A Structured Comparison of the Corporate Information Security Maturity Level

Michael Schmid, Sebastian Pape

A Structured Comparison of the Corporate Information Security Maturity Level

Michael Schmid[1,2][0000−0002−3534−313X] and
Sebastian Pape[1,3][0000−0002−0893−7856]

[1] Chair of Mobile Business & Multilateral Security
Goethe University Frankfurt, Germany
{michael.schmid,sebastian.pape}@m-chair.de
[2] Hubert Burda Media Holding KG
[3] Chair of Information Systems, University of Regensburg, Germany

Abstract.

Generally, measuring the information security maturity is the first step to build a knowledge information security management system in an organization. Unfortunately, it is not possible to measure information security directly. Thus, in order to get an estimate, one has to find reliable measurements. One way to assess information security is by applying a maturity model and assess the level of controls. This does not need to be equivalent to the level of security. Nevertheless, evaluating the level of information security maturity in companies has been a major challenge for years. Although many studies have been conducted to address these challenges, there is still a lack of research to properly analyze these assessments. The primary objective of this study is to show how to use the analytic hierarchy process (AHP) to compare the information security controls' level of maturity within an industry in order to rank different companies. To validate the approach of this study, we used real information security data from a large international media and technology company.

Keywords: *Information security · Information security management · ISO 27001 · Analytic hierarchy process · Information security controls · Capability Maturity Model · Security Maturity Model · Security metrics framework*

1 Introduction

Information security can only be measured indirectly [6]; unfortunately there is still no gold standard. One way to indirectly measure it is to use metrics and KPIs[1] which aim to approximate the real status of information security. This approach is not always reliable [22]. Some information to build those metrics are obtained from technical systems (e.g. firewalls, intrusion detection/prevention systems, security appliances). However, most of these metrics and KPIs have to be quantified by humans and are therefore prone to errors.

This can lead to possible inaccuracies, measurement errors, misinterpretations, etc. [4]. If these metrics are then compared across the board, the information security managers face a major challenge. As a consequence, this could lead to bad

decisions based on wrong conclusions. Moreover, by just comparing the metrics, without any weighting the specifics of the respective industry are not considered. Thus, a prioritisation within the comparison is not possible [3]. This problem is reinforced when the comparison of information security metrics between different companies or departments would take place [9], which is exactly on of the current challenges enterprises face today: How to compare their (sub-)companies of a specific industry (e.g. eCommerce) in terms of information security.

The main goal of this paper is to compare the effect of multiple factors in the information security assessment process. Aiming at achieving this goal, the analytic hierarchy process (AHP) is applied. The Analytical Hierarchy Process (AHP) is one of the most commonly used Multiple Criteria Decision Methods (MCDM), combining subjective and personal preferences in the information security assessment process [20]. It allows a structured comparison of the information security maturity level of companies with respect to an industry [25] and to obtain a ranking[13]. This allows us to define a separate weighting of information security metrics for each industry with to respect their specifics while using a standardized approach based on the maturity levels of the ISO 27001:2013 controls [12]. ISO 27001 was in particular selected, because this standard is shown to be mature, widespread and globally recognized. This minimizes the additional effort for collecting the required metrics. In this study, the maturity level is based on a hierarchical, multi-level model to analyze the information security gap for the ISO 27001:2013 security standard [20]. As a prerequisite for the comparison, we assume companies have implemented an information security management system (ISMS) in accordance with ISO 27001 [26].

To validate the approach of this study, we used real information security data (i.e. security controls' maturity level) from Hubert Burda Media (HBM) a large international media and technology company consisting of over 200 individual companies. This provides sufficient data with a high degree of detail in the area of information security. The result from our AHP-based approach is then compared with the perceived status of information security by experts.

The remainder of this work is structured as follows: In Sect. 2 we give a brief overview of related work. Section 3 describes our methodology when we developed our approach shown in Sect. 4. Our results are shown in Sect. 5 followed by a discussion and our conclusion in Sect. 6, respectively Sect. 7.

2 Background and Related Work

In addition to the differences in the assessment of information security, all assessment procedures have in common that the ratings of the maturity level and the weighting of weights remain separate judgements and are not allocated to a common overall value in the sense of an 'information security score'. It is therefore up to the evaluator to carry out the respective evaluation, as he or she is forced to choose between these two quantitative aspects of the evaluation, i. e. the ratings on the one hand and the weighting on the other [15]. In contrast to this, the works of Boehme [6] and Anderson [3] deal more with the economic impact

of investments in information security. The focus of this work is to compare the degree of maturity within an industry. This could later lead to a monetary assessment of information security or maturity.

A solution which involves to merging ratings and weights and thus integrates different assessment measures at the same time offers multi-attribute decision-making procedures[8]. These are methods that offer support in complex decision-making situations, i. e. when a decision has to be made in favour of one of several options against the background of several decision criteria (so-called attributes).

The prerequisite for using the multi attribute decision procedure is, as described above, the determination of weights. A popular method of doing this is the Analytic Hierarchy Process (AHP) method developed by Saaty [23]. Nasser [2] describes how to measure the degree of maturity using AHP. In contrast to our paper which deals with the comparison of the maturity level within an industry, Nasser [20] focuses on the determination of inaccurate expert comparison judgement in the application of AHP.

Some recent works deals with this problem setting using the AHP but there exist further restrictions. Watkins [27] uses for his approach not the control maturity level and is only valid in the cyber security environment. Bodins' [5] approach is based on the comparison of the CIA-Triangle and not on ISO 27001-controls. Peters [21] has already shown the application of AHP in the domain of project management but did not use real data to validate the approach.

2.1 Multiple Criteria Decision Methods

Multi criteria decision problems which could be solved with a multiple-criteria decision analysis method (MCDM) are a class of procedures for the analysis of decision or action possibilities characterized by the fact that they do not use a single superordinate criterion, but a multitude of different criteria. Problems in evaluating multiple criteria consist of a limited number of alternatives that are explicitly known at the beginning of the solution process. For multiple criteria, design problems (multiple objective mathematical programming problems), the alternatives are not explicitly known. An alternative (solution) can be found by solving a mathematical model. However, both types of problems are considered as a kind of subclass of multi-criteria decision problems [17]. MCDM helps to determine the best solution from multiple alternatives, which may be in conflict with each other. There are several methodologies for MCDM such as: Analytical hierarchical process (AHP), Grey relational analysis (GRA), Technique for order preference by similarity to ideal solution (TOPSIS), Superiority and inferiority ranking (SIR), Simple additive weighting (SAW), and Operational competitiveness rating (OCRA) [7].

2.2 The Analytical Hierarchy Process

The AHP, is a method developed by the mathematician Thomas L. Saaty [24] to support decision-making processes. Because of its ability to comprehensively

analyse a problem constellation in all its dependencies, the AHP is called 'analytical'. It is called a 'process' because it specifies how decisions are structured and analysed. In principle, this procedure is always the same, which makes the AHP an easy-to-use decision tool that can be used more than once and is similar to a routine treatment [16]. The goal of the Analytic Hierarchy Process method is to structure and simplify complex decision problems by means of a hierarchical analysis process in order to make a rational decision. The AHP breaks down a complex evaluation problem into manageable sub-problems.

3 Research Methodology

Many companies use the maturity level measurement of the controls from ISO standard 27001 to obtain a valid and reliable metric. The ISO standard is well established and the maturity assessment of the standard's controls is an adequate possibility to create a picture of the information security processes of a company. While this might be sufficient for a continuous improvement within the same company, a problem arises if one wants to compare the information security processes of different companies or departments. Depending on the field of industry, some of the processes might be more important than others.

The general aim of this approach is to determine which company within an industry is better or worse in a (sub)area of information security, in order to create transparency among the companies within an industry concerning information security. Positive effects of this approach would be the improvement or deterioration of the information security in a sector within an industry recognizable up to the question where the management should invest money economically for information security in order to improve a sector.

We define the requirements in the next subsection, then determine the proper algorithm and finally describe the data collection for our approach.

3.1 Requirements

The most important requirement is that the metrics we rely on should be easy to gather. Assuming that the investigated company is running an information security management system (ISMS), a natural approach is to rely on the controls of the ISO/IEC 27001 standard and their maturity level. Existing data (e.g. information security maturity level) should be used wherever possible. Furthermore, the approach should consider the environment of the industry in which the company is located. Additionally, the information gathering should be repeatable and stable. Comparing and evaluating over a long period should be possible as well as an overall as an comparison of security levels of business units or companies in a similar area. Finally, the approach should allow it to visualize and explain the results of the comparison and allow to derive the areas where companies could improve.

3.2 Algorithm Selection

Taking all requirements into account, our problem is a multi-dimensional decision problem, and thus can be addressed by a multiple-criteria decision analysis method (MCDM). Our comparison criteria (dimensions) are the ISO/IEC 27001 controls and we compare the different companies based on their corresponding maturity levels for each control. Thus, the MCDM needs discrete, quantitative input and a criteria weighting method. Since the underlying controls are hierarchically and therefore very structured, the chosen method/model should reflect that also.

This leads us to the analytical hierarchy process (AHP) as a best fit method in the above described context. The AHP is a mature structured technique for organizing and analyzing complex decisions, combining subjective and personal preferences. The AHP has been the most widely used technique of multi-criteria decision making during the last twenty five years [19]. The advantage of this method over the utility value analysis, for example, is that it goes beyond the evaluation of ideas and generates a clear selection recommendation. Its hierarchical structuring of decision making fits well to the ISO/IEC 27001 controls' hierarchy and the qualitative evaluation part of the AHP is very much in line with the maturity level for information security. Since the AHP compares the maturity level for each control company-wise, it naturally allows to understand where each company's security level is ranking related to each control. Additionally, the weight of each criteria (control) can be easily derived. In the concrete application case it is possible to compare the importance of individual controls of ISO 27001 very granularly with each other (pairwise). This is in particular necessary in order to be able to establish an industry reference. Furthermore, the AHP enables precise calculations of weights, in this case the information security maturity ratings of companies in a specific sector.

Thus, we used a paired comparison questionnaire based on the AHP to compare controls and their maturity level for an industry.

3.3 Data Collection

To test the above approach it is necessary to set up the model and verify it with real data. We need a maturity assessment of the ISO/IEC controls and to weight them according to the considered industry. We focused on the eCommerce industry for the following reasons:

- Available data from a large range of companies
- Excellent data quality and validity
- High actuality of the existing data
- Very good know-how available in the expert assessment of the industry

Maturity Assessment of ISO/IEC 27001 Controls We collected data from Hubert Burda Media (HBM), an international media and technology company (over 10,000 employees, more than 2 billion annual sales, represented in over 20 countries). This group is divided into several business units that serve various business areas (including print magazines, online portals, e-commerce, etc.). The

business units consists of over 200 individual companies with about 30 of them being in the eCommerce industry. Each subsidiary operates independently of the parent corporation. There is a profit center structure, so the group acts as a company for entrepreneurs and the managing directors have the freedom to invest money into information security or choose the appropriated level of security.

We will briefly describe how this data is collected before going into more detail on the data used for the comparison. Each individual company in the group operates its own Information Security Management System (ISMS) in accordance with ISO/IEC 27001:2013, which is managed by an Information Security Officer (ISO) on site and managed by a central unit in the holding company. As part of the evaluation of the ISMS, the maturity level for the respective ISO 27001 controls is ascertained - very granularly at the asset level. The maturity level is collected/updated regular once a year as part of a follow-up.

First, the information values of the respective company (e. g. source code, customer data, payment data, etc.) are determined according to the protection goals of confidentiality, integrity and availability and assigned to a technical system (e. g. application, client, server, etc.).

Second, these technical systems undergo a threat analysis[4] of the assets in relation to the respective asset type as part of information security risk management. The threat analysis is classically evaluated with regard impact[5] and the probability of occurrence. This results in an aggregated risk value (1-5) for each asset after a pre-defined settlement. This risk value is later transferred to the control valuation as the *target maturity level*. In this way, a comparison is made between the protection requirements of the information values and the protection level of the respective (IT) system.

Third, the control evaluation is then carried out using the Cobit maturity level. The controls are dynamically selected[6] according to the previously evaluated threats. The Cobit maturity level is a 6-step evaluation scale (0-5) with which a continuous improvement can be measured and a potential improvement can be identified. This allows it to evaluate the actual maturity level per control and asset. The assessment of the current status of the controls is carried out by the information security officer of the respective company. The collected data is therefore not technical data but subjectively quantified data with a possible bias. Although, the evaluated data is reviewed by further experts, a complete review cannot be carried out due to resource limits. The target maturity level is already determined by the risk value / protection level of the system. This provides a clear picture of the ISMS status at a very granular asset level.

Fourth, the picture is completed by the Cobit maturity analysis of the IT-/ISM processes[7]. For each of these processes, the controls (e. g. A.16 for incident

[4] threat catalogue according to ISO/IEC 27005:2011

[5] referring to the protection goals of confidentiality, integrity and availability

[6] by a predefined threat/control matrix

[7] Business Continuity Management, Compliance, Incident Management, Information Security Management, Organizational Information Security, Protection Requirement Assessment

management) are evaluated with an actual maturity level [10]. In the later evaluation (typically by means of a spider graphic) the complete ISO 27001 standard is evaluated with the aid of the Cobit degree of maturity [14].

The available data is very granular on asset level (application, client, server, etc.). However, although the companies are from the same industry, they do not necessarily have the same kind of assets. Thus, we decided to abstract from the assets and to aggregate the data at company level. To do this automatically, we used the mean value of all evaluated assets per control. For the following proof of concept, we only show data from 5 companies.

4 The Approach - the AHP-Implementation

In this section, we discuss how the AHP is applied to our comparison. The first step of the AHP, to model the problem as a decision hierarchy, we have already done by deciding that our decision-criteria will be the ISO/IEC 27001 controls. The goal is clearly defined: to find the subsidiary within the company with the best information security/level of maturity within an industry. Appendix A of ISO 27001 helps us to select criteria and sub criteria, which is divided into 14 Control Categories, 35 Control Objectives and 114 Controls (see Fig. 1).

The next step is the prioritization of all criteria and sub criteria (Sect. 4.1). This represents the domain specific part of the AHP calculations and it only needs to be done once per domain. It is followed by the evaluation of the alternatives (Sect. 4.2). The alternatives represent the agile part of the calculation. We describe in the corresponding section, how the evaluation can be directly derived from the maturity level of a company's control. Based on the individual evaluations and prioritizations of controls, the AHP uses a mathematical model to determine a precise weighting of all alternatives in relation to the respective criteria and assembles them in a percentage order (Sect. 4.3).

In the next subsections we describe in detail how the AHP was used and show how the applied AHP model was implemented in a statistical software (in this case in R).

4.1 Pairwise Comparison of the Control Categories and Controls

The characteristics of an industry have a significant influence on the pairwise comparison when comparing the individual controls. If the information security of companies is to be compared with each other, e.g. in the e-commerce sector, it will differ significantly from that of companies in other sectors, e.g. publishing or the manufacturing industry. On the one hand this is due to the different business models within the industries, because the IT strategy and the information security strategy are derived from the business strategy. On the other hand this is due to the different focus in information security. For example, the eCommerce industry is very focused on application development and (confidentiality) protection of customer data, whereas the highest commodity to be protected in the manufacturing industry is the availability of systems.

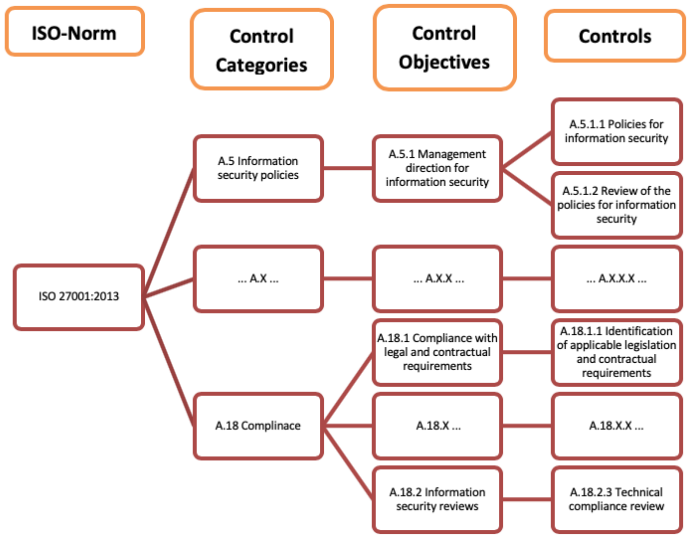

Fig. 1: *Exemplary ISO 27001 Appendix A structure*

The decision-maker must compare each criterion with its pair and denotes which of the two criteria appears more important to him/her. This method of pairwise comparisons allows the decision-maker to elicit a very precise evaluation from the multitude of competing criteria. The comparisons must be carried out specifically for one industry (e. g. eCommerce). In the case of our hierarchy based on the ISO/IEC 27001 controls, 91 pairwise comparisons have to be made for the control categories and 208 for the controls, respectively. This leads to a ranking order in which the criteria are ranked according to their importance.

The comparison is done as follows: Each result of a pairwise comparison of two criteria entered in the evaluation matrix shows how much more significant a criteria is in relation to the criteria of the level above. To do this, refer to the scale in Tab. 1a. In order to make a comparison for one criteria, i.e. the control categories, we compare the individual control categories with each other. The authors made this comparison in a straight forward Excel spreadsheet. The assessment of the relative importance of the criteria at the criterion level can be found in Tab. 1b. These pairwise comparisons are always carried out by an expert with the background knowledge and with reference to the industry (here eCommerce). The comparison for the sub criteria, the controls, follows the same guidelines.

4.2 Pairwise Evaluation of the Controls' Maturity Levels

The alternatives in our example are the information security maturity of 5 eCommerce companies of HBM. For each control and each company there is a corresponding maturity level based on the Cobit Maturity Model. 0 represents

Table 1: *AHP Scores and their Application*

AHP Score	Verbal description
9 8	Extreme preference
7 6	Very strong preference
5 4	Strong preference
3 2	Moderate preference
1	Equal preference

(a) *Fundamental AHP Score*

Sub criteria A	Sub criteria B	A/B	Score
Control A.12.1.1[1]	Control A.12.1.2	B	$\frac{1}{7}$
Control A.12.1.1	Control A.12.1.3	B	$\frac{1}{7}$
Control A.12.1.1	Control A.12.1.4[4]	B	$\frac{1}{7}$
Control A.12.1.2[2]	Control A.12.1.3	B	$\frac{1}{3}$
Control A.12.1.2	Control A.12.1.4	A	3
Control A.12.1.3[3]	Control A.12.1.4	A	3

[1]Documented operating procedures [2]Change management
[3]Capacity management [4]Separation of development

(b) *AHP Comparison with sub criteria (Controls) from control group A.12.1*

the worst and 5 the best result, always in relation to the evaluation of a control. As already discussed in Sect. 3.3, the maturity levels for each company were based on assets and we aggregated the maturity levels by calculating the average maturity level for each control over all evaluated assets of the respective company.

For the pairwise comparison, the gap between the comparative maturity levels of two companies' controls is considered to decide which company is doing better at a specific control. For that purpose, we need to map the 6-stage scale of the Cobit maturity grade gaps (see Tab. 2) to the 9-stage AHP score. The result is a table where each GAP Cobit interval represents an AHP score, which is verbally described. An exemplary calculation can be found in Tab. 2c). Alternative A (Company 1) is compared with the alternatives B (Company 2 to 5). A Cobit GAP -2 (i.e. 1-3) means hat Company 2 is 2 control maturity better than Company 1, the AHP score is, corresponding to the Cobit GAP interval, 4, respectivly 1/4. This can be used to calculate which of the 5 companies performs best in Control A.5.1.1.

The step of comparing the companies' maturity levels for each control represents the business unit specific part of the analysis. Note that, due to our mapping of the GAP Cobit interval and the AHP score, this can be done fully automatic if the corresponding maturity levels are provided. The pairwise comparison, the calculation of the difference and the 'translation' to the GAP intervals is done in the statistics software R.

4.3 Calculation of the Comparison

As mentioned above, the actual calculation of the AHP is done with R. The implementation in R worked with the help of a YAML (Ain't Markup Language) script executed in R. The YAML script is a simplified markup language for data serialization. The YAML script contains all results of the pairwise comparison of criteria and sub criteria, as well as the maturity levels of the 114 controls

Table 2: *Combined GAP of Cobit Maturity Model and AHP Score*

Cobit Maturity Model	Cobit level
Optimized	5
Managed and Measurable	4
Defined Process	3
Repeatable but Intuitive	2
Initial/Ad Hoc	1
Non-existent	0

(a) *Maturity Model vs. level*

AHP Score	Cobit GAP Interval	Verbal description
9	4.45 - 5.00	Extreme
8	3.89 - 4.44	preference
7	3.34 - 3.88	Very strong
6	2.78 - 3.33	preference
5	2.23 - 2.77	Strong
4	1.66 - 2.22	preference
3	1.12 - 1.65	Moderate
2	0.56 - 1.11	preference
1	0.00 - 0.55	Equal preference

(b) *AHP Score vs. GAP Cobit level*

Alt. A	Alt. B	Cobit GAP	Score
Co. 1	Co. 2	-2	$\frac{1}{4}$
Co. 1	Co. 3	1	2
Co. 1	Co. 4	-3	$\frac{1}{6}$
Co. 1	Co. 5	1	2

(c) *Comparison for Control A.5.1.1*

of the 5 eCommerce companies. The decision hierarchy built up in the YAML script corresponds to the ISO standard. The decision hierarchy is then enriched with alternatives. The paired comparison of the alternatives is executed by a function of the R-package 'ahp' (version 0.2.12 from Christoph Glur) at script runtime for a simple data processing flow. The runtime of the script (with data from 5 companies) on an iMac (3.2 GHz Intel Core i5) was less than 10 seconds, indicating that it is efficient enough to handle large amounts of data easily.

5 Results of the Comparison

The AHP was used to compare the maturity level in order to find the company with the best information security within an industry (here eCommerce).

Prioritization of Controls Here we show which priority the control categories (criteria) and controls (sub criteria) have in relation to the complete appendix A of ISO 27001 over all. The pairwise comparison for the eCommerce industry shows that the controls of the control category 'A.14' have the highest priority (17.6 %), followed by 'A.17' (14.7 %) and 'A.12' (10.1 %). Within control category 'A.14', controls 'A.14.2.8' (22.6 %), 'A.14.2.7' (15.2 %) and 'A.14.2.6' (11.8 %) are the most important as shown in Fig. 2.

Comparision of the Companies The Control Category 'A.14' was used to exemplarily show the evaluation. Figure 2 also shows how the individual eCommerce companies weighting compare with each other in the control category 'A.14' in detail. Overall (cf. Fig. 3), Company3 (21.0 %), Company5 (20.9 %) and Company1 (20.5 %) came out best in a direct comparison. The differences are marginal and only on closer inspection are there more pronounced differences observed at the control level. In relation to a control category e.g. of 'A.14', the maturity of Company1 (4.4 %) and Company4 (4.0 %) is better in detail, but

	Priority	Company3	Company5	Company1	Company4	Company2
Comparison eCommerce	100.0%					
A.14 System acquisition	17.6%					
A.14.2.8 System security testing	22.6%	16.7%	4.3%	32.7%	32.7%	13.7%
A.14.2.7 Outsourced development	15.2%	23.3%	27.6%	27.6%	17.0%	4.5%
A.14.2.6 Secure development environment	11.8%	19.8%	22.4%	22.4%	13.1%	22.4%
A.14.2.1 Secure development policy	8.0%	4.4%	39.6%	19.4%	19.4%	17.2%
A.14.1.2 Securing application services on public networks	7.4%	5.9%	23.5%	23.5%	23.5%	23.5%
A.14.1.3 Protecting application services transactions	7.0%	6.1%	5.4%	30.3%	30.3%	27.9%
A.14.1.1 Information security requirements analysis and specification	6.2%	21.6%	23.3%	23.3%	23.3%	8.5%
A.14.2.9 System acceptance testing	5.1%	17.5%	19.8%	19.8%	19.8%	23.2%
A.14.2.2 System change control procedures	4.9%	14.3%	28.6%	14.3%	28.6%	14.3%
A.14.2.4 Restrictions on changes to software packages	4.4%	28.6%	14.3%	14.3%	14.3%	28.6%
A.14.2.5 Secure system engineering principles	3.9%	20.0%	20.0%	20.0%	20.0%	20.0%
A.14.2.3 Technical review of applications after operating platform changes	3.5%	28.6%	14.3%	14.3%	14.3%	28.6%
A.17 Information security aspects of business continuity management	14.7%					
A.17.1.2 Implementing information security continuity	48.1%	40.0%	10.0%	20.0%	10.0%	20.0%
A.17.1.1 Planning information security continuity	40.5%	28.6%	14.3%	28.6%	14.3%	14.3%
A.17.1.3 Verify review and evaluate information security continuity	11.4%	40.0%	10.0%	20.0%	10.0%	20.0%
A.12 Operations security	10.1%					
A.12.1.3 Capacity management	13.9%	40.0%	21.9%	21.9%	11.4%	4.8%
A.12.4.1 Event logging	13.2%	35.9%	5.4%	19.6%	19.6%	19.6%
A.12.6.1 Management of technical vulnerabilities	12.4%	19.4%	36.7%	19.4%	19.4%	5.2%
A.12.4.2 Protection of log information	11.5%	24.4%	3.7%	23.7%	23.7%	24.4%
A.12.1.2 Change management	11.3%	20.0%	20.0%	20.0%	20.0%	20.0%
A.12.4.3 Administrator and operator logs	10.2%	5.3%	5.3%	30.5%	30.5%	28.4%
A.12.1.4 Separation of development	9.3%	9.2%	4.5%	29.7%	29.7%	27.0%
A.12.6.2 Restrictions on software installation	7.1%	6.6%	26.3%	12.2%	26.3%	28.7%
A.12.4.4 Clock synchronisation	5.6%	24.3%	12.2%	12.2%	6.7%	44.6%
A.12.1.1 Documented operating procedures	5.6%	5.3%	38.8%	21.7%	21.7%	12.5%

Fig. 2: *Top3 Control Categories prioritized and companies ranked*

	Weight	Company3	Company5	Company1	Company4	Company2
Comparison eCommerce	95.1%	21.0%	20.9%	20.5%	16.3%	16.2%
A.14 System acquisition	17.6%	3.0%	3.3%	4.4%	4.0%	3.0%

Fig. 3: *Control category A.14 weight contribution and ranked companies*

considering the control category 'A.17', Company3 (5.2 %) is clearly ahead of Company4 (1.7 %).

6 Discussion

Based on these results, we discuss the main findings as follows. The results show that with the pairwise comparison it is possible to obtain a priority for each individual control, and thus very granular, in the overall context of ISO/IEC 27001 for the eCommerce industry. The priorities of the larger control categories are also very helpful, as a quick comparison of priorities is possible here. The approach with the pairwise comparison by AHP meets all requirements of the methodology part. Similarly, it is shown that the weighting of the pairwise comparisons of the maturity level of eCommerce companies can be mapped very

granularly to the controls of the ISO/IEC 27001 standard. It was also possible to derive the AHP score from the maturity levels automatically. This makes it easy to compare the rankings of the companies. The only effort which needs to be invested (for each industry) is the prioritization of the controls.

The results suggest that the approach works in conjunction with real data (the maturity levels of HBM's eCommerce companies) at least for the chosen area. The results of the comparison also withstand the reality that one of the authors observes in his daily professional life. The results also showed that the ranking results reflect the reality of at least the HBM eCommerce companies. However, it can be strongly assumed that the method is directly applicable to other companies with the same or similar results.

6.1 Limitations

For reasons of simplification and clarity, we have demonstrated the approach only with a small number of companies. But is easily possible to run the approach with the full set of HBM's companies and to extend it to other business units by readjusting the ISO/IEC 27001 controls' priorities.

The application of the AHP methodology is not undisputed in technical literature. At this point the authors consider some points of this criticism. On the one hand, these are points concerning the mathematical part of the AHP and on the other hand, the criticism is based on the procedure. In the model calculated above, the pairwise comparison of the criteria and sub criteria has been carried out by one person (with expert knowledge), which can be regarded as a very subjective survey of all pair comparisons. This assumes that there are high demands on the respondent due to the many pair comparisons, which is why there are often problems with validity [18]. This could lead to a limitation of the size of the decision model and is seen as a critical and possible optimization point of the AHP methodology in literature and practice [11].

If you take a closer look at the origin of the maturity level, you immediately notice that it is determined by the information security officer's self-disclosure. As with all quantification, the human factor, a lack ob objectivity or bias, cannot be excluded here. However, it can be largely validated by a team of experts. Another point concerns the type of data collection, the resulting prevailing data quality and possible imponderables in data evaluation. These issues could only be reduced but not completely eliminated by several iterations of quality assurance.

In the next chapter, some of the limitations will be discussed and further improvements of the methodology/model will be proposed.

7 Conclusion and Future Work

The results of the pairwise comparison suggest that AHP is very well suited to compare the information security maturity of different companies and to find the company with the best information security within an industry.

It has been proven that a comparison within the eCommerce industry is possible using this model and thus ranking the prioritization of control categories and, above all, the individual controls can follow. The AHP provides in this case a robust and comprehensive treatment for decision makers in both qualitative and quantitative ways as found in this study and it can be assumed that this will also work for other companies in the same environment. The real insight is to adapt the AHP or the data so that it works together. The AHP-model has shown how AHP might be used to assist decision maker evaluate information security in one branch. Very interesting, and also for validation, would be the pairwise comparison for other industries such as publishing houses, manufacturing industry. Companies with very different degrees of maturity could also be interesting here.

Some of the limitations mentioned above regarding the AHP methodology deal with the comparison of pairs. A possible improvement of the model would be to compare it with the help of a team of experts from the eCommerce industry. This would have the advantage that the pair comparison is subject to validation.

In future work, the focus will be on the details of implementing this model across a variety of different examples, as well as working on more expanded decision hierarchy with an additional level of sub criteria (control objectives). In addition, it would be interesting to calculate the approach with different aggregated data (min, max, median) in addition to the mean value and to observe the effects. Furthermore, it would be interesting to apply the AHP methodology to other industries (e. g. publishing, manufacturing industry etc.). Ultimately, this would provide the prerequisites for comparing information security across industries, comparing apples and pears, so to speak.

References

1. Abbas Ahmed, R.K.: Security Metrics and the Risks: An Overview. International Journal of Computer Trends and Technology **41**(2), 106–112 (2016)
2. Al-shameri, A.A.N.: Hierarchical Multilevel Information security gap analysis models based on ISO 27001 : 2013. International Journal of Scientific Research in Multidisciplinary Studies **3**(11), 14–23 (2017)
3. Anderson, R., Barton, C., Böhme, R., Clayton, R., van Eeten, M.J., Levi, M., Moore, T., Savage, S.: Measuring the cost of cybercrime. In: The Economics of Information Security and Privacy, pp. 265–300. Springer Berlin Heidelberg (2013)
4. Axelrod, C.W.: Accounting for Value and Uncertainty in Security Metrics. Information Systems Control Journal **6**, 1–6 (2008)
5. Bodin, L.D., Gordon, L.A., Loeb, M.P.: Evaluating information security investments using the analytic hierarchy process. Communications of the ACM **48**(2), 78–83 (2005)
6. Böhme, R.: Security metrics and security investment models. In: Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics). vol. 6434 LNCS, pp. 10–24 (2010)
7. Choo, K.K., Mubarak, S., Mani, D., Others: Selection of information security controls based on AHP and GRA. Pacific Asia Conference on Information Systems **1**(Mcdm), 1–12 (2014)

8. Eisenführ, F., Weber, M.: Rationales Entscheiden. Rationales Entscheiden p. 415 (2003)
9. Gordon, L.a., Loeb, M.P.: The economics of information security investment. ACM Transactions on Information and System Security **5**(4), 438–457 (2002)
10. Haufe, K.: Maturity based approach for ISMS. Ph.D. thesis, University Madrid (2017)
11. Ishizaka, A., Labib, A.: Review of the main developments in the analytic hierarchy process. Expert Systems with Applications **38**(11), 14336–14345 (2011)
12. ISO/IEC 27001:: Information Technology — Security Techniques — Information Security Management Systems — Requirements. International Organization for Standardization (2013)
13. Khajouei, H., Kazemi, M., Moosavirad, S.H.: Ranking information security controls by using fuzzy analytic hierarchy process. Information Systems and e-Business Management **15**(1) (2017)
14. Le, N.T., Hoang, D.B.: Capability maturity model and metrics framework for cyber cloud security. Scalable Computing: Practice & Experience **18**(4), 277–290 (2017)
15. Lee, M.c.: Information Security Risk Analysis Methods and Research Trends : AHP and Fuzzy Comprehensive Method. International Journal of Computer Science & Information Technology (IJCSIT) **6**(February), 29–45 (2014)
16. Liu, D.L., Yang, S.S.: An Information System Security Risk Assessment Model Based on Fuzzy Analytic Hierarchy Process. 2009 International Conference on E-Business and Information System Security pp. 1–4 (2009)
17. Majumder, M.: Impact of Urbanization on Water Shortage in Face of Climatic Aberrations. Springer Singapore (2015)
18. Millet, I.: Ethical Decision Making Using the Analytic Hierarchy Process. Journal of Business Ethics **17**(11), 1197–1204 (1998)
19. Mu, E., Pereyra-Rojas, M.: Pratical Decision Making: An Introduction to the Analytic Hierarchy Process (AHP) Using Super Decisions (v2). Springer Berlin Heidelberg (2017)
20. Nasser, A.A.: Measuring the Information Security Maturity of Enterprises under Uncertainty Using Fuzzy AHP. I.J. Information Technology and Computer Science **4**(April), 10–25 (2018)
21. Peters, M.L., Zelewski, S.: Analytical Hierarchy Process (AHP) – dargestellt am Beispiel der Auswahl von Projektmanagement-Software zum Multiprojektmanagement. Institut für Produktion und Industrielles Informationsmanagement (2002)
22. Rudolph, M., Schwarz, R.: Security Indicators – A State of the Art Survey Public Report. FhG IESE **VII**(043) (2012)
23. Saaty, T.L., Vargas, L.G.: Decision Making with the Analytic Network Process: economic, political, social and technological applications with benefits, opportunities, costs and risks. Springer Berlin Heidelberg (2006)
24. Saaty, T.L., Vargas, L.G.: Models , Methods , Concepts & Applications of the Analytic Hierarchy Process, vol. 175. Springer Berlin Heidelberg (2012)
25. Syamsuddin, I., Hwang, J.: The application of AHP to evaluate information security policy decision making. International Journal of Simulation: Systems, Science and Technology **10**(4), 46–50 (2009)
26. Vaughn, R.B., Henning, R., Siraj, A.: Information assurance measures and metrics - State of practice and proposed taxonomy. In: Proceedings of the 36th Annual Hawaii International Conference on System Sciences, HICSS 2003 (2003)
27. Watkins, L.: Cyber Maturity as Measured by Scientific-Based Risk Metrics. Journal of Information Walfare **14.3**(November), 60–69 (2015)