Comparative Study of Information Security Risk Assessment Models

Filipe Macedo and Miguel Mira da Silva

Instituto Superior Técnico, Universidade Técnica de Lisboa,
Av. Rovisco Pais, 1049-001, Lisboa, Portugal

pipomacedo@gmail.com, mms@ist.utl.pt

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 case study was put into practice in a real organization.

Keywords: Risk Assessment Models, Information Security Risk, Information Security Risk Assessment, Risk Assessment Models Comparison

1 Introduction

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.

One risk that’s particularly hazardous in today’s global economy is Information Security Risk.

This work is a detailed study of information security risk assessment models. The result will be a comparative and critic analysis of those models, and their significant concepts.

1.1 Motivation

There are strong drivers for addressing risk management in a new perspective, especially for managing information security risk. Some of these factors are described below and summarized in Figure 1. Disregarding any of these factors can affect the organization’s income, reputation, customer confidence, public image and brand.
1.1.1 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.

1.1.2 Information and information systems dependence
Access to reliable information has become an indispensable component of conducting business, indeed, in a growing number of organizations, **information is the business** [1]. 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. 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 [5].

1.1.3 Change in organizations
There are certain factors that induce change in organizations. Factors like the pressure to innovate, the pressure to cut costs, the implementation of new technologies. 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.

1.1.4 Exposure and boundaries
Key drivers in the business environment, such as the globalization, 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.

1.1.5 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 [10]. For that reason, information security risk tends to underestimated or even disregarded. 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 [7].

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.

1.2 Problem
Why is information security risk assessment so hard to achieve effectively? Here are two main reasons:

1.2.1 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 [2]. 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 [8]. So it’s clear that our old-world risk assessment model cannot keep up with permanent change of information security risks. 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.
1.2.2 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 different risk assessment methods are emerging. 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. 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 [8]. 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.

2 Context

2.1 Introduction
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 [1]. The best example of those regulations is the USA Sarbanes-Oxley Act and the EU 8th directive.

2.2 Risk Categories
Organizations are exposed to various types of business risk. These risks can be categorized in a number of ways. In this work, the various risk categories are divided according to the purpose of the study. 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 [15].

- **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.
- **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, Physical Risk, Fraud Risk, Human Resources Risk and Outsourcing Risk.
- **Strategic Risk**: 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.
- **Reputation Risk**: the current and prospective impact on earnings and capital arising from negative publicity regarding an institution’s business practices [17].
- **Legal & Regulatory Compliance Risk**: compliance risk is usually considered as part of Operational risk but nowadays it's gaining strength of his own.
- **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.

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.

Organizations that do not perform proper risk management could see their ability to conduct business damaged or even destroyed. Organizations that manage risk effectively and efficiently are more likely to achieve their objectives and do so at lower overall cost [20].

2.3.1 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 1).

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) [21].

Risk Assessment

The main purpose of the risk assessment process is to identify risks and their potential impact. 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) [22]. Risk assessment is the part of the risk management process this work is focused in.

Risk Response

Once a risk has been assessed a business decision needs to be made on what, if any, action to take. The possible risk responses are to Accept, Avoid, Transfer or Reduce the risk.

Controls

The COSO [12] framework defines Control as the policies, procedures, practices, and organizational structures designed to provide reasonable assurance that the risk responses are effectively carried out. 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.

Residual Risk

The remaining risk after the implementation of new or enhanced controls is called Residual Risk (or retained risk).

Risk Reporting and Communication

The continuous or iterative process that an organization conducts to provide, share and obtain information regarding the management of risk.

Monitoring and Review

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.

2.4 Information Security Risk Assessment

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 [28]. 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.

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. Proper contextualized risk assessment is the best way to approach the organization’s need for information security. 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 [32]. It identifies threats, classifies assets and rates system vulnerabilities as it provides key information and guidelines to implement effective controls. Information risk assessment is divided in two activities: risk analysis and risk evaluation.

2.4.1 Information Security Risk Analysis
Risk Analysis (or Identification) involves the identification of several aspects:

- **Asset** is defined as anything having value to an organization [30].
- **Threat** is a potential cause of an unwanted incident, which may result in harm to a system or organization [30]. **Vulnerability** is a weakness of an asset or group of assets that can be exploited by one or more threats [30].
- **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.

2.4.2 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 [21]. 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.

3 Proposal
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. This will be achieved by studying and comparing in detail different models to assess information security. The study will identify what each model has to offer, what topics it addresses, and its 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 purpose of the work isn’t the conception of a groundbreaking model, the purpose is to bring the best solutions together, and organize them in a practical and usable way. All the studied models have a common goal of estimating the overall risk value. However, there are no methods that 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.

3.1 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 and identify existing information security risk assessment models;
- Select the models that will be subject of detailed comparison based on concise criteria;
- Thorough study of each information security risk assessment model, aiming to produce a comparative analysis;
- Model comparison based in the theoretical study made until this point;
- Case study in a real organization (implementing the studied models);
- Comparison of the theoretical study and case study results.
4 Existing 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. This chapter provides an overview of those methods, and a comparison that evaluates those different methodologies. The identified models are the following: OCTAVE, Mehari, MAGERIT, IT-Grundschutz, EBIOS, IRAM, SARA, SPRINT, ISO 27005, NIST SP800-30, CRAMM, MIGRA, MAR, ISAMM, GAO/AIMD-00-33, IT System Security Assessment, MG-2 and MG-3, Dutch A&K Analysis, MARION, Austrian IT Security Handbook, Microsoft’s Security Risk Management Guide and Risk IT. Note that this is not an exhaustive list of methods due to the limited time and resources.

4.1 First selection iteration

The first selection iteration pretends to exclude some of the models based on the following criteria:

- Is the model a method or just guidelines? Exclude if it isn’t a method.
- Does the model specifically identify Information Security Risks? Exclude if it doesn’t.
- Price and availability of documentation. Exclude if it is unavailable or too hard to obtain.
- Last review or update. Exclude if discontinued, obsolete or not recently updated/reviewed.

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>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>Available only to ISF Members</td>
<td>Up-to-date</td>
<td>Yes</td>
</tr>
<tr>
<td>SARA</td>
<td>Method</td>
<td>Yes</td>
<td>Discontinued</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>SPRINT</td>
<td>Method</td>
<td>Yes</td>
<td>Discontinued</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>ISO 27005</td>
<td>Guideline</td>
<td>Yes</td>
<td>Available</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>NIST SP800-30</td>
<td>Guideline</td>
<td>Yes</td>
<td>Free</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>CRAMM</td>
<td>Method</td>
<td>Yes</td>
<td>Expensive</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>MIGRA</td>
<td>Method</td>
<td>Yes</td>
<td>Expensive</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>MAR</td>
<td>Guideline</td>
<td>No</td>
<td>Free</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>ISAMM</td>
<td>Method</td>
<td>Yes</td>
<td>Unavailable</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>GAO/AIMD-00-33</td>
<td>Guideline</td>
<td>Yes</td>
<td>Free</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>IT System Security Assessment</td>
<td>Guideline</td>
<td>Yes</td>
<td>Unavailable</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>MG-2 and MG-3</td>
<td>Guideline</td>
<td>Yes</td>
<td>Unavailable</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>Security Risk Management Guide</td>
<td>Guideline</td>
<td>Yes</td>
<td>Unavailable</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>Dutch A&amp;K Analysis</td>
<td>Method</td>
<td>Yes</td>
<td>Unavailable</td>
<td>Obsolete</td>
<td></td>
</tr>
<tr>
<td>MARION</td>
<td>Method</td>
<td>Yes</td>
<td>Unavailable</td>
<td>Obsolete</td>
<td></td>
</tr>
<tr>
<td>Austrian IT Security Handbook</td>
<td>Guideline</td>
<td>Yes</td>
<td>Unavailable</td>
<td>Obsolete</td>
<td></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>
<tr>
<td>RiskIT</td>
<td>Framework</td>
<td>No</td>
<td>Available</td>
<td>N/A</td>
<td></td>
</tr>
</tbody>
</table>

Table 1 – First iteration criteria applied to each model

As a result of applying the 4 criteria, 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. 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.
4.2 Second selection iteration

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 the following:

- 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)
- Approach of the model (the risk assessment approach each model advocates (e.g. self-assessment, interviews, workshops)
- Tool (if the model provides supporting tools and how can we obtain them)
- Origin (in this study three possible sources for a model were considered: Academic, Governmental or Commercial)
- Geographical spread (countries in which the model is known to have been implemented)

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>
</tr>
</thead>
<tbody>
<tr>
<td>OCTAVE</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>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>The method suggests more than one technique to calculate risk</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>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>Self Assessment</td>
<td>Paid tool</td>
<td>Governmental</td>
<td>Used in many EU member states</td>
</tr>
<tr>
<td>Mehari</td>
<td>Bases its analysis on formulas, parameters, and a knowledge database; Audits are carried out to identify potential vulnerabilities;</td>
<td>Paid tool</td>
<td>Commercial</td>
<td>Used in many EU member states and non-EU member states</td>
</tr>
</tbody>
</table>

Table 2 – Criteria applied to each of the second iteration model

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, this 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.

4.3 Comparative Study

The study of the three final models aims to compare in greater detail the three different approaches. The new set of criteria is: Concept definition; Approach to information security risk assessment; Results and output; Complexity. The result of applying the criteria to the 3 models is described below.

According to the first criterion used in this comparison, concept definitions, the three models don’t diverge. 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.

4.4 Summary

This section showed 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.

5 Practical application of the models

The three information security risk assessment models under study were applied 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. The case study took place in a public hospital (Centro Hospitalar de Lisboa Ocidental), during the months of April, May and June.
5.1 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
   The critical assets selected were the hospital’s two main information systems: Sonho and HCIS (HealthCare Information System).
   1.2 Gathering key information about each information asset necessary to begin the risk assessment process

2. Assessment of impacts and protection requirements
   2.1 Define impact areas/damage scenarios according to the organization
   The output is a 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.
   2.2 Assessment of business impacts and protection requirements for each information asset on each impact area

3. Threat assessment
   3.1 Identification of threat scenarios for each asset
   3.2 Determine overall threat ratings
   3.3 Assess factors affecting vulnerability and determine overall vulnerability rating

4. Risk Identification
   4.1 Calculation of the risk score

5.2 Results

This section presents the final results of the experience summarized for an overall perspective.

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

Table 3 and 4 –Security Requirements

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></td>
<td>HCIS</td>
<td>SONHO</td>
<td>HCIS</td>
<td>SONHO</td>
</tr>
<tr>
<td>Deliberate External Attack</td>
<td>18</td>
<td>17</td>
<td>Medium</td>
<td>Low</td>
</tr>
<tr>
<td>Internal Misuse and Abuse</td>
<td>18</td>
<td>16</td>
<td>Medium</td>
<td>Medium</td>
</tr>
<tr>
<td>Theft</td>
<td>14</td>
<td>11</td>
<td>Low</td>
<td>Low</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>

6 Conclusion

6.1 Evaluation

In the practical 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 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.

The practical experience proved right most of the conclusions taken from the theoretical study regarding the approach, output and complexity of the models.
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.

6.2 Final Comments

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 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.
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.

6.3 Future Work

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.
7 References

10. Managing Information Technology Risk – A Global Survey for the Financial Services Industry, Ernst & Young
11. IT Governance Institute, Board Briefing on IT Governance, 2nd Edition, USA (2003), www.itgi.org
17. Fombrun, Foss: Developing a Reputation Quotient, 2000
18. Federation of European Risk Management Associations (FERMA), http://www.ferma.eu/
23. CobiT 4.1, IT Governance Institute, USA (2007)