Aggregating Corporate Information Security Maturity Levels of Different Assets

Michael Schmid[1,2(✉)] and Sebastian Pape[1(✉)]

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

Abstract. General Data Protection Regulation (GDPR) has not only a great influence on data protection but also on the area of information security especially with regard to Article 32. This article emphasizes the importance of having a process to regularly test, assess and evaluate the security. The measuring of information security however, involves overcoming many obstacles. The quality of information security can only be measured indirectly using metrics and Key Performance Indicators (KPIs), as no gold standard exist. Many studies are concerned with using metrics to get as close as possible to the status of information security but only a few focus on the comparison of information security metrics. This paper deals with aggregation types of corporate information security maturity levels from different assets in order to find out how the different aggregation functions effect the results and which conclusions can be drawn from them. The required model has already been developed by the authors and tested for applicability by means of case studies. In order to investigate the significance of the ranking from the comparison of the aggregation in more detail, this paper will try to work out in which way a maturity control should be aggregated in order to serve the company best in improving its security. This result will be helpful for all companies aiming to regularly assess and improve their security as requested by the GDPR. To verify the significance of the results with different sets, real information security data from a large international media and technology company has been used.

Keywords: Information security · Information security management · ISO 27001 · Aggregation functions · Information security controls · Capability maturity model · Security maturity model · Security metrics framework

1 Introduction

Approximately 18 months ago the General Data Protection Regulation (GDPR) containing requirements regarding the processing of personal data of individuals

became operative. The GDPR states that organizations must adopt appropriate policies, procedures and processes to protect the personal data they hold. Article 32 of the GDPR specifically requires organizations to ensure confidentiality, integrity, availability and resilience (core principles of the information security) of processing systems and services, and to implement a process for regularly testing, assessing and evaluating the effectiveness (e.g. with KPIs) of technical and organizational measures for ensuring secure processing [27]. Thus, in addition to presenting a state of the art security level, this article emphasizes the importance of a process for regularly testing, assessing and evaluating the security. However, it does not provide detailed guidance on how to achieve these goals.

It is difficult to judge whether the security level is sufficient from a management perspective. Managers often act according to the maxim 'minimal effort maximum success', since the budget is usually limited. Of course, this also applies to the area of information security and varies depending on the industry and the self-perception of IT security within it. This is justifiable from an economic point of view, but it has an influence on how information security is dealt with in the company. In this situation, it is important to create transparency regarding the state of information security, within an organization to determine how good the process is, as well as in comparison to other companies operating in the same environment. This transparency can be used to demonstrate/ensure that (information) security does not suffer from budget constraints.

An established way to monitor and steer the information security is the implementation of an information security management system (ISMS). With the most popular standard in this field, ISO/IEC 27001 [14], it is possible to manage the information security in a company through the ISO-controls. An effective ISMS that conforms to ISO/IEC 27001 meets all requirements of GDPR's article 32.

The information security status of an environment like a company is a very individual observation [1]. To estimate the actual status of information security normally metrics or key performance indicators (KPI) are taken into account [21]. The information gathering of these KPIs is usually done through different technical or organizational metrics of a company. Using KPI/Metric/-Maturity for the status of information security is only an indicator of improvement or deterioration since there is unfortunately no gold standard for this [4]. It would be very complex and expensive to first collect or generate these KPIs for this evaluation. It is important therefore, to work with the data/metrics already available and no need for further data collection. In this context, it should not go unmentioned that another standard exists in this environment, the ISO/IEC 27701 [15]. This standard deals with how to establish and run a Privacy Information Management System (PIMS) that adds Personally Identifiable Information (PII) security protection to an existing ISMS. In order to assess the status of information security as well as the quality of the process, mostly a maturity model is used. A common method for the assessment of the maturity is the COBIT control maturity model from the ISACA framework [13]. With the help of this model it is possible to assess the goodness of the ISO-controls on a 0 to 5 scale. The assessment supports the improvement of the organization's security and delivers the management perspective in the fulfillment of regulatory requirements.

With the maturity level, the manager has a relatively good overall view of the status of information security. However, this is usually a very aggregated view of the status, as a company will operate different types of IT systems/applications to support its business process. The information assets worth protecting (e.g. customer data, trade secrets, source code, etc.) are not only processed or stored on one IT system, but on several. As a consequence, the maturity level may differ between systems. Therefore, many companies not only collect a maturity level for the whole company, but also a maturity level per system for each control [11]. An ISO control such as A.12.6.1 (Vulnerability Management) will only be able to reflect a combined value from several IT systems/applications. That's why, different values exist for different assets per ISO control (see Fig. 1).
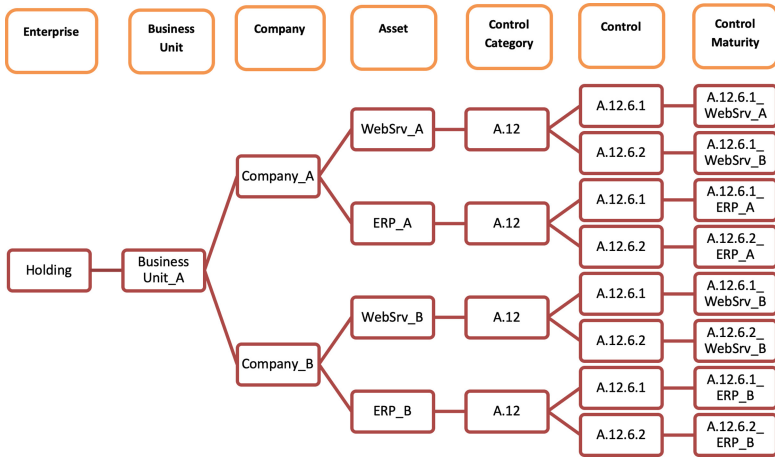

Fig. 1. Exemplary holding structure with different assets and control maturity for ISO-controls

In order to derive a KPI from the assets' control maturity level or use them as input for existing approaches [24, 25], the questions arises how they can be meaningfully aggregated.

RQ1: How can maturity levels for one control be meaningfully aggregated across different assets?
Different aggregation types can not only influence the outcome of the approach, but also influence the managers which security controls should be improved.
RQ2: How would a manager's optimization strategy depend on the different aggregation methods?
And finally, it's equally important to consider the aggregation's influence on the final result of the algorithm.
RQ3: How much does the outcome of a holistic approach actually change depending on different aggregation types?

To examine this research question, we first discuss different types of aggregation for maturity levels. In the next step, for each of the aggregations we derive possible security managers' optimization strategies in order to establish which control to improve next. For a reality check, we examine asset's maturity levels from real company data to check if our assumptions are realistic. As a final step, we also use real companies' maturity levels to examine how much the outcome of [24] would be changed by applying a different aggregation.

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 how we developed our approach for each research question shown in Sect. 4. Our results are shown in Sect. 5 and discussed 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 also have in common that the ratings of the maturity level and the weighting of weights 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, e.g. the ratings on the one hand and the weighting on the other [17]. Savola [23] discussed a broader approach to finding a metrics which can be used in the field of different security disciplines like management and engineering practices. In contrast to this, the works of Böhme [8] and Anderson [4] deal more with the economic impact of investments in information security. There are also other models that deal with the measurement of information security using maturity levels e.g. the Information security maturity model (ISMM) [22] and the Open Information Security Maturity Model (O-ISM3) [22]. ISMM is intended as a tool to evaluate the ability of organizations to meet the objectives of security and O-ISM3 aims to ensure that security processes operate at a level consistent with business requirements. However, both models refer more to the process level than to the asset level. The focus of this work is to compare the different aggregation types of maturity within an industry. This could later lead to a monetary assessment of information security or maturity.

2.1   Aggregation Types

Unfortunately, the precise process of how to aggregate maturity levels is neither well documented nor comprehensively studied or understood (from a psychological perspective), so most of this labor is done by rule-of-thumb [26]. As mentioned, our approach varies between four aggregation types - namely the minimum, maximum, average and median - to compare their different potential impacts on decision making. Regarding the two measures of central tendency (average, median), strengths and weaknesses have been discussed in scientific literature. Averages are strongly influenced by extreme values. In our context, this could lead to an over- or underestimate of control maturity. In contrast,

the median is not skewed by extreme values, consequently running the risk of overestimating control maturity [10]. The opposite can be the case when there are multiple non-values (e.g. zeros) in a data sample, as laid out by Anderson et al. [5]. The relative position of average and median differs in skewed distributions. A distribution skewed to the left will lead to a smaller median compared to the average, while a right-skewed distribution reverses the relation [18]. Overall, it makes sense to include both measures of central tendencies in our analysis to compensate for weaknesses and bias. The minimum and maximum further alleviate potential misrepresentations of control maturity, as they provide the numerical range of scores and expose potential outliers [7]. Logically, both measures are most sensitive to outliers in a data set but are nevertheless useful in our analysis when used in combination with the measures of central tendency.

2.2   Aggregation of Security Metrics

Although the domain of security metrics has been covered by a number of authors [3], only limited work on the area of metrics aggregation has been carried out. Ramos et al. [20] provided a detailed survey on models for quantifying networks resilience to attacks. The authors used stochastic techniques and attack graphs to map the possible routes an attacker could take to compromise a system. Abraham et al. [2] discussed the challenges faced by practitioners in the field of security measurements and highlighted the need to develop a mechanism for quantifying the overall security of all the systems on the network. The authors proposed a predictive framework that uses stochastic techniques based on attack graphs and incorporated temporal factors relating to the vulnerabilities such as availability of patch and exploits predicting the future state of the system. Cheng et al. [9] proposed a model for aggregating security metrics using Common Vulnerability Scoring System (CVSS) base metrics to estimate the exploitability of the vulnerabilities. Homer et al. [12] and Beck et al. [6] proposed a mathematical security model for aggregating vulnerabilities in risks in enterprise networks based on attack graphs. An aggregated numeric value was assigned to show the likelihood of a vulnerability being exploited by an attacker.

3   Research Methodology

The general aim of our approach is to determine which effect the different aggregation types of the maturity control of assets have on the information security of the companies. In order to do this it is important to create transparency around the state of information security. The method should take into account the different requirements of the different research questions set out in Sect. 1.

We derive the different aggregation methods in the next subsection for our approach, then determine the proper algorithm and finally describe the data collection of our approach.

3.1 Different Aggregation Functions

First, we examine which functions are suitable to verify the approach described above. As shown in Sects. 2.1 and 2.2 with the different aggregation functions e.g. average, median, minimum and maximum it is possible to form a single summary value from a group of data. The challenge now is to find the right aggregation functions to support the approach provided. These aggregation functions have in common that they can represent the impact of decisions by information security managers, each type in its own way. The hypotheses provide an outlook how information security managers might behave in terms of aggregation.

3.2 Data Collection

It would be very complex and expensive to first collect or generate these KPIs for this evaluation. It is important to use data/metrics already available (e.g. information security maturity level). 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 and aggregate them according to the specific 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

We collected data from Hubert Burda Media (HBM), an international media and technology company (over 12,500 employees, more than 2.5 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, eCommerce etc.). The business units consist of over 250 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 in information security and to choose the appropriate 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, 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 of the respective ISO 27001 controls is ascertained - very granularly at the asset level (application, web-server, CRM etc.). The maturity level is collected/updated regularly once a year as part of a follow-up procedure.

3.3 Algorithm Method Selection

Taking all requirements of the method into account, a previously developed approach from Schmid and Pape [24] is applicable. The primary objective of this

approach was to show how to use the analytic hierarchy process (AHP) to compare the information security controls of a level of maturity within an industry in order to rank different companies. The AHP is one of the most commonly used Multiple Criteria Decision Methods (MCDM), combining subjective and personal preferences in the information security assessment process [19]. It allows a structured comparison of the information security maturity level of companies with respect to an industry [26] and to obtain a ranking [16]. This allows the definition of a separate weighting of information security metrics for each industry with respect to their specifics while using a standardized approach based on the maturity levels of the ISO/IEC 27001 controls.

To achieve the aim of this paper it is necessary to calculate the control maturity of the assets with different aggregation types such as: minimum, maximum, average or median. This shows how strong the characteristics of the individual aggregation types are in comparison to the real data. Out of this, the first indicators can then be derived to clarify which effect the aggregation types have on the information security for individual companies. The following chapter describes the implementation of the approach for each of the 3 research questions.

4   Discussion of Different Aggregations

As outlined in the previous chapter the different aggregation functions have a very likely a different outcome when it comes down comparing them with each other. Among other things, this chapter will describe the different characteristics of the aggregation functions as well as the effects of the various IT assets of a company and how they affect the results. A vivid example with real world data illustrates how the various aggregations affect the final result and ultimately the behaviour of those responsible for information security.

4.1   General Aggregation Functions

The great advantage of the aggregation functions average, median, minimum and maximum is that by aggregating (key) figures differences can be identified in the results and thus comparisons can be made. These could be a strength or weakness per each aggregation type. In contrast to this, there is no difference in the comparison of the results for the aggregation functions sum, range and count, for example. A further advantage of the four aggregation functions mentioned above is the adaptability of these types to a different number of values. They work nicely even if each company has a different number of assets considered. This makes it possible to derive different scenarios for the comparison.

4.2   Derived Optimization Strategies

If the results of the different aggregation functions are compared with each other, different optimization strategies can be derived in the end. This is particularly

Table 1. Maturity levels of different collective assets for the ISO-control A.12.6.1 from five companies

Asset	Company1	Company2	Company3	Company4	Company5
1	4	**0**	3	3	4
2	4		**2**	2	**4**
3	**4**		2	3	
4	1			1	
5	0				

Table 2. Maturity level results from different aggregation functions

Aggregation	Company1	Company2	Company3	Company4	Company5
average	2.6	0	2.3	2.25	4
median	4	0	2	2.5	4
minimum	0	0	2	1	4
maximum	4	0	3	3	4

important for those who are responsible for information security. Due to the different aggregations, it is possible that different optimization possibilities can be shown in the evaluation of information security. The information security manager can then decide which optimization strategy/aggregation function brings him the most benefit. If we take a closer look at the 4 aggregation functions mentioned above and examine them for the possible outcome, we obtain the following hypotheses:

- minimum → improve only the worst value (weakest chain, can make sense),
- maximum → improve only the best value (is this desirable?),
- average → improve any value (probably the easiest ones first) and
- median → may lead to a really two-fold security level with $\frac{n-1}{2}$ insecure services and $\frac{n+1}{2}$ secure services.

As next step we validate these hypotheses using an example with real world data.

4.3 Example with Real World Data

In order to compare the results of the different aggregation functions we need real data. Section 3.2 describes how these real data, in this case the COBIT maturity, are collected. For a concrete example we use the maturity level for a specific ISO-Control (here A.12.6.1 'Management of Technical Vulnerabilities') because this control focuses on an IT asset. As an example, we use data from five companies and their various IT assets (see Table 1).

Based on this data, the calculations of the four different aggregation functions are now performed (see Table 2) for the five companies. The colored cells highlight the aggregation functions and the maturity levels used. These exemplary calculations are based on the maturity levels of companies with different IT assets. A company uses many different IT assets to support its core and support processes. The next chapter examines these different types of IT assets in more detail.

4.4   More Complex Aggregations

In order to steer manager's optimization strategy one needs to integrate weightings for the different assets. This leads to the problem that many approaches, e.g. AHP [24] only work with a fixed number of assets. Considering only a fixed set of assets for each domain would narrow the defined scope, thus it should be possible to still evaluate a different number of assets. Conclusion: Define most important assets and their weighting and build an asset class for all remaining assets. This way, at least the impact of the manager's optimization strategies is more limited and only usable among the assets within the 'special class'. Arising Question: How to derive the priorities for all the classes?

When considering the core business processes for an eCommerce company, the web presence, a merchandise management system and a customer management system are normally expected. For this stage, we examined the prevailing situation of the IT assets used by 25 eCommerce companies from HBM and evaluated them. Almost all eCommerce companies had a web sever (24), a database server (24), an ERP system (22) and a CRM system (20). Further IT assets, which did not have such a high frequency were mail servers (14), file servers (14), dev servers (12), git (9), ftp servers (7), etc. This also coincides with the assumption resulting from the core business processes. Resulting from this the core IT assets of an eCommerce company, a web sever, a database server, an ERP system and a CRM system were selected.

Only considering these core IT assets would not reflect the overall picture of an eCommerce company. In order to have a comprehensive picture we also need the assets that are used in the IT department (e.g. file server, dev server, ftp server etc.). We have combined these IT assets into one collective asset for the comprehensive picture. In a further step, this collective asset, or better the maturity level, is calculated or evaluated using various aggregation types (minimum, maximum, average, median). In combination with the 4 core assets, aggregated values of the collective assets are included in the calculation as 5th assets (with 20%). This can provide the first insights as to whether a certain aggregation method might influence the units or sub-companies decision, hence which control should be improved next.

4.5   Priorization of Asset Classes

The core IT assets are equally important (e.g. 25% for each) at the moment. An interesting question would be e.g. how much more important is the web server

of an eCommerce company compared to the ERP system? It would be necessary to add an additional layer of prioritization in order to differentiate between the differing control requirements. In order to implement this we could use the CIA triad model which encompasses a triangle of tension between the three principles Confidentiality, Integrity and Availability. When applied to our use case, the principles of importance vary between control objectives and is represented by a score for the CIA principles according to their importance for these control objectives. This would provide for an extension of the approach by the CIA values of the individual assets. In order to do this, we need the CIA evaluation per IT asset. The information (e.g. customer data, contracts etc.) is stored or processed on an IT asset. It allows conclusions to be drawn as to how this asset should be treated in terms of confidentiality, integrity and availability. This means that there is at least one information asset per asset, but usually several information assets per asset, which are evaluated according to the CIA criteria with a 3-step classification (normal, advanced and high). A web server will, for example, process or even store information assets such as customer data, bank details, etc. If the information values 'customer data' and 'bank details' for a web server are uniformly evaluated for confidentiality, integrity and availability according to a given system, this can be set in relation to an ERP system with the information values 'purchasing conditions' and 'master data'. A further step was needed to convert our CIA data to pairwise comparisons on our AHP score, as depicted in Table 3a. We define a factor of equal importance regarding the CIA triad of all four core assets as a proportion percentage of 25% each. Consequently, we can conduct pairwise comparisons related to the proportion gaps in our data, which are then normalized based on the AHP preference score i.e. equal importance (AHP score: 1) is expressed by tiny differences in proportion to percentage of smaller than 2.77%, while the highest order of relative importance (AHP score: 9) means a difference of 25% in proportion to percentage (see Table 3b).

Table 3. Combined GAP of core assets and AHP Score

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

(a) Fundamental AHP Score

AHP Score	Proportional CIA differences	Verbal description
9	22.22 - 25.00	Extreme
8	19.45 - 22.21	preference
7	16.67 - 19.44	Very strong
6	13.89 - 16.66	preference
5	11.12 - 13.88	Strong
4	08.34 - 11.11	preference
3	05.56 - 08.33	Moderate
2	02.78 - 05.55	preference
1	00.00 - 02.77	Equal preference

(b) AHP Score vs. GAP of the CIA differences

5   Results of the Holistic Approach Considering Different Aggregation Types

The aim of this paper is to find out which effects the different aggregation functions have on the results and which conclusions can be drawn from them. The different aggregation functions can not only influence the outcome of the approach, but also influence the manager's decision as to the order in which control's maturity levels should be increased. They can influence the manager's optimization strategy depending on the different aggregation functions. At present, the maturity levels have not yet been examined with a view to optimization.

Table 4. Comparison of different aggregation types from 5 companies only for control A.12.6.1

Aggregation/proportion	Company1	Company2	Company3	Company4	Company5
Average	15.4%	7.7%	30.8%	30.8%	15.4%
Median	12.6%	12.6%	27.4%	34.9%	32.0%
Minimum	10.0%	10.0%	40.0%	20.0%	20.0%
Maximum	22.2%	11.1%	22.2%	22.2%	22.2%

Table 5. Comparison (proportion) of different aggregation types from 5 companies for control category A.12

Aggregation	Company1	Company2	Company3	Company4	Company5
Average	1.7% (17.9%)	1.2% (12.6%)	2.3% (24.2%)	2.1% (22.1%)	2.2% (23.1%)
Median	1.6% (16.8%)	1.7% (17.9%)	2.4% (25.3%)	1.9% (20.0%)	1.9% (20.0%)
Minimum	1.4% (14.7%)	1.2% (12.6%)	2.8% (29.5%)	2.1% (22.1%)	2.0% (21.0%)
Maximum	1.8% (18.9%)	1.3% (13.7%)	1.7% (17.9%)	1.6% (16.8%)	3.1% (32.6%)

5.1   Results of Aggregated Maturity Levels

The AHP was used to compare the maturity levels in order to work out how a maturity control should be determined to best serve the company in improving its security with reference to the first research question [24]. Table 4 shows a comparison of results with different aggregation types from five companies only for control A.12.6.1 'Management of Technical Vulnerabilities'. Because this control is asset-based, this value is composed of different IT assets that were calculated with each of the 4 different aggregation types.

As expected, Company 2 is very weakly developed if the raw data in Table 1 is considered. Company 1 is also quite clearly recognizable with regard to the minimum and maximum. Company 3 has the highest proportion concerning the

minimum (40.0%). The results show that a detailed look at Company 5 would be worthwhile, as the largest fluctuations between average and median (15.4%–32.0%) can be observed here.

If we now abstract this comparison to a higher level, e.g. no longer to the control level but to control category level, the results should no longer fluctuate greatly. In the case of control categories, we are concentrating only on the most important ones for the eCommerce industry. The weighting of the respective control categories can be seen from the results of the AHP [24]. 'A.14' (System Acquisition, Development and Maintenance) is the most important for the eCommerce industry with 16.5%, followed by 'A.17' (Information Security Aspects of Business Continuity Management) with 14.7% and then 'A.12' (Operations security) with 9.5%. Table 5 shows how the individual eCommerce companies weighting is compared with each other and the four different aggregation types for 'A.12' Operations security are compared in detail.

Table 6. Comparison of different aggregation types from 5 companies for the complete ISO/IEC 27001

Aggregation/proportion	Company1	Company2	Company3	Company4	Company5
Average	16.7% *(4.)*	15.4% *(5.)*	19.8% *(1.)*	18.3% *(3.)*	19.5% *(2.)*
Median	16.7% *(4.)*	16.3% *(5.)*	19.8% *(1.)*	18.8% *(2.)*	18.1% *(3.)*
Minimum	16.6% *(4.)*	14.6% *(5.)*	21.3% *(1.)*	18.7% *(2.)*	18.5% *(3.)*
Maximum	17.5% *(2.)*	15.6% *(5.)*	16.1% *(4.)*	16.2% *(3.)*	24.2% *(1.)*

The rows total up to 9.5% because it is the ratio of 'A.12' weighting in contrast to the overall control categories. The distribution of values within an aggregation type per company is specified in brackets. The differences are marginal but a closer inspection more pronounced differences can be observed at the control level and therefore tendencies are recognizable. Company 3 has again the highest proportion concerning the minimum (29.5%)

The last comparison in this environment is the application of the four different aggregation types to the complete controls of Annex A of ISO/IEC 27001. This is ultimately the highest expected level of aggregation of this approach. It is to be expected that the results will no longer differ so much from each other. Table 6 shows the results of the comparison.

The rows total up only to 89.9% because 11.1% is a 'measure of the error due to inconsistency' which is provided by the AHP. The ranking within all companies is specified in brackets. Concerning the outcome of the comparison, Company 5 stands out with a high value for maximum aggregation (24.2%) and Company 1 looks very stable concerning the different aggregation types. Generally, the minimum does not fluctuate as much as the maximum. Company 1 to 3 have no high fluctuation in common and concerning Company 3 there is not a lot of variance can be observed.

5.2 Results of Priorization the Asset

The descriptive statistic of HBMs information asset presence is used to begin with the set of four core assets, namely web server (24), database server (24), ERP system (22) and CRM system (20). Besides, computing our input scores as well as defining our priorities for sub criteria level requires the processing of the CIA inputs. The summarizing statistic is presented in Table 7 below.

All CIA scores are summed up for each asset and divided by the total number (see Table 8). The lowest sum resulted from the CRM asset with 100, and is hence our base value.

Concerning the priorization of asset classes Table 9 shows a pairwise comparison of the core assets from one eCommerce company. The deviation is then transformed into the AHP scores with the help of the intervals from the GAP of core assets (see Table 3b). It is clear that the biggest difference lies between the web server and the CRM system (11.7%) and the smallest difference between

Table 7. CIA of information assets from different IT assets of one company

Company	Information asset for	Confidentiality	Integrity	Availability	Sum of CIA
Company_1	Web-Server	2	2	3	**7**
	Web server	3	3	3	**9**
	Web server	3	3	2	**8**
	Web server	2	3	2	**7**
	Web server	3	3	2	**8**
	Database server	2	2	2	**6**
	Database server	2	2	2	**6**
	ERP system	2	2	2	**6**
	ERP system	2	2	2	**6**
	ERP system	2	2	2	**6**
	ERP system	2	2	2	**6**
	CRM system	2	2	2	**6**
	CRM system	2	2	2	**6**
	CRM system	1	2	2	**5**
	CRM system	1	2	2	**5**
Company_2	...	...	...	...	...

Table 8. Distribution of assets

Asset	CIA sum	Distribution
WEB	156	32.5%
ERP	104	25.0%
DB	120	21.7%
CRM	100	20.8%

the CRM system and the database server (0.7%). With the help of this score it is possible to weight the core assets based on their CIA assessment and process them with the AHP.

6   Discussion

Based on these results, we discuss the main findings as follows. The results show that it is possible to elaborate differences in the assessment and comparison of IT assets with the help of different aggregation types. The main goal of this paper, to assist managers in how they can improve their information security by comparing different aggregated information security maturity levels on asset level has shown several outcomes. The results show that a certain type of aggregation affects a company when trying to improve its maturity levels (see Table 4). Company 1 and 2 would improve first the collective assets with a low control maturity if a minimum aggregation is used. If the aggregation function maximum is used Company 3 would try to improve one collective asset in order to maximize only one control maturity (see Table 5). Concerning the big picture in Table 6 the ranking of the companies differs only for Company 1 and 3. Company 1 has already very high control maturities, so it is not as easy for them to improve. Company 3 almost a very homogenous control maturity thats why the would probably improve only one collective assets if the maximum aggregation is chosen. The other companies are more or less stable concerning the ranking, e.g. Company 2 does not changes at all.

Table 9. AHP Comparison with core assets

Sub criteria A	Sub criteria B	A/B	Deviation	Score
WEB	ERP	A	+7.25%	3
WEB	DB	A	+10.8%	4
WEB	CRM	A	+11.7%	5
ERP	DB	A	+2.3%	1
ERP	CRM	A	+4.1%	2
DB	CRM	A	+0.7%	1

With the help of the CIA prioritization is possible to first weight and then aggregated the different IT systems and applications with each other (see Table 9). The results show hat for an eCommerce company it is obvious that the web server is more important than the ERP-System in supporting the business processes.

6.1   Limitations

Maturity levels are not assessed automatically but by each of the individual companies' information security officer (ISO). Therefore, there may be discrepancies in the way the maturity levels are understood and assessed. This is clearly a limitation of any approach based on security maturity levels, but it might limit the informative value of the collected maturity levels. Moreover, the maturity levels are reported to the management and they result in a key performance indicator (KPI) for security for that specific unit. Thus, it can be assumed that each ISO has an interest in having a good evaluation. Therefore, ISOs might be tempted to assess the maturity levels more optimistically or to limit the scope of the information security management system in order to achieve better evaluations more easily. A common understanding of the different maturity levels is already established by guidelines and manuals provided to the ISOs (of HBM). This could be expanded further in order to reach a better understanding for the assessment of control maturity levels. Furthermore, deviations can be addressed if the companies are (externally) audited from time to time to double check the maturity levels.

7   Conclusion and Future Work

The discussion of how an overall score for a maturity level for security controls across different assets shows that the aggregation is an important tool needed to distinguish how the information security managers would optimize information security. In practice it makes a big difference which aggregation is used because it could lead to optimizing only the control maturity levels which are easily reachable. The defined priorization is necessary in order not to depend too much on the different kind of optimization strategies of the managers. This way, it can be steered more directly where the security should be enhanced and it probably also reflects better the current security level of companies. This approach is a helpful result for all companies aiming to regularly assess and improve their security as requested by the GDPR in order to ensure the confidentiality, integrity, availability and resilience of IT assets and evaluating the effectiveness of the technical and organizational measures for ensuring the security process.

As future work the outcome with other approaches could be compared to sen how the aggregation has changes the influence. Additionally, one might need to find other ways to prioritize the different controls, since in this case it was easy since it's one of the AHPs natural properties. Further investigations have to been carried out in order to clarify the validity of the control maturity levels because of the containing bias. Additional work could also be carried out to check validity of scope in order to measure any changes in the results after the metrics have been introduced.

References

1. Abbas Ahmed, R.K.: Security metrics and the risks: an overview. Int. J. Comput. Trends Technol. **41**(2), 106–112 (2016)

2. Abraham, S., Nair, S.: A predictive framework for cyber security analytics using attack graphs. Int. J. Comput. Netw. Commun. **7**(1), 1–17 (2015)
3. Ahmed, Y., Naqvi, S., Josephs, M.: Aggregation of security metrics for decision making: a reference architecture. In: ACM International Conference Proceeding Series (2018)
4. Anderson, R., et al.: Measuring the cost of cybercrime. In: Böhme, R. (ed.) The Economics of Information Security and Privacy, pp. 265–300. Springer, Heidelberg (2013). https://doi.org/10.1007/978-3-642-39498-0_12
5. Anderson, R., et al.: Measuring the changing cost of cybercrime our framework for analysing the costs of cybercrime. In: Workshop on the Economics of Information Security (WEIS), pp. 1–32 (2019)
6. Beck, A., Rass, S.: Using neural networks to aid CVSS risk aggregation - an empirically validated approach. J. Innov. Digit. Ecosyst. **3**(2), 148–154 (2016)
7. Bland, M.: Estimating mean and standard deviation from the sample size, three quartiles, minimum, and maximum. Int. J. Stat. Med. Res. **4**(1), 57–64 (2015)
8. Böhme, R.: Security metrics and security investment models. In: Echizen, I., Kunihiro, N., Sasaki, R. (eds.) IWSEC 2010. LNCS, vol. 6434, pp. 10–24. Springer, Heidelberg (2010). https://doi.org/10.1007/978-3-642-16825-3_2
9. Cheng, P., Wang, L., Jajodia, S., Singhal, A.: Aggregating CVSS base scores for semantics-rich network security metrics. In: Proceedings of the IEEE Symposium on Reliable Distributed Systems (2012)
10. Doane, D.P., Seward, L.E.: Applied Statistics in Business and Economics. McGraw-Hill Higher Education, New York (2016)
11. Gordon, L.A., Loeb, M.P.: The economics of information security investment. ACM Trans. Inf. Syst. Secur. **5**(4), 438–457 (2002)
12. Homer, J., et al.: Aggregating vulnerability metrics in enterprise networks using attack graphs. J. Comput. Secur. **21**(4), 561–597 (2013)
13. ISACA: COBIT 5: A business framework for governance and management of enterprise IT (2012)
14. ISO/IEC 27001: Information technology - security techniques - information security management systems - requirements. International Organization for Standardization (2013)
15. ISO/IEC 27701: Security techniques - extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management - requirements and guidelines. International Organization for Standardization (2019)
16. Khajouei, H., Kazemi, M., Moosavirad, S.H.: Ranking information security controls by using fuzzy analytic hierarchy process. Inf. Syst. e-Bus. Manag. **15**(1), 1–19 (2017)
17. Lee, M.C.: Information security risk analysis methods and research trends: AHP and fuzzy comprehensive method. Int. J. Comput. Sci. Inf. Technol. (IJCSIT) **6**, 29–45 (2014)
18. Manikandan, S.: Measures of central tendency: median and mode. J. Pharmacol. Pharmacother. **2**(3), 214–215 (2011)
19. Nasser, A.A.: Measuring the information security maturity of enterprises under uncertainty using fuzzy AHP. I.J. Inf. Technol. Comput. Sci. **4**, 10–25 (2018)
20. Ramos, A., Lazar, M., Filho, R.H., Rodrigues, J.J.: Model-based quantitative network security metrics: a survey. IEEE Commun. Surv. Tutor. **19**(4), 2704–2734 (2017)
21. Rudolph, M., Schwarz, R.: Security indicators - a state of the art survey public report. FhG IESE VII(043) (2012)

22. Saleh, M.: Information security maturity model. Int. J. Comput. Sci. Secur. (IJCSS) **5**, 21 (2011)
23. Savola, R.M.: Towards a taxonomy for information security metrics. In: Proceedings of the ACM Conference on Computer and Communications Security, pp. 28–30 (2007)
24. Schmid, M., Pape, S.: A structured comparison of the corporate information security maturity level. In: Dhillon, G., Karlsson, F., Hedström, K., Zúquete, A. (eds.) SEC 2019. IAICT, vol. 562, pp. 223–237. Springer, Cham (2019). https://doi.org/10.1007/978-3-030-22312-0_16
25. Schmitz, C., Pape, S.: LiSRA: lightweight security risk assessment for decision support in information security. Comput. Secur. **90** (2020)
26. Syamsuddin, I., Hwang, J.: The application of AHP to evaluate information security policy decision making. Int. J. Simul. Syst. Sci. Technol. **10**(4), 46–50 (2009)
27. Vinet, L., Zhedanov, A.: A 'missing' family of classical orthogonal polynomials. J. Phys. A Math. Theor. **44**(8), 16 (2011)