Evaluating Information Systems Security using a Multicriteria Decision Analysis approach

Marcelo Silva
Técnico Lisboa
marcelotsilva@ist.utl.pt

Abstract. *In the last decade, organizations are increasingly becoming dependent on Information Systems (IS) which brings a corresponding increase of the security abuses on IS. Many security methodologies were created to evaluate the security level in organizations but often those methodologies are very generic and can't manage the real security concerns. Currently, organizations before acquiring new IS need to evaluate its security to guarantee that is according to the organization's internal policies, but the existing methodologies don't permit to decision maker's making an adapted decision for their organization. To reduce this problem, we propose the definition of a set of security evaluation criteria that will help decision maker's to make the decision for one specific IS, using Multiple Criteria Decision Analysis (MCDA). We'll use Design Science Research (DSRM) to guide our work and to evaluate the results we are going to use interviews, feedback from the scientific community, Moody and Shanks Quality Framework, and Östrele principles.*

Keywords: *Security, Information Systems, Information Systems Security, Cloud Computing security, Measurement Criteria, Multiple Criteria Decision Analysis.*

1. Introduction

In the last decades, the entire world has become increasingly computerized. Today most of the businesses can't work without technology and Information Systems, and some of them are totally based on these technologies. According to *Moore's Law* and to the Internet development this situation is growing fast and because of this, the technological problems are no longer a problem. When someone wants to build a system all depends on the effort to spend money and time to build it. This creates a major problem – the security of the Information Systems [1].

For many reasons organizations are adopting Cloud solutions to help in their business processes. Nowadays, ensure IS security in organizations is a daily concern [2] and therefore decide which IS brings more security guarantees, when the organization need to acquire a new IS, is a difficult task due to multiple existing criteria to be taken into account and so little time to decide [3].

To answer this problem there are best practices, standards and frameworks (ISO, COBIT, etc), but the effort required in terms of time and money to implement these controls is big, apart from the problems related to the fact that these methods are very generic [4]. Also the fact that these methods do not take into account the environment of each specific organization is a problem, because the solutions that are presented by these methods are based on many assumptions.

Therefore, the problem we address in this paper is that do not exist a method to compare the security of two equivalent Information Systems with different deployments – in house vs Cloud.

Take into account the defined problem, our proposal is one methodology that help organizations to make the decision between two equivalent IS in terms of security concerns but taking into account the specificity of each organization, the decision maker experience, organizations environment, etc.. This methodology is based on a Multiple Criteria Decision Analysis (MCDA) approach – MACBETH [5]. This method has three steps, one of them the creation of a set of security criteria to evaluate the security of two alternatives.

This paper describes the building process of the proposed multicriteria evaluation model that was demonstrated in a Portuguese City Council that wanted to migrate their mail software to the Cloud but did not know how to evaluate the security of the options, including their actual solution.

We chose this type of organization due the importance to the country and for all population related. In terms of security, are interesting case studies because typically the security subject is not addressed, due to the existent contingency plans. The IS chosen is the mail due to the high importance to all organizations, and because it is a bottleneck, even it is not considered in most cases.

The alternatives evaluated and compared were Microsoft Office 365 and the in house of the City Council. At the end of the process we obtained an overall value score for each option, which depicted their overall attractiveness for the City Council.

In order to evaluate our proposal, we used interviews to practitioners and clients, the decision maker feedback, the Moody and Shanks Framework [6] and the four Österle et al. principles [7]. After the evaluation we concluded the proposed method is suitable for evaluating the security of Information Systems.

This research was conducted by using Design Science Research Methodology (DSRM) that aims at creating a commonly accepted framework for research in Information Systems as well as creating and evaluating

artifacts to solve relevant organization problems [8]. The steps of DSRM that are used to organize the paper are: problem identification and motivation; objectives of a solution definition; design and development; demonstration; evaluation; and communication [8].

2. Problem

This section corresponds to the problem identification and motivation step of DSRM, which defines a specific research problem and justifies the value of the solution.

Nowadays, organizations are becoming dependent on Information Systems to improve business operations, facilitate decision-making and implement new business strategies [9]. Many organizations have their Information on web due to the growth of the internet in the past years, which makes interactions with clients faster; however brings consequently a set of new security concerns [2]**.**

These concerns are gaining more importance due to the fact that all organizations want to keep their information secure and protected to hacker's attacks. When an organization need to acquire a new Information System need guarantees that Information will remain secure in the new system. The problem is in the fact that do not exist a clear and direct way to evaluate the security of an IS, to compare all the existing alternatives.

Currently, the IS suppliers are creating and moving their products to the Cloud, due to the internet growth and to the new capabilities and advantages discussed [10]. To evaluate the security aspects were over time proposed many methods, where security checklists and standards are widely used [4]. But these methods have many associated problems, for example: the fact that do not pay attention to the specificities of each organization.

The challenges and problems presented above make the decision for a specific IS, taking into account security aspects, a difficult task. Then we define our research problem as: how to compare the security of two equivalent Information Systems with different deployments – in house vs Cloud?

Our main motivation to solve this problem is related to the fact that, increasingly, organizations are searching new IS solutions for their business that allow them to save resources and improve security at the same time they are technologically updated. So, our proposal brings concrete benefits to decision-makers, to help them making reasonable and appropriate choices.

3. Related Work

This section covers half the step of the definition of the objectives of a solution of DSRM, in which we will infer the goals of a solution from the problem definition and related work. We will divide this section in two sub-sections: first we will give an overview about Information Systems Security, including Cloud Computing Security (Section 3.1); after that, we will describe the models to evaluate security found in literature (Section 3.2).

3.1 Information Systems Security

Nowadays organizations are trusting on IS to improve business operations. The increase of organizational dependence on IS has led to a correspondent increase of the impact of the security abuses against IS [9]. Even if this question should be an important aspect to manage, due to its criticality, the leaders in organizations give little importance and attention to IS security, comparatively to other problems [9].

One survey done in 2010 by the Computer Security Institute, where participated 349 security practitioners, found that 45,6% of the interviewees that experienced a security incident in the last year, were subject to at least one well-defined attack [11].

There are many plausible reasons that explain the poor management of the security problems of IS [9]:

- First, the poor investment in the security of IS, because the leaders think that the risk of security abuses is low.
- Second, the leaders are skeptics about the effectiveness of the security in IS, due to the difficulty of evaluate the benefits of implementing.
- Third, the leaders may not have the knowledge about the existing mechanisms to reduce the security abuses in IS.

It's important to demonstrate to the leaders that these are important questions, showing the benefits of the implementation of security in IS, indicating them which are the security measures that are effective to their organizations [9].

When it comes to security in SI, the size of the organizations have a big influence, so the bigger spend more time and money on security and audits than smaller ones. The large organizations have proportionally more workers in areas of security than smaller ones [9]. But the general lack of awareness of these issues amongst the leaders in organizations, suggests that all organizations should make better management of issues of IS security [9].

3.1.1 Cloud Computing Security

Nowadays, when the optimization of costs and economic crisis are imminent concerns, the Cloud computing can be seen as an effective approach when it comes to cost and technological support for business. However, concerns about data privacy and security are seen as critical issues and even as barriers to the adoption of Cloud computing services [12].

The Cloud computing is composed on three service models: Infrastructure-as-a-Service, Platforms-as-a-Service and Sofware-as-a-Service; four models of implementation: Public Cloud, Community Cloud, Private Cloud and Hybrid Cloud; and their key features are: On-demand self-service, broad network access, resource pooling, rapid elasticity and measured service, proposed definitions in [12].

In addition to these advantages, Cloud computing is creating new risks and threats related mainly with the one critical factor - the new visibility. The risks to the assets transferred to the Cloud, described in [12] are:

- **Unavailability**—The asset is unavailable and cannot be used or accessed by the enterprise. The cause can be accidental (failure of the infrastructure), intentional (distributed denial-of-service attacks) or legal (subpoena of database holding all data in a case of multitenancy architecture where one client's data are subject to legal investigation).
- **Loss**—The asset is lost or destroyed. The cause can be accidental (natural disaster, wrong manipulation, etc.) or intentional (deliberate destruction of data).
- **Theft**—The asset has been intentionally stolen and is now in possession of another individual/enterprise. Theft is a deliberate action that can involve data loss.
- **Disclosure**—The asset has been released to unauthorized staff/enterprises/ organizations or to the public. Disclosure can be accidental or deliberate. This also includes the undesired, but legal, access to data due to different regulations across international borders.

3.2 Evaluating Security Models

In this sub-section we are going to describe the main existing methodologies and models found in literature that try to assess the security of IS.

Management Standards of Information Security

The methods that are widely used globally in organizations are security checklists and management security standards, which are supported by a large number of academic articles written by security practitioners [4]. Baskerville in 1993, and Dhillon and Backhouse, 2001, have a different opinion about this type of methods, criticizing the checklists for not paying sufficient attention to the fact that security requirements differ between organizations and also do not take into account the nature and environment of organizations [4].

ISO 27001 is a standard created by security practitioners from around the world, focused on security of information. Its goal is to provide a methodology for implementing information security in an organization. This methodology is holistic because it aggregates various topics - telecommunications, application security, physical protection, human resources, business continuity, etc. [13]. This methodology can be applied to all types of organization in order to analyze the state of information security and is independent of suppliers as it is focuses on the processes and procedures which are then transported to the reality of each organization to different ways, with different specificities of each technological and organizational environment [13].

However, according to [4], there are four assumptions usually made in the standards: "is from ought" naive inductionism, irrationalist research process and the inference problem.

Integrated Solution for Information Security Framework (I-SolFramework)

I-SolFramework aims to help stakeholders on assess the level of compliance of your organization with the ISO 27001. This framework is organized on six layers of components: organization, stakeholder, tools & technology, policy, culture and knowledge [3]. This proposal represents a significant contribution to the organizations understand the controls of ISO 27001, its evaluation problems, as well as the time that is usually necessary in order to accomplish this, 12 to 24 months [3].

This approach has the same problem noted above - the only use of the Standards. The fact that stakeholders evaluate parameters based only on ISO 27001 makes this approach very limited; they do not have the specificities of their organization in mind.

Automated Risk and Utility Management (AURUM)

AURUM is a methodology for managing information security risks, including objective measures of risk, reducing the risk and cost of protection [14]. This proposal is based on ontologies and takes into account the overall picture of the organization. Was designed to minimize the necessary interaction between the user and the

system and to provide decision-makers an intuitive solution that can be used without a thorough knowledge of information security. This approach consists of five steps [14] Inventory of the organization, Characterization System, Threat and Vulnerability Assessment, Risk Considerations and Control Assessment and Implementation.
In short, it is an approach that takes into account the organization's environment and its specificities. Makes a thorough risk analysis of each asset, graphically showing the likelihood of a threat exploiting a specific vulnerability and also shows possible solutions to avoid that threat, based on controls of the main standards and best practices.

4. Multicriteria Decision Analysis

A decision problem involves usually take into account multiple criteria, often contradictory. According to [15], is "a set of formal approaches that seek to take into account multiple criteria to assist individuals or groups to make decisions that matter". Then, we will describe some of the most commonly used methodologies MCDA. We suggest the reading of - [16] - where are described in detail all the methodologies related to this topic.

Outranking Methods

Outranking methods are applied directly to partial preference functions, which are de- fined for each criterion. These preference functions may corresponds to natural attributes on a cardinal scale, or may be constructed in some way, as ordinal scales, and do not need to satisfy all of the properties of value functions, only the ordinal preferential independence would still necessary. In outranking methods, for two alternatives *a* and *b*, where $zi(a) \geq zi(b)$ for all criteria *i*, we can say that *a* outranks alternative *b* if there is sufficient evidence to justify a conclusion that *a* is least as good as *b*, taking all criteria into account [15].

AHP

AHP (Analytical Hierarchy Process) is a method based on evaluating alternatives in terms of an additive preference function. The initial steps in using the AHP are to develop a hierarchy of criteria (value tree) and to identify alternatives. AHP uses pairwise comparisons of alternatives to score the alternatives on each criterion and uses pairwise comparison of criteria to weight the criteria, assuming ratio scales for all judgments. The overall score of an alternative is obtained by the weighted summation of its scores on the different criteria [15].

UTA Methods

The UTA methods have the philosophy of evaluation of a set of functions for value or utility, assuming the basic axioms of MAUT and adopting the principle of unbundling of preference. In practice this approach infers functions value / usefulness, so that they are as far as possible consistent with the goals and preferences of decision makers - Principle of Inference [16]. A abordagem desagregação-agregação tem como intuito analisar o comportamento e o estilo cognitivo do decisor. O objetivo desta abordagem é ajudar o decisor a melhorar o seu conhecimento sobre a situação de decisão e também as suas preferências, o que resultará na tomada de uma decisão mais consistente [16].

MACBETH

MACBETH (Measuring Attractiveness by a Categorical Based Evaluation Technique) is an approach for multicriteria value measurement [17]. It uses semantic judgments about the differences in attractiveness of several stimuli to help a DM quantify the relative attractiveness of each alternative. It employs an initial, iterative, questioning procedure that compares two elements at a time, requesting only a qualitative preference judgment. As the answers are entered into the MACBETH decision support system [17] it automatically verifies their consistency. It subsequently generates a numerical scale by solving a linear programming problem that is representative of the DM's judgments. Through a similar process it permits the generation of weighting scales for criteria [17].

Outranking methods differ from the others in that there is no underlying aggregative value function, so they do not produce an overall preference scale for each alternative.

AHP generates global scores to represent the overall preference upon the alternatives, which is a wanted fea- ture. However, there are known issues regarding this method concerning, for example, the appropriateness of the conversion from the semantic to the numeric scale used in AHP [17] [18].
The UTA approaches infer functions of value/utility consistent with the preferences of the users but some do not take into account the weights of criteria, which make it a less accurate method.

A MACBETH advantage over other methods for multi-criteria value measurement is that it only requires qualitative judgments to score alternatives and to weight criteria, instead of requiring quantitative judgments. Furthermore, its decision support system – *M-MACBETH* - is able to compute the overall values of the alternatives by applying the additive model, and to make extensive sensitivity and robustness analysis.

5. Objectives of the solution

In this section covers the step of definition of the objectives of a solution of DSRM, in which we will define the objectives of the solution, based in the problem identified and in the related work described previously.

Looking back to the problem we identified in Section 2, the main issue is the fact that there isn't a set of security criteria sufficiently wide and also the fact that do not exist one way to evaluate the IS security in an easy way and with concrete and adapted results. The main aim is therefore, is to create a mechanism that allows to any organization to evaluate the IS security in a simple manner appropriate to their organization. We have also secondary objectives we intend to achieve: (1) clarify doubts and fears about the security of Cloud systems; (2) applicable to all IS and any organization; (3) clarify the real problems of IS security; (4) easy to understand; (5) more accessible to evaluate IS security; (6) allow sensivity and robustness analysis.

6. Proposal

This section corresponds to the design and development step of DSRM, in which we create an artifact to solve the problem identified. The problem described in section 2 was: how to compare the security of two equivalent Information Systems with different deployments – in house vs Cloud? Our proposal is a method based on MACBETH approach to evaluate de security of two IS equivalents, through a set of security criteria approved by the decision maker.

The MACBETH approach [17] is composed by three major steps, which we will use and adapt on the creation of our method. So, we will divide this section in three sub-sections, one for each step of the method. We will start with the structuring the model (section 6.1); the second step is evaluating the alternatives (section 6.2); finally, analyzing the results (section 6.3).

6.1 Structuring the model

The method begins with the structure of the model. In this step we will identify the evaluation criteria and their respective descriptors of performance (qualitative or quantitative) used to measure the degree to which each criterion can be satisfied. The evaluation criteria will be set taking into account the real security concerns for today existing IS in organizations.

To create the evaluation criteria we started by doing a literature review of existing criteria of IS security. After that, we did a validation of a standard of information security management - ISO 27001 - because is composed by a very complete wide set of controls that covers all areas of information security.

To do the literature review we follow the methodology proposed for Webster and Watson [19], doing an extensive search, with some time constraints. For our search we used the search engine Google Scholar with combinations and variations of the following keywords: Information Systems Security, Information Systems attacks, Information Systems Security evaluation criteria, Security, Information Security attributes, Information Systems Security criteria, criteria Security, Security concerns, problems Security best practices, criteria Cloud Security and Cloud Security.

In the search we found 100 articles. Through an analysis of the abstract, introduction and conclusion, we identified the articles that specifically spoke of evaluation security criteria for IS and security problems of IS. After that, we made a careful review of those articles, with the goal of finding those who could be useful to our research; at the end we select 17 articles as a basis for creating our set of security criteria for IS.

Then, we realized that the literature could help us, but would not be sufficient for the creation of the security criteria. Hereupon, we validated the standard ISO 27001. After doing an analysis of ISO 27001 and their controls, we wanted to validate it with security practitioners in organizations, and potential decision makers, aiming to understand what controls are directly applicable in the evaluation of IS security. This evaluation is described in section 8.1.

As result we define 11 families, composed by 39 specific security criteria. After, we create the descriptors of performance to each criterion. According to the analysis, these criteria are sufficient and necessary to evaluate all the IS in terms of security, but as already mentioned each decision maker can add or modify the set existent, to cover their specific needs.

In the creation of our proposal, we validated the criteria that make sense in the specific case chosen to demonstrate our proposal. As result, decision maker selected 31 of 39 criteria. Each criterion has associated a descriptor of qualitative performance, whose goal is to know the extent to which each criterion is being met. The descriptors of performance also contribute to the intelligibility of the criteria and to clarify it's meaning. For each criterion is also necessary to define two reference levels on the performance scale. We define with decision maker, for each criterion, the "Good" level that is a very attractive level and the "Neutral" which is a level of performance that is neither positive nor negative.

Three examples of criteria and descriptors of performance used for the demonstration of our proposal are in Figure 1.

Security Policy		**Information security policy**	
	Performance Levels	Existence of an Information Security Policy document published, reviewed on agreed dates and communicated to all employees and external parties.	L1 = Good
		Existence of an Information Security Policy document published, reviewed on agreed dates and communicated to some employees and external parties.	L2 = Neutral
		Existence of an Information Security Policy document published, reviewed on agreed dates and not communicated to employees and external parties.	L3
		Existence of an Information Security Policy document published and never reviewed.	L4
		There is no Information Security Policy document.	L5
Organization of Information Security		**Internal Organization**	
	Performance Levels	Existence of an Information Security committee, a well-defined Information Security roles and responsibilities and independent reviews of the Information Security on agreed dates.	L1 = Good
		Existence of an Information Security committee, a well-defined Information Security roles and responsibilities and independent reviews of the Information Security once in a while.	L2 = Neutral
		Existence of an Information Security committee, a well-defined Information Security roles and responsibilities and no existence of independent reviews of the Information Security.	L3
		Existence of an Information Security committee and a poorly defined Information Security roles and responsibilities.	L4
		There is no Information Security committee.	L5
		External parties	
	Performance Levels	Existence of an identification of risks related to external parties and an identification of the controls to implement to secure the information.	L1 = Good
		Existence of an identification of risks related to external parties and a non-identification of the controls to implement to secure the information.	L2 = Neutral
		Non-identification of risks related to external parties.	L3

Figure 1 - Security Evaluation Criteria with respective descriptors of performance, distributed per family

We believe that these criteria and descriptors of performance can be used as a catalog to evaluate the security of all IS, always paying attention to the necessary adjustments for each decision maker.

6.2 Evaluating the alternatives

The second step is the evaluation of the alternatives. Here, the decision maker is asked about their preferences in order to build a value function for each criterion and to weight the criteria. The starting point is the definition of two reference levels on each descriptor of performance ("Neutral" and "Good"), task described in previous section. After that, the decision maker is asked to judge the differences in attractiveness between each two levels of performance by choosing one (or more) of the MACBETH semantic categories: **very weak, weak, moderate, strong, very strong, or extreme**. Then, M-MACBETH (software that implements MACBETH approach) uses a linear programming problem to generate a numerical value scale compatible with the decision maker's judgments.

Next, the decision maker has to weight the criteria. To do this, the decision maker ranks the neutral–good swings of the criteria by their overall attractiveness. Afterwards, the decision maker is asked to judge the difference in attractiveness between each two neutral–good swings using the MACBETH semantic categories, and his answers are used by M-MACBETH to create a weighting scale. Finally, the decision maker should validate the proposed weights.

6.3 Analyzing the results

The final step of the method is the placement of the performances of alternatives to compare in the M-MACBETH. The software then transforms these performances in value scores, using the value functions previously built and calculates the score of overall value of each alternative weighted by the sum of their partial scores. A final ranking of the alternatives is then achieved using their overall scores. Afterwards, and before giving a selection recommendation, the sensivity and robustness analysis are done, to know how sensitive or robust is the ranking to small changes in the parameters of the model. These analyses are supported by M-MACBETH software.

The demonstration and application of our proposal is described in the next section, where we will present each step of our proposal in a real case study.

7. Demonstration

This section corresponds to the demonstration step of DSRM, in which we demonstrate that the proposal can be used to solve one or more instances of the problem.

The objective of our proposal is to create a method to evaluate the IS security. To make the demonstration, we chose one City Council in Portugal due to its importance in the context of our country and because the CIO wanted to evaluate their internal security comparatively with Cloud products; the IS chosen was the Mail application. The decision maker in our case study was the CIO of the City Council and the decision analyst in the decision making process was the author of this article.

Which identified the best services in the market at this level - Google Apps, Microsoft Office 365 and PTEMAIL. We will use Microsoft Office 365 as alternative to the in house.

This section is divided in three subsections, corresponding to the steps of our method described previously.

7.1 Structuring the model

This step begins with the definition of the screening criteria and validation of the set of evaluation security criteria in the context of meetings with the decision maker.

In our demonstration, the decision maker has validated 31 of the 39 criteria as being necessary and sufficient to evaluate the security of the Mail in her organization. "System planning and acceptance" and "Correct processing in applications" were two of the criteria that were not validated, for not being relevant security concerns in the choice of IS. The tree value, in **Error! Reference source not found.**, shows the evaluation criteria selected grouped into eleven families.

7.2 Evaluating the alternatives

To evaluate the alternatives into account - Microsoft Office 365 and in-house - we ask the decision maker to validate the descriptors of performance and reference levels, after a rigorous analysis, accepted all the descriptors and performance levels.

Then we ask the decision maker to judge the differences of attractiveness between the levels of performance for each criterion (qualitative) through MACBETH approach. After the M-MACBETH generated a value scale for criteria based on the judgments placed in of judgments matrix. Figure 2 shows the matrix of judgments and value scale for the criterion "Backup".

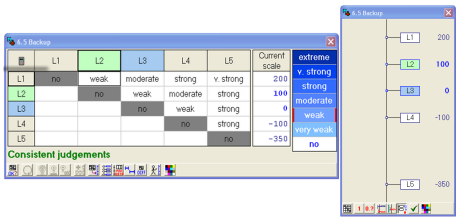


Figure 2 - MACBETH judgements matrix and value scale for the criterion "Backup"

Afterwards, the next step is the assignment of the weights for the criteria. Here the decision maker was asked to order the swings "neutral-good" criteria in descending order of importance and then to fill the judgments matrix of weights.

Making judgments of difference in attractiveness between pairs with 31 fictitious alternatives would be a difficult task for the decision maker, so we ask the decision maker to make comparisons by families, taking into account existing criteria within each of the 11 existing families. After this, we used the criterion with best score of each family and we ask the decision maker to make the comparisons using this subset of 11 criteria (one per family). Then we did some additional calculations on them to create a common scale across all criteria and then obtain the final weights that are shown in the histogram in Figure 3.

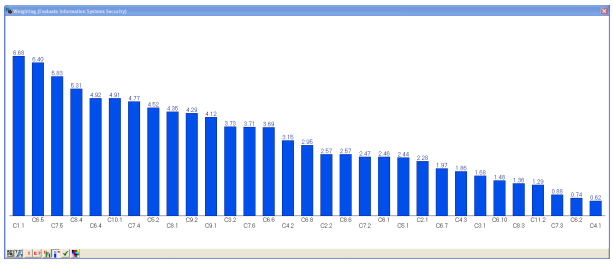


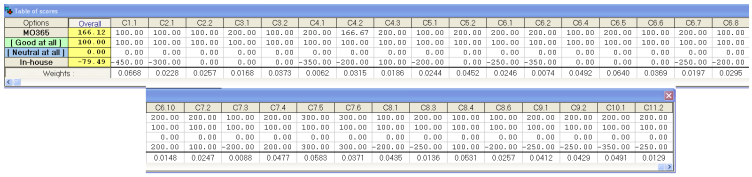
Figure 3 - Histogram of weighting scale

The last step of the evaluation of the alternatives is the collection and analysis of performance levels of each criterion for each alternative and input on the M-MACBETH. Relatively to the in house alternative, this collection was made through interviews with CIO and workers of the City Council and also with visits to the facilities where the IS is deployed. In case of Microsoft Office 365, the collection and analysis was made through the intensive analysis of a public Microsoft document, referenced by a security and risk officer of Microsoft Portugal. This document is validated by international organizations like Cloud Security Alliance [20].

7.3 Analyzing the results

The performances of the Microsoft Office 365 and in house upon each of the criteria were inputted in M-MACBETH. The software transformed the performances into the value scores, presented in Figure 4, using the value functions previously built, and calculated the overall scores for the alternatives (column “Overall” in Figure 4). Microsoft Office 365 ranked first with 166.12 overall units and in house ranked second with -79.49 overall units. Only Microsoft Office 365 obtained and overall score higher than the hypothetical alternative

“Neutral at all” (i.e a fictitious alternative that has a neutral performance in all the criteria), which shows that Microsoft Office 365 is a very attractive alternative for the City Council. Differently, in house alternative is not an attractive alternative, because its overall score is bellow to the neutral performance, defined by decision maker.



Options	Overall	C1.1	C2.1	C2.2	C3.1	C3.2	C4.1	C4.2	C4.3	C5.1	C5.2	C6.1	C6.2	C6.4	C6.5	C6.6	C6.7	C6.8
MO365	166.12	100.00	100.00	100.00	200.00	100.00	200.00	166.67	200.00	100.00	200.00	200.00	200.00	100.00	200.00	100.00	200.00	100.00
[Good at all]	100.00	100.00	100.00	100.00	100.00	100.00	100.00	100.00	100.00	100.00	100.00	100.00	100.00	100.00	100.00	100.00	100.00	100.00
[Neutral at all]	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
In-house	-79.49	-450.00	-300.00	0.00	0.00	0.00	-350.00	-200.00	100.00	-200.00	0.00	-250.00	-350.00	0.00	0.00	0.00	-250.00	-200.00
Weights :		0.0668	0.0228	0.0257	0.0168	0.0373	0.0062	0.0315	0.0186	0.0244	0.0452	0.0246	0.0074	0.0482	0.0640	0.0369	0.0197	0.0295

C6.10	C7.2	C7.3	C7.4	C7.5	C7.6	C8.1	C8.3	C8.4	C8.6	C9.1	C9.2	C10.1	C11.2
200.00	200.00	100.00	200.00	300.00	300.00	100.00	200.00	100.00	100.00	200.00	200.00	200.00	200.00
100.00	100.00	100.00	100.00	100.00	100.00	100.00	100.00	100.00	100.00	100.00	100.00	100.00	100.00
0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
200.00	100.00	-200.00	200.00	300.00	300.00	-200.00	-250.00	100.00	-200.00	-250.00	-250.00	-350.00	-250.00
0.0148	0.0247	0.0088	0.0477	0.0683	0.0371	0.0495	0.0196	0.0651	0.0267	0.0412	0.0429	0.0491	0.0129

Figure 4 - Overall value scores of the alternatives

Relatively to sensitivity analysis, IN-MACBETH showed that independently of the percentage of weights, the in house alternative never ranks first. The best result that can exist for the in house alternative is to stick with the same overall score than Microsoft Office 365, if the weights on some criterion are 100%. The result of the robustness analysis is extracted directly by the table generated by the M-MACBETH. As we can see in Figure 5, the intersection between "MO365" (line) and "In-house" (column) is a red triangle, which means that Microsoft Office 365 alternative dominates, in the classic sense, the in-house, i. e., Microsoft Office 365 is no worse than in house on any criterion and is better in at least one criterion. We can also extract the Microsoft Office 365 also dominates the fictional alternative “Good at all”.

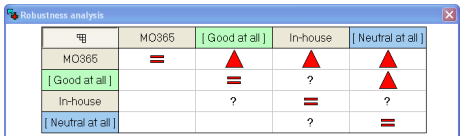


Figure 5 - Robustness analysis

As conclusion, we recommended to the City Council the selection of Microsoft Office 365, because it is the better alternative taking into account all the defined criteria and the judgments of preference made by the decision maker. In addition, the sensivity and robustness analysis showed that Microsoft Office 365 is a robust choice.
Another alternative to this recommendation is to improve and correct the actual in house IS, in the worst criteria identified through our method.

8. Evaluation

This section corresponds to the evaluation step of DSRM, which aim to observe and measure how well the artifact supports a solution of the problem. To make the evaluation we used interviews with practitioners and the Moody and Shanks Quality Framework [6]. We will divide this section in the two evaluations.

8.1 Interviews with practitioners

The purpose of the interviews with practitioners is, to validate our research, the problem, the proposal and the results of the demonstrations. Our solution was designed based on the literature, giving us strong theoretical foundations for the beginning of our research. But we felt it was important also take the point of view of security practitioners that working in this area daily.

So, we interviewed eight security officers with 17 years average of experience in Information Technology and 9 years experience in Security of Information Technology, of the largest banking institutions and public institutions in Portugal. Our goal was to understand what are the security criteria that really matter when evaluating the security of an IS.

We chose to use ISO 27001 as a basis. The choice of this standard has already been justified but even if it is the most broadly used to evaluate the security of information in organizations, we felt it was important to validate that all controls of this standard are valid for our research. The results are shown in Figure 6.

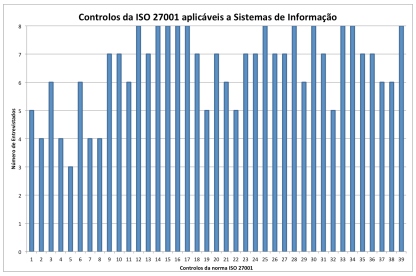


Figure 6 - Analysis of the proposed evaluation criteria

The results showed that all controls of the standard are directly related to the security of IS, even some controls have been less chosen by interviewees. After analyzing the results, we found that all interviewees chose 11 controls and three interviewees chose only 1 control. As conclusion, we used all the controls of ISO 27001 for the construction of our set of evaluation security criteria, because this set must contain the criteria that are necessary and sufficient to evaluate the security of the majority of the IS. In this case all the controls were important for, at least, three interviewees.

8.2 Moody and Shanks Quality Management Framework

The Moody and Shanks Quality Framework is the result of research on how to evaluate and improve the quality of data models from the perspective of the multiple stakeholders and proposes eight factors [6]. We applied this framework to the demonstration by asking the decision maker about these eight quality factors and the results are shown then:

- **Completeness:** the proposal is complete since the main criteria to evaluate the security of IS are present, and each decision maker can add or change criteria or their descriptors of performance depending on your needs.
- **Simplicity:** our artifact is simple to follow, taking into account the opinion of the decision maker, and confirmed that it is easy to implement, requiring only the decision maker with their qualitative judgments.
- **Flexibility:** the difficulty of making changes is directly proportional to the amount of change the criteria by the decision maker.
- **Integration:** our proposal is consistent with the needs and goals of the organization, since it is built directly with the decision maker. The result of our proposal is a response to the need to compare the security among IS and therefore helps the decision maker to make a decision.
- **Understandability:** practitioners consider our proposal easy to understand, because the security concepts used are the same as traditional concepts of security, but in relation to the concepts of MCDA is more difficult because there is no knowledge of such concepts and is therefore difficult to perform without instructions.
- **Implementability:** practitioners expressed interest in using our proposal, but the implementability depends on the internal policies of each organization; anyway admit to using it as a decision tool not only for security reasons.
- **Integrity:** is dependent on the maker, since there is no other constraint for the definition of the criteria and descriptors of performance. Our proposal relies on interviews and observations.
- **Correctness:** the proposal is correct and valid for their intentions.

The field case study done in the City Council allowed to us to test our proposal in response to the research problem stated. This evaluation showed that the method is a suitable tool for evaluating the security of IS and the decision maker showed very interest in using it.

9. Conclusion

Given the identified problem: how to compare the Security of two equivalent Information Systems with different deployments - in house vs. Cloud, a problem existent in all organizations when the need to purchase a new IS or when there is a need to evaluate their own internal security compared to other solutions, our research proposes a solution: method to compare the security of two equivalent Information Systems using the MACBETH. This solution is based on the a MCDA method that uses defined security evaluation criteria to evaluate the security and give as a result the best alternative for the decision maker and their specific needs.

The demonstration was done in a Portuguese City Council to compare the Mail application. The two alternatives were in house and Microsoft Office 365 and the recommendation was the choice of the alternative Microsoft Office 365.

In relation to lessons learned, we observed that these security concerns are growing faster and the organizations don't know how to manage them. Indeed, each organization has their own notion of security problems and solutions. So, our method is a very good method to normalize these security evaluation criteria and to help all organizations to compare various alternatives.

The limitations are related directly to the M-MACBETH application used, because of it's old fashion design; are related also to the fact that we cannot say that our solution is applicable to all IS and organizations, because we only have one demonstration. This is due to the fact that many organizations refused our demonstration due to the sensitive and confidential nature of this topic.

Our research contributions were the fact that we identified a real problem and proposed a solution. We proposed a set of security evaluation criteria and through them we could give a recommendation to the decision maker. We also proposed improvement proposals of the security of the in house IS to decision maker, with concrete actions related with the results obtained by the application of the method. And we hope we have passed the message that Cloud Computing it's not less secure than in house solutions, it's quite the opposite.

As future work, is necessary to make more demonstrations of the method with more decision makers and with other type of IS, to prove that our proposal is really useful to the organizations. The M-MACBETH should have an interactive guide to end with existent doubts related with it's using and an improved user interface.

References

[1] Xiaohui Yang, Sheng Zhang, Fu Liu, and Guo Jian, *A Study on Security Evaluation for Information Systems Based on Grey Clustering*. San Diego, California: IEEE, 2010.

[2] Azah Anir Norman and Norizan Mohd Yasin, "An Analysis of Information Systems Security Management (ISSM): The Hierarchical Organizations vs. Emergent Organization," *nternational Journal of Digital Society (IJDS),* , vol. 1, no. 3, September 2010.

[3] Heru Susanto, Mohammad Nabil Almunawar, Yong Chee Tuan, Mehmet Sabih Aksoy, and Wahyudin P Syam, "Integrated Solution Modeling Software: A New Paradigm on Information Security Review and Assessment," *International Journal of Science and Advanced Technology*, vol. 1, no. 10, pp. 90-99, December 2011.

[4] Mikko T. Siponen, *Information Security Management Standards: Problems and Solutions*. Adelaide, South Australia: 7th Pacific Asia Conference on Information Systems , 2003.

[5] Carlos A. Bana e Costa, Jean-Marie De Corte, and Jean-Claude Vansnick, "Macbeth," *International Journal of Information Technology & Decision Making* , vol. 11, no. 2, pp. 359-387, 2012.

[6] D.L. Moody and G.C Shanks, "Improving the quality of data models: Empirical validation of a quality management framework," *Information Systems*, vol. 28, pp. 619-650, 2003.

[7] H Osterle et al., "Memorandum on Design-Oriented Information Systems Research," vol. 20, pp. 7-10, 2011.

[8] Alan Hevner, Salvatore March, Jinsoo Park, and Sudha Ram, *Design Science in Information Systems Research*.: MIS Quarterly, Vol.28, No.1, pp.75-105, Society for Information Management and The Management Information Systems Research Center, 2004.

[9] Atreyi Kankanhalli, Hock-Hai Teo, Bernard C.Y. Tan, and K wok-Kee Wei, "An Integrative study of information systems security effectiveness," *International Journal of Information Management*, vol. 23, pp. 139-154, 2003.

[10] ISACA, *Cloud Computing: Business Benefits With Security, Governance and Assurance Perspectives*. Rolling Meadows , USA: ISACA, 2009.

[11] Computer Security Institute, "2010/2011 Computer Crime and Security Survey," 2011.

[12] ISACA, *Security Considerations for Cloud Computing*., 2012.

[13] ISO 27001 Standard. (2013) ISO 27001 Basics. [Online]. http://www.iso27001standard.com/en/what-is-iso-27001

[14] Andreas Ekelhart, Stefan Fenz, and Thomas Neubauer, "Ontology-based Decision Support for Information Security Risk Management," in *Fourth International Conference on Systems*, 2009, pp. 80-85.

[15] Valerie Belton and Theodor J Stewart, *Multiple Criteria Decision Analysis - An Integrated Approach*.: Kluwer Academic Publishers, 2002.

[16] José Figueira, Salvatore Greco, and Matthias Ehrgott, *Multiple Criteria Decision Analysis State of the Art Surveys*.: Springer, 2005.

[17] Carlos A. Bana e Costa , Jean-Marie De Corte, and Jean-Claude Vansnick , "On The Mathematical Foundations Of Macbeth," in *Multiple Criteria Decision Analysis: State of the art surveys*. United States of America, 2005.

[18] J. S. Dyer and R. K. Sarin, "Measurable Multiattribute Value Functions," *Operation Research*, vol. 24, no. 4, pp. 810-822.

[19] Webster Jane and Watson T. Richard, "Analyzing the Past to Prepare for the Future: Writing a Literature Review," *MIS Quarterly*, vol. 26, no. 2, pp. 13-23, June 2002.

[20] Microsoft Corporation, "Office 365 mapping of CSA Security, Compliance, and Privacy requirements," 2014.