It is usually measured by calculating the standard deviation (volatility) of the historical returns or average returns of a specific investment.

Nevertheless, financial risk is a wide concept that can also refer to some of these other types of risk:

- **Credit Risk** - The extension of loans is the primary activity of most financial institutions. Lending activities require banks to make judgments related to the creditworthiness of borrowers. These judgments do not always prove to be accurate and the creditworthiness of a borrower may decline over time due to various factors. Consequently, a major risk that financial institutions face is credit risk or the failure of a counterparty to perform according to a contractual arrangement. This risk applies not only to loans but to other on- and off-balance-sheet exposures such as guarantees, acceptances and securities investments.

- **Market Risk** - Risk of losses in on- and off-balance-sheet positions arising from supply and demand functions or global prices for commodities.

- **Liquidity Risk** - Risk that a given security or asset cannot be traded quickly enough in the market to prevent a loss (or make the required profit). Insufficient cash or cash-equivalents to meet the needs of depositors and borrowers.
• Economic Risk - Risk of harm by the effect of global economy on the organization’s country and environment (e.g. exchange rates affecting costs of international transactions or interest rates affecting credits).

In the mid-1990s, the topic of financial risk (especially market and credit risk) became the subject of much debate and research, with the result that financial institutions have made significant progress in the identification, measurement and management of both these forms of risk. Financial markets are now considered to be a proving ground for general methods of risk assessment.

2.1.2 Operational Risk

It is relatively straightforward for an organization to set and observe specific, measurable levels of market risk and credit risk. By contrast it is relatively difficult to identify or assess levels of operational risk and its many sources. Historically organizations have accepted operational risk as an unavoidable cost of doing business but devastating events such as the September 11 terrorist attacks, rogue trading losses (at Société Générale, Barings, AIB and National Australia Bank) and the subprime mortgage crisis serve to highlight the fact that the scope of risk management extends beyond merely market and credit risk. Organizations are now changing the way to address operational risk. Unfortunately, there is no universally accepted definition of the term operational risk.

Operational risk arises from execution of business functions so it exists in every organization in a number of forms and exists regardless of the organization’s size. As such, it is a very broad concept including:

• Health and Safety Risk - Risks affecting employee health and safety (e.g. buildings, vehicles, equipment, fire, noise, vibration, asbestos, chemical and biological hazards, food safety, traffic management, stress, lone working).
• Physical Risk - Risks affecting physical assets (e.g. theft, vandalism, arson, storm, flood or other related weather, damage to vehicles, mobile plant and equipment).
• Fraud Risk - Organization’s susceptibility to internal or external fraud; Risk of having people trying to intentionally secure an unfair or unlawful gain.
• Human Resources Risk - Risk resulting from inadequacy of human resources (in qualitative and quantitative terms), recruiting processes, training programmes and employee motivation.
• Outsourcing Risk - Risk of organization’s regular activity being affected or compromised (in terms of continuity, integrity or quality) due to the use of outsourced resources.
The identification and measurement of operational risk is a real and live issue for modern-day organizations. Particularly to the financial institutions since the decision by the Basel Committee on Banking Supervision (BCBS) to introduce a capital charge for this risk as part of the new capital adequacy framework (Basel II).

2.1.3 **STRATEGIC RISK**

Strategic risk is the current and prospective impact on earnings or capital arising from adverse business decisions, improper implementation of decisions, or lack of responsiveness to industry changes. This risk is a function of the compatibility of an organization’s strategic goals, the business strategies developed to achieve those goals, the resources deployed against these goals, and the quality of implementation.

2.1.4 **REPUTATION RISK**

A corporate reputation is a collective representation of a firm’s past actions and results that describe the firms’ ability to deliver outcomes to multiple stakeholders. It gauges a firms’ relative standing both internally and externally. This reputation, particularly the trust afforded it by customers and counter-parties can be irrevocably tarnished due to perceived or real breaches in its ability to conduct business securely and responsibly.

“It takes twenty years to build a reputation and five minutes to destroy it.” (Warren Buffet)

Reputation risk is the current and prospective impact on earnings and capital arising from negative publicity regarding an institution’s business practices. This affects the institution’s ability to establish new relationships or services, or continue servicing existing relationships. This risk may expose the institution to litigation, financial loss, or a decline in its customer base. Reputation risk exposure is present throughout the organization and includes the responsibility to exercise an abundance of caution in dealing with its customers and the community.

2.1.5 **LEGAL & REGULATORY COMPLIANCE RISK**

Compliance risk is usually considered as part of Operational risk but nowadays it’s gaining strength of his own. It’s currently being debated if this risk should be heightened to the same level as financial and operational level.

Compliance risk is the current and prospective risk to earnings or capital arising from violations of, or non-conformance with, laws, rules, regulations, prescribed practices, internal policies, and procedures, or ethical standards. Compliance risk also arises in situations where the laws or rules may be ambiguous or untested. This risk exposes the institution to fines, civil money penalties, payment of damages, and the voiding of contracts. Compliance risk can lead to diminished reputation, reduced franchise value, limited business opportunities, reduced expansion potential, and an inability to enforce contracts.
2.1.6 Information Systems Risk

Information Systems risk is being increasingly recognized as a major category of business risk in their own right instead of being subsumed in other categories such as strategic and operational risks. This is mostly due to the wider range of information systems risks an organization is exposed to. Information Systems risk requires the effective control of processes, people and systems, and the monitoring of, and response to, external events.

A possible definition to information systems risk is the probability of occurring negative impact on capital on results due to an unadjusted information systems strategy or in consequence of its inadaptability to new requirements and business needs. Other factors that can lead to this negative impact are the information systems inability to stop unauthorized accesses, to guarantee data integrity or to assure business continuity in case of failure.

2.3 Risk Management

In order to overcome the challenge of effectively dealing with uncertainty, and associated risk and opportunity, organizations have to address the specific problems that are most likely to cause the most damage and evaluate them accurately (identify and assess risk). This balance between enhancing the capacity to build value while minimizing losses is Risk Management.

This section provides an overview of risk management, clarifying related terms and concepts, and defines a generic common approach to this process.

Risk management was focused primarily on financial, predictable and quantifiable risks related to loss prevention. Since the 1980s, risk management has evolved to include alignment to strategic objectives, capital adequacy and stakeholder value. The recent increase in rules and regulations is also helping to change the importance of risk management within the corporation. It's becoming a management practice that is as important as financial or facilities management.

2.2.1 Definition

The European Union gives the following risk management definition: The process, distinct from risk assessment, of weighing policy alternatives in consultation with interested parties, considering risk assessment and other legitimate factors, and, if need be, selecting appropriate prevention and control options.

Note that risk management is not the same as risk avoidance. Risk management is all about reducing the risk. Risk management are coordinated activities to direct and control an organization with regard to risk while risk avoidance is the decision not to become involved in, or action to withdraw from, a risk situation.

2.2.2 Motivation

Organizations that do not perform proper risk management could see their ability to conduct business damaaed or even destroyed. Risk management helps an entity get to where it wants
to go avoiding pitfalls and unwanted surprises along the way. Organizations that manage risk effectively and efficiently are more likely to achieve their objectives and do so at lower overall cost.

Therefore organizations should regularly undertake comprehensive, focused management of potential risks, considering external and internal factors.

### 2.2.3 Risk Management Cycle

Risk management is a logical and systematic method of establishing the context, analyzing and evaluating the risks, implementing controls to treat the risks, communicating, monitoring and reviewing the risks, and maintaining and improving the system of risk controls (Figure 2).

**Context**

Risk Management context refers to the process of identifying information that may have an influence on the management of risk (goals, objectives, strategies, scope and parameters). Good risk management also involves reviewing organization’s operations.

Identifying the scope is an extremely important step in the process. The scope separates what is covered and what is not covered in the assessment, it can be either the whole organization or parts of the organization.

**Risk Assessment**

Risk Assessment is a basis for determining how risks should be managed, so it’s one of the first steps in a risk management process. The main purpose of the risk assessment process is to identify risks and their potential impact. Note that sometimes the reality of some risks may be disputed and in such cases leadership may choose to deny the risk. This is itself a potential risk.
The risk assessment process includes the systematic approach of estimating the magnitude of risks (Risk Analysis) and the process of comparing the estimated risks against risk criteria to determine the significance of the risks (Risk Evaluation).

- **Risk Analysis**: Risk Analysis is the systematic process to comprehend the nature of risk (by finding, recognizing and describing risks) and to deduce the level of risk (by assigning values to consequences and their probability). Risk analysis provides the basis for risk evaluation and decisions about risk treatment.

- **Risk Evaluation**: Risk Evaluation is the process of comparing the estimated risk against given risk criteria (predefined risk scale or terms of reference) to determine the significance of risk. Risk Evaluation includes:
  - *Determination of the criteria for risk acceptance*. This should describe the circumstances under which the organization is willing to accept the risks.
  - *Identification of acceptable levels of risk*. Whatever risk assessment approach is chosen, the levels of risk that the organization considers acceptable need to be identified.

Risk criteria should be based on internal and external context and be regularly reviewed to ensure continued relevance. It can be derived from standards, laws and policies.

The next step in this generic risk management process is to identify the appropriate Risk Response action for each of the risks that have been identified and evaluated in the risk assessment.

**Risk Response**

Once a risk has been assessed a business decision needs to be made on what, if any, action to take. Different business circumstances will dictate what kind of decision is made.

The ideal approach to treat risk would be their elimination (reduction of the frequency of an unfavourable event and/or its severity to zero). But the elimination of all risk is usually impractical or close to impossible. So for each of the risks identified in the risk assessment process, management needs to select the more appropriate risk response.

The two main factors that might influence that decision are:

a) the impact if the risk is realized, i.e. the cost each time it happens;

b) how frequently it is expected to happen.

These will give an indication of the loss that might be expected to occur, if nothing is done to mitigate the assessed risk.

The risk response chosen must be proportional. It must consider the effect on productivity, the cost effectiveness, and the value of the asset(s) being protected.

Possible risk responses:
• **Accept:** Risk Acceptance is the informed decision to take a particular risk. But before deciding whether to accept a certain risk, the organization should decide criteria for determining whether or not risks can be accepted. Examples of criteria for risk acceptance are accepting the risk based upon the relative low value of the asset, the relative low frequency of occurrence, and the relative low impact on the business. Or even if the cost of the solution is higher then the potential financial impact of the risk being addressed, management should consider living with part of the risk, or accepting and living with the risk completely. Risks accepted should be subject to monitoring and review.

• **Avoid:** Risk Avoidance is deciding not to be involved in, or to withdraw from, an activity based on the level of risk involved.

• **Transfer:** In some cases, the risk can be transferred to another party (e.g. buying insurance or out-sourcing to another business). However, legal or regulatory requirements can limit or prohibit the transfer of certain risk due to the new risks it creates.

• **Reduce:** Risk Reduction involves prioritizing, evaluating, and implementing the appropriate risk-reducing controls (recommended from the risk assessment process) to reduce the negative effect of the risk to an acceptable level. Risk Reduction is the combination of risk prevention, risk repression and/or risk mitigation. Risk prevention are measures taken to reduce the likelihood that an undesired event occurs; risk repression are measures taken to reduce the likelihood that an undesired event leads to a consequence; risk mitigation are measures taken to reduce the effect of an undesired consequence.

**Controls**

The COSO framework defines Control as the policies, procedures, practices, and organizational structures designed to provide reasonable assurance that the risk responses are effectively carried out. That is, business objectives will be achieved and undesired events will be prevented or detected and corrected.

Risks can be managed and mitigated through a combination of prevention and detection controls. Preventive controls block actions that would increase the risk, while detective controls are designed to detect certain actions or levels of performance that indicate an increased risk. Controls can also be divided between:

• **Administrative or Procedural Controls** (approved written policies, procedures and guidelines);
• **Logical or Technical Controls** (use software and data to monitor and control access to information and computing systems);
• **Physical Controls** (monitor and control the environment of the work place and the access to and from such facilities).
The countermeasures (controls) selected to manage risks must be balanced between productivity, cost, effectiveness of the countermeasure, and the value of the informational asset being protected. Over-protection can introduce unnecessary costs and overhead.

Organizations should only implement controls and safeguards that are actually needed, controls that address specific business needs and risks of that particular organization, otherwise controls won’t solve the security problems it should and will be far from effective. Due to the great decrease of productivity ineffective controls can cause, assessing risk before addressing controls is an essential practice. Only after this assessment process, should the organization implement the controls actually needed, not the other way around. Implementing controls just because their recommended in some model or standard or because the technology is available is a waste of precious resources.

But, as we can see by recent organizational failures and scandals, this logic approach is not yet followed by many companies. Mostly because business leaders won’t tolerate controls or security measures that could slow down business.

**Residual Risk**

No organization is ever risk free, not even right after assessing and mitigating risks. Reasons for this fact are the impossibility to identify all risks or to eliminate all risk through controls. And sometimes implemented controls can’t eliminate the risk they are intended to address or reduce the risk to an acceptable level. This remaining risk after the implementation of new or enhanced controls is called Residual Risk (or retained risk).

\[
\text{Residual Risk} = (\text{identified risks}) - (\text{risk covered by controls}) + (\text{unidentified risks})
\]

**Risk Reporting and Communication**

Risk Communication refers to the continuous or iterative process that an organization conducts to provide, share and obtain information regarding the management of risk. The internal communication may be in the form of a report as a support for decision making. Reports include strategic, operational, financial and compliance-related risk information.

- **Internal Reporting**: Different levels within an organization need different information from the risk management process.
- **External Reporting**: A company needs to report to its stakeholders on a regular basis setting out its risk management policies and the effectiveness in achieving its objectives.

A maintained Risk Register (document for recording the risk management process) provides a useful vehicle for communication. A risk register should include the date of the last assessment, a description of the risk, an estimate of the impact and the likelihood, any mitigating controls, and a statement of action required, with target date and owner. Arranging risks in the register
linked to objectives converts risk information into risk knowledge, and facilitates the ownership and management of each risk.

**Monitoring and Review**

Organizations are dynamic and operate in dynamic environments. So we cannot assume we have all of the facts necessary to assess risk. Changes in the organization and in the environment in which it operates must be identified. There are several factors that could change the originally assessed risks, so new risks will probably surface and risks previously mitigated may again become a concern. Therefore, the process of risk management shouldn't be a means to an end. It should be an ongoing iterative process that re-evaluates old risks and identifies new ones.

Over time there is a tendency for the performance of any service or mechanism to deteriorate. So an organization has to ensure that controls function correctly and effectively and that changes in the environment have not rendered them ineffective.

Monitoring is the ongoing operational activity intended to detect risk controls deterioration and initiate corrective action. This monitoring process should provide assurance that there are appropriate controls in place for the organization’s activities and that the procedures are understood and followed.

After all these different changes have been taken into account, the risks identified in the original risk assessment should be re-calculated and necessary changes to the risk treatment decisions and controls identified and documented (review).

**2.4 SUMMARY**

This section tried to clarify concepts closely related to the subject of this work. It addressed risk and its main areas of application. Not only the traditional financial, operational and strategic areas were considered but also the emerging ones like reputation, compliance and information systems.

It was also provided an overview of risk management, clarifying related terms and concepts, and defines a generic common approach to this process. Risk management is simply a practice of systematically selecting cost effective approaches for minimizing the effect of threat realization to the organization.

All risks can never be fully avoided or mitigated simply because of financial and practical limitations. Therefore all organizations have to accept some level of residual risks.

Risk assessment is the part of the risk management process this work is focused in. It is used to identify threats, classify assets and to rate system vulnerabilities as it provides key information and guidelines to implement effective controls. Despite its complexity, the risk assessment process is a very critical step for good risk management. But surprisingly, few are the organizations that invest in proper risk assessment before implementing the controls to mitigate
risk (another step in the risk management process cycle). And even companies that feel they assess risk fairly well still need to continue to focus on improving its risk management practices and procedures.

The consequences of improper risk assessment can be profound, not only are some threats overlooked, but also resources and budgets are misapplied to threats that do not exist or have minimal impact. These consequences will largely decrease organizations’ productivity and efficiency.

Despite claiming to have risk management processes implemented, several organizations weren’t able to avoid harsh consequences including bankruptcy. Among the reasons for that fact are:

- **Organizations were using wrong techniques** - The risk management methods introduced and deployed in the 1990’s were simple checklists, scoring tables, and, sometimes, complex calculation tools.

- **Risk management was too bureaucratic** - Many organizations took the bureaucratic route: they defined plentiful of report templates and standards on how to do risk management and many lengthy reports were produced – but not necessarily read nor acted upon. In such situations, risk management created a high overhead cost but produced little value.

- **Risk management was too standard** - Many risk management approaches and tools aim to make their use easier by standardizing some aspects in their models. Risks are often valued only through money, calendar, or effort impacts. The reality, of course, is more complex.

- **Risk management was not transparent** - Many risk management methods and tools use complex calculations and forms to document and analyze risk information: little attention was spent on making sure that the decision makers fully understand all steps and pieces of information in the process. Consequently, as people did not fully understand the risk analysis process, they did not have much confidence in it and could not communicate the results well.
3. INFORMATION SECURITY RISK ASSESSMENT

3.1 INFORMATION SECURITY RISK

In information security, a risk can be defined as the probability that a particular threat-source will exercise (accidentally trigger or intentionally exploit) a particular information security vulnerability and the resulting impact.

It’s quite hard to insert information security risk into one risk category. Most consider it as an information systems risk, but information security implies more than information technology and consequently it goes beyond the range of information systems risk.

Despite implying more than technology, the focus of information security had always been, until recently, on protecting the IT (Information Technology) systems that process and store the vast majority of information, rather than on the information itself. Yet, information security is not synonymous of computer security. Information security is concerned with the confidentiality, integrity and availability of information regardless of the form it may take. Information can be printed or written on paper, stored electronically, transmitted by post or by using electronic means, shown on films, or spoken in conversation. So technology is only one concern of information security, people and processes are other aspects that have to be taken into consideration (Figure 3).

As this risk is the one this work addresses, it is described here, and not in the risk categories section (2.1).

2.3.1 INFORMATION SECURITY

The term “information security” means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity and availability. Ensuring the Confidentiality, Integrity and Availability (CIA Triad) of vital information assets may be essential to minimize business risks and therefore maintaining competitive edge, cash flow, profitability, legal compliance, and commercial image.

- **Confidentiality**: the property of preserving authorized restrictions on access and disclosure of information covering all the processes, policies, and controls employed to do so. Confidentiality is necessary (but not sufficient) for protecting personal privacy and proprietary information;

- **Integrity**: the property of safeguarding the accuracy and completeness of assets. In information security, integrity relate to the processes, policies, and controls used to
ensure information has not been modified without authorization and that systems are free from unauthorized manipulation that will compromise accuracy, completeness, and reliability. Integrity includes ensuring information non-repudiation and authenticity.

- **Availability**: For any information system to serve its purpose, the information must be available when it is needed. Availability is the property of being accessible and usable upon demand by an authorized entity. This means that the computing systems used to store and process the information, the security controls used to protect it, and the communication channels used to access it must be functioning correctly. This objective protects against intentional or accidental attempts to deny legitimate users access to information or systems (Denial-of-Service, or DoS).

**Motivation**

We’ve already seen that information can become a serious risk for organizations nowadays. That’s the main reason why information security is so important in risk management.

Information security is especially important in our increasingly interconnected business environment (with interconnection of public and private networks and the sharing of information resources). Information is now more difficult to control and is exposed to a growing number and a wider variety of threats and vulnerabilities from a wide range of sources, including computer-assisted fraud, espionage, sabotage, vandalism, fire or flood.

Governments, military, financial institutions, hospitals, and private businesses are examples of organizations that amass a great deal of confidential information about their employees, customers, products, research, and financial status. Should confidential information about a business’s customers or finances or new product line fall into the hands of a competitor, such a breach of security could lead to lost business, law suits or even bankruptcy of the business. Information itself has become a regulated asset, with specific criteria for its protection, privacy, use and retention so protecting confidential information is a business requirement, and in many cases also an ethical and legal requirement. Note that most of this information is now collected, processed and stored on electronic computers and transmitted across networks to other computers, so its protection, privacy, use and retention often involves information technology.

Information security risk is definitely a real and serious issue nowadays. Awareness of its importance continues to grow with new reports of hackers, organized crime, fringe groups, and even terrorists exploiting technology for their own profit and motives. One can rarely open a newspaper without reading about yet another computer security breach. For this reason, much time is spent on protecting against external threats, but one of the biggest potential threats to information security and one of the weakest links in the security value chain are the people who handle the information. Information security polls continue to reveal that **insider threat**, due to disgruntled or dishonest employees, represent one of the most significant information security
risks. The Société Générale case is, once again, an excellent example of the dangers insider threat can bring.

These statistic facts make us understand that the security that can be achieved through technical means is limited and that physical security is often becoming a discounted discipline. Technology software alone cannot protect organizations from all security threats. We are learning that organizations now need hardened security processes, procedures and stated policies that are based on internationally accepted best practices, to solidify their Information Security defences and meet legal, contractual and regulatory requirements.

3.2 INFORMATION SECURITY RISK ASSESSMENT

Information security risk assessment is the process (part of Risk Management) that identifies and valuates the risks to information security by determining the probability of occurrence and the resulting impact. It identifies threats, classifies assets and rates system vulnerabilities as it provides key information and guidelines to implement effective controls.

Information Security Risk Analysis

Risk Analysis (or Identification) generally involves (Figure 4):

1. **Identification of assets:**
   - *Information* (databases and data files, contracts and agreements, system documentation, research information, user manuals, training material, operational or support procedures, business continuity plans, fallback arrangements, audit trails, and archived information);
   - *Software Assets* (application software, system software, development tools, and utilities);
   - *Physical Assets* (computer equipment, communications equipment, removable media, and other equipment);
   - *Services* (computing and communications services, general utilities, e.g. heating, lighting, power, and air-conditioning);
   - *People* and their qualifications, skills, and experience;
   - *Intangibles*, such as reputation and image of the organization.

2. **Identification of legal and business requirements** relevant for the identified assets.

3. **Collecting all policies, procedures and controls** currently in place. Assess whether or not the existing policies, procedures and controls implemented are adequate.

4. **Identification of significant threats or risk sources.** These threats can be split into Human and Nonhuman elements. (Acts of nature, acts of war, accidents, among others malicious acts originating from inside or outside the organization).

5. **Identification of vulnerabilities for the identified assets.**
Figure 2 – Information Security Risk Analysis

- **Asset** is defined as anything having value to an organization.

- **Threat** is a potential cause of an unwanted incident, which may result in harm to a system or organization. **Vulnerability** is a weakness of an asset or group of assets that can be exploited by one or more threats. It is the susceptibility to injury or attack. In computer security, the term vulnerability is applied to a weakness in a system which allows an attacker to violate the integrity of that system.

- A **requirement** is a singular documented need of what a particular asset should be, do or respect.

- **Impact** can be defined as the severity of the consequences of an event or incident. In the context of information security, the impact is a loss of availability, integrity, and confidentiality of information.

- **Likelihood** is the probability of a threat materialize.

**Information Security Risk Evaluation**

Risk evaluation or estimation is the process used to assign values to consequences, their likelihood and to the level of risk. It involves:

1. Assessment of the likelihood of the threats and vulnerabilities to occur;
2. Calculation of the impact that each threat would have on each asset;
3. Determination of quantitative (measurable) or qualitative (descriptive) value of risk.

One important thing to take into consideration is that these three variables rarely are independent from each other. In information security, there’s a probable relation between asset value, impact and probability. For example, it’s more likely a hacker will exploit a vulnerability that causes a bigger impact than one with low impact. Likewise, a valuable asset has more probability of being compromised than a valueless one. Therefore, in this field we have to take
into consideration more than simply random or accidental acts. And besides this relation, we should remind ourselves that given enough time and determination, people can circumvent almost every security measure. They can be extremely creative when motivated. Therefore this motivation factor should be seriously addressed in the information security risk assessment process.

In addition to this relation, new threats and vulnerabilities are continuously appearing and when considering risks to information infrastructures, the number, type, and variation are overwhelming. Despite being hard to keep up with all these new vulnerabilities and threats, they need to be managed adequately or else the organization future and existence can be threatened.

### 3.3 INFORMATION SECURITY RISK ASSESSMENT MODELS

There are several models and methods with different approaches that help in the risk assessment process.

This study will address the methods that support the risk assessment process and those which can be applied to information security. Therefore, methods that are not classified as risk assessment or risk management oriented or that are general management oriented (i.e. corporate governance) frameworks like Coso, Cobit or Basel II have been excluded from the study. High-level reference documents like the ISO Guide 73 are also not taken into consideration in this section.

Risk assessment models can be separated into quantitative and qualitative.

#### 3.3.1 QUALITATIVE VS. QUANTITATIVE MODELS

Risk assessment models can be separated into **quantitative** and **qualitative**.

Quantitative models use measurable, objective data to determine asset value, probability of loss, and associated risk(s). The goal is to try to calculate objective numeric values for each of the components gathered during the risk assessment and cost-benefit analysis.

Qualitative methods use a relative measure of risk or asset value based on ranking or separation into descriptive categories such as low, medium, high; not important, important, very important; or on a scale from 1 to 10. A qualitative model assesses the impact and likelihood of the identified risks in a rapid and cost-effective manner. The sets of risks recorded and analyzed in qualitative risk assessment can provide a foundation for a focused quantitative assessment.

Both qualitative and quantitative approaches to security risk management have their advantages and disadvantages. Certain situations may call for organizations to adopt the quantitative approach. Alternatively, organizations of small size or with limited resources will probably find the qualitative approach much more to their liking. The following table summarizes the benefits and drawbacks of each approach:
<table>
<thead>
<tr>
<th>Benefits</th>
<th>Quantitative</th>
<th>Qualitative</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• Risks are prioritized by financial impact; assets are prioritized by financial values.</td>
<td>• Enables visibility and understanding of risk ranking.</td>
</tr>
<tr>
<td></td>
<td>• Results facilitate management of risk by return on security investment.</td>
<td>• Easier to reach consensus.</td>
</tr>
<tr>
<td></td>
<td>• Results can be expressed in management-specific terminology (for example, monetary values and probability expressed as a specific percentage).</td>
<td>• Not necessary to quantify threat frequency.</td>
</tr>
<tr>
<td></td>
<td>• Accuracy tends to increase over time as the organization builds historic record of data while gaining experience.</td>
<td>• Not necessary to determine financial values of assets.</td>
</tr>
<tr>
<td></td>
<td>• Enables visibility and understanding of risk ranking.</td>
<td>• Easier to involve people who are not experts on security or computers.</td>
</tr>
<tr>
<td></td>
<td>• Easier to reach consensus.</td>
<td>• Insufficient differentiation between important risks.</td>
</tr>
<tr>
<td></td>
<td>• Not necessary to quantify threat frequency.</td>
<td>• Difficult to justify investing in control implementation because there is no basis for a cost-benefit analysis.</td>
</tr>
<tr>
<td></td>
<td>• Not necessary to determine financial values of assets.</td>
<td>• Results are dependent upon the quality of the risk management team that is created.</td>
</tr>
<tr>
<td></td>
<td>• Easier to involve people who are not experts on security or computers.</td>
<td></td>
</tr>
</tbody>
</table>

| Drawbacks         | • Impact values assigned to risks are based on subjective opinions of participants. | • Insufficient differentiation between important risks.                      |
|                   | • Process to reach credible results and consensus is very time consuming.       | • Difficult to justify investing in control implementation because there is no basis for a cost-benefit analysis. |
|                   | • Calculations can be complex and time consuming.                               | • Results are dependent upon the quality of the risk management team that is created. |
|                   | • Results are presented in monetary terms only, and they may be difficult for non-technical people to interpret. |                                                                              |
|                   | • Process requires expertise, so participants cannot be easily coached through it. |                                                                              |

<table>
<thead>
<tr>
<th>Table 1 - Qualitative vs. Quantitative</th>
</tr>
</thead>
<tbody>
<tr>
<td>In years past, the quantitative approaches seemed to dominate security risk management; however, that has changed recently as more and more practitioners have admitted that strictly following quantitative risk management processes typically results in difficult, long-running projects that see few tangible benefits.</td>
</tr>
</tbody>
</table>

**3.4 SUMMARY**

Information security was the broad concept addressed by this state-of-the-art. It is clear after the last two chapters that security and risk management are not a status or a snapshot but running processes.

It’s also understandable throughout this chapter that the key asset for an organization is the information, and not the systems that process it. Information must be adequately protected regardless how it is handled, processed, transported or stored. Therefore organizations must address the universe of risks, benefits and processes involved with all information resources, and not only with the technological resources. Organizations also have to take into account how people, processes and technology interoperate in a dynamic networked environment while dealing with information. Security depends more on people than on technology and employees.
are a far greater threat to information security than outsiders. Security is like a chain, it is as strong as its weakest link.

The key to effective information security is to work **smarter, not harder**. In order to work smarter and make the right decisions managers need to be extremely well informed about their organizations. An organization should always first understand their specific needs, and what must be really monitored and protected (risk profile) before implementing any strategy. Only an enlightened approach like this will accomplish the level of integration, process assurance and overall protection that is now required.

All these facts inevitably lead to the conclusion that information security risk is a management and not a purely technical issue.

Proper contextualized risk assessment is the best way to approach the organization's need for information security. Due to the great decrease of productivity ineffective controls can cause, assessing risk before addressing security controls is an essential practice.
4. PROPOSAL

4.1 INTRODUCTION

The first part of this research work was to ask a question, identify a problem, and define an area of exploration (Chapter 1). The question that originated this research study basically is “Why is information security risk assessment so hard to achieve effectively?”. We’ve seen earlier that two of the main reasons for this problem are the great variety of assessment models as well as the fact that Information Security Risk is different from other more traditional risks. So, in sum, the main issue addressed by this study is how to effectively select an information security risk assessment model to start a risk assessment process in an organization.

After that first part I had to gather relevant data and information to build an overall picture of the problem and describe the actual situation (Chapters 2 and 3).

This chapter pretends to clarify this study’s purpose and give insight on how its objectives are going to be achieved. The next chapters will explore and analyze in detail specific issues directly related to the problem identified.

Chapter 5 demonstrates how the detailed study of the models was carried out. It shows the various steps taken to come up with a sustained selection and comparison of models. Chapter 6 tries to look at the studied models in a different perspective. It describes a practical application of the models in a real organization.

4.2 OBJECTIVES

This study proposes to clarify some of the most important information security risk assessment models. The main goal is to provide practical information for organizations wanting to initiate or to enhance their risk management process or that want to implement some sort of controls regarding information security.

The reason for trying to clarify, analyse and compare a variety of risk assessment models is the fact that these models, standards and best practices are not workless solutions for the information security risk assessment problem as they may seem. Instead, they are more helpful for organizing and communicating organizations’ risk posture. Therefore this work seeks to study and compare in detail different models to assess information security, identify what each model has to offer, what topics it addresses, and it’s main up and downsides. By clarifying what each model has best (their main advantages relatively to the other models) it will be easier to choose between them.

The information will be useful because organizations usually don’t know which existing risk assessment model best applies to their specific context or the one that best addresses their law and regulation requirements. So the study will help in the creation of an information security risk
assessment process adapted to the organization’s individual reality, but at the same time aligned with the best standards and leading practices.

Note that the purpose of the work isn’t the conception of a groundbreaking model or methodology for assessing information security risk (there are plenty of these already). The purpose is to bring the best solutions together, and organize them in a practical and usable way.

4.3 Process

The approach used to address the stated problem and to accomplish the above mentioned objectives is divided into the following tasks:

- Widely explore the risk management theme;
- Identify existing information security risk assessment models;
- Define concise criteria for the selection of the information security risk assessment models previously identified;
- Select the models that will be subject of detailed comparison;
- Thorough study of each information security risk assessment model, aiming to produce a comparative analysis between them:
  - Identification and definition of the concepts involved in each model (e.g. the concept of risk, asset, vulnerability, threat, impact, control, residual risk, among others);
  - Identification of the risk assessment approach recommended by each model (e.g. self-assessment, interviews);
  - Definition of detailed criteria for model analysis and comparison;
- Model comparison based in the theoretical study made until this point;
- Practical experience in a real organization (implementing the studied models);
- Comparison of the theoretical study and practical experience results.

4.4 Summary

Currently there are numerous risk analysis models available, some of which are qualitative while others are quantitative in nature. These models have a common goal of estimating the overall risk value. However, there are no method which will assist organisations in determining which model is the best to be employed within an organisation.

The best way to choose between models is to compare them, using objective, quantifiable criteria. If the criteria that are used are applicable to all risk analysis models, an organization can compare different models objectively, and decide on the best one. Different risk analysis methodologies have to be analyzed to help determining common criteria for selection and comparison.
5. **EXISTING MODELS**

5.1 **INTRODUCTION**

This chapter illustrates clearly how the study was carried out. It exposes the methods and processes used to do the comparative study starting with a considerable list of information security risk models. The chapter includes a thorough study of the most relevant models and a comparison between those same models.

5.2 **MODEL SELECTION**

There are several models and methods that help in the risk assessment process. This study will address the methods that support the risk assessment process and those which can be applied to information security. Therefore, methods that are not classified as risk assessment or risk management oriented or that are general management oriented (i.e. corporate governance) frameworks like Coso, Cobit or Basel II are not considered in this study. High-level reference documents like the ISO Guide 73 are also not taken into consideration as risk assessment models.

This document provides an overview of existing Information Security Risk Assessment methods, and a comparison that evaluates those different methodologies. It aims to describe and compare properties of Information Security Risk Assessment methods in a concise manner. Unless otherwise stated, the words “model” and “method” are used in this document to refer to an “information security risk assessment method or model”, though often times the full phrase is also used.

The remainder of this section is organized as follows:

- Section 5.2.1 lists and briefly describes the models identified during the research.
- Sections 5.2.2 and 5.2.5 present the criteria used to select the final models for a more detailed comparison,
- Sections 5.2.3 and 5.2.6 describe the two selection iterations, where the criteria was applied to the models.
- Section 5.2.7 summarizes and concludes the selection process.

**Scope limits**

Due to the limited time and resources available, only a limited number of products were addressed. Therefore, this document will not contain a complete or exhaustive list of methods and standards dealing with information security risks.
5.2.1 IDENTIFIED MODELS

After a period of some research some models were identified as suitable for assessing information security risk. These models are the following:

1. OCTAVE
2. Mehari
3. MAGERIT
4. IT-Grundschatz
5. EBIOS
6. IRAM
7. SARA
8. SPRINT
9. ISO 27005
10. NIST SP800-30
11. CRAMM
12. MIGRA
13. MAR
14. ISAMM
15. GAO/AIMD-00-33
16. IT System Security Assessment
17. MG-2 and MG-3
18. Dutch A&K Analysis
19. MARION
22. Risk IT

As was stated before, this is a non-exhaustive list.

Each model listed above is briefly described in Appendix A of this document according to the following attributes:

- General Information (includes Name, Website, Owner, Country)
- Description (a brief description of the method and its approach)
- Target Organizations (the model was created to be used in this kind of organizations)
- Risk estimation method (quantitative or qualitative risk level estimation?)

This list of attributes is limited to the specific purpose of this study and does not prejudge the quality (i.e. efficiency and effectiveness) of the products.

5.2.2 FIRST ITERATION SELECTION CRITERIA

In the last section 22 risk assessment models were identified. However, some of them are more adequate to assess information security risks than others. Therefore, this first selection iteration pretends to exclude some of the models based in a criteria described below. These criteria
assess four essential model features. If a model doesn’t hold any of those properties it will be excluded from the universe to study.

The criteria used in this selection iteration are the following:

- **Method/Guideline?**
  
  Is the model really a method? Or just a standard or guideline?

  Method is defined as an orderly arrangement of parts or steps to accomplish an end, a regular and systematic procedure of accomplishing something. Guidelines are advice or instructions given in order to guide or direct an action. A standard is a set of rules widely recognized or employed (especially because of its excellence) that control how people develop and manage materials, products, services, technologies, tasks, processes, and systems.

  *Exclude the model if it isn’t a method.*

- **Identifies Information Security Risks?**
  
  Does the document identify Information Security Risks?

  Information security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification or destruction.

  The Security Risk level of a system is a combination of the importance of maintaining the Availability that system, the Integrity of data housed on or managed by that system and the Confidentiality of sensitive information stored on that system.

  *Exclude the method if it doesn't identify Information Security risks.*

- **Price and availability of documentation?**
  
  Is the information publicly available sufficient to properly evaluate and compare the model with others? Does the information help to answer all criteria questions?

  What’s the estimated price to obtain all documentation and tools needed to implement the model?

  *Exclude the model if it is unavailable or too hard/expensive to purchase.*

- **Last review**
  
  When was the model last reviewed or updated?

  *Exclude if discontinued, obsolete or not updated/reviewed in more than a decade.*

**5.2.3 Criteria applied to each model**

After the defining the selection criteria, each model was analyzed and evaluated using those criteria.
The results of the model selection’s first iteration are summarized in the following table (a green colour means the criterion was satisfied, red means it wasn’t):

<table>
<thead>
<tr>
<th>Name</th>
<th>Method or Guideline?</th>
<th>Identifies IS Risks?</th>
<th>Documentation?</th>
<th>Last Review</th>
<th>2nd Iteration?</th>
</tr>
</thead>
<tbody>
<tr>
<td>OCTAVE</td>
<td>Method</td>
<td>Yes</td>
<td>Free</td>
<td>Up-to-date</td>
<td>Yes</td>
</tr>
<tr>
<td>Mehari</td>
<td>Method</td>
<td>Yes</td>
<td>Free</td>
<td>Up-to-date</td>
<td>Yes</td>
</tr>
<tr>
<td>MAGERIT</td>
<td>Method</td>
<td>Yes</td>
<td>Free</td>
<td>Up-to-date</td>
<td>Yes</td>
</tr>
<tr>
<td>IT-Grundschutz</td>
<td>Standard and Method</td>
<td>Yes</td>
<td>Free</td>
<td>Up-to-date</td>
<td>Yes</td>
</tr>
<tr>
<td>EBIOS</td>
<td>Method</td>
<td>Yes</td>
<td>Free</td>
<td>Up-to-date</td>
<td>Yes</td>
</tr>
<tr>
<td>IRAM</td>
<td>Method</td>
<td>Yes</td>
<td></td>
<td>Up-to-date</td>
<td>Yes</td>
</tr>
<tr>
<td>SARA</td>
<td>Method</td>
<td>Yes</td>
<td>Available only to ISF Members</td>
<td>Discontinued</td>
<td>No</td>
</tr>
<tr>
<td>SPRINT</td>
<td>Method</td>
<td>Yes</td>
<td></td>
<td>Discontinued</td>
<td>No</td>
</tr>
<tr>
<td>ISO 27005</td>
<td>Standard/Guideline</td>
<td>Yes</td>
<td>Available</td>
<td>Up-to-date</td>
<td>No</td>
</tr>
<tr>
<td>NIST SP800-30</td>
<td>Guideline</td>
<td>Yes</td>
<td>Free</td>
<td>Up-to-date</td>
<td>No</td>
</tr>
<tr>
<td>CRAMM</td>
<td>Method</td>
<td>Yes</td>
<td>Expensive</td>
<td>Up-to-date</td>
<td>No</td>
</tr>
<tr>
<td>MIGRA</td>
<td>Method</td>
<td>Yes</td>
<td>Expensive</td>
<td>Up-to-date</td>
<td>No</td>
</tr>
<tr>
<td>MAR</td>
<td>Guideline</td>
<td>No</td>
<td>Free</td>
<td>Up-to-date</td>
<td>No</td>
</tr>
<tr>
<td>ISAMM</td>
<td>Method</td>
<td>Yes</td>
<td>Unavailable</td>
<td>N/A</td>
<td>No</td>
</tr>
<tr>
<td>GAO/AIMD-00-33</td>
<td>Guideline and Case Studies</td>
<td>Yes</td>
<td>Free</td>
<td>N/A</td>
<td>No</td>
</tr>
<tr>
<td>IT System Security Assessment</td>
<td>Guideline</td>
<td>Yes</td>
<td>Unavailable</td>
<td>N/A</td>
<td>No</td>
</tr>
<tr>
<td>MG-2 and MG-3</td>
<td>Guideline</td>
<td>Yes</td>
<td>Unavailable</td>
<td>N/A</td>
<td>No</td>
</tr>
<tr>
<td>Security Risk Management Guide</td>
<td>Guideline</td>
<td>Yes</td>
<td>Unavailable</td>
<td>N/A</td>
<td>No</td>
</tr>
<tr>
<td>Dutch A&amp;K Analysis</td>
<td>Method</td>
<td>Yes</td>
<td>Unavailable</td>
<td>Obsolete</td>
<td>No</td>
</tr>
<tr>
<td>MARION</td>
<td>Method</td>
<td>Yes</td>
<td>Unavailable</td>
<td>Obsolete</td>
<td>No</td>
</tr>
<tr>
<td>Austrian IT Security Handbook</td>
<td>Guideline</td>
<td>Yes</td>
<td>Unavailable</td>
<td>Up-to-date</td>
<td>No</td>
</tr>
<tr>
<td>Microsoft's security risk management guide</td>
<td>Guideline</td>
<td>Yes</td>
<td>Free</td>
<td>Up-to-date</td>
<td>No</td>
</tr>
</tbody>
</table>
### 5.2.4 CHOSEN MODELS

As a result of applying the 4 criteria described in 5.2.2, 16 of the 22 initial models were excluded. These models didn’t comply with one or more criterion and for that reason they won’t be studied in more depth. The assessment of all the models according to the criteria is summarized in the table above.

Nonetheless, six models were in conformance with all the criteria. These models are: **Octave**, **Mehari**, **Magerit**, **IT-Grundschutz**, **Ebios** and **IRAM**. Only these models will be considered after this point.

### 5.2.5 SECOND ITERATION SELECTION CRITERIA

Despite having reduced the initial universe of models to almost one fourth, six is still a significant number of models to study in detail (considering the existent time and people limitations of this work). Therefore, the universe of models will again be reduced through another set of criteria. The 5 selected criteria are described below:

- **Complexity, Effort and preparation**

  This criterion tries to reflect the level of preparation, information, effort and skills needed to implement the model, and the level of detail and scope of the risk analysis results. To express this criterion in a more quantitative manner, models are classified under three levels of complexity:

  - Little preparation needed; less detail/accuracy in the output. Quick assessment
  - Some preparation needed; medium output detail/accuracy.
  - Extensive preparation and effort needed; more detail/accuracy on the output.

- **Approach of the model**

  The risk assessment approach each model advocates (e.g. self-assessment, interviews, workshops).

  This criterion doesn’t pretend to analyse the approach in great detail. It will only consider the main concepts and strategies of each model. A more detailed analysis will take place in the next section.
• **Tool**

If the model provide supporting tools and how can we obtain them. This criterion is divided into the following categories:

- Free tool;
- Paid tool (but with a trial period);
- Paid tool (with no trial available);
- No software tool but has supporting documentation (e.g. worksheets, questionnaires, forms);
- No supporting tools.

• **Origin**

In this study three possible sources for a model were considered. These entities can be:

- Academic;
- Governmental;
- Commercial.

• **Geographical spread**

Countries in which the model is known to have been implemented.

- **Used in EU member states**: list of EU member states in which implementation is known by working group members. This includes organisation as:
  
  European institutions (e.g. European Commission, European Union Council, European agencies).

  International organisations located in Europe (e.g. NATO, UNO, OECD, UNESCO).

- **Used in non-EU countries**: used within potential new member states of the European Union or outside the EU (e.g. Switzerland or USA).

5.2.6 **Criteria applied to each 2nd iteration model**

On this second iteration each model was evaluated again. Now according to a second set of criteria, described in the previous section.

The results of the model selection’s second iteration are summarized in the following table (the green coloured table lines are the models that satisfied the selected criteria):
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>OCTAVE</td>
<td>1 (Low)</td>
<td>Workshop-style, collaborative setting and is supported with guidance, worksheets, and questionnaires, which are included in the method.</td>
<td>No software tool but has supporting documentation</td>
<td>Academic</td>
<td>Used mainly in the USA</td>
</tr>
<tr>
<td>EBIOS</td>
<td>2 (Medium)</td>
<td>Self assessment and discussions in a mixed work group (managers, IT and users)</td>
<td>Free tool</td>
<td>Governmental</td>
<td>Used in many EU member states and non-EU member states</td>
</tr>
<tr>
<td>MAGERIT</td>
<td>2 (Medium)</td>
<td>The method suggests more than one technique to calculate risk (Interviews, Meetings, Questionnaires, Charts, Analysis using tables, Algorithmic analysis, Attack trees)</td>
<td>Free tool</td>
<td>Governmental</td>
<td>Used in many EU member states and non-EU member states</td>
</tr>
<tr>
<td>IRAM</td>
<td>2 (Medium)</td>
<td>Workshop based (typically conducted with business and IT staff)</td>
<td>Free tool (for members)</td>
<td>Commercial</td>
<td>Used in many EU member states and non-EU member states</td>
</tr>
<tr>
<td>IT-Grundschutz</td>
<td>3 (High)</td>
<td>Self Assessment</td>
<td>Paid tool (but with a trial period)</td>
<td>Governmental</td>
<td>Used in many EU member states</td>
</tr>
<tr>
<td>Mehari</td>
<td>3 (High)</td>
<td>Bases its analysis on formulas, parameters, and a knowledge database; Audits are carried out to identify potential Information System (IS) vulnerabilities; Questionnaires or direct assessment for the evaluation of security services.</td>
<td>Paid tool (with no trial available)</td>
<td>Commercial</td>
<td>Used in many EU member states and non-EU member states</td>
</tr>
</tbody>
</table>

Table 3 – Criteria applied to each of the second iteration model

5.2.7 Selection summary

The criteria used in the first iteration were objective and allowed to immediately exclude some of the models. The selection was, therefore, a straightforward and easy to understand process.

However, the second part of the selection wasn’t as simple as the first. The six considered models in the second iteration were all excellent candidates to the next phase of the study, and for that reason, selecting three out of the six required more complex criteria. Most of these criteria were much more subjective and unquantifiable, making the final selection harder.
The strategy adopted in this case was to select the models that, together, formed a representative sample of the existent models universe. Therefore, the selected models should come from different backgrounds and should have different approaches and complexities.

The first criterion to be considered in the selection process was the complexity of each model. As in this work this feature is divided into three levels, the final models should represent all those three levels. Accordingly, models were divided into three groups: models with low complexity (OCTAVE); models with medium complexity (EBIOS, MAGERIT, IRAM); and models with high complexity (MEHARI, IT-Grundschutz). One model from each group will be part of the final set of models to study.

The second criterion considered, the origin of each model, is also divided into three categories, like the first criterion. Therefore, the process will be similar to the one already described above. After combining these two criteria, there were still three possible final sets of models: OCTAVE, EBIOS and MEHARI; OCTAVE and MAGERIT, MEHARI; or OCTAVE, IRAM and IT-Grundschutz.

The third criterion used was the availability of the models’ supporting tools. OCTAVE, EBIOS, MAGERIT and IRAM all had free or easy-to-get supporting tools, only MEHARI and IT-Grundschutz had tools requiring payment. But the difference between those last two is that IT-Grundschutz’s supporting tool offers the possibility of a 30-day period trial, while MEHARI’s one doesn’t. For this reason, IT-Grundschutz was favoured over MEHARI.

This third criterion left only one possibility for the final set of models. Those being OCTAVE, IRAM and IT-Grundschutz.

The other two criteria (approach and geographical spread) were also taken into consideration but, as they don’t clearly differentiate models from each other, their role in the selection process was not as important.

5.3 COMPARATIVE STUDY

The study of the three final models aims to compare in greater detail the three different approaches. This study will not only interpret the models theoretically, but also test the approaches in a real organization (in the next chapter).

5.3.1 COMPARISON CRITERIA

This section introduces the criteria that will be used to evaluate and compare the three information security risk assessment models in more detail. Some of the models’ characteristics were already analysed during the selection process described above. Some of these comparison criteria are similar to the criteria used before, but in this section the models will be analysed in more depth. Below we have the description of the new set of criteria:
• **Concept definition**

This criterion pretends to clarify and distinguish the three information security risk assessment models by identifying and defining their basic and most relevant concepts. It evaluates the similarities and differences between the concept definitions each model proposes.

The concepts that will be under evaluation in this study are: Risk, Asset, Vulnerability, Threat, Impact, Control (or Risk Treatment), Residual Risk, and Security Requirements or Objectives.

• **Approach to information security risk assessment**

The risk assessment approach each model advocates (e.g. self-assessment, interviews, workshops).

This criterion analyses the approach with greater detail than the previous section analysis and also compare the three final models accordingly. To assess the approach at this stage models are characterized under the following aspects:

- Description (of the approach)
- Main activities
- How risk is calculated

• **Results and output**

This criterion analyses the detail of each models’ output after the risk assessment is completed. It tries to evaluate the quality, clarity of the information produced. It also distinguishes models that generate qualitative and quantitative data, and models that recommend information security controls of countermeasures, allowing the organization to continue the risk management process.

• **Complexity**

This criterion tries to reflect the level of preparation, information, effort and skills needed to implement the model, and the level of detail and scope of the risk analysis results. This criterion was also used in the selection process, but in this section the final models will be compared in more detail.

To asses this level models are characterized under the following aspects:

- Level of detail;
- Inputs / Preparation needed (ease of gathering the needed information);
- Techniques;
- People involved;
- Effort;
• Time;
• Skills needed;

The above mentioned criteria will be applied to the three models in the following sections.

5.3.2 Comparing Concept Definitions of the Three Models

**Risk:** All three models have a very similar definition for risk. All of them consider risk as a function of the probability/likelihood of a threat materialising through a vulnerability, and the impact/consequences of that event.

**Asset:** All the three models focus their risk assessment approach on information assets (in some cases also named as IT assets, but both terms refer to the same concept). The difference is that OCTAVE distinguishes the information itself from its container, i.e. the physical or electronic form where information exists is a different concept in OCTAVE (called information container), while the other two models don’t separate the actual information from its containers, considering it all as one concept.

**Vulnerability:** IRAM and IT-Grundschutz have the same definition for vulnerability and they both consider this concept in their approaches in a very similar way. On the other hand, OCTAVE, despite identifying the concept of vulnerability, doesn’t include a vulnerability assessment in its approach. It identifies the containers of each information asset and only considers threats to those containers.

**Threat:** All three models define threat very similarly as a potential undesirable security event. The differences are, for example, that OCTAVE only identifies a threat when a threat actor exploits a vulnerability. This definition is the same as the one in IT-Grundschutz for Applied Threat. IT-Grundschutz also defines Basic Threat as a threat that hasn’t yet exploited a vulnerability. IRAM defines threat and also Security Incident. A security incident occurs when threats materialise.

**Impact:** All three models define Impact as the consequences of a security incident on business with no significant differences between them.

**Control/Risk Treatment:** All definitions are alike, despite the use of several terms form the same concept (control, safeguard, mitigation approach, risk treatment, security precaution, protective measure)

**Residual Risk:** Similar definitions. Residual risk is the risk that remains after the risk treatment process.

**Security Requirements or Objectives:** Requirements that explain how each asset should be protected. All three models take into consideration the three main information security vectors, Confidentiality, Integrity and Availability.
5.3.3 Approaches

In this section we don’t fully explain the approach of each model. The information security risk assessment approach of each of the three selected models (OCTAVE, IRAM and IT-Grundschutz) is described in detail in Appendix B of this document. The purpose here is to compare, not describe, the referred approaches.

**OCTAVE**

*Description*

OCTAVE is mainly a self-directed information security risk evaluation method. It was designed to be used in cases where people from an organization manage and direct an information security risk assessment for their own organization. It takes a business rather than a technologic-centric view of security risks.

It identifies information-related assets (e.g., information and systems) that are important to the organization and focus risk analysis activities on those assets judged to be most critical to the organization (focus on the few critical assets, no more than 5). The OCTAVE’s approach focus primarily on information assets in the context of how they are used, where they are stored, transported, and processed, and how they are exposed to threats, vulnerabilities, and disruptions as a result.

OCTAVE can be performed in a workshop-style, collaborative setting and is supported with guidance, worksheets, and questionnaires, which are included in the model. However, OCTAVE is also well suited for use by individuals who want to perform risk assessment without extensive organisational involvement, expertise, or input. OCTAVE has adaptable measures, with the ability to be customized to organizational needs.

However, OCTAVE doesn’t provide a software tool or Excel tables to help the assessment process. It only provides the necessary paper documentation.

*Activities*

- **Phase 1: Build Asset-Based Threat Profiles** – This is an organizational evaluation. Staff members from the organization contribute their perspectives on what is important to the organization (information-related assets) and what is currently being done to protect those assets (elicitation workshops). The analysis team consolidates the information and selects the assets that are most important to the organization (critical assets). The team then describes security requirements for the critical assets and identifies threats to the critical assets, creating threat profiles.

- **Phase 2: Identify Infrastructure Vulnerabilities** – This is an evaluation of the information infrastructure. The analysis team identifies key information technology systems and components that are related to each critical asset. The team then examines the key components for weaknesses (technology vulnerabilities) that can lead to unauthorized action against critical assets (technological view of information security).
• Phase 3: Develop Security Strategy and Plans – During this part of the evaluation, the analysis team identifies risks to the organization’s critical assets and decides what to do about them. The team creates a protection strategy for the organization and mitigation plans to address the risks to the critical assets, based upon an analysis of the information gathered.

**Risk Calculation**

First OCTAVE defines the risk evaluation criteria for impact and probability, establishing a common understanding of the qualitative measures (high, medium, low). Then these values (high, medium, low) are assigned intuitively to each risk/impact by the assessment team based on the evaluation criteria.

The method uses an Expected Value Matrix (Loss = Impact/consequence x Probability).

**IRAM**

**Description**

IRAM is a workshop based information risk assessment model (typically conducted through face-to-face interviews with business and IT staff). IRAM is very well structured and rigorous model that focus its analysis on the organization's information systems and determines key information risks to those systems. IRAM's approach helps to determine the criticality and importance of information systems.

Despite having been designed to meet the demanding needs of information risk analysts in modern risk-oriented organisations, IRAM's approach proved to be very practical, flexible and above-all easy-to-use. It's a process oriented approach that provides a great deal of support documentation, forms, tables and tools.

**Activities**

- Phase 1 - Business Impact Assessment
- Phase 2 - Threat and Vulnerability Assessment
- Phase 3 - Control Selection

**Risk Calculation**

Tables, forms and formulas provided by the tools. The actual risk calculation formula is not publicly available. The tools calculate the risk ratings automatically.

**IT-Grundschutz**

**Description**

IT-Grundschutz provides a method for an organization to establish an Information Security Management System (ISMS). It comprises both generic IT security recommendations for establishing an applicable IT security process and detailed technical recommendations to achieve the necessary IT security level for a specific domain. So, the key approach in IT-
Grundschutz is to provide a framework for IT security management, offering information for commonly used IT components (modules). IT-Grundschutz modules include lists of relevant threats and required countermeasures in a relatively technical level. These elements can be expanded, complemented or adapted to the needs of an organisation.

Under the traditional risk analysis approach, first of all the threats are identified and assigned a likelihood of occurrence. The results of this analysis are then used to select the appropriate IT security measures, following which the residual risk can be assessed. For IT-Grundschutz this task has already been completed for each module, and the appropriate IT security measure, selected for a typical office environment. When applying IT-Grundschutz this task is reduced to a target versus actual comparison between the security measures recommended in the IT-Grundschutz Catalogues and those already implemented. Security measures that are found to be missing or inadequately implemented reveal security deficits that can be rectified by implementing the recommended security measures. Only where the protection requirements are significantly higher is it necessary to also perform a supplementary security analysis, weighing up the cost-effectiveness of implementing additional measures.

**Activities**

1. The information and business processes that are to be protected must be identified;
2. All the relevant threats pertaining to the information and business processes that are to be protected must be identified;
3. Vulnerabilities which the threats can use to take effect must be identified;
4. The possible damages due to a loss of confidentiality, integrity or availability must be identified and assessed;
5. The assumable repercussions on the business activities or fulfilment of tasks through IT security incidents must be analysed;
6. The risk of suffering damages due to IT security incidents must be assessed.

**Risk Calculation**

Traditional risk analysis approach, first of all the threats are identified and assigned a likelihood of occurrence. Repeat this task for each module.

**5.3.4 RESULTS AND OUTPUT**

**OCTAVE**

The information produced after undertaking the OCTAVE methodology is the following:

- Critical Assets
- Security Requirements for Critical Assets
- Threats to Critical Assets (including the consequences to an organization if a threat is realized)
• Risks to Critical Assets (the risks are a simple quantitative measure of the extent to which the organization is impacted by a threat. This relative risk score is derived by considering the extent to which the consequence of a risk impacts the organization against the relative importance of the various impact areas, and possibly the probability)

**IRAM**

IRAM methodology generates the following information and reports:

• Phase 1: Business impact rating and assessment summary forms;
• Phase 2: Threat and vulnerability assessment reports, detailed security requirements report;
• Phase 3: Control evaluation and selection reports;
• BIA Summary
• T&VA Summary
• CS Summary

IRAM’s approach helps to determine the criticality and importance of information systems.

**IT-Grundschutz**

• Relation between main IT applications, their protection requirements and the rationales behind the assignment of protection requirements categories.
• IT assets under review (business-critical information and IT applications) mapped with IT-Grundschutz modules.
• IT security/risk level of the organisation (obtained through a security check that verifies if relevant security measures are implemented or not)

Provides detailed technical recommendations

5.3.5 **Complexity**

**OCTAVE**

**Level of detail**

There are different OCTAVE methods based on OCTAVE Criteria. The methods are specific guidelines for implementation planning with a good level of detail but with no technical details.

**Inputs / Preparation needed**

Obtain management support and allocate appropriate organizational resources to the process.
Evaluation Scope (the extent of each evaluation must be defined);

Establish risk evaluation criteria according to the organization;

Identify the people that will participate in the workshops and interviews.

**Techniques**

Workshop-style, collaborative setting and is supported with guidance, worksheets, and questionnaires, which are included in the method.

**People involved**

In OCTAVE, an interdisciplinary team, called the analysis team, leads the evaluation. The analysis team should include people from both the business units and the IT department (because information security includes both business- and technology related issues), and from multiple organizational levels (senior management, middle management, and staff).

**Effort (time)**

Some days or weeks of training are sufficient.

**Skills needed**

Business and IT skills and knowledge.

**IRAM**

**Level of detail**

Analyses information risk at different levels of detail depending on factors such as management discretion, perceived criticality / importance or available time (e.g. high-level analysis through to detailed analysis).

**Inputs / Preparation needed**


**Techniques**

Workshop based (typically conducted with business and IT staff), Face-to-face interviews, One user guide for each phase, Process oriented, Business Impact Reference Table (BIRT), ISF threat information analysis.

**People involved**

Business and IT staff.

**Effort (time)**

3-5 days (for each system). 1-2 weeks per risk analysis.
**Skills needed**
Medium level of expertise needed (Risk Analysis practitioner, little technical knowledge needed).

**IT-Grundschutz**

**Level of detail**
Very detailed (more than 3000 pages). It comprises both generic IT security recommendations for establishing an applicable IT security process and detailed technical recommendations to achieve the necessary IT security level for a specific domain.

**Inputs / Preparation needed**
Specifying the area of application within which the method should apply. The information and business processes that are to be protected must be identified;

Ascertaining the prevailing conditions;

**Techniques**
Has a methodology that demonstrates how the threats listed in the IT-Grundschutz Catalogues [GS-KAT] can be used to carry out an analysis of IT risks.

**People involved**
Aimed at persons responsible for IT operations and IT security as well as IT security officers, experts, consultants and all interested parties entrusted with IT security management.

**Effort (time)**
Some weeks of training are sufficient.

**Skills needed**
Specialist (thorough knowledge and experience is required)

### 5.3.6 Supporting tools brief analysis

**OCTAVE**
No software tool but provides other type of support to the method (guidance, worksheets, forms, tables and questionnaires).

**IRAM**
Name: BIA Assistant
Description: The BIA Assistant provides the information risk analyst with an automated means of recording the results of a business impact assessment.

Name: T&VA Assistant

Description: The T&VA Assistant enables the information risk analyst to assess threats and vulnerabilities, determine the likelihood of information incidents and the key information risks in a system.

Name: CS Assistant

Description: The CS Assistant enables the information risk analyst to identify, evaluate and select controls to help mitigate the key information risks in a system.

Availability: Free for ISF Members

**IT-Grundschutz**

Name: GSTool (Trial for 30 days)

Site: [http://www.bsi.bund.de/english/gstool/](http://www.bsi.bund.de/english/gstool/)

Last Version: 2004

Compliance: IT Baseline Protection Manual (IT-Grundschutz)

Description: GSTool has been developed by Federal Office for Information Security (BSI) in order to support users of the IT Baseline Protection Manual.

Identification, Analysis, Evaluation: Assessment of Protection Requirements

Availability: Free, 30-day free trial

5.3.7 **COMPARISON SUMMARY**

According to the first criterion used in this comparison, concept definitions, the three models don’t diverge. Almost all key definitions are similar between models. Therefore, this criterion doesn’t help to differentiate the three models.

The second criterion, the information security risk assessment approach of each model, is much more complex than the first one and starts to differentiate the models from each other.

The simpler approach is, without a doubt, the one advocated by OCTAVE. It takes a business perspective and has almost no technical details. It’s suited for small teams and doesn’t require extensive organisational involvement, expertise, or input. It’s an intuitive and quick approach to assess risk that only produces the essential information. One of the benefits of this approach is its adaptable measures, which can be customized to organizational needs.

IRAM’s approach is more complex than OCTAVE’s, it’s more rigorous and detailed. The main focus are information systems, therefore this model is more technical than OCTAVE. Nonetheless, it’s still mainly business-centred, and its approach is workshop based. Information is gathered through face-to-face interviews and questionnaires. This process oriented approach
provides plenty of supporting tools and documentation, making the whole process easier to use and more practical. Similarly to OCTAVE, IRAM is also a very flexible model, easily adaptable to different organizations.

IT-Grundschutz is based in a more traditional risk analysis approach (identify threats, assign a likelihood of occurrence, and select the appropriate IT security measures), but in IT-Grundschutz this task has already been completed for each module. IT-Grundschutz modules include lists of relevant threats and required countermeasures in a relatively technical level. IT-Grundschutz’s approach is therefore reduced to a target versus actual comparison between the security measures recommended in the IT-Grundschutz Catalogues and those already implemented.

Despite all the simplifications describe above, IT-Grundschutz is a very complex model that helps an organisation to establish an Information Security Management System (ISMS). Note that in this work, only the part regarding the risk assessment was considered.

The third criterion used to compare the three models was the information resulting from applying each information security risk assessment model. As it was described before, OCTAVE is a simple and straightforward model and consequently doesn’t produce much information. The output of this model is just the essential information to understand what the critical assets are and what the main risks to those assets are. The two other models, IRAM and IT-Grundschutz, also provide this essential information, but in greater detail and also in different ways. Besides offering the same information that OCTAVE offers in greater detail, IRAM’s approach also helps to determine the criticality and importance of information systems. It produces detailed reports with threats, vulnerabilities and security requirements.

IT-Grundschutz, as it was explained before, can be characterized as a target versus actual comparison. Security measures that are found to be missing or inadequately implemented reveal security deficits (risks). IT-Grundschutz calculates the IT security level of the organisation and provides very detailed technical recommendations.

The fourth and last criterion, complexity, also differentiates models from each other. Under this criterion, models were characterized according to 5 different aspects. OCTAVE needs little preparation compared to the other two models. It can be completed with small teams of people and few technical skills, in a small period of time. IRAM needs just slight more preparation than OCTAVE but with a greater level of detail. It also needs a higher level of expertise. But despite more complex that OCTAVE, IRAM can also be completed rather quickly.

IT-Grundschutz is a very detailed model (it has more than 3000 pages of documentation). The amount of information needed to start the process is much higher than any of the other two models, but after this task is completed, the process becomes much more straightforward. This model also requires much more experience and knowledge than the other two, and will involve more resources and time.
5.4 Summary

This chapter demonstrated how the study was executed. It shows the various steps taken to come up with a sustained comparison. The first step was to select three information security risk assessment models from the initial group of 22 suitable models identified in the research phase. Different and relevant criteria were used in the two iterations of the selection process.

The next step was the detailed analysis and comparison of the three chosen models according to detailed criteria. The models were first compared by the assessment of similarities and differences between the models’ definition of general concepts. After this, the risk assessment approaches, the output and the complexity of each model are also compared.
6. Practical Application of the Models

In order to look at the three studied models in a different perspective, a practical experience was put into practice. This experience’s goal was to apply the three information security risk assessment models under study in a real organization. This practical application of the models complements and brings added value to the theoretical study previously initiated by helping to better compare and analyze each of the three models.

Note that this wasn’t a case study, where someone studies a particular case or phenomenon without actively participating in it. This was a practical experience in which I participated actively.

The experience took place in a public hospital (Centro Hospitalar de Lisboa Ocidental), during the months of April, May and June.

6.1 Work Plan

Scope

For this particular experience, and as the time and people resources were limited, only a part of the whole hospital was considered. The study only considers the hospital’s pediatric emergency.

All the three methods focus their analysis on information assets, and how these assets are used, transported, processed and stored. Given this fact, there were some key aspects that had to be considered during the experience. These aspects are:

- Information
- Processes
- Technology (infrastructure and applications)
- Physical environment
- People

Resources Needed (Documents, Systems, People)

Some resources and collaboration is essential or the success and credibility of the risk assessment. The risk assessment process must include people from the business units under review, as well as people from the IT department. This people should also be from different organizational levels (senior management, middle management, and staff). System profiles and access to the IT department is also required elements for the assessment.

Senior management is essential especially during the initial phase (defining and limiting the scope, establishing criteria, reviewing security policies and defining business impact types and values).
Main steps

• Define and limit the scope, establish risk measurement criteria, reviewing security policies and requirements.

• Identify information assets, analyze and create a profile for each asset.

• Threat and vulnerability analysis for each information asset.

• Identify and assess information security risks.

Techniques/Methods used

• Workshops, questionnaires and interviews (with members of the organization)

• Knowledge bases and catalogues (list and describe typical types of assets, threats, vulnerabilities, controls and security requirements)

6.2 Activities

1. Asset profiling

In this activity a profile for the target information assets was created and the information and business processes that are to be protected were identified.

1.1 Identification of critical information assets

Description: Identifying a collection of important information assets and choosing the critical ones from that collection.

Interlocutor: Senior Management.

Information to collect: List of all information assets important to the organization.

Method: Self-assessment, meetings.

Models:

   OCTAVE: Step 2 (Activities 1 and 2)

   IRAM: -

   IT-Grundschutz: Chapter 4

Output: Critical information assets that were the focus of the risk assessment. The critical assets selected for this experience were the hospital’s two main information systems: Sonho and HCIS (HealthCare Information System).

1.2 Gathering information about each information asset

Description: Gather key information about the information asset that is necessary to begin the structured risk assessment process. A profile is a representation of an information asset describing its unique features, qualities, characteristics, and value.
Identify and map an information asset to all of the containers in which it lives, thus defining the boundaries and unique circumstances that must be examined for risk. IT applications, IT systems, networks, rooms and buildings as well as responsible staff members, must all be ascertained for the examined information asset.

**Interlocutor:** Assets’ owners (and technical specialist).

**Information to collect:** Description of critical assets. Containers in which your information asset is stored, transported, or processed (technical containers, physical locations and people). The relationships and dependencies between the items to be protected must also be described.

**Method:** Interviews, workshops. The profile for each asset is captured on a single worksheet that forms the basis for the identification of threats and risks in subsequent steps.

**Models:**

- **OCTAVE:** Step 2 (Activities 3 to 8); Step 3
- **IRAM:** Phase 1 (Step 2)
- **IT-Grundschutz:** Section 4.1

**Output:** A profile worksheet of critical information for each asset (Appendix C).

### 2. Assessment of impacts and protection requirements

#### 2.1 Define impact/damage categories and ratings

**Description:** Choose impact areas/damage scenarios according to the organization; Define risk measurement/rating criteria for each impact area (Qualitative set of measures against which you will be able to evaluate risk’s effect on the organization’s mission and business objective). Define each business impact rating/category (5 different rating levels for OCTAVE and 3 for IRAM and IT-Grundschutz). Prioritize the impact areas from most important to least important.

**Interlocutor:** Senior Management

**Information to collect:** Impact areas and measurement criteria

**Method:** Meetings, workshops. The impact categories and ratings are captured on a single worksheet.

**Models:**

- **OCTAVE:** Step 1
- **IRAM:** Phase 1 (Business Impact Reference Table)
- **IT-Grundschutz:** Section 4.2.1 Step 1
**Output:** Business Impact Table with rating criteria and areas prioritized from most to least important. The identified impact areas are: Reputation and Public Image, Health, Productivity/Performance and Financial. (Appendix D)

### 2.2 Assessment of business impacts and protection requirements for each information asset

**Description:** Assess possible business impact that could arise from a loss of confidentiality, integrity and availability in each impact area (Give a rating to each impact area). Determine security requirements for each information asset based on the business impact assessed previously (security requirements are often derived from legislation and regulation).

**Interlocutor:** Key users/stakeholders of the information asset

**Information to collect:** The maximum level of damage to the organization that could arise in each of the damage categories. The extent of the possible damage ultimately determines the protection requirements of the IT asset (If it has high, medium or low protection requirements for confidentiality, integrity and availability)

**Method:** Meetings, workshops. The business impacts and protection requirements for each information asset are captured on several worksheets (three for each model, one for confidentiality, other for integrity and other for availability).

**Models:**

- OCTAVE: Step 2 (Activity 7 and 8)
- IRAM: Phase 1 (Step 3)
- IT-Grundschutz: Section 4.2 (repeat this step for each IT application)

**Output:** Impacts of an information security incident on each impact area (valid for the three models). Overall security classification for the three main security vectors (confidentiality, integrity, and availability).

**HCIS**

<table>
<thead>
<tr>
<th>Impact Types</th>
<th>Impact Types</th>
<th>Impact Ratings</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Confidentiality</td>
</tr>
<tr>
<td>1 Reputation</td>
<td></td>
<td>Very High</td>
</tr>
<tr>
<td>2 Health</td>
<td></td>
<td>Very High</td>
</tr>
<tr>
<td>3 Performance</td>
<td></td>
<td>Low</td>
</tr>
<tr>
<td>4 Financial</td>
<td></td>
<td>Very High</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Impact Types</th>
<th>Impact Ratings</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Very High</td>
</tr>
</tbody>
</table>

**SONHO**

<table>
<thead>
<tr>
<th>Impact Types</th>
<th>Impact Ratings</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Confidentiality</td>
</tr>
</tbody>
</table>

**Table 4 – HCIS Impact Ratings**
### 3. Threat assessment

#### 3.1 Identification of areas of concern and threat scenarios for each asset

**Description:** Brainstorming about possible conditions or situations that can threaten an organization’s information asset. These real-world scenarios are referred to as areas of concern and may represent threats and their corresponding undesirable outcomes.

Using the questions “What would happen if …?” realistic threat scenarios are developed from the areas of concern. Threat scenarios are a more detailed expression of the properties of a threat.

**Interlocutor:** information key users/stakeholders.

**Information to collect:** conditions or situations that can threaten the organization’s information assets.

**Method:** brainstorming, discussions (a set of questions is presented below for each of the damage scenarios mentioned, as a tool for examining the possible effects), self assessment, threat threes.

**Models:**
- **OCTAVE:** Step 4 and Step 5
- **IRAM:** Phase 2 (Step 1.1)
- **IT-Grundschutz:** Section 4.3

**Steps:**
- Map the asset under review with the modules in IT-Grundschutz
- Identify modules relevant to the identified information assets
- Use the catalogue of threats to identify threats for each asset
- Discuss, brainstorm about possible areas of concern and document them (with users of the information asset)
- Use the questionnaires and suggestions (provided by the models) to expand the areas of concern into damage/threat scenarios, therefore identifying specific threat types that need to be assessed in more detail.

---

<table>
<thead>
<tr>
<th></th>
<th>Reputation</th>
<th>High</th>
<th>Very High</th>
<th>Medium</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Health</td>
<td>Very low</td>
<td>Very High</td>
<td>High</td>
</tr>
<tr>
<td>3</td>
<td>Performance</td>
<td>Very Low</td>
<td>Very High</td>
<td>Very High</td>
</tr>
<tr>
<td>4</td>
<td>Financial</td>
<td>Low</td>
<td>Very High</td>
<td>Very High</td>
</tr>
</tbody>
</table>

**Table 5 – SONHO Impact Ratings**
After performing the steps described above, the result was a compiled list of threats applicable to the information assets under study and valid for the three models (each threat is described in Appendix E of this document):

**Deliberate External Attack**
1. Carrying out denial of service attacks
2. Hacking/Unauthorized use of IT systems
3. Cracking passwords / Poor or non-existent authentication
4. Spoofing user identities/Identity theft
5. Line tapping / Eavesdropping / Interception of data transmissions
6. Computer viruses, Trojan horses or any kind of malicious code
7. Carrying out social engineering

**Internal Misuse and Abuse**
8. Gaining unauthorised access to systems or networks
9. Abuse of administrator rights
10. Loss of database integrity/Consistency
11. Abuse of user rights / Misusing systems to cause disruption
12. Improper use of the IT system
13. Unauthorised disclosure of confidential information

**Theft**
14. Theft of identity information
15. Theft of computer equipment

**Service Interruption / Technical failure**
16. Failure of IT System
17. Malfunction of computer/network components
18. Damage to or Loss of computer facilities
19. Damage to or Loss of Communications Links/Services
20. Loss of power (failure of mains electricity or back-up power supply)

**Force Majeure**
- Damage to or loss of ancillary equipment (e.g., computer cooling equipment)
21. Natural Disasters, include earthquakes, fires and extreme weather
22. System overload

**Human Error**
23. User errors
24. IT/network staff errors

### 3.2 Threat assessment rating

**Description:** Determine overall threat ratings for the main threats that could affect the system.

**Interlocutor:** IT/Technical specialist

**Information to collect:** Previous security incidents (ISF threat information gathered from the ISF’s Security Status Survey)

**Method:** Self assessment.

**Models:**
**OCTAVE**: Step 5

**IRAM**: Phase 2 (Step 1.2)

**IT-Grundschutz**: -

**Output**: Threat rating values (Table 6 in the next section).

### 3.3 Vulnerability assessment

**Description**: Assess factors affecting vulnerability rating and determine overall vulnerability rating. Discover which standard security measures have been implemented adequately or inadequately using a target versus actual comparison.

**Interlocutor**: People responsible for each information asset (and its security).

**Information to collect**: Vulnerabilities applicable to the information asset; existing safeguards and recommended safeguards.

**Method**: Interviews/questionnaires, sampling checks.

**Models**:

**OCTAVE**: -

**IRAM**: Phase 2 (Step 2)

**IT-Grundschutz**: Section 4.4 (Basic Security Check)

**Steps**:

- Identify existing controls and safeguards. Inspect documentation which controls IT security-relevant processes to ascertain the degree of implementation of the security measures. (Use control analysis on IRAM to come up with the vulnerability rating)

- Performing the target versus actual comparison. Check which of the standard security safeguards that have been identified as necessary in the modeling process have already been implemented and where shortcomings still exist (IT-Grundschutz's Basic Security Check).

- Determining overall results for the threat and vulnerability assessment. Determine the likelihood ratings (based on both threat and vulnerability ratings).

**Output**: Vulnerability and likelihood ratings (Table 6); Basic Security Check results (Table 7). The overview of the existing security level is summarized in the following tables:

<table>
<thead>
<tr>
<th>Threat</th>
<th>Threat Rating</th>
<th>Vulnerability Rating</th>
<th>Likelihood Rating</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Low</td>
<td>Medium</td>
<td>Low</td>
</tr>
<tr>
<td>2</td>
<td>Very Low</td>
<td>Low</td>
<td>Very Low</td>
</tr>
<tr>
<td>3</td>
<td>Very Low</td>
<td>Low</td>
<td>Very Low</td>
</tr>
<tr>
<td>4</td>
<td>Very Low</td>
<td>Low</td>
<td>Very Low</td>
</tr>
<tr>
<td>5</td>
<td>Very Low</td>
<td>Very Low</td>
<td>Very Low</td>
</tr>
<tr>
<td>No.</td>
<td>Module name</td>
<td>Target objects</td>
<td>Degree of control implementation</td>
</tr>
<tr>
<td>-----</td>
<td>-----------------------------------------------</td>
<td>----------------</td>
<td>----------------------------------</td>
</tr>
<tr>
<td>6</td>
<td>Very Low</td>
<td>Low</td>
<td>Very Low</td>
</tr>
<tr>
<td>7</td>
<td>Very Low</td>
<td>Low</td>
<td>Very Low</td>
</tr>
<tr>
<td>8</td>
<td>Very Low</td>
<td>Low</td>
<td>Very Low</td>
</tr>
<tr>
<td>9</td>
<td>Very Low</td>
<td>Low</td>
<td>Very Low</td>
</tr>
<tr>
<td>10</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
</tr>
<tr>
<td>11</td>
<td>Very Low</td>
<td>Low</td>
<td>Very Low</td>
</tr>
<tr>
<td>12</td>
<td>Very Low</td>
<td>Low</td>
<td>Very Low</td>
</tr>
<tr>
<td>13</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
</tr>
<tr>
<td>14</td>
<td>Very Low</td>
<td>Low</td>
<td>Very Low</td>
</tr>
<tr>
<td>15</td>
<td>Low</td>
<td>Medium</td>
<td>Low</td>
</tr>
<tr>
<td>16</td>
<td>High</td>
<td>Low</td>
<td>Medium</td>
</tr>
<tr>
<td>17</td>
<td>Very High</td>
<td>Low</td>
<td>Medium</td>
</tr>
<tr>
<td>18</td>
<td>Very Low</td>
<td>Low</td>
<td>Very Low</td>
</tr>
<tr>
<td>19</td>
<td>High</td>
<td>Low</td>
<td>Medium</td>
</tr>
<tr>
<td>20</td>
<td>Medium</td>
<td>Low</td>
<td>Low</td>
</tr>
<tr>
<td>21</td>
<td>Very Low</td>
<td>Low</td>
<td>Very Low</td>
</tr>
<tr>
<td>22</td>
<td>Very Low</td>
<td>Low</td>
<td>Very Low</td>
</tr>
<tr>
<td>23</td>
<td>Medium</td>
<td>Low</td>
<td>Low</td>
</tr>
<tr>
<td>24</td>
<td>High</td>
<td>Low</td>
<td>Medium</td>
</tr>
<tr>
<td>25</td>
<td>Very High</td>
<td>Low</td>
<td>Medium</td>
</tr>
</tbody>
</table>

Table 6 – Security Level (IRAM and OCTAVE)

<table>
<thead>
<tr>
<th>No.</th>
<th>Module name</th>
<th>Target objects</th>
<th>Degree of control implementation</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>IT-Grundschutz</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Generic IT security aspects</td>
<td></td>
<td></td>
</tr>
<tr>
<td>B 1.1</td>
<td>Organisation</td>
<td>HCIS Sonho</td>
<td>Yes</td>
</tr>
<tr>
<td>B 1.2</td>
<td>Personnel</td>
<td>HCIS Sonho</td>
<td>No</td>
</tr>
<tr>
<td>B 1.3</td>
<td>Contingency planning</td>
<td>HCIS Sonho</td>
<td>No</td>
</tr>
<tr>
<td>B 1.4</td>
<td>Data Backup Policy</td>
<td>HCIS Sonho</td>
<td>Yes</td>
</tr>
<tr>
<td>B 1.7</td>
<td>Crypto-concept</td>
<td>HCIS Sonho</td>
<td>No</td>
</tr>
<tr>
<td>B 1.8</td>
<td>Handling of security incidents</td>
<td>HCIS Sonho</td>
<td>No</td>
</tr>
<tr>
<td>B 1.9</td>
<td>Hardware and software management</td>
<td>HCIS Sonho</td>
<td>Partially</td>
</tr>
<tr>
<td>B 1.13</td>
<td>IT security awareness and training</td>
<td>HCIS Sonho</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>Security of the infrastructure</td>
<td></td>
<td></td>
</tr>
<tr>
<td>B 2.1</td>
<td>Building</td>
<td>HSFX</td>
<td>Yes</td>
</tr>
<tr>
<td>B 2.3</td>
<td>Office</td>
<td>Instalações SSTI</td>
<td>Partially</td>
</tr>
<tr>
<td>B 2.4</td>
<td>Sever Room</td>
<td>Data Center HSFX</td>
<td>Yes</td>
</tr>
<tr>
<td>B 2.6</td>
<td>Technical Infrastructure Room</td>
<td>Data Center HSFX</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Security of IT Systems</td>
<td></td>
<td></td>
</tr>
<tr>
<td>B 3.101</td>
<td>General Server</td>
<td>HCIS Sonho</td>
<td>Partially</td>
</tr>
<tr>
<td>B 3.201</td>
<td>General Client</td>
<td>HCIS Sonho</td>
<td>Partially</td>
</tr>
<tr>
<td></td>
<td>Security in the network</td>
<td></td>
<td></td>
</tr>
<tr>
<td>B 4.1</td>
<td>Heterogeneous Networks</td>
<td>HCIS Sonho</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Security of applications</td>
<td></td>
<td></td>
</tr>
<tr>
<td>B 5.7</td>
<td>Databases</td>
<td>HCIS Sonho</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Table 7 – Security Level (IT-Grundschutz)
4. Risk Identification

4.1 Calculation of the risk score

Description: Compute a simple quantitative measure of the extent to which the organization is impacted by a threat (Information risk ratings).

Interlocutor: Someone who understands threat impacts on business and someone familiar with implemented security measures (IT manager, CIO).

Information to collect: Implemented and missing security controls.

Method: Compute the score for each impact area by multiplying the impact area rank by the impact value. Self assessment.

Models:

- OCTAVE: Step 6 and Step 7
- IRAM: Phase 2 (Step 3)
- IT-Grundschutz: Section 4.5 and 4.6

Steps:

- For each threat scenario documented, determine how your organization would be impacted if this threat scenario was realized. Using the impact categories and ratings from 2.1 as a guide, evaluate the consequence relative to each of the impact areas and record a value of High, Medium or Low. Compute the score for each impact area by multiplying the impact area rank by the impact value. The total score will be the relative risk score. Sort each of the identified risks by their risk scores. (OCTAVE)

- Combine values from threat and vulnerability assessment to give a clear indication of the main information risks in the system. (IRAM)

- Identify which assets have missing or only partially implemented IT-Grundschutz security measures from the results of the basic security check (Identifying and quantifying risks according to IT-Grundschutz’s methodology is a non trivial task due to the fact that this model doesn’t specifically identifies risks, but identifies vulnerable information security areas and recommends security controls. However, these vulnerable areas can also be viewed as information security risks)

Output: Information risk ratings and score;

<table>
<thead>
<tr>
<th>HCIS</th>
<th>Threat</th>
<th>Health (4)</th>
<th>Reputation (3)</th>
<th>Performance (2)</th>
<th>Finance (1)</th>
<th>Relative Risk Score (OCTAVE)</th>
<th>Risk Rating (IRAM)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Low</td>
<td>Medium</td>
<td>Medium</td>
<td>Low</td>
<td></td>
<td>15</td>
<td>Very Low</td>
</tr>
<tr>
<td>2</td>
<td>High</td>
<td>High</td>
<td>Medium</td>
<td>High</td>
<td></td>
<td>28</td>
<td>Medium</td>
</tr>
<tr>
<td></td>
<td>Threat</td>
<td>Health (4)</td>
<td>Reputation (3)</td>
<td>Performance (2)</td>
<td>Finance (1)</td>
<td>Relative Risk Score (OCTAVE)</td>
<td>Risk Rating (IRAM)</td>
</tr>
<tr>
<td>---</td>
<td>--------</td>
<td>------------</td>
<td>----------------</td>
<td>----------------</td>
<td>------------</td>
<td>-----------------------------</td>
<td>------------------</td>
</tr>
<tr>
<td>1</td>
<td>Low</td>
<td>Medium</td>
<td>Medium</td>
<td>Medium</td>
<td>16</td>
<td>Medium</td>
<td>Medium</td>
</tr>
<tr>
<td>2</td>
<td>Medium</td>
<td>High</td>
<td>Medium</td>
<td>High</td>
<td>24</td>
<td>Medium</td>
<td>Medium</td>
</tr>
<tr>
<td>3</td>
<td>Low</td>
<td>Medium</td>
<td>Low</td>
<td>Medium</td>
<td>14</td>
<td>Medium</td>
<td>Medium</td>
</tr>
<tr>
<td>4</td>
<td>Low</td>
<td>High</td>
<td>Medium</td>
<td>Medium</td>
<td>19</td>
<td>Very Low</td>
<td>Very Low</td>
</tr>
<tr>
<td>5</td>
<td>Low</td>
<td>Medium</td>
<td>Low</td>
<td>Low</td>
<td>13</td>
<td>Very Low</td>
<td>Very Low</td>
</tr>
<tr>
<td>6</td>
<td>Low</td>
<td>Medium</td>
<td>Medium</td>
<td>Medium</td>
<td>16</td>
<td>Medium</td>
<td>Medium</td>
</tr>
<tr>
<td>7</td>
<td>Medium</td>
<td>Low</td>
<td>Low</td>
<td>Medium</td>
<td>18</td>
<td>Very Low</td>
<td>Very Low</td>
</tr>
<tr>
<td>8</td>
<td>Low</td>
<td>Low</td>
<td>Medium</td>
<td>Medium</td>
<td>13</td>
<td>Very Low</td>
<td>Very Low</td>
</tr>
<tr>
<td>9</td>
<td>Low</td>
<td>Low</td>
<td>Medium</td>
<td>Medium</td>
<td>13</td>
<td>Medium</td>
<td>Medium</td>
</tr>
<tr>
<td>10</td>
<td>Medium</td>
<td>Medium</td>
<td>High</td>
<td>Medium</td>
<td>22</td>
<td>High</td>
<td>High</td>
</tr>
<tr>
<td>11</td>
<td>Low</td>
<td>Medium</td>
<td>High</td>
<td>Medium</td>
<td>18</td>
<td>Medium</td>
<td>Medium</td>
</tr>
<tr>
<td>12</td>
<td>Medium</td>
<td>Low</td>
<td>Medium</td>
<td>Medium</td>
<td>17</td>
<td>Medium</td>
<td>Medium</td>
</tr>
<tr>
<td>13</td>
<td>Low</td>
<td>Medium</td>
<td>Low</td>
<td>Low</td>
<td>13</td>
<td>Very Low</td>
<td>Very Low</td>
</tr>
<tr>
<td>14</td>
<td>Low</td>
<td>Medium</td>
<td>Low</td>
<td>Medium</td>
<td>11</td>
<td>Very Low</td>
<td>Very Low</td>
</tr>
<tr>
<td>15</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
<td>10</td>
<td>Medium</td>
<td>Medium</td>
</tr>
<tr>
<td>16</td>
<td>Low</td>
<td>Medium</td>
<td>High</td>
<td>Medium</td>
<td>26</td>
<td>Very High</td>
<td>Very High</td>
</tr>
<tr>
<td>17</td>
<td>Low</td>
<td>High</td>
<td>High</td>
<td>Medium</td>
<td>21</td>
<td>Very High</td>
<td>Very High</td>
</tr>
<tr>
<td>18</td>
<td>Medium</td>
<td>High</td>
<td>Medium</td>
<td>Medium</td>
<td>22</td>
<td>Medium</td>
<td>Medium</td>
</tr>
<tr>
<td>19</td>
<td>Low</td>
<td>Medium</td>
<td>Medium</td>
<td>Low</td>
<td>15</td>
<td>High</td>
<td>High</td>
</tr>
<tr>
<td>20</td>
<td>Low</td>
<td>Medium</td>
<td>High</td>
<td>Medium</td>
<td>18</td>
<td>Medium</td>
<td>Medium</td>
</tr>
<tr>
<td>21</td>
<td>Low</td>
<td>Low</td>
<td>Medium</td>
<td>Medium</td>
<td>13</td>
<td>Medium</td>
<td>Medium</td>
</tr>
<tr>
<td>22</td>
<td>Medium</td>
<td>Low</td>
<td>High</td>
<td>High</td>
<td>20</td>
<td>Medium</td>
<td>Medium</td>
</tr>
<tr>
<td>23</td>
<td>Low</td>
<td>Low</td>
<td>High</td>
<td>High</td>
<td>15</td>
<td>Medium</td>
<td>Medium</td>
</tr>
<tr>
<td>24</td>
<td>Low</td>
<td>Low</td>
<td>Medium</td>
<td>Medium</td>
<td>13</td>
<td>Very High</td>
<td>Very High</td>
</tr>
</tbody>
</table>
The next step would be to determine which risks require mitigation (starting from the most critical) and assign a mitigation approach for each information risk (Mitigate, defer, accept, transfer). However, this following step is out of the scope of this study and therefore the practical experience ended in this phase.

6.3 Final Results

This section presents the experience findings. The obtained data is digested and condensed, with important trends extracted for an overall perspective.

- Security requirements for each information asset (identical for the three models):
  
<table>
<thead>
<tr>
<th>HCIS</th>
<th>Confidentiality</th>
<th>Integrity</th>
<th>Availability</th>
</tr>
</thead>
<tbody>
<tr>
<td>Very High</td>
<td>High</td>
<td>Low</td>
<td></td>
</tr>
</tbody>
</table>

Table 9 – HCIS Security Requirements

<table>
<thead>
<tr>
<th>SONHO</th>
<th>Confidentiality</th>
<th>Integrity</th>
<th>Availability</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low</td>
<td>Very High</td>
<td>High</td>
<td></td>
</tr>
</tbody>
</table>

Table 10 – SONHO Security Requirements

- Threats and vulnerabilities applicable to the assets: (Table 6, 7)
- List of critical information security risks (prioritized):

According to OCTAVE, the most critical risks are:

<table>
<thead>
<tr>
<th>OCTAVE</th>
<th>HCIS</th>
<th>SONHO</th>
</tr>
</thead>
<tbody>
<tr>
<td>No.</td>
<td>Threat</td>
<td>Score</td>
</tr>
<tr>
<td>16</td>
<td>Failure of IT System</td>
<td>29</td>
</tr>
<tr>
<td>2</td>
<td>Hacking/Unauthorised use of IT systems</td>
<td>28</td>
</tr>
<tr>
<td>17</td>
<td>Malfunction of computer/network components</td>
<td>25</td>
</tr>
<tr>
<td>20</td>
<td>Loss of power</td>
<td>25</td>
</tr>
<tr>
<td>4</td>
<td>Spoofing user identities/identity theft</td>
<td>24</td>
</tr>
<tr>
<td>10</td>
<td>Loss of database integrity/consistency</td>
<td>22</td>
</tr>
<tr>
<td>22</td>
<td>Natural Disasters</td>
<td>22</td>
</tr>
</tbody>
</table>

Table 11 – Critical Risks according to OCTAVE

According to IRAM, the most critical risks are:

<table>
<thead>
<tr>
<th>IRAM</th>
<th>HCIS</th>
<th>SONHO</th>
</tr>
</thead>
<tbody>
<tr>
<td>No.</td>
<td>Threat</td>
<td>Score</td>
</tr>
<tr>
<td>16</td>
<td>Failure of IT System</td>
<td>Very</td>
</tr>
<tr>
<td></td>
<td></td>
<td>High</td>
</tr>
</tbody>
</table>
Table 12 - Critical Risks according to IRAM

According to IT-Grundschutz, the most critical risks/security concerns are

<table>
<thead>
<tr>
<th>No.</th>
<th>Module name</th>
<th>Assets</th>
</tr>
</thead>
<tbody>
<tr>
<td>B 1.2</td>
<td>Personnel</td>
<td>HCIS Sonho</td>
</tr>
<tr>
<td>B 1.3</td>
<td>Contingency planning</td>
<td>HCIS Sonho</td>
</tr>
<tr>
<td>B 1.7</td>
<td>Crypto-concept</td>
<td>HCIS Sonho</td>
</tr>
<tr>
<td>B 1.8</td>
<td>Handling of security incidents</td>
<td>HCIS Sonho</td>
</tr>
<tr>
<td>B 1.13</td>
<td>IT security awareness and training</td>
<td>HCIS Sonho</td>
</tr>
</tbody>
</table>

Table 13 - Critical Risks according to IT-Grundschutz

IT-Grundschutz identified three other potential risks/areas of concern:

- **Loss of personnel**
  - Illness, accident, death or a strike can result in an unforeseen loss of personnel resources. Due account should also be taken of the foreseeable staff shortages during vacation and in-service training. A loss of personnel resources could also mean a loss of specialist knowledge (medical or IT) and sensitive information, preventing duties being taken over by replacement staff.
  - Example: Due to prolonged illness, the network administrator was away from work. When the system crashed after two weeks, no one was able to resolve the problem. As a result the network was out of service for several days.

- **Lack of rules or insufficient knowledge of rules and procedures**
  - The importance of organisational rules and requirements for IT security objectives increases with both the scope of information processing and the protection requirements of the information to be processed.
  - Drawing up rules and regulations does not of itself guarantee the smooth flow of IT operations. All employees must be aware of the relevant regulations, especially those in charge. The damage which can result from inadequate knowledge of existing rules and procedures cannot be excused by saying: "I didn’t know that I was responsible for that," or "I didn’t know what to do."

- **Inappropriate handling of security incidents**
  - In practice, the possibility of a potentially extremely damaging security incident can never be eliminated, even where extensive security measures have been implemented. If appropriate action is not taken in response to a security incident, considerable damage or loss could occur or the situation could even develop into a catastrophe.
  - Example: Failure to take action when there is evidence that confidential data has been compromised could result in additional confidential information being leaked.
• Quantification and evaluation of the top priority risks:

<table>
<thead>
<tr>
<th>Information Risk Rating Summary</th>
<th>OCTAVE</th>
<th>IRAM</th>
<th>IT-Grundschutz</th>
<th>Global</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deliberate External Attack</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>HCIS</td>
<td>18</td>
<td>17</td>
<td>Medium</td>
<td>X</td>
</tr>
<tr>
<td>SONHO</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Internal Misuse and Abuse</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>HCIS</td>
<td>18</td>
<td>16</td>
<td>Medium</td>
<td>X</td>
</tr>
<tr>
<td>SONHO</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Theft</td>
<td>14</td>
<td>11</td>
<td>Low</td>
<td>-</td>
</tr>
<tr>
<td>Service Interruption / Technical failure</td>
<td>22</td>
<td>24</td>
<td>Medium</td>
<td>High</td>
</tr>
<tr>
<td>Force Majeure</td>
<td>17</td>
<td>16</td>
<td>Very Low</td>
<td>Medium</td>
</tr>
<tr>
<td>Human Error</td>
<td>19</td>
<td>15</td>
<td>High</td>
<td>Very High</td>
</tr>
</tbody>
</table>

Table 14 – Evaluation of the top priority risks

7. CONCLUSION

7.1 EVALUATION

This section is dedicated to evaluate the results of applying the three models to an organization (6.3) and comparing those results with previous conclusions obtained in the comparative study (5.3.7).

In this experience we considered two critical information assets (Sonho and HCIS). The objective was to apply the three models to better compare the approaches and final results. The best way to put this into practice would be to apply each model separately and independently. However, the people and time resources were very limited, and therefore all three models were implemented at the same time. This was possible due to the fact that most of the information required by one model is useful to another. This statement is supported by the fact that almost all key concept definitions are similar between the three models (5.3.2).

The first phase of this experience was to analyse what information and input each of the three models would need and then collect all that information. This task is the most time consuming of the whole process. Several difficulties came up during this task. Mostly because some of the information needed wasn’t available. The organization itself didn’t have all the information needed to perform a proper risk assessment. It wasn’t the purpose of this work to come up with that information. The purpose of the experience was to use the available information to assess information security risk in the organisation.

The practical experience proved right the conclusions taken from the theoretical study regarding the approach, output and complexity of the models. OCTAVE is unquestionably the more straightforward approach that needs little preparation and few technical skills. It is an easy to learn and easy to use model. IRAM’s approach is more detailed and complex than OCTAVE’s (needs some more preparation and expertise) but without losing flexibility and usability. IT-Grundschutz is based in a more traditional risk analysis approach and much more complex than the other two, although it has some simplifications that facilitate the application of the model. IT-Grundschutz is a very detailed model and needs a great amount of information to start the
process. This fact allied to the amount of experience and knowledge required to manage this method difficulted the task of applying this model in such a short period of time.

In my personal opinion, without regarding an organization’s specific needs, IRAM is the approach that better conciliates usability, complexity, flexibility and final results. OCTAVE, despite simple and quick, just produces the essential information with no great detail. On the other hand we have IT- Grundschutz that calculates the IT security level of the organisation and provides very detailed technical recommendations, but at a very high cost (time, expertise and resources).

The practical experience helped getting to the conclusion that IRAM’s approach helps to determine the criticality and importance of information systems and produces detailed reports with threats, vulnerabilities and security requirements in a relatively effortless process.

The application of the three models at the same time didn’t facilitate the comparison. However, the practical implementation of the three models helped to clarify what information is needed, how it’s used and processed and what is the resulting information. It’s much easier for the reader to understand the studied model if he has access to a real and concrete example. Through this example the reader can validate the conclusions obtained in earlier chapters, regarding the level of detail, process, results, and other aspects of each model.

Users had an extremely important role during this practical experience, much more important than the initial expectation. IT staff has a completely different perspective of how information is used. This experience proved that it’s vital to consider and analyse all perspectives.

After the experience we can also conclude that most of the criteria used along the study proved to be effective and a real factor of differentiation. It was appropriate for this specific model analysis and comparison.

### 7.2 Final Comments

Today, an IT disruption conclusion comment can paralyze a company’s ability to make its products, deliver its services, and connect with its customers, not to mention foul its reputation. Yet few companies have done a thorough job of identifying and tempering their vulnerabilities. Worrying about what might go wrong may not be as glamorous a job as speculating about the future, but it is a more essential job right now. Risk assessment is an essential practice to find out what might go wrong in an organisation, and also an unquestionably worthwhile subject to explore.

Throughout this study I tried to simplify risk assessment concepts and methods in order to make this task more straightforward and easier to approach. This document started by introducing risk management, the broader concept where risk assessment fits in, and explaining the factors driving the growing need to manage risk. After this introduction, the particular set of problems...
and difficulties related to information security risk assessment were exposed. The state-of-the-art in information security risk assessment was the next step to contextualize the reader, followed by the actual proposal. The proposal clarifies the study’s purpose and gives insight on how its objectives are going to be achieved.

The second part of the study describes in detail how the study was carried out, explaining the methods used to select, analyse and compare the studied models. This part of the study also describes the practical experience carried out in a real organization during the study. This experience provides a practical example of the application of the information security risk assessment models in a real organisation.

In sum, this study produced a comparative and critic analysis of three information security risk assessment models, as it was proposed. It explained the models’ approaches and clarified the advantages and disadvantages of each one of them. Hopefully the information produced will help to shed light on the information security risk assessment topic and assist organisations wanting to initiate a risk assessment process. The final results and conclusions of this comparative study represent a valuable and constructive contribution to knowledge.

Almost all subjects addressed by this work were new to me. It's a theme that isn't part of my degree’s curriculum. Therefore, I first had to study risk management and information security in order to learn the basics and assimilate concepts. It was a time consuming process due to the fact that this are very broad subjects I never have worked with. But it was definitely a worthy process that made more comfortable around these themes. I now understand much better risk management and information security and I feel ready to go on with this work and study in detail some information security risk assessment models.

7.3 Future Work

It is clear throughout this work that risk management and information security are both critical business issues in our days. Therefore, deep analysis and detailed studies on these subjects are crucial.

This study helped clarify the topic of information security risk assessment, but at the same time indirectly suggested other interesting further avenues. The information produced by this study can definitely be improved and complemented by future workers.

A considerable number of ideas that can lead to future work in this area were generated while I was working in this project. For example, a lot more models can still be studied in more depth so they can also be compared to the three models addressed in this study. Models can also be compared with different criteria so that overlaps, redundancies, inconsistencies, gaps, and conflicts among the studied models can be tracked and identified.

Models should be applied in different organizations and in a larger period of time so results from different contexts can be analysed and better evaluated. Testimonials of practical applications
could also be collected and compared. The results of having an information security risk assessment process implemented can also be compared to the theoretical benefits already presented in this work.

Other path that can be explored is the creation of a methodology or mechanism that explicitly indicates which model is best to a particular organization. A function that considers the organization’s specific needs and characteristics and that, based on those parameters, points towards the most compatible model.

8. References


7. IT Governance Institute, Board Briefing on IT Governance, 2nd Edition, USA (2003), www.itgi.org


10. MAR, Modelo de Avaliação de Riscos. Banco de Portugal, DSB (2007)


19. CobiT 4.1, IT Governance Institute, USA (2007)
TECHNICAL REPORT CMU/SEI-2007

34. Adrian Munteanu, A., Ioan A.: Information Security Risk Assessment: The Qualitative
   Solutions
   227

   University


37. Business Impact Analysis and Risk Assessment for Information Assets: General
   Information & Process Description. Georgia Institute of Technology, Department of Internal
   Auditing (2003)


APPENDIX A — IDENTIFIED INFORMATION SECURITY RISK ASSESSMENT MODELS

1. OCTAVE

General Information
Name: OCTAVE
Website: http://www.cert.org/octave/
Owner: Carnegie Mellon University, SEI (Software Engineering Institute)
Country: USA

Description
OCTAVE is an asset-driven evaluation approach. OCTAVE requires the analysis team to consider the relationships among critical assets, the threats to those assets, and vulnerabilities (both organizational and technological) that can expose assets to threats. It identifies information-related assets (e.g., information and systems) that are important to the organization and focus risk analysis activities on those assets judged to be most critical to the organization (focus on the few critical assets, no more than five).

OCTAVE is mainly a self-directed information security risk evaluation. This core concept of OCTAVE is defined as a situation where people from an organization manage and direct an information security risk evaluation for their organization.

There are different OCTAVE methods based on OCTAVE Criteria. OCTAVE, OCTAVE-S and OCTAVE Allegro.

Target Organizations
OCTAVE Method - large organizations
OCTAVE-S - small and medium organizations (manufacturing companies with 100 people or less)
OCTAVE Allegro – All organizations

Risk estimation method: Qualitative

2. MEHARI

General Information
Name: Mehari
Website: https://www.clusif.asso.fr/en/clusif/present/
Owner: CLUSIF - Club de la Sécurité de l'Information Français
Country: France

Description
It's a risk management model, with modular components and processes. The assessment module covers, apart from the information system, the overall organization, and site protection in general, as well as the work environment and legal and regulatory aspects.

Target Organizations: Big and medium sized enterprises.
Risk estimation method: Both qualitative and quantitative.

3. MAGERIT

General Information
Name: MAGERIT
Website: http://www.csi.map.es/csi/pg5m20.htm
Owner: Ministerio de Administraciones Publicas (Spanish Ministry for Public Administrations)
Country: Spain

Description
Magerit is an open methodology for Risk Analysis and Management offered as a framework and guide:
• To make those responsible for information systems aware of the existence of risks and of the need to treat them in time.
• To offer a systematic method for analyzing these risks.
• To help in describing and planning the appropriate measures for keeping the risks under control.
• Indirectly, to prepare the organization for evaluation, audit, certification or accreditation processes, as relevant in each case.

Target Organizations: Information and Communications organizations.
Risk estimation method: Both qualitative and quantitative.

4. IT-GRUNDSCHUTZ

General Information
Name: IT-Grundschutz
Website: http://www.bsi.de/english/gshb/
Owner: Federal Office for Information Security (BSI)
Country: Germany
Description:
IT-Grundschutz provides a method for an organization to establish an Information Security Management System (ISMS). It comprises both generic IT security recommendations for establishing an applicable IT security process and detailed technical recommendations to achieve the necessary IT security level for a specific domain.
It includes three BSI-standards for IT Security:
• 100-1 Information Security Management Systems (ISMS)
• 100-2 IT-Grundschutz Methodology (The IT-Grundschutz Methodology includes a qualitative method for risk assessment)
• 100-3 Risk Analysis Based on the IT-Grundschutz (demonstrates how the threats listed in the IT-Grundschutz Catalogues [GS-KAT] can be used to carry out a simplified analysis of IT risks. But is a complement to the methodology, it can't be performed separately. It's a supplementary security analysis)
And IT-Grundschutz catalogues:
• Modules
• Catalogues of threats
• Catalogues of safeguards

Target Organizations: All
Risk estimation method: Qualitative

5. EBIOS

General Information
Name: EBIOS
Website: http://www.ssi.gouv.fr/en/confidence/ebiospresentation.html
Owner: DCSSI (Direction Centrale de la Sécurité des Systèmes d'Information, Premier Ministre)
Country: France
Description:
EBIOS is a comprehensive set of guides (plus a free open source software tool) dedicated to Information System risk managers. EBIOS gives risk managers a consistent and high-level approach to risks. EBIOS formalises an approach for assessing and treating risks in the field of information systems security (ISS).
The method takes into account all technical entities (software, hardware, networks) and non-technical entities (organisation, human aspects, physical safety).
Target Organizations: All
Risk estimation method: Qualitative

6. IRAM

General Information
Name: IRAM
Website: https://www.securityforum.org/index.htm
Owner: Information Security Forum (ISF)
Country: International
Description:
IRAM is the ISF’s information risk analysis methodology. Structured and rigorous yet practical, flexible and above-all easy-to-use, IRAM has been developed to meet the demanding needs of information risk analysts in modern risk-oriented organisations. It helps to determine the criticality / importance of information systems by conducting a full risk analysis on those systems.
Target Organizations: All
Risk estimation method: Qualitative

7. SARA

General Information
Name: SARA
Website: https://www.securityforum.org/index.htm
Owner: Information Security Forum (ISF)
Country: International
Description:
SARA is a detailed methodology for analyzing information risk in critical information systems.
Target Organizations: All
Risk estimation method: Qualitative

8. SPRINT

General Information
Name: SPRINT
Website: https://www.securityforum.org/index.htm
Owner: Information Security Forum (ISF)
Country: International
Description:
SPRINT is a simple yet formal method for analysing the business risks associated with an information system, and for agreeing what safeguards or controls are necessary. SPRINT is a relatively quick and easy-to-use methodology for assessing business impact and for analyzing information risk in important but not critical information systems. Complements the SARA methodology.
Target Organizations: All
Risk estimation method: Qualitative

9. ISO 27005

General Information
Name: ISO 27005
Website: http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=42107
Owner: ISO (the International Organization for Standardization)
Country: International
Description:
This International Standard describes the requirements for information security risk management which can be used to assess risks, identify security requirements and supports the establishment and maintenance of an ISMS.
The standard doesn't specify, recommend or even name any specific method, although it does specify a structured, systematic and rigorous method of analyzing risks through to creating the risk treatment plan.
Target Organizations:
This International Standard is applicable to all types of organizations (e.g. commercial enterprises, government agencies, non-profit organizations), which intend to manage risks that could compromise the organization’s information security.
Risk estimation method: Qualitative
10. NIST SP800-30

General Information
Name: NIST SP800-30
Website: http://www.csrc.nist.gov
Owner: National Institute for Standards and Technology (NIST)
Country: USA
Description: This guide provides a foundation for the development of an effective risk management program, containing both the definitions and the practical guidance necessary for assessing and mitigating risks identified within IT systems.
Target Organizations: These guidelines are for use by Federal organizations which process sensitive information. This document may be used by non-governmental organizations on a voluntary basis. It is not subject to copyright.
Risk estimation method: Qualitative

11. CRAMM

General Information
Name: CRAMM
Website: http://www.cramm.com/capabilities/risk.htm
Owner: British CCTA (Central Communication and Telecommunication Agency)
Country: UK
Description: CRAMM is a risk analysis method developed by the British government organization CCTA. At present CRAMM is the UK government’s preferred risk analysis method, but CRAMM is also used in many countries outside the UK. CRAMM is especially appropriate for large organizations, like government bodies and industry.
Target Organizations: Government agencies, Large companies
Risk estimation method: Qualitative

12. MIGRA

General Information
Name: MIGRA (Metodologia Integrata per la Gestione del Rischio Aziendale)
Website: N/A
Owner: AMTEC/Elsag Datamat S.p.A.
Country: Italy
Description: MIGRA is a qualitative risk assessment and management methodology suitable to deal with both information and tangible assets risks. The methodology provides an analysis framework based on the classical vision of risk as a multidimensional entity depending on the answers to three questions: a) what could go wrong? b) how likely is it to go wrong? c) given that it happens, what are the consequences?
Target Organizations: Government, agencies and large companies
Risk estimation method: Qualitative

13. MAR

General Information
Name: MAR (Modelo de Avaliação de Risco)
Website: N/A
Owner: Banco de Portugal
Country: Portugal
Description: MAR is a tool to support the supervisor work, establishing objective and systematized criteria and procedures, in order to assess the magnitude of the risks underlying the business of an organization. It also assesses the quality and
robustness of the internal governance and also the adequacy of solvency and liquidity position and its management processes.

Target Organizations: Banks and financial companies
Risk estimation method: Qualitative

14. ISAMM

General Information
Name: ISAMM (Information Security Assessment & Monitoring Method)
Website: http://www.telindus.com
Owner: Telindus N.V.
Country: Belgium
Description:
ISAMM is an ISMS supporting risk management method, with supporting tools. It is a quantitative type of risk management methodology where the assessed risks are expressed, through their Annual Loss Expectancy (ALE), in monetary units. ALE being the annual expected loss or cost should a threat or a group of threats being materialised.
Annual Loss Expectancy (ALE) = [probability] x [average impact]
This forms the basis for the Return On Investment (ROI) based approach and the economical justification capabilities of ISAMM with respect to the risk treatment plan. ISAMM allows showing and simulating the reducing effect on the risk ALE for each improvement control and to compare this with its cost of implementation.
The latest evolution in the ISAMM methodology introduces an asset based approach which means it can be used to run risk assessments against an asset or a grouped set of assets.
An ISAMM risk assessment contains three main parts: scoping; assessment - compliance and threats; result – calculation and reporting.
Target Organizations: All
Risk estimation method: Quantitative

15. GAO/AIMD-00-33

General Information
Name: Information Security Risk Assessment – Practices of Leading Organizations
Website: N/A
Owner: Accounting and Information Management Division
Country: USA
Description:
This guide is intended to help federal managers implement an ongoing information security risk assessment process by providing examples, or case studies, of practical risk assessment procedures that have been successfully adopted.
Target Organizations: N/A
Risk estimation method: N/A

16. IT SYSTEM SECURITY ASSESSMENT

General Information
Name: IT System Security Assessment
Website: N/A
Owner: UK Department of Trade and Industry (DTI)
Country: UK
Description:
A guide produced by the UK Department of Trade and Industry (DTI), which describes the parameters that need to be considered in order to understand the risk to an organization's information assets handled by its IT systems.
Target Organizations: N/A
Risk estimation method: N/A
17. MG-2 and MG-3

General Information
Website: http://www.cse-cst.gc.ca/its-stl/publications/itsg-csti-eng.html
Owner: CSE (Communications Security Establishment)
Country: Canada
Description:
The document is primarily intended for use by risk analysts and security engineers in the performance of risk assessments and safeguard selections. It may also be of value to system and project managers as a means of understanding these two processes.
Target Organizations: N/A
Risk estimation method: N/A

18. Dutch A&K Analysis

General Information
Name: A&K Analysis
Website: N/A
Owner: Dutch ministry of internal affairs
Country: The Netherlands
Description:
The method ‘Afhankelijkheids- en kwetsbaarheidsanalyse’ (A&K analysis) was developed in draft by the Dutch public company RCC. The Dutch ministry of internal affairs completed the development in 1996 and published a handbook describing the method. The method has not been updated afterwards. Since 1994 the A&K analysis is the only preferred method for risk analysis for Dutch government bodies. Outside the Dutch government Dutch companies often use A&K analysis.
Target Organizations: All
Risk estimation method: N/A

19. Marion

General Information
Name: MARION: Méthodologie d'Analyse des Risques Informatiques et d'Optimisation par Niveau
Website: https://www.clusif.asso.fr/en/clusif/presen/
Owner: CLUSIF - Club de la Sécurité de l'Information Français
Country: France
Description:
The method MARION (Methodology of Analysis of Computer Risks Directed by Levels) is about a methodology of audit, which, as its name indicates it, allows estimating the level of IT security risks of a company through balanced questionnaires giving indicators under the shape of notes in various subjects concurrent in the security. The objective of the method is to obtain a vision of the company audited with regard to a level considered “correct”, and on the other hand with regard to companies having already answered the same questionnaire. The level of security is estimated according to 27 indicators distributed in 6 big subjects, each of them assigns a grade between 0 and 4. The level 3 is the level to be reached to assure a security considered as correct. At the conclusion of this analysis, a more detailed analysis of risk is realized to identify the risks (threats and vulnerabilities) that press on the company.
Target Organizations: Large companies
Risk estimation method: N/A


General Information
Name: Austrian IT Security Handbook
Website: http://www.cio.gv.at/securenetworks/sihb/
Owner: Austrian Federal Chancellery
Country: Austria
Description:
The Austrian IT Security Handbook consists of 2 parts. Part 1 gives a detailed description of the IT security management process, including development of security policies, risk analysis, design of security concepts, implementation of the security plan and follow-up activities. Part 2 is a collection of 230 baseline security measures. A tool supporting the implementation is available as a prototype.
The handbook is compliant with ISO/IEC IS 13335, the German IT-Grundschutz and partly with ISO/IEC IS 17799 also. It contains a generic description of Risk Analysis, but does not specify a special method.
Target Organizations: All
Risk estimation method: N/A

21. MICROSOFT’S SECURITY RISK MANAGEMENT GUIDE

General Information
Name: Microsoft's security risk management guide
Owner: Microsoft
Country: International
Description: This prescriptive guide helps customers of all types plan, build, and maintain a successful security risk management program. In a four phase process, the guide explains how to build an ongoing process to measure and drive security risks to an acceptable level. The Microsoft security risk management process offers a combination of various approaches including pure quantitative analysis, return on security investment (ROSI) analysis, qualitative analysis, and best practice approaches. It is important to note that this guide addresses a process and has no specific technology requirements.
Target Organizations: All
Risk estimation method: Qualitative

22. Risk IT

General Information
Name: Risk IT
Website: http://www.isaca.org/Template.cfm?Section=Risk_IT&Template=/TaggedPage/TaggedPageDisplay.cfm&TPLID=79&ContentID=48749
Owner: ISACA (Information Systems Audit and Control Association)
Country: International
Description: Provides the missing link between enterprise risk management (ERM) and IT risk management and control, fitting in the overall IT governance framework of ITGI, and building upon all existing risk related components within the current frameworks, i.e., COBIT and Val IT.
This IT enterprise risk management framework was designed to allow business managers to identify and assess IT-related business risks and manage them effectively.
Target Organizations: All
Risk estimation method: Qualitative
APPENDIX B – INFORMATION SECURITY RISK ASSESSMENT APPROACH OF EACH OF THE THREE MODELS

This appendix identifies and describes with more detail each model’s information security risk assessment approach.

OCTAVE

The OCTAVE method currently has three different approaches (OCTAVE, OCTAVE-S and OCTAVE Allegro). Since all approaches are based on the same framework, only one of them was considered for this study. The one chosen was OCTAVE Allegro, the more recent of the approaches.

This approach differs from previous OCTAVE approaches by focusing primarily on information assets in the context of how they are used, where they are stored, transported, and processed, and how they are exposed to threats, vulnerabilities, and disruptions as a result. Like previous methods, OCTAVE Allegro can be performed in a workshop-style, collaborative setting and is supported with guidance, worksheets, and questionnaires, which are included in the model. However, OCTAVE Allegro is also well suited for use by individuals who want to perform risk assessment without extensive organizational involvement, expertise, or input.

The OCTAVE Allegro approach consists of eight steps that are organized into four phases, as illustrated in Figure 1.
The four phases or activity areas are

- **Establish drivers**, where the organization develops risk measurement criteria that are consistent with organizational drivers.

- **Profile assets**, where the critical assets that are the focus of the risk assessment are identified and profiled. This profiling process establishes clear boundaries for the asset, identifies its security requirements, and identifies all of the locations where the asset is stored, transported, or processed (assets’ containers).

- **Identify threats**, where threats to the information assets—in the context of their containers—are identified and documented through a structured process.

- **Identify and mitigate risks**, where risks are identified and analyzed based on threat information, and mitigation strategies are developed to address those risks.

The outputs from each step in the process are captured on a series of worksheets which are then used as inputs to the next step in the process. The individual steps of the methodology are described in more detail below.

**Step 1 – Establish Risk Measurement Criteria (Worksheets 1 to 7)**

The first step in the OCTAVE Allegro process establishes the organizational drivers that will be used to evaluate the effects of a risk to an organization’s mission and business objectives (Activity 1). These drivers are reflected in a set of risk measurement criteria that is created and captured as part of this initial step. Risk measurement criteria are a set of qualitative measures against which the effects of a realized risk can be evaluated and form the foundation of an information asset risk assessment.

In addition to evaluating the extent of an impact in a specific area, an organization must recognize which impact areas are the most significant to its mission and business objectives. This prioritization of impact areas is also performed in this initial step (Activity 2).

The OCTAVE Allegro method provides a standard set of worksheet templates to create these criteria in several impact areas and then to prioritize them.

**Interlocutor:** Senior management (someone who understands the business as a whole)

**Information to collect:** Impact areas and measurement criteria for each area.

**Method:** Meetings.

**Output:** Impact areas prioritized from most to least important.

**Step 2 – Develop Information Asset Profile (Worksheet 8)**
The OCTAVE Allegro methodology focuses on the information assets of the organization and Step 2 begins the process of creating a profile for those assets.

The first two (2) activities involve identifying a collection of important information assets and choose the critical ones from that collection. In the following activities (3-8) you gather information about your information asset that is necessary to begin the structured risk assessment process.

The profile for each asset is captured on a single worksheet that forms the basis for the identification of threats and risks in subsequent steps. A profile is a representation of an information asset describing its unique features, qualities, characteristics, and value.

**Interlocutor:** Senior Management, information assets’ owners/administrators

**Information to collect:** List of all information assets important to the organization, description of critical assets and the security requirements for confidentiality, integrity and availability (often derived from legislation and regulation)

**Method:** Meetings, interviews, workshops.

**Output:** Profile of critical information assets,

---

**Step 3 – Identify Information Asset Containers (Worksheets 9a, 9b, 9c)**

In Step 3 of the OCTAVE Allegro method, all of the containers in which an asset is stored, transported, and processed, whether internal or external to the organisation, are identified. In this step the analysis team maps an information asset to all of the containers in which it lives, thus defining the boundaries and unique circumstances that must be examined for risk.

**Interlocutor:** Assets’ owners (IT staff?)

**Information to collect:** containers in which your information asset is stored, transported, or processed (technical containers, physical locations and people)

**Method:** worksheets, interviews

**Output:** Information Asset Containers

---

**Step 4 – Identify Areas of Concern (Worksheet 10)**

Step 4 begins the risk identification process by brainstorming about possible conditions or situations that can threaten an organization’s information asset. These real-world scenarios are referred to as areas of concern and may represent threats and their corresponding undesirable outcomes.

**Interlocutor:** information assets’ key users/stakeholders

**Information to collect:** risk information for each information asset

**Method:** brainstorming, discussions
Output: Areas of concern, part of the Information Asset Risk Worksheet

Step 5 – Identify Threat Scenarios (Worksheet 10)

In the first half of Step 5, the areas of concern captured in the previous step are expanded into threat scenarios that further detail the properties of a threat. But the collection of threats developed from these areas of concern does not necessarily provide a robust consideration of possible threats to an organization’s information asset. Thus, in the second half of Step 5, a broad range of additional threats is considered by examining threat scenarios.

A range of threat scenarios can be represented visually in a tree structure commonly referred to as a threat tree. Threat trees are brought from the OCTAVE method.

A series of threat scenario questionnaires have been developed and are provided to help with this task.

Interlocutor: information assets’ key users/stakeholders

Information to collect: scenarios that could affect your information asset

Method: threat trees, questionnaires

Output: Threat scenarios, part of the Information Asset Risk Worksheet

Step 6 – Identify Risks (Worksheet 10)

In Step 5 threats are identified, and in Step 6 the consequences to an organization if a threat is realized are captured, completing the risk picture. A threat can have multiple potential impacts on an organization. The activities involved in this step ensure that the various consequences of risk are captured.

\[
\text{Threat (condition)} + \text{Impact (consequence)} = \text{Risk} \\
\quad [\text{Steps 4 and 5}] + [\text{Step 6}] = \text{Risk}
\]

Interlocutor: someone who fully understands the business process

Information to collect: impact/consequences on the organization of each threat scenario.

Method: interview

Output: part of the Information Asset Risk Worksheet

Step 7 – Analyze Risks (Worksheet 10)

In Step 7 of this assessment, a simple quantitative measure of the extent to which the organization is impacted by a threat is computed. This relative risk score is derived by considering the extent to which the consequence of a risk impacts the organization against the relative importance of the various impact areas, and possibly the probability.
Interlocutor: -

**Information to collect:** (information from previous steps)

**Method:** Compute the score for each impact area by multiplying the impact area rank by the impact value.

**Output:** Impact value and relative risk score

---

**Step 8 – Select Mitigation Approach**

In Step 8, the final step of the OCTAVE Allegro process, organizations determine which of the risks they have identified require mitigation and develop a mitigation strategy for those risks.

**Interlocutor:** Management

**Information to collect:** (information from previous steps), implemented controls

**Method:** Meetings

**Output:** Mitigation strategy for the risks with the highest score

Note that this approach and its artifacts are intended to be used on a single information asset. Organizations that desire to assess more than one information asset will need to repeat the process (beginning with Step 2, Activity 3) for each information asset included in their risk assessment scope.
IRAM

IRAM, the ISF’s next generation information risk analysis approach, has three main components: Business Impact Assessment, Threat and Vulnerability Assessment, Control Selection.

**Phase 1 - Business Impact Assessment**

To assess possible business impact that could arise as a result of an incident that compromises information in a system and determine the business security requirements for protecting information in a system.
Step 1 – Define the Business Impact Reference Table

1.1 Modify, add or delete Business impact types

1.2 Modify, add or delete Business impact ratings

1.3 Freeze the BIRT

Step 2 – Completing the System profile form

Step 3 – Completing the BIR forms

3.1 Business Impact Rating – Confidentiality

3.2 Business Impact Rating – Integrity

3.3 Business Impact Rating - Availability

Step 4 – Completing the BIA Summary form

4.1 Confirm Business Impact Assessment Ratings

4.2 Determine Overall Classification

**Interlocutor**: Senior management, stakeholders of the information asset
**Information to collect:** business impacts; brief profile of the key business and technical characteristics of the system.

**Method:** Workshops, meetings

**Output:** Business impact rating and assessment summary forms and BIA Summary

**Phase 2 - Threat and Vulnerability Assessment**

To determine the threats and vulnerabilities that increase the likelihood of serious incidents occurring in a system.

**Step 1 – Assessing threats**

1.1 Determine threats applicable to the system

1.2 Assess factors affecting threat rating

**Step 2 – Assessing vulnerabilities**

2.1 Assess factors affecting vulnerability rating

**Step 3 – Determining overall results**

1. Determine likelihood ratings
2. Determine information risk ratings
3. Determine information risk profile and system risk classification
4. Review results of assessment
5. Agree next steps
3.1 Determine likelihood ratings

3.2 Determine information risk ratings

Step 4 – Generating reports

**Interlocutor:** information asset’s key users/stakeholders (technical specialist)

**Information to collect:** vulnerabilities threats applicable to the system

**Method:** workshops, discussions, brainstorming, self assessment

**Output:** Threat and vulnerability assessment reports, detailed security requirements report and T&VA Summary

**Phase 3 - Control Selection**

To evaluate and select controls to reduce the likelihood of serious incidents occurring.

**Interlocutor:** Management

**Information to collect:** main information risks applicable to the system; main controls available that can be used to help mitigate information risk in the system.

**Method:** workshop, meetings
**IT-Grundschutz**

The IT security process/approach suggested by IT-Grundschutz consists of the steps described below. However, only the step 2 of the process refers to the risk assessment part, and only that step will be fully studied.

1. **Initiating the IT Security Process:**

1.1. **Designing and Planning the IT Security Process**

1.1.1. **Determining the Environmental Conditions (Definition of IT security goals and business environment)**

- Appoint contact persons for all business processes and specialist applications
- Perform basic assessment on the value of information, business processes and specialist applications
- Determine environmental conditions

**Interlocutor:** relevant information owner or specialist responsible and the relevant person responsible for IT.

**Information to collect:** most important business processes and their dependence on IT

**Method:** short security meeting (brainstorming) for each business process

**Output:** Environmental conditions

1.1.2. **Formulate General IT Security Objectives**

- Estimate the importance of business processes, specialist tasks and information
- Set general IT security objectives
- Obtain the agreement of management

**Interlocutor:** Senior management

**Information to collect:** institution's fundamental objectives and the general environment, requirements for availability, integrity and confidentiality

**Method:**

**Output:** IT Security Objectives, protection values, IT security level

1.1.3. **Drawing up an Information Security Policy**

- Obtain request from the management to produce an IT security policy
- Stipulate scope
- Convene a group to develop the IT security policy
- Organise management approval of IT security policy
• Publish IT security policy
• Regularly check and if necessary update IT security policy

Note: Out of the Risk Assessment scope.

1.2. Setting Up an IT Security Organisation

• Establishment of an organisational structure to promote and implement the IT security process.

Note: Out of the Risk Assessment scope.

1.3. Provision of Necessary Resources for IT Security

• Consider appropriateness and cost-effectiveness throughout the IT security process
• Ensure a balance between organisational and technical IT security
• Request appropriate resources for IT operation, security management and monitoring IT security
• If necessary, fall back on external resources

Note: Out of the Risk Assessment scope.

1.4. Integrating All Employees in the IT Security Process

• Involve employees and the staff council or supervisory board in the planning and design of IT security measures and rules at an early stage
• Train all employees in the relevant aspects of IT security and regularly raise their awareness
• Explain the purpose of the IT security measures to all employees
• Stipulate the contact person for IT security questions and announce responsibilities
• Stipulate and announce reporting and escalation routes for IT security incidents
• Ensure that essential security measures are adhered to when an employee leaves or rotates jobs.

Note: Out of the Risk Assessment scope.
2. Creating/Producing an IT Security Concept: (Plan)

2.1. Defining the IT Assets (Chapter 4)

The IT assets to which the IT security concept applies must first be defined. "IT assets" refers to all the infrastructural, organisational, personnel and technical components which assist with the performance of tasks in a particular area in which information processing is applied.

**Interlocutor:** Senior management

**Information to collect:** list of IT assets

**Method:** meetings, self-assessment

**Output:** IT assets that will be the focus of the risk assessment

2.2. IT-Structure Analysis (Section 4.1)

Within the framework of the IT structure analysis, the relevant items to be protected, such as information, IT applications, IT systems, networks, rooms and buildings as well as responsible staff members, must be ascertained for the examined IT asset (i.e. area of application or business process).

During the IT structure analysis, the relationships and dependencies between the items to be protected must also be described. By recording these dependencies it is possible to identify the effects of IT security incidents on business activities so that an appropriate response can be provided.

**Example:** If "server XY" is affected by an IT security incident, it is necessary to find out very quickly which IT applications or business processes have been affected by this.
2.2.1. Documenting the IT Assets
2.2.2. Preparing a Network Plan
2.2.3. Collecting Information on the IT Systems
2.2.4. Collecting Information about the IT Applications and Related Information
2.2.5. Documenting the Rooms
2.2.6. Reducing Complexity by Identifying Groups of Similar Assets

**Interlocutor:** IT Staff

**Information to collect:** identify items to be protected, summary/profile of those items

**Method:** Interviews, Forms/worksheets

**Output:** business-critical information and IT applications

2.3. Defining/Assessment of protection requirements (Section 4.2)

The degree of protection required is determined for each of the values ascertained during the IT structure analysis.

**Example:** If the failure of an IT system can result in a great deal of damage, the value has correspondingly high protection requirements.

The protection requirements of the business processes must first be ascertained. Subsequently, one must examine what information needs to be processed where and with what IT systems in order to be able to accomplish the business processes. On the basis of this, the protection requirements of the IT applications that were registered during the IT structure analysis can then be determined. In the process, one must consider what type of information is being processed with these applications. In most institutions it is sufficient at this point to consider only very few information groups. Examples of this are customer data, publicly accessible information (e.g. addresses, opening times) or strategic data for the management.

The protection requirements of the IT applications are also conferred upon the IT systems that support the particular IT applications. The protection requirements of the IT rooms are derived from the protection requirements of the IT systems that are operated there.

**Example:** The business process involving the management of customer data is essential for maintaining business operations. This business process runs on server XY which consequently has high protection requirements. The room in which the server is housed therefore also has at least a high protection requirement.

2.3.1. Defining Protection Requirements for IT Applications
- Customise the assignment table
- Consider damage scenarios (Law, financial, safety,...)
- Document results

2.3.2. Defining Protection Requirements for IT Systems

The protection requirements of the individual IT systems are derived from the results of the previous activity.

2.3.3. Defining Protection Requirements for Communications Links

The results from activity 2.3.2 produce the protection requirements for the transfer routes.

2.3.4. Defining Protection Requirements for Rooms

The results from activity 2.3.2 produce the protection requirements for the rooms that are used for IT.

2.3.5. Interpreting the Results of the Protection Requirements Definitions

**Interlocutor:** Senior Management, key users/stakeholders

**Information to collect:** protection requirements of each asset, damage scenarios

**Method:** meetings, self-assessment

**Output:** table that shows the main IT applications, their protection requirements and the rationales behind the assignment of protection requirements categories.

2.4. Modelling (Section 4.3)

Modelling is a central step in the application of the IT-Grundschutz methodology. During modelling, the modules in the IT-Grundschutz Catalogues are assigned to the existing processes and components ("target objects"). The IT-Grundschutz Catalogues contain a precise description of how a real set of IT assets can be modelled as accurately as possible using the existing modules.

2.4.1. The IT-Grundschutz Catalogues

2.4.2. Modelling IT Assets

**Interlocutor:** -

**Information to collect:** (information from previous activities)

**Method:** self assessment

**Output:** assets under review mapped with the IT-Grundschutz modules

2.5. Basic IT Security Check (Section 4.4)

The basic security check is an organisational tool which provides a rapid overview of the existing IT security level.
If the IT-Grundschutz methodology is applied to an existing set of IT assets, it is necessary to check which of the standard security safeguards that have been identified as necessary in the modelling process have already been implemented and where shortcomings still exist. To this end, interviews are carried out with those responsible and spot checks are performed.

2.5.1. Organisational Preliminary Work

2.5.2. Performing the Target Versus Actual Comparison

2.5.3. Documentation of Results

Interlocutor: people responsible for each information asset (and its security)

Information to collect: implemented security safeguards

Method: interviews/questionnaires, sampling checks

Output: catalogue in which the implementation status of each of the relevant security measures is classified as "Unnecessary", "Yes", "Partially" or "No".

2.6. Supplementary Security Analysis

The standard IT-Grundschutz security measures normally provide appropriate, adequate protection. However, if the protection requirements are high or very high, it may be appropriate to check whether more stringent IT security measures are needed. Appropriate security measures for areas that have higher protection requirements should be selected by means of additional security analyses. A simple methodology for this is described in the BSI "Risk analysis based on IT-Grundschutz" document. This methodology identifies additional threats to target objects under review with high protection requirements.

3. Implementation planning and fulfilment of IT Security Measures (Do) (Section 4.6)

A satisfactory level of IT security can only be established if existing vulnerabilities are ascertained in the security analysis, the status quo is recorded in a security concept, the security measures that are necessary are identified and, above all, these security measures are also implemented systematically.

4. Maintenance, monitoring and improvement of the process (Check, Act)

5. IT-Grundschutz Certification (optional)

The IT-Grundschutz Methodology and the Catalogues are not only used for the IT security design but also increasingly as reference in terms of a security standard. Through IT-Grundschutz Certification or Qualification, an institution can document internally and externally that they have achieved the required level of IT-Grundschutz.
### APPENDIX C – PRACTICAL EXPERIENCE: INFORMATION ASSETS PROFILES

<table>
<thead>
<tr>
<th>Perfil do Activo de Informação</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>1. Geral</strong></td>
</tr>
<tr>
<td><strong>(1) Nome</strong></td>
</tr>
<tr>
<td><strong>(2) Estado</strong></td>
</tr>
<tr>
<td><strong>(3) Idade</strong></td>
</tr>
<tr>
<td><strong>(4) Owner</strong></td>
</tr>
<tr>
<td><strong>(5) Principal função</strong></td>
</tr>
<tr>
<td><strong>(6) Descrição</strong></td>
</tr>
<tr>
<td><strong>(7) Área/Processos de negócio</strong></td>
</tr>
<tr>
<td><strong>(8) Importância deste activo para o negócio</strong></td>
</tr>
<tr>
<td><strong>(9) Âmbito</strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>2. Informação Técnica (Technical Containers)</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>(1) Origem</strong></td>
</tr>
<tr>
<td><strong>(2) Infraestrutura de rede e interfaces de comunicação</strong></td>
</tr>
<tr>
<td><strong>(3) Plataforma/Hardware</strong></td>
</tr>
<tr>
<td><strong>(4) Numero de plataformas</strong></td>
</tr>
<tr>
<td><strong>(5) Gestão Operacional</strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Informação Física (Physical Containers)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Localização Hardware</strong></td>
</tr>
<tr>
<td><strong>Localizações da Informação física</strong></td>
</tr>
<tr>
<td>Que pessoas têm conhecimento da informação?</td>
</tr>
<tr>
<td>------------------------------------------</td>
</tr>
</tbody>
</table>

### Actividade

<table>
<thead>
<tr>
<th>Utilizadores</th>
<th>Administrativos</th>
</tr>
</thead>
<tbody>
<tr>
<td>Num de utilizadores com acesso ao activo</td>
<td>Internos 100 Terceiros -</td>
</tr>
<tr>
<td>Num de IT staff com acesso ao activo</td>
<td>Internos 10 Externos (ACSS)</td>
</tr>
<tr>
<td>Num de transacções processadas por dia</td>
<td>Normal - Peak -</td>
</tr>
<tr>
<td>Custo operacional anual estimado</td>
<td>Custos Internos - Custos Externos -</td>
</tr>
</tbody>
</table>

### Tendências (últimos 12 meses)

<table>
<thead>
<tr>
<th>Num Utilizadores</th>
<th>Diminui ____ Manteve <strong>X</strong> Aumentou ____</th>
</tr>
</thead>
<tbody>
<tr>
<td>Num Transacções</td>
<td>Diminui ____ Manteve <strong>X</strong> Aumentou ____</td>
</tr>
<tr>
<td>Operations</td>
<td>Diminui ____ Manteve <strong>X</strong> Aumentou ____</td>
</tr>
<tr>
<td>Management Activity</td>
<td>Diminui ____ Manteve <strong>X</strong> Aumentou ____</td>
</tr>
</tbody>
</table>

### Requisitos de Segurança (quais os que se aplicam a este activo?)

<table>
<thead>
<tr>
<th>Regulamentações ou requisitos de segurança especiais</th>
<th>-</th>
</tr>
</thead>
<tbody>
<tr>
<td>Requisito de segurança mais importante</td>
<td>Disponibilidade</td>
</tr>
</tbody>
</table>

### Perfil do Activo de Informação

#### 1. Geral

<table>
<thead>
<tr>
<th>(1) Nome</th>
<th>HCIS (HealthCare Information System)</th>
</tr>
</thead>
<tbody>
<tr>
<td>(2) Estado</td>
<td>Operacional</td>
</tr>
<tr>
<td>(3) Idade</td>
<td>1 ano</td>
</tr>
<tr>
<td>(4) Owner</td>
<td>SSTI (Serviço? de Sistemas e Tecnologias de Informação)</td>
</tr>
<tr>
<td>(5) Principal função</td>
<td>Processo clínico electrónico (parte de saúde)</td>
</tr>
<tr>
<td>(6) Descrição</td>
<td>-</td>
</tr>
<tr>
<td>(7) Área/Processos de negócio</td>
<td>Processo clínico do doente</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>---------------------------</td>
</tr>
<tr>
<td>(8) Importância deste activo para o negócio</td>
<td>Média/Alta</td>
</tr>
<tr>
<td>(9) Âmbito</td>
<td>Organização Inteira</td>
</tr>
</tbody>
</table>

**2. Informação Técnica (Technical Containers)**

<table>
<thead>
<tr>
<th>(1) Origem</th>
<th>HP</th>
</tr>
</thead>
<tbody>
<tr>
<td>(2) Infraestrutura de rede / interfaces de comunicação</td>
<td>Intranet / Cabo</td>
</tr>
<tr>
<td>(3) Plataforma/ Hardware</td>
<td>Cluster HP</td>
</tr>
<tr>
<td>(4) Numero de plataformas</td>
<td>Mainframes</td>
</tr>
<tr>
<td>(5) Gestão Operacional</td>
<td>Interna</td>
</tr>
</tbody>
</table>

**Informação Física (Physical Containers)**

<table>
<thead>
<tr>
<th>Localização Hardware</th>
<th>Data Center HSFX (Hospital São Francisco Xavier)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Localizações da Informação física</td>
<td>-</td>
</tr>
<tr>
<td>Que pessoas têm conhecimento da informação?</td>
<td>Todos os utilizadores do sistema</td>
</tr>
</tbody>
</table>

**Actividade**

<table>
<thead>
<tr>
<th>Utilizadores</th>
<th>Médicos, enfermeiros, administrativos e técnicos superiores de saúde</th>
</tr>
</thead>
<tbody>
<tr>
<td>Num de utilizadores com acesso ao activo</td>
<td>Internos</td>
</tr>
<tr>
<td>Num de IT staff com acesso ao activo</td>
<td>Internos</td>
</tr>
<tr>
<td>Num de transacções processadas por dia</td>
<td>Normal</td>
</tr>
<tr>
<td>Custo operacional anual estimado</td>
<td>Custos Internos</td>
</tr>
</tbody>
</table>

**Tendências (últimos 12 meses)**

<table>
<thead>
<tr>
<th>Num Utilizadores</th>
<th>Diminui ____</th>
<th>Manteve ____</th>
<th>Aumentou _X</th>
</tr>
</thead>
<tbody>
<tr>
<td>Num Transacções</td>
<td>Diminui ____</td>
<td>Manteve ____</td>
<td>Aumentou _X</td>
</tr>
<tr>
<td>Operations Management Activity</td>
<td>Diminui ____</td>
<td>Manteve ____</td>
<td>Aumentou _X</td>
</tr>
</tbody>
</table>

**Requisitos de Segurança (quais os que se aplicam a este activo?)**
APPENDIX D – PRACTICAL EXPERIENCE: BUSINESS IMPACT TABLE

<table>
<thead>
<tr>
<th>Type</th>
<th>Impact measurement criteria</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Very High</td>
</tr>
<tr>
<td>1 Health</td>
<td>Loss of customers’ or staff members’ lives.</td>
</tr>
<tr>
<td>2 Reputation and public image</td>
<td>Nation-wide reputation is severely damaged, causing potential patients to refuse doctor recommendations to the hospital.</td>
</tr>
<tr>
<td>3 Productivity/Performance</td>
<td>Impairment of the performance of duties would be assessed as unacceptable by all individuals concerned.</td>
</tr>
<tr>
<td>4 Financial</td>
<td>The organization may not be able to survive the financial loss.</td>
</tr>
</tbody>
</table>
APPENDIX E – PRACTICAL EXPERIENCE: THREAT'S DESCRIPTION

Deliberate External Attack

Which particular threats arise from deliberate attacks by outsiders? This refers to people that are not part of the institution itself and have no access to internal resources through special arrangements.

T1 – Carrying out denial of service attacks

Deliberately overloading systems and network devices or re-directing traffic
A denial-of-service attack is intended to prevent IT users from using functions or devices that are normally available to them. This attack often takes place in conjunction with distributed resources, with the attacker using these resources to such a degree that other users are prevented from carrying out their work.

T2 – Hacking/Unauthorised use of IT systems

Gaining unauthorised access to systems and networks
Without mechanisms for the identification and authentication of users, any control over unauthorised use of IT systems is virtually impossible. Even in IT systems that have identification and authentication functions in the form of user IDs and password verification, there is a risk of unauthorised use, if passwords and user IDs are obtained illicitly.

T3 – Cracking passwords / Poor or non existent authentication

Determining the plaintext version of an encrypted password
Authentication mechanisms can be used to authenticate users or components, or to determine the origin of data. If authentication mechanisms are missing or if the quality is too poor, there is a risk that unauthorised persons can gain access to IT systems or data, the causes of problems cannot be identified or the source of data cannot be determined. Passwords which are too simple can be discovered by systematic trial-and-error.

T4 – Spoofing user identities/identity theft

The unauthorised use of valid user identity information by a malicious third party to gain access to a system, typically as a result of "identity theft"

T5 - Line tapping / Eavesdropping / Interception of data transmissions

The unauthorised interception of information in transit
Due to the low risk of detection, tapping of lines is a potential threat to IT security which should not be overlooked.

T6 - Computer viruses, Trojan horses or any kind of malicious code

A computer virus is a program which inflicts damage. The most serious damage that can be caused as a result is the loss or corruption of data or programs. Such program functions can be triggered both intentionally and accidentally.
A Trojan horse, sometimes only called Trojan, is a program with a hidden, undocumented function or effect. The user therefore has no influence over the execution of this function, making its effect similar to that of a computer virus. However, unlike computer viruses, Trojan horses are not self-propagating. Any application program can serve as carrier for a Trojan horse.

T7 – Carrying out social engineering

The deliberate manipulation of staff to elicit information that can be used to undertake an attack (e.g. by providing user id and password details)
Social engineering is a collection of techniques used to gain unauthorised access to information or IT systems. Social engineering works by exploiting human characteristics such as helpfulness, trust, fear, and respect of authority. Staff can be manipulated to the point where their actions become illegal. A typical example of an attack using social engineering manipulation methods is making a telephone call to a member of staff.

Internal Misuse and Abuse

How can insiders affect the proper, secure operation of the target object under review through deliberate actions? Particular threats frequently arise as a result of existing access authorisation and insider knowledge.

T8 – Gaining unauthorised access to systems or networks

Deliberately gaining access to computer systems or networks to which a user is not authorised, by means of password theft or other covert action

T9 – Abuse of administrator rights
Abuse of Administrator rights occurs when superuser (root) privileges, acquired either rightfully or illicitly, are deliberately used to harm the system or its users.

Changing or adding software to produce unauthorised system behaviour or actions;

Changing or adding transactions, files or databases to produce unauthorised system behaviour or actions

Failure of a single component in an IT system can result in failure of the entire IT operation. Such failures are especially likely to occur where faults develop in components which are central to the IT system, e.g. LAN server or data transmission facilities. Failure of components of the technical infrastructure, for example air conditioning or power supply facilities, can also help induce an IT system failure.

A failure or malfunction of active network components impairs the availability of the entire network or sections of it.

Service Interruption / Technical failure

Which special security problems could occur to the target object under review due to technical failure?

T10 – Loss of database integrity/consistency

Changing or adding software to produce unauthorised system behaviour or actions

T11 - Abuse of user rights / Misusing systems to cause disruption

Misuse of user rights entails the deliberate exploitation of opportunities acquired either rightfully or illicitly to harm a system or its users.

T12 – Improper use of the IT system

Improper use of the IT system involving disregard or circumvention of IT safeguards jeopardises the security of the IT system. IT security incidents can arise if, for example, access rights are granted too widely, passwords are easy to guess, insufficient backup copies are made of data media, or terminals are not locked during temporary absence.

Similarly, data can be accidentally deleted or changed though incorrect use of IT systems or IT applications.

T13 – Unauthorised disclosure of confidential information

In the case of classified information (such as passwords, person-related data, certain business-related and official information, research & development data) there is an inherent danger of the confidentiality of this information being impaired inadvertently or intentionally. Classified information can be tapped from various sources, including - Internal storage media (hard disks) - External storage media (floppy disks, magnetic tapes) - Printed paper (hardcopies, files) and - data communications lines. There are various ways of actually obtaining the confidential information: - Reading out data - Copying data - Reading of data backups - Theft of data media for the purpose of evaluation - Monitoring data transmission lines - Viewing data on a screen.

T14 - Theft of Identity Information (Theft of Personally Identifiable information (eg credit card numbers, employment IDs, personal health details))

T15 - Theft of computer equipment (eg laptops, PDAs, mobile phones)

T17 - Malfunction of computer/network components (eg routers, hubs, switches)
T18 – Damage to or Loss of computer facilities (eg data centres, computer/network rooms, trading floors or process control systems)

T19 - Damage to or Loss of Communications Links/Services

In a building, a variety of networks exist for supply and disposal and thus serve as a basis for IT processes. Supply network failure, such as:
- electricity,
- telephone and
- air conditioning / ventilation
can all lead to immediate breakdown of the IT operation.

T20 – Loss of power (failure of mains electricity or back-up power supply)

However supposedly secure a power supply is, power failures are actually a regular occurrence. In most cases of power failure, the power is down for less than a second so that it can escape notice. However, IT operations can be disrupted even by failures lasting as little as 10 ms.

Force Majeure

Which potential force majeure events represent particular threats for the IT assets?

T21 – Damage to or loss of ancillary equipment (eg computer cooling equipment)

Every device has a defined temperature range within which its proper functioning is ensured. A rise or fall in the room temperature to a value outside that range could result in operational malfunctions or equipment failures.

T22 - Natural Disasters, include earthquakes, fires and extreme weather (eg flooding or freezing)

If a building is directly hit by lightning, damage will be caused by the dynamic energy of the lightning strike. This may include physical damage to the structure (roof and façade), damage caused by resultant fire, or overvoltage damage to electric devices.

Fires can be caused not only by careless handling of combustible material (e.g. Christmas candles, welding and soldering work etc.), but also by improper use of electric devices (e.g. unattended coffee machines, overloading of multiway socket outlets). Technical faults on electrical equipment can also cause fires.

An uncontrolled flow of water into buildings or rooms can damage supply facilities or IT components.

T23 – System overload (excessive system activity causing performance degradation or failure)

Human Error

Which human errors represent a particular threat to the IT operation?

T24 – User errors (Mistakes made by staff who use systems, eg mistakes in inputting data, incorrect operation of workstations, sending material to the wrong address)

- Loss of data confidentiality/integrity as a result of IT user error
  Inappropriate actions on the part of IT users can cause or enable a loss of data confidentiality or integrity. The extent and nature of the damage induced will depend on the sensitivity of the data involved.
  Example: Printouts containing patient-related data are accidentally left lying on the network printer.

- Negligent destruction of equipment or data
  Negligence, but also untrained handling, may lead to the destruction of equipment or data which can severely disrupt further operation of the IT system. The same results can be caused by the improper use of IT applications, leading to incorrect results or inadvertent modification or deletion of data. Careless use of a single deletion command can delete entire file structures.

- Hazards posed by cleaning staff or outside staff
  Hazards posed by visitors, cleaning staff and external staff range from improper handling of technical equipment and attempts to "play" on IT systems right through to the theft of IT components.

- Incorrect change of PC users
  In the case that several users work on one IT system at different times, an exchange of users is inevitable. If this is not adequately organised and administered, it may not fulfil security requirements.
  It may also happen that the previous user does not log off and the new user does not log on correctly as a result of negligence or convenience. This incorrect behaviour leads to a situation whereby the auditing of all user log-on and user log-off procedures and therefore also accountability will (partially) fail.

- Carelessness in handling information
  It is frequently observed that although a number of organisational or technical security procedures are in place, these are undermined through careless handling of the technology. A typical example of this is the almost proverbial sticker on the monitor which contains a list of all the access passwords.
  Even the use of well thought out authentication procedures will be of little avail if the users are careless in handling the necessary access-granting means. Whether the access-granting means used are passwords, PINs or authentication tokens, in practice they are often disclosed to other persons or not kept safe.

T25 – IT/network staff errors (Mistakes made by staff responsible for operating and maintaining computer or networks)

- Improper administration of the IT system
Improper IT system administration can jeopardise the security of the system if it results in disregard or circumvention of IT security safeguards.