Prioritizing Information Security Controls: An Evaluation of Human Factors

Michael Schmid[a,b]

michael.schmid@m-chair.de

Sebastian Pape[a,c,*]

sebastian.pape@m-chair.de

[a]*Chair of Mobile Business & Multilateral Security*
Goethe University Frankfurt, Germany
[b]*Deutsche Lufthansa AG*
[c]*Social Engineering Academy (SEA) GmbH*

Abstract

While security management systems are not new [1], they recently received widespread attention fostered by regulations: e. g., the general NIS2 Directive [2] requires organizations to introduce information security management systems (Article 21.1 and 21.2 (a)) and the domain specific UN regulation 155 [3] requires automotive companies to introduce cybersecurity management systems. The security management systems have the goal to manage and improve security which is also required in the NIS 2 Directive (Article 21.2 (f): assess the effectiveness of cybersecurity risk-management measures). However, to do so, security needs to be measurable. A common approach to do so is to have a list of objectives, respectively controls, often from standards such as ISO/IEC 27001:2013 [4] and assess to which degree they are fulfilled.

To determine the overall security level of an organization, the different objectives, respectively controls, are weighted by their importance and an overall weighted score is derived. The weights can be derived individually for an organization or for a specific domain, such as sectors of critical infrastructure, automotive or e-commerce (e-commerce is in the scope of NIS2 Directive as

*Corresponding author

Preprint not peer reviewed

This preprint research paper has not been peer reviewed. Electronic copy available at: https://ssrn.com/abstract=5143868

a digital provider) organizations. The latter allows a comparison of different organizations within a domain. The quality of security maturity level assessments of security objectives, respectively controls, has already been studied [5]. However, the quality of experts' assessment of importance (weights) for security objectives, respectively controls, or groups of them has not been sufficiently investigated yet.

In this paper, we investigate the reliability of determining weights on the basis of the controls of ISO/IEC 27001:2013. In particular, we examine the experts' capabilities to assess the importance of security controls individually compared to group discussions. For this purpose, we ran an experiment where experts from the e-commerce domain had to assess and discuss priorities for two selected ISO/IEC 27001:2013 control groups.

Our key result is that the individual assessments have a huge deviation while the results from the groups discussions share the same tendency. Based on qualitative feedback, we provide guidance how to optimize the assessment of the weight.

Keywords: `security metric, security controls, measuring security, domain specific weights, security management system, human factor`

---

1. Introduction

Managing information security is as important as managing the core of the business itself. This has also been recognized by regulators resulting in laws requiring measures to manage and improve information/cyber security, i. e. the NIS 2 Directive [2] targeting critical infrastructure, but also domain specific regulations such as UN regulation 155 [3] for the automotive domain. One shared measure of the above-mentioned regulations and many others is the introduction of a information/cyber security management system. This is accompanied by legal and audit institutions which expect every organization to comply with certain rules when implementing them. Therefore, building and implementing effective information security infrastructure is one of the priorities for most

Preprint not peer reviewed

This preprint research paper has not been peer reviewed. Electronic copy available at: https://ssrn.com/abstract=5143868

business organizations.

In the event that companies or organizations (have to) address the topic of information security governance, they very often fall back on proven and established norms and standards. These norms and standards very often consist of a collection of best-practice methods and requirements to achieve a certain level of security (whatever that may mean in the eye of the beholder). This is usually achieved through various types of controls. These controls guide the company towards the desired level or to achieve compliance. The structure of these controls is similar in many standards (see [6] and [7]), mostly structured hierarchically. In most companies, the assessment of these controls is the responsibility of experts, either in their own area or in information security, or ideally in both.

These assessments, either by the organizations' internal experts or by external auditors assessing the fulfillment of regulations have in common that they are done by humans. As a consequence, there may be deviations between the assessments of different assessors or even between the assessments of the same assessor at different times – even if the security level of the organization stays unchanged. In either case, it is desirable that the assessors' judgments are consistent and reliable. The human factor of security maturity levels assessments has already been investigated [8, 9] with mixed results.

However, there is another dimension of the human factor. These assessments refer directly or indirectly to the organizations' assets. Since each organization has an individual set of assets, it is necessary to prioritize the different controls, i. e. controls referring to none existing assets can be assigned a low priority while those referring to assets which are essential for business continuity should be prioritized. The prioritization is a basis for improving an organization's security level as one would want to target the effort on the controls where the investment has the strongest effect. The prioritization can be done individually for each organization, but it is also common to have priorities for specific domains, such as specific sectors of critical infrastructure (see NIS2 Directive [2]), automotive (see ISO/SAE 21434 [10]) or e-commerce (see ISO 32111:2023 [11]). The assump-

Preprint not peer reviewed

This preprint research paper has not been peer reviewed. Electronic copy available at: https://ssrn.com/abstract=5143868

tion is that organizations within a domain are similar since their assets share a similar structure. Additionally, a common prioritization of controls would allow the comparison of organizations' security level within a domain.

Analogous to the security assessments, these priorities should be defined by experts in a reliable way. In order to investigate the reliability and challenges of determining priorities for a specific domain, we have conducted an experiment with 10 experts from the e-commerce domain. They had to assess the priorities for the e-commerce domain on the basis of the controls of ISO/IEC 27001:2013. After doing their assessments individually, we invited the experts to two focus groups and asked them to discuss their results, to come up with a common assessment and state the challenges and possible improvements for this task. This allowed us not only to compare the experts individual results, but also the results of the two focus groups as team assessments.

The remainder of this paper is structured as follows: Section 2 provides background and reviews related work. Section 3 introduces the methodology of our research. Section 4 describes the results of our experiment along with a discussion in Section 5. Section 6 concludes the work. The questionnaire and further results can be found in the appendix.

2. Background and Related Work

The background section covers how the importance of controls is dealt with, how experts assess this and whether experts can agree on the importance of controls. This is followed by the related work, which reflects the state of research in this field.

2.1. Background

In order to manage information security within an organization, it is important to be able to evaluate it (from different perspectives). There are many different norms/standards with a different focus: e. g., ISO/IEC 27001:2013 [4]

Preprint not peer reviewed

This preprint research paper has not been peer reviewed. Electronic copy available at: https://ssrn.com/abstract=5143868

covers information security risk assessment and information security risk treatment processes; ISO/SAE 21434 [10] covers how to build a security management system to fulfill UN regulation 155 [3]; ISO 32111:2023 specifies security measures for transaction assurance in e-commerce. Furthermore, there exist frameworks (e. g. Capability Maturity Model (CMM) [12], COBIT [13]) and best practice approaches (e. g. ITIL) to deal with compliance [14].

This compliance must in the other hand be proven in other regulatory contexts such as NIS2 Directive [2]. Most of them (except best practice) work with a high level structure of controls to assess compliance in information security [6]. This is comparable to other areas, e.g. (IT-)auditing, which follow similar approaches [15]. Information security controls are measures taken to reduce information security risks such as information systems breaches, data theft, and unauthorized changes to digital information or systems. These security controls are intended to help protect the availability, confidentiality, and integrity of data and networks, and are typically implemented after an information security risk assessment and thus support compliance (e.g. according to NIS2 Directive). The above standards address their controls generally but without reference to a specific industry. This means that the evaluation of the controls with regard to their protection goals takes place without consideration of the respective specifics of the industry.

All controls are equally weighted and do not differ in their importance. This means that access, procedural, technical and compliance controls are treated equally in terms of weighting or importance. This has not yet been sufficiently investigated in the field of information security and this paper will be able to make a modest contribution to this. Another aspect in this context is the fact that almost all controls (except for a few technical controls) are (or sometimes have to be) assessed by people/experts. This per se leaves room for interpretation [16]. This raises the question of how this human judgment by the experts appears to the importance of these controls. The weighting of information security controls by individual experts and whether experts agree among themselves on the importance of controls has not yet been investigated. In order to inves-

Preprint not peer reviewed

This preprint research paper has not been peer reviewed. Electronic copy available at: https://ssrn.com/abstract=5143868

tigate this, an experiment was conducted in the context of this paper that will provide insights into the importance of controls.

2.2. Related Work

The challenge of establishing the importance of controls exists in many different areas [17]. Oliveira et al. investigated uncertainty in decision-making in small and medium sized enterprises (SMEs) national and international equally. Their results showed that especially in the international environment, uncertainty in decision-making processes is of crucial importance due to the respective use of control.

The approaches to this challenge are very different and mostly use prioritization and evaluation procedures [18]. Aldya et al. examined the effectiveness of controls using the ISO/IEC 27004:2013 and ISO/IEC 27001:2013 standards, focusing more on the methods used to measure effectiveness and leaving out the importance of controls. They found that specific and appropriate metrics are needed to measure the effectiveness of controls.

On the other hand, Neubauer et al. [19] investigated the effectiveness of ISO/IEC 27001:2013 controls. They investigated a method that enabled decision makers to select the optimal controls for them from the ISO standard. For this purpose, they used the ontology-based determination of security controls based on the security relationship model presented in the National Institute of Standards and Technology Special Publication 800-12 for this purpose. However, this approach completely excludes the industry context in which the company is located.

Tariq et al. [20] used different methods in SMEs to prioritize the controls of ISO/IEC 27001:2013. The Fuzzy Technique for Order of Preference by Similarity to Ideal Solution (TOPSIS) was applied which performed a linguistic evaluation of the answers of interviewed experts to prioritize the controls.

These procedures use the comparison as input in order to make the assessment and to reach a decision. Ahonen-Jonnarth et al. [21] investigated the importance of criteria in the context of decision-making. For this purpose, the analytic hierarchy process (AHP) was used to determine the importance of criteria among

Preprint not peer reviewed

This preprint research paper has not been peer reviewed. Electronic copy available at: https://ssrn.com/abstract=5143868

decision-makers through a pairwise comparison for this purpose. In order to achieve this, subjects were asked to perform a multi-stage experiment with the AHP. It was shown that the subjects reached a decision or agreement based on the pairwise comparison of the criteria. This experiment was independent of specific controls.

Briliyant et al. [22], on the other hand, applied the AHP approach to the control selection process (of ISO/IEC 27001:2013) in a gap analysis in the planning phase of an Information Security Management System (ISMS). They used the hierarchical structure of the ISO standard to map the controls as criteria of the AHP. As a result, they prioritized the importance of the controls according to the gap analysis. The case study also lacked a reference to the industry in which the company operates.

Sengupta [23] deals with the (in)dependencies of the controls within an ISO/IEC 27002:2013 standard. He examines the ISO standard itself to see whether, and if so how, the controls are inter-dependent. In doing so he categorizes the controls and examines them with regard to their (in)dependence on each other. This can provide indications of how important a control is in relation to other controls.

It appears from the literature reviewed that overall the importance of controls is a relevant issue and that the industry reference has not been sufficiently investigated so far. There are different approaches with various prioritization and evaluation procedures. Furthermore, it can be seen that the tools of Multiple Criteria Decision Analysis (MCDM) are very well suited to determine the priority and thus the importance of controls. The AHP seems to be an excellent tool for this. In the area of information security, the ISO standard ISO/IEC 27001:2013 is used almost exclusively, which is ideally suited for the AHP due to its hierarchical structure. To the best of our knowledge, the importance of information security controls within an industry focus has not yet been investigated in the literature.

Preprint not peer reviewed

This preprint research paper has not been peer reviewed. Electronic copy available at: https://ssrn.com/abstract=5143868

3. Research Methodology

To examine the experts' capabilities to assess the importance of information security controls, it is necessary to take a closer look at the experts' assessments. For this purpose, an experiment was set up in which the magnitude of the lack of reliability was measured. The setup of the experiment was divided into two stages. First, experts were asked individually about the importance of the information security controls concerning a specific industry. This serves to obtain an initial assessment of how experts generally assess the importance of information security controls. Second, focus groups were gathered out of these experts and the experts were asked to jointly discuss and assess the importance of the controls. This makes it possible on the one hand to compare the individual assessments of the experts in order to recognise similarities and differences and on the other hand to discuss the reasons for the assessment of the individual experts with each other. Based on this discussion, if there are differences in the assessment of the importance of information security controls among the experts, it is possible to examine whether experts can agree on a common assessment. Figure 1) shows an overview of the two steps in the experiment.

We describe first, how the experiment was setup, e. g. suitable controls must be identified for the comparison of importance and suitable experts needed to be identified and invited to participate in our study. In the following subsections, we describe how the experiment was conducted (cf. Sect. 3.2) and how we analyzed the results (cf. Sect. 3.3).

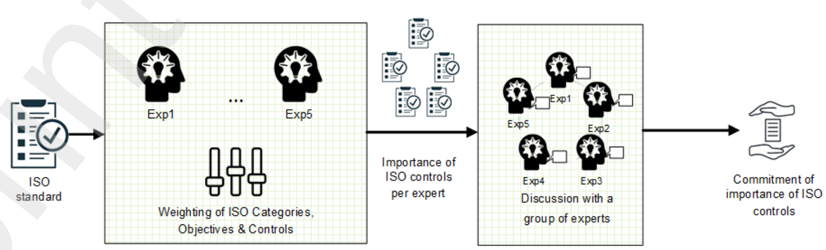

Figure 1: Procedure of the experiment

Preprint not peer reviewed

This preprint research paper has not been peer reviewed. Electronic copy available at: https://ssrn.com/abstract=5143868

3.1. Experiment Setup

In the following, it is described how the experiment was set up. However, an exempt status was obtained from the institutional ethics review board (IRB) prior to conducting the experiment with the experts. It was confirmed by the IRB that in particular all experts participated voluntarily, all experts knew how the experiment was conducted, and all experts were aware that they could drop out of the experiment at any time. Thus, according to the rules of the IRB, the research project was eligible for an exempt status, which was confirmed by the IRB and no full ethical review was needed. The data of the experiment was stored encrypted on a German server with ristricted access rights only for the authors. The personal identifiable information (pii) of the participants was reduced to a minimum and are subject to the restrictions of the General Data Protection Regulation (GDPR). The participants' pii was largely omitted from the experiment. The preparatory survey was conducted anonymously and the pii was only known to the moderator. After successful analysis, all participant data was deleted.

3.1.1. Control Selection

In order to investigate the importance of controls, it is essential to find controls that are known by a large majority in the respective domain. In this particular case, controls that are established for the information security domain have been used. Many different standards and frameworks are available providing guidance to correctly implement and maintain information security. The most popular standard in this environment is ISO/IEC 27001:2013 (incl. ISO/IEC 27002:2013). It contains guidelines for organizational information security management practices including the selection, implementation and management of controls, taking into consideration the organization's information security risk environment(s) [4]. The controls of the 27001-standard are hierarchically structured and divided into 14 control categories. These control categories are further subdivided into control objectives and finally into individual controls. The individual controls address different areas of information

Preprint not peer reviewed

This preprint research paper has not been peer reviewed. Electronic copy available at: https://ssrn.com/abstract=5143868

security, e. g. organizational, technical, legal, physical, etc. This is an ideal approach to understanding the importance of controls in an organization. This is desirable for comparing the importance of controls in a control category or objective. Overall, the ISO/IEC 27001:2013 standard has a holistic approach and is very comprehensive with 114 individual controls.

However, requiring the experts to do a full assessment, followed by a discussion about all individual controls would require them too much time. Thus, it is necessary to limit the number of controls in order to reduce the effort for the experts and to prevent a drop in concentration from impacting on the results due to the number of comparisons that have to be made (see [24]) for the experiment. It is important that a representative comparison of the importance of controls of the 27001-standard is still possible despite the control reduction. Looking at the distribution of the different types of controls (see figure 2), it quickly becomes clear that almost ¾ of the controls focus on the technical and organisational area of information security. This distribution is also found in other standards and best practice approaches (see [25]).

In order to apply this distribution to a control selection in a representative manner and not to overwhelm the experts with the range of expertise, the control category A.6 'Organization of information security' with 7 single controls is suitable for the organizational area (in order to establish a management framework for initiating and controlling the implementation and functioning of information security within the organization) and A.14 'System acquisition, development and maintenance' with 13 single controls for the technical area (covers controls for the identification, analyses, and specification of information security requirements, securing application services in development and support processes, technical review restrictions on changes to software packages, secure system engineering principles, secure development environment, outsourced development, system security testing, system acceptance testing and protection of test data). The two control categories reflect the distribution of controls from the two areas (technical and organisational) as well as a certain reduction in the total number of controls.

Preprint not peer reviewed

This preprint research paper has not been peer reviewed. Electronic copy available at: https://ssrn.com/abstract=5143868

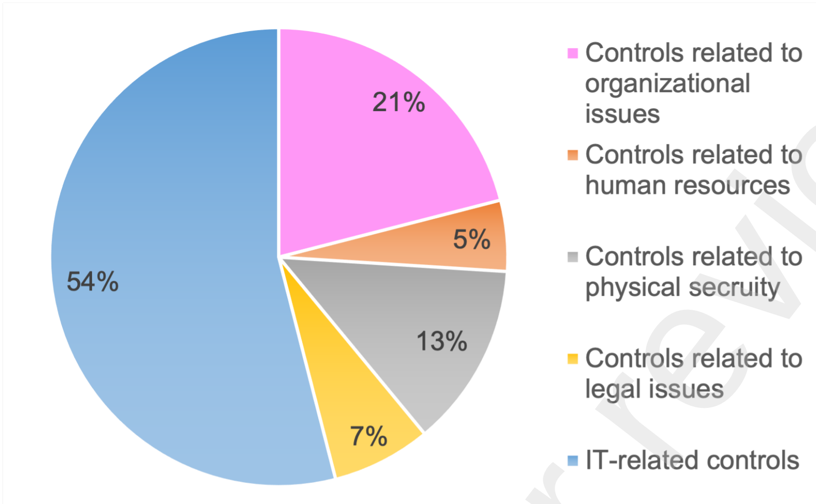

Figure 2: Breakdown of ISO/IEC 27001:2013 Controls

3.1.2. Judgement Comparison

Evaluation and prioritization procedures are needed to find out if experts agree on the importance of controls. The importance of the controls corresponds to the prioritization. The expert prioritize the controls with the help of a weighting. This has the advantage that the results are also comparable with other expert weightings and prioritization.

Taking all requirements into account, this is a multi-dimensional decision problem, and thus can be addressed by a multiple-criteria decision analysis method (MCDM). The comparison criteria (dimensions) are the ISO/IEC 27001:2013 controls and they compare the different expert judgments with their corresponding importance 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 per-

Preprint not peer reviewed

This preprint research paper has not been peer reviewed. Electronic copy available at: https://ssrn.com/abstract=5143868

sonal preferences through pairwise comparisons. The AHP has been the most widely used technique of multi-criteria decision making during the last twenty five years (see [26]). 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 27001:2013 controls' hierarchy and the qualitative evaluation part of the AHP is very much in line with the importance of the controls for information security. Since the AHP compares the importance of each control expert-wise, it naturally allows the understanding of where each expert-importance ranks in relation to each control (see figure 3). Additionally, the weight of each criteria (control) can be easily derived. In the concrete case it is possible to compare the importance of individual controls of ISO/IEC 27001:2013 from each expert very granularly with each other (pairwise).

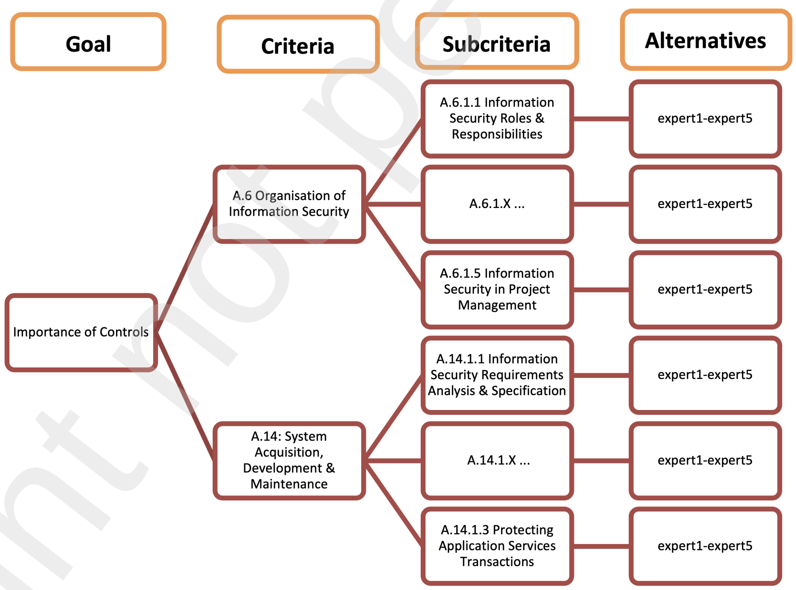

Figure 3: Decision hierarchy ISO/IEC 27001:2013 for expert judgments

The AHP's comparison is done as follows: The result of a pairwise comparison of two criteria entered in the evaluation matrix shows how much more important a criteria is in relation to the criteria of the level above (refer to the

Preprint not peer reviewed

This preprint research paper has not been peer reviewed. Electronic copy available at: https://ssrn.com/abstract=5143868

Table 1: Fundamental 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

scale in table 1). In order to make a comparison for one criteria, i.e. the control category, the individual control categories are compared with each other. A score of 1, for example, means both criteria are of equal importance. When a criterion is compared to itself, its relative importance is 1, because the criteria being compared are the same. Larger numbers show a criterion is increasingly more important, with 9 being the highest score.

If this prioritization procedure AHP is applied to the selected controls (see Section 3.1.1) of the 27001-standard, the following comparisons are made:

- Control Categories A.6 and A.14
- Control Objectives of A.6 (A.6.1 and A.6.2)
- Controls of A.6.1 and A.6.2
- Control Objectives of A.14 (A.14.1, A.14.2 and A.14.3)
- Controls of A.14.1, A.14.2 and A.14.3

The number of pairwise comparisons increases with the number of criteria. Overall, the experts have to perform 52 comparisons of the importance of controls, which represents a good cross-section of the complete 27001-standard.

Preprint not peer reviewed

This preprint research paper has not been peer reviewed. Electronic copy available at: https://ssrn.com/abstract=5143868

3.1.3. Sampling and Demography of Experts

The help of experts is needed to tackle the research question. These experts should be familiar with the prevailing domain of information security and in a best case scenario familiar with ISO/IEC 27001:2013. To conduct the experiment with the quality of these experts, it is necessary to find experts who have this degree of experience. To ensure this, the experts should represent an assortment of employees as well as information security consultants, auditors and scientific advisors. They should have many years of experience in the information security sector as well as an expertise in technical and organizational aspects.

Furthermore, it would be appropriate for the experiment that the experts have industry knowledge. This industry knowledge is important to establish a common basis for comparing the importance of controls.

Each industry has specific information security challenges and requirements that emphasize its dependence on robust security measures. As a result of the Corona pandemic, some sectors have seen a strong increase in turnover and a growth in the number of customers and employees. This was marked in the e-commerce sector (see [27]) in particular. The challenges of retail and e-commerce have shown that retail companies process a lot of customer data, including payment information. In addition, the security of online transactions is crucial to prevent fraud and identity theft. and customer trust and business reputation can be damaged by security incidents.

In the broadest sense, e-commerce is the marketing of goods and services via the internet. e-commerce provides programs and software for shops, payment processing and professional websites. Web hosting, i. e. the creation and maintenance of an internet presence, is also part of this sector.

The e-commerce sector is, of course, extremely dependent on information security (from various points of view such as availability, confidentiality and integrity) and is, therefore, very well suited for the experiment.

Preprint not peer reviewed

This preprint research paper has not been peer reviewed. Electronic copy available at: https://ssrn.com/abstract=5143868

In order to find participants with these requirements, the relevant associations and organizations related to information security in the e-commerce industry in Germany were contacted and experts with the required profile were found.

The call for the experts was distributed to security practitioners from various organisations between 15 November and 23 December 2020. The call for participation was sent to (chief) information security officers but also to a number of professional mailing lists [1]. Additionally, the call for participation was also distributed in selected professional forums [2].

To ensure that the experiment is carried out with the requirements described above, the experts should have at least 5 years of experience

- in information security and with the ISO/IEC 27001:2013 standard,
- as an information security employee, consultant, auditor or scientific advisor and
- in the e-commerce sector.

The sampling of the experts has been made based on these requirements and led to the following demographics:

- ¾ of the experts had more than 10 years of experience in information security,
- ¾ of the experts had up to 10 years of experience with the ISO controls and
- ¾ of the experts stated that they had more than 10 years of experience

[1] GI-SECMGT (security management working group of the German Informatics Society),UP KRITIS – BAKs (sector-specific working groups for critical infrastructure protection), ERFA CyberSecurityAllianz (experience exchange group of the cybsersecurity alliance), Teletrust, CAST (competence centre for applied security technology), DCSO (german cybersecurity organisation), local chapter of the (ISC)^2 (international information system security certification consortium), newsletters (BSI alliance for cybersecurity (ACS), ISACA (information systems audit and control association) working group Information security and IT risk management)

[2] LinkedIn, XING and COBIT website

Preprint not peer reviewed

This preprint research paper has not been peer reviewed. Electronic copy available at: https://ssrn.com/abstract=5143868

in the e-commerce industry

3.2. Conducting the Experiment

As already sketched in the introduction, the experiment was run in two stages. Individual assessments and focus groups.

Individual Assessments. The individual experts were asked about the importance of controls. Since experts are usually in great demand and have little spare time, it was decided to stick with a survey. This survey was conducted online due to the Corona pandemic. The free online survey application Limesurvey [28] was used to make it as easy as possible for the individual experts. The full survey can be found in the appendix (see Section Appendix A). The first part consisted of questions on some demographic factors such as how many years of experience the experts have in information security, with ISO/IEC 27001:2013 and the e-commerce industry. In the second part, experts were asked to assess the importance of the controls of Control Category A.6 'Organisation of information security' and A.14 'System acquisition, development and maintenance'. The assessment was done by a pairwise comparison of the controls, following the previously described approach of the AHP (cf. Table 1). Through the pairwise comparison the importance of the controls to the individual expert were obtained.

A pre-test was conducted in order to validate the online questionnaire. This pre-test took place in the context of a scientific workshop with an information security background. The pre-test expanded the Limesurvey (LimeSurvey Cloud Version 3.27.19) questionnaire in terms of length, type of questions and hints for tooltips. The pre-test resulted in positive feedback, so only minor changes, e. g. correcting spelling were done.

3.2.1. Focus Groups

Roughly two weeks after the experts were asked to do the individual assessment of the controls, they have been invited to a focus group. The aim of the

Preprint not peer reviewed
This preprint research paper has not been peer reviewed. Electronic copy available at: https://ssrn.com/abstract=5143868

focus group was to discuss the importance of controls following a brief overview of the individual expert opinions already submitted.

There are several methods for conducting discussions among experts. The most suitable method for such an experiment is a focus group (see [29]). A focus group is a form of group discussion that is used, for example, in qualitative social research and market research. It is a moderated discussion of several participants, which is usually based on a guideline. It is also called a partially standardized interview because of the guideline with open questions. The method is based on the principles of communication, openness, familiarity and strangeness as well as reflexivity. Its application is particularly useful in the early development stages of studies in which ideas are being developed, concepts are being created and requirements are to be elicited [29].

The aim was not only to see whether the experts are able to agree on a common assessment and control priorities they agree on, but also to ask them how they managed their assessment of the importance of controls and to discuss with them if there are different opinions within the expert group. If different opinions would show up, the experts would be asked why they assessed the importance of the controls differently and, above all, whether and how all the experts could then agree on a common assessment.

The experts have been divided into two groups with five members each for the focus groups. Again, due to limitations caused by the Covid pandemic, the focus groups were conducted online and (with the consent of the participants) recorded for later evaluation.

At the beginning of each focus group, the experts introduced themselves to each other and presented their past and current field of work. The moderator introduced the topic of pairwise comparison with the help of the AHP and the current setting of the experiment. Before the experts started the discussion, the individual results of the experts were presented. The main part of the focus group time was spent on agreement as a group on the importance of controls. Shortly afterwards, the results of the agreement were presented by the moderator and discussed by the experts. This was followed by a presentation by

Preprint not peer reviewed

This preprint research paper has not been peer reviewed. Electronic copy available at: https://ssrn.com/abstract=5143868

an expert from the group on the topic of information security in the e-commerce sector, which was then discussed in the group. Finally, the experts were asked how they felt about the experiment. Short bio breaks were inserted between the individual sections.

3.3. Evaluation of the Experiment

For the individual assessments, a descriptive statistic was used to show the results. Furthermore, a part of the AHP's algorithms was used to determine priorities for the different controls based on the pairwise comparisons. This was not only done for the comparisons of each expert, but also for the average of each group and the agreement after the expert's discussion in the focus groups. Additionally, some minor statistical tests were run (Shapiro-Wilk test for normal distribution and Wilcoxon rank sum test) to get a better understanding of the results.

The focus groups were on the one hand evaluated by using the agreements the experts came up with (as described in the paragraph before). Additionally, the discussions were screened and the results above the values of the focus groups' agreements were screened and then evaluated by summarizing the participants' statements during the discussions.

4. Conducting the Experiment with the Experts

This experiment involving 10 information security experts from 10 different companies with an e-commerce background. The experts are currently working in various fields of activity (information security staff, consultants and auditors) in the context of information security in their respective companies.
The 10 experts were randomly divided into 2 groups of 5 experts each. On the one hand, this was necessary for organizational reasons and on the other hand, a smaller group size is better for the discussions in the focus groups. The focus group meeting was coordinated with all participants. In preparation for this meeting the Limsurvey questionnaire was sent out 2 weeks in advance

Preprint not peer reviewed

This preprint research paper has not been peer reviewed. Electronic copy available at: https://ssrn.com/abstract=5143868

of the actual meeting. The experts had 2 weeks to complete the Limesurvey questionnaire. This time span gave them sufficient time to finish the survey, but also ensured that the experts were still aware of the questionnaires when the focus groups were executed. The completed questionnaires had been analyzed and evaluated before the actual meeting in order to discuss the results (see Figure 1). The two focus group meetings were held virtually because of the Corona pandemic. The first focus group took place at the end of January and the second focus group end of February 2021. The results of the individual steps of the experiment are presented below.

Section 4.1 deals with the results of the first step of the experiment, the comparison of the individual weighting and ranking (through the pairwise comparison) of the experts. The results of the experts' discussion within the focus groups and the agreement on a common weighting of the importance of controls are then presented in section 4.2.

4.1. Results from the Expert Judgement concerning the Importance of Controls

In order to analyze the results of the experts, the first step is to examine their individual results and compare them with each another with in the defined group.

4.1.1. Pairwise Comparisons

The analysis of the results from the Limesurvey questionnaire was carried out in the statistics program R and plotted as a graph. The figure 4 shows the individual weighting from the pairwise comparison of the controls by each expert. The AHP weightings (Score) are plotted on the Y-axis of the graph and the comparisons made are plotted on the X-axis. The different symbols (circle, square, triangle etc.) represent the individual experts and the agreement within the group of experts (red filled circle). The standard error is represented with a bar for the upper and lower tails as well as the mean (red filled square). For reasons of simplification, the following results are only shown for Control Objective A.6.1, as this can be presented very transparently with 5 controls and 10

Preprint not peer reviewed
This preprint research paper has not been peer reviewed. Electronic copy available at: https://ssrn.com/abstract=5143868

comparisons (which are numbered from left to right). The upper graph represents the result for the first group of 5 experts and the lower one for the second group with also 5 experts. The results of the other control objectives/categories are to be considered equivalent (see Section Appendix B).

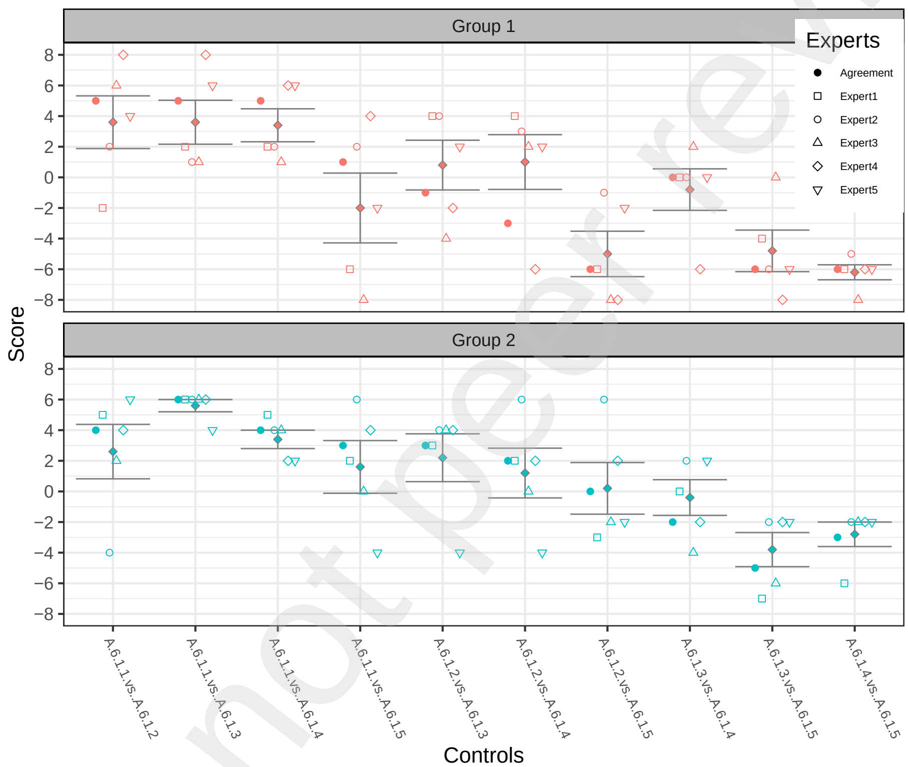

Figure 4: Results of Weighting A.6.1 controls

It can be seen that in some comparisons of the first group there are strong differences between the individual experts, e. g. in the 1st, 4th and 6th comparison, partly over 10 AHP intervals. In contrast, the first group also achieves comparisons in which the differences are not very large, e.g. the 4th and 10th comparison (between 2-4 AHP intervals). Expert4 and partly Expert1 of the first group very often (approx. 8 times) have a different weighting than the remaining experts. In the second group, Expert2 and Expert5 more often (ap-

Preprint not peer reviewed

This preprint research paper has not been peer reviewed. Electronic copy available at: https://ssrn.com/abstract=5143868

prox. 5 times) disagree with the other experts. Differences between the individual experts are not as prominent in this group (maximum 8 AHP intervals) and frequent, e.g. 1st, 5th and 6th comparison. In the second group, the experts are of a similar opinion 3 times (difference here AHP interval 2-3), e.g. 2nd, 3rd and 10th comparison.

We also compared the means of both groups for the control groups A.6.1 (group 1: -0.64; group 2: 0.98) and A.14 (group 1: -0.70; group 2: 0.46). To test for normal distribution, a Shapiro-Wilk test was performed and showed that the distribution of the comparisons departed significantly from normality (A.6.1: $W = 0.945$, p-value < 0.001 A14: $W = 0.968$, p-value < 0.001). Since the comparisons do not follow a normal distribution, we used a non-parametric test, the Wilcoxon rank sum test, to compare the different means. The Wilcoxon test showed that the difference for A.6.1 was only slightly significant (p-value ≈ 0.07), but was highly significant for A.14 (p-value < 0.001).

4.1.2. Weighting and Ranking of Controls

The previous subsection showed that there are some differences in and between the groups related to the pairwise comparisons. However, as it is hard to imagine the different controls' priorities from the pairwise comparison, we ran the first part of the AHP to assess the controls' priorities for each expert, the average (AVG) and the agreement from the focus group as shown in figure 5. It can also be seen that the individual assessments in both groups do not give a clear picture. If at all, one can conclude that in group 1 control A.6.1.5 was always among the top two priorities and in group 2 a similar picture with A.6.1.1 arises. The exact evaluation of the mean pairwise comparisons are shown in Table 2. Regarding the three remaining controls (A.6.1.2, A.6.1.3 and A.6.1.4), the two groups have a similar or almost equal ranking results (also similar weighting values).

Figure 6 shows the experts individual assessments with a focus on the rank for each control. The number (and coloring) shows how often a certain control was ranked on the given position. We have marked the result from each group's

Preprint not peer reviewed

This preprint research paper has not been peer reviewed. Electronic copy available at: https://ssrn.com/abstract=5143868

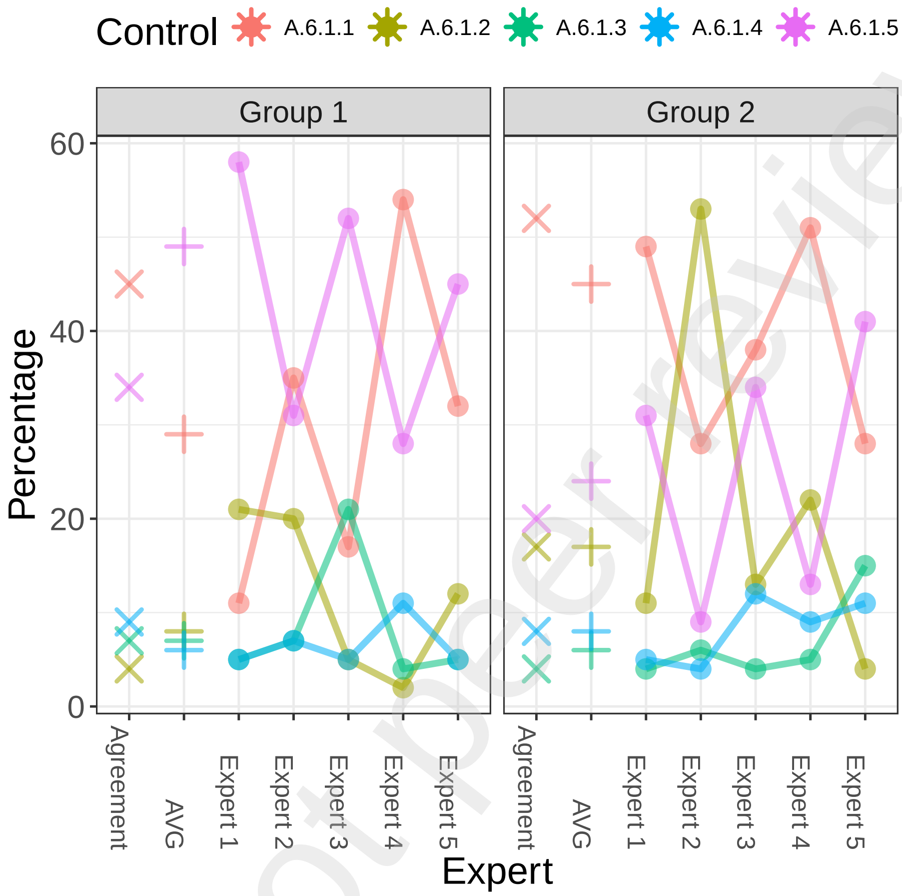

Figure 5: Percentage A.6.1 controls

average with a red/cyan "x", and we marked the result of the agreement within the focus groups with a red/cyan "+".

4.1.3. Expert Judgement Conclusion

If the experts' results on the weighting and ranking of controls are compared with each other, it can be seen that each expert has a slightly different picture of the importance of controls (see figure 4). These differences are generally greater for some controls (e. g. A.6.1.1 and A.6.1.5) than for others (e. g. A.6.1.2 and A.6.1.3) as shown also in figure 5.

Preprint not peer reviewed

This preprint research paper has not been peer reviewed. Electronic copy available at: https://ssrn.com/abstract=5143868

Table 2: Results of Ranking A.6.1 Controls (AVG)

	Focus Group 1		Focus Group 2	
Criterion	Weights	Rank	Weights	Rank
A.6.1.1	28.8%	2	42.4%	1
A.6.1.2	10.4%	3	17.2%	3
A.6.1.3	7.7%	4	6.7%	5
A.6.1.4	7.0%	5	8.6%	4
A.6.1.5	46.1%	1	25.1%	2

This is also reflected in the ranking of the controls among each other (see figure 6). The experts in the focus group were asked how they could explain these fluctuations in the individual results. One expert reported *«a very strict interpretation of the controls»*, another referred to the *«evidence from his daily work»* and another expert mentioned *«difficulties in prioritizing the individual controls»*.

4.2. Agreement among Experts on the Importance of Controls

In this section, we discuss the result from the two focus groups. The focus group meetings were prepared based on the evaluation of the Limesurvey questionnaire. A major part of these meetings was to discuss the results of the Limesurvey questionaire with the experts. The discussion was intended to achieve a better understanding of the decision regarding the importance of controls and whether it is possible for a group of experts to agree on the importance of controls.

In order to achieve this goal, each of the focus groups discussed each pairwise comparison of controls. These comparisons per focus group are shown in figure 4 as the red or cyan filled circle for the agreement as discussed in Section 3.2.1. The results are also shown in figure 5 and figure 6 as already described.

The discussion among the experts was very much characterized by collaborative and homogeneous style. None of the experts was particularly dominant

Preprint not peer reviewed

This preprint research paper has not been peer reviewed. Electronic copy available at: https://ssrn.com/abstract=5143868

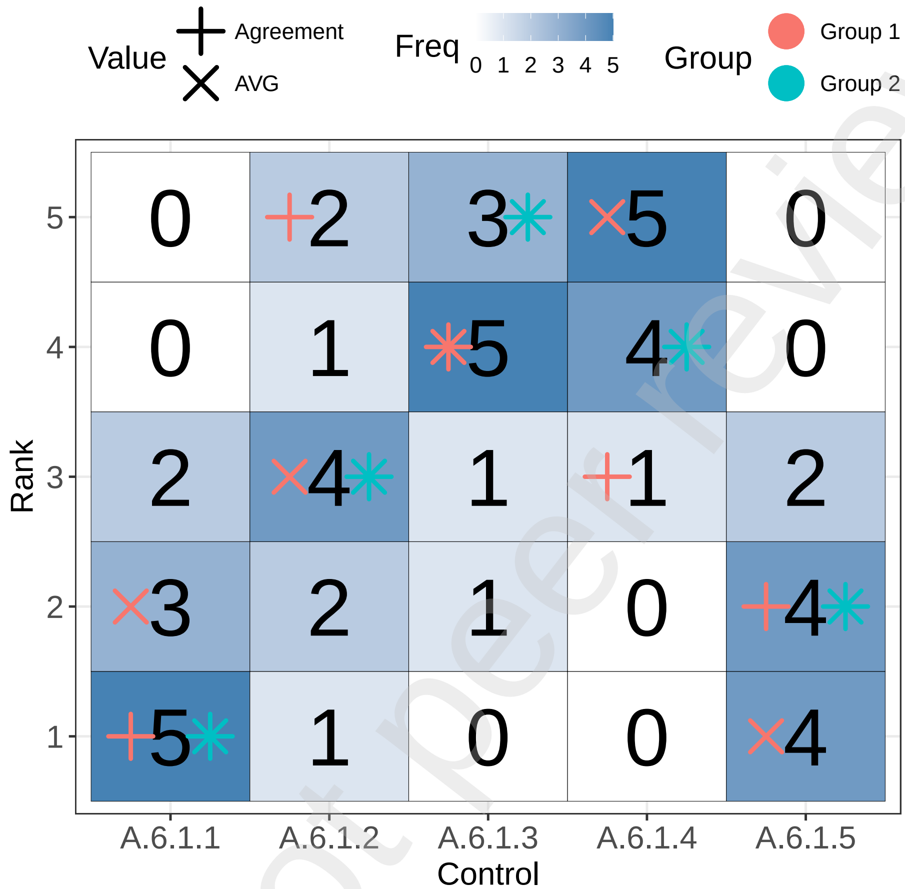

Figure 6: Heatmap Rank A.6.1 controls

or tried to strongly convince the other experts of their opinion. As the results show, the experts were able to agree on an equal weighting of the controls. The agreement among the experts means that the experts were able to agree on the importance of information security controls by means of an AHP scale through discussion within the focus group. In focus group 1, the agreement is sometimes closer to the individual results of the experts (e.g. the 2nd, 3rd and 10th comparison) and sometimes a little further away (e. g. the 4th and 6th comparison). There the experts were able to agree on the importance of the controls, although the individual results were very scattered. Considering the

Preprint not peer reviewed

This preprint research paper has not been peer reviewed. Electronic copy available at: https://ssrn.com/abstract=5143868

discussion of the experts for the 6th comparison (A.6.1.2 vs. A.6.1.4), the argument of one expert was able to change the minds of the other experts *«if the 'Segregation of duties' (A.6.1.2) works, then this control is more important than the 'Contact with special interest groups' (A.6.1.4)»*. In this comparison, all experts had come closer to the individual result of Expert4. The other experts said *«that they were convinced by the argumentation of one expert»*. In the 8th comparison it was the other way round, most experts agreed on the importance of the controls (A.6.1.3 vs. A.6.1.4). The Expert4 stated *«that they had agreed in the middle through the discussion»*.

In the focus group 2, most agreements are within or slightly outside the standard error (e.g. 2nd, 3rd and 10th comparison). There are only a few agreements are outside the standard error (e.g. 8th comparison). It is noticeable that Expert3 and Expert5 are almost always very far from the agreement with their individual opinions. The two experts were asked about this and both said that *«they had assessed the importance of the controls differently, but were convinced by the arguments of the other experts»*.

The more homogeneous picture of focus group 2 can be confirmed as the agreement of the focus group does not differ much from the evaluation of the average pairwise comparisons (AVG). On the other hand, the agreement in focus group 1 looks slightly different from the average of the pairwise comparisons. While the top2 and the bottom3 controls are clearly seperated, their order is changed an in particular for the top2 controls (A.6.1.1 and A.6.1.5) there is a huge gap. However, for both groups there seems to be an agreement that these two are the most important controls in this group (cf. figure 5).

Considering the ranking of the agreement from the two focus groups resulting from the weighting (see Table 3), focus group 1 switched the ranking of Control A.6.1.1 (now the first rank) with A.6.1.5 (the second rank). The ranking of the other controls (A.6.1.2, A.6.1.3 and A.6.1.4) changed the order.

For focus group 2 the ranking has not changed, there were only slight changes in the weighting. For them Control A6.1.1 is still the most important control ahead of Control A.6.1.5. The ranking of the other controls (A.6.1.2, A.6.1.3

Preprint not peer reviewed

This preprint research paper has not been peer reviewed. Electronic copy available at: https://ssrn.com/abstract=5143868

and A.6.1.4) also did not change.

Table 3: Ranking A.6.1 controls for the agreement

	Focus group 1		Focus group 2	
Criterion	Weights	Rank	Weights	Rank
A.6.1.1	45.5%	1	52.6%	1
A.6.1.2	4.3%	5	16.1%	3
A.6.1.3	7.2%	4	4.0%	5
A.6.1.4	9.5%	3	7.7%	4
A.6.1.5	33.4%	2	19.6%	2

Both focus groups concluded that Control A.6.1.1 was the most important and Control A.6.1.5 the second most important, although with varying degrees of weighting.

In direct comparison, it can be seen that both focus groups have slightly aligned themselves in terms of symptoms (decreasing importance of controls within a control objective).

Figure 4 and table 3 show very clearly a conditional dependency of the controls within a control objective. According to the experts, the first controls of a control objective are more important than the following controls (execpt A.6.1.5 in this case) in the control objective.

5. Discussion

The results of the experiment to determine the importance of controls with the help of experts clearly show the challenges in this environment. It indicates that it is difficult for the individual but that a joined assessment could balance that out. When each expert did the assessment on his/her own the results were different from having experts evaluate the importance of controls as a team. The results of the agreement from the experts within a focus group have shown that it is possible, even in groups with differing individual assessments, to agree

Preprint not peer reviewed

This preprint research paper has not been peer reviewed. Electronic copy available at: https://ssrn.com/abstract=5143868

on the weighting. This indicates that experts should work together to determine the importance of controls.

The experts' results allow different conclusions to be drawn with regard to the importance of controls. On the one hand, the experts individually assessed the importance of the controls differently, on the other hand, a group/team of experts can very well agree on a common denominator for the importance of controls. This is especially evident from the discussions among the experts in the focus groups. The experts are *«satisfied with the result (the agreement), although they personally disagreed at first»* and said that *«the discussion contributed to their understanding»*.

Hence the experts might have performed better if they had individually evaluated a real world scenario instead of a hypothetical one.

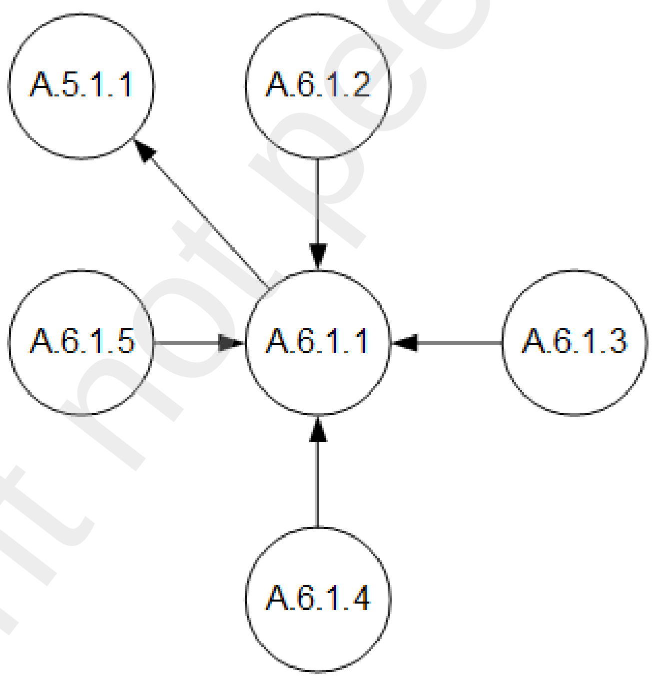

Figure 7: Visualisation of the A.6.1 Control Object dependencies

The results also show that the importance of controls within a control objective follows a certain dependency. The first control in the control object is more

Preprint not peer reviewed

This preprint research paper has not been peer reviewed. Electronic copy available at: https://ssrn.com/abstract=5143868

important than the following controls. This, that has already been investigated by Sengupta [23], that there are dependencies for controls. For example, for control objective A.6.1, according to Sengupta, controls A.6.1.2, A.6.1.3, A.6.1.4 and A.6.1.5 all refer to control A.6.1.1 (see figure 7). This can also be seen in the results in the ranking of table 3 (except A.6.1.5 in this case) and thus confirms the studies by Sengupta whereby he does not deal with the sectoral reference.

Furthermore, according to the experts, the results of the comparison are strongly influenced by the perspective from which the sectors are viewed. The experts mentioned several times that they are aware of the importance of controls within an industry. In their opinion, the importance of the controls depends strongly on the industry reference. One expert referred in the discussion *«to the automotive industry, which has a central office for the topic of information security in which the ISO controls are already selected for the sector according to their importance»*. According to another expert, this would *«also be helpful for other sectors such as e-commerce»*.

The qualitative feedback from the experts suggested using different approaches in order to support an improvement during the assessment. According to the experts to keep the structure of the ISO standard, the detailed description of the controls and the control hierarchy alongside would be helpful in assessing the importance of controls.

5.1. Limitations

A general limitation of this kind of experiment is the self-selection bias since the experts who decided to participate in the experiment might not be a representative sample of all experts. This can lead to biased results.

Furthermore, group discussions show a tendency to avoid dissent, often at the expense of a critical examination of alternative perspectives. There is a strong desire for harmony and agreement. It can lead to members suppressing dissent or censoring themselves in order to avoid conflict and maintain group unity, which is also a limitation.

Another limitation is the number of experts. A higher number of experts

Preprint not peer reviewed

This preprint research paper has not been peer reviewed. Electronic copy available at: https://ssrn.com/abstract=5143868

would make it possible to measure smaller effects, which might influence the experts' ability to assess the importance of controls as well. Besides the total number of participants, also the high number (¾) of experts with more than 10 years experience with ISO controls in the e-commerce industry could also have led to non-representative results.

Apart from that, the results are only valid for the German market since the experts were all German. The results might be different with experts from other countries, who are more or less familiar with the e-commerce industry and with the ISO/IEC 27001:2013 controls.

Schmitz et al. [5] showed that the assessment capability is higher when experts assess a real setting e. g. with their own organisation. It might be possible to transfer that result in the way that it might have been easier for the experts to compare the different controls with regard to their own organization instead of aiming to do the comparison for the whole e-commerce domain.

In addition a limitation of the experiment was also the duration of the discussion that led to the agreement. The expert discussion decisions took approximately 5 minutes per agreement. For the Control Category A.6 thus the experts required 60 minutes (for 12 comparisons). Due to the limited resources of the experts, it was therefore not possible to discuss the complete Control Category A.14. This would have taken at least 180 minutes (with 36 comparisons). The experts commented on the time required for the discussion that *«it was only 5 minutes of discussion, but very intensive»* and *«when several comparisons are discussed one after the other you have to concentrate a lot»*. That means, that the results for a 3 hour discussion on control group A.14 would most likely have been biases by the experts' exhaustion or would have needed to be done in several rounds which would have induced other effects.

6. Conclusion and Future Work

Do experts agree on the importance of ISO/IEC 27001:2013 controls for a specific industry? In order to answer this question, it was necessary to ask the

Preprint not peer reviewed

This preprint research paper has not been peer reviewed. Electronic copy available at: https://ssrn.com/abstract=5143868

experts from a specific industry individually and to discuss these results with the experts in order to have a common understanding of the importance of controls.

However, these assessments are carried out by humans, and thus the 'human factor' of the evaluation may lead to possible uncertainties and subjectivity, i. e. because a pool of experts with different physical and mental conditions working on separate days was involved.

The main goal of the paper was to examine the experts' capabilities to assess the importance of security controls. In contrast to other studies, the agreement between the experts concerning the importance of security controls following the involved standard ISO/IEC 27001:2013 had a focus to the related industry.

It has been shown that, when experts have to evaluate the importance of controls individually, the results can be quite different for a specific industry. Furthermore, it was shown that experts from the same industry can agree on a common level of importance of controls. Even if the average is taken from the individual answers of the experts, it does not equal the agreement. The result confirms the design decision and the need to compare the experts' assessments to a joint agreement and not only to each other.

We can derive the recommendation that if an industry standard regarding the importance of information security controls had to be published, then it should be established by consensus of several experts working as a team in this specific industry.

A further advantage of this approach is that it is applicable to other industries and standards (e. g. NIST, ISO standards etc.) that have a similar high level structure.

In future work, larger sample with more experts and other sectors could, on the one hand, reduce the uncertainty of the assessments and, on the other hand, show that the study design is also valid for other sectors. As this ties up a lot of resources (time and experts), it might also be useful to clarify whether it makes a difference to first interview the experts individually and then for them to discuss them as a whole, or whether it is sufficient to discuss the importance of the controls directly in the group.

Preprint not peer reviewed

This preprint research paper has not been peer reviewed. Electronic copy available at: https://ssrn.com/abstract=5143868

Acknowledgements

This work has received funding from the European Union's Horizon Europe programme under Grant Agreement No. 101070586 (PHOENI2X project [30]).

References

[1] G. Disterer, Iso/iec 27000, 27001 and 27002 for information security management, Journal of Information Security 4 (2) (2013). doi:10.25968/opus-938.

[2] E. Parliament, Council, Directive (eu) 2022/2555 of the european parliament and of the council of 14 december 2022 on measures for a high common level of cybersecurity across the union, amending regulation (eu) no 910/2014 and directive (eu) 2018/1972, and repealing directive (eu) 2016/1148 (nis 2 directive) (text with eea relevance)text with eea relevance (2022).
URL https://eur-lex.europa.eu/eli/dir/2022/2555

[3] U. N. E. C. for Europe, Un regulation no 155 – uniform provisions concerning the approval of vehicles with regards to cybersecurity and cybersecurity management system [2021/387] (2021).

[4] ISO/IEC 27001 information technology – security techniques – information security management systems – requirements (2013).

[5] C. Schmitz, M. Schmid, D. Harborth, S. Pape, Maturity level assessments of information security controls: An empirical analysis of practitioners assessment capabilities, Computers and Security 108 (2021) 102306. doi:10.1016/J.COSE.2021.102306.

[6] A. A. N. Al-shameri, Hierarchical multilevel information security gap analysis models based on ISO 27001:2013, International Journal of Scientific Research in Multidisciplinary Studies 3 (2017) 14–23.

Preprint not peer reviewed

This preprint research paper has not been peer reviewed. Electronic copy available at: https://ssrn.com/abstract=5143868

[7] K. Beckers, I. Côté, S. Fenz, D. Hatebur, M. Heisel, A structured comparison of security standards, 2014, pp. 1–34.

[8] A. Ramos, M. Lazar, R. H. Filho, J. J. Rodrigues, Model-based quantitative network security metrics: A survey (2017).

[9] C. Schmitz, S. Pape, Lisra: Lightweight security risk assessment for decision support in information security, Computers and Security (2019).

[10] I. O. for Standardization/Society of Automotive Engineers, Iso/sae 21434 - road vehicles – cybersecurity engineering (2021).

[11] I. O. for Standardization, Iso 32111:2023 - transaction assurance in e-commerce - principles and framework (2023).

[12] M. Paulk, B. Curtis, M. Chrissis, C. Weber, Capability maturity model, version 1.1, IEEE Software 10 (4) (1993) 18–27. doi:10.1109/52.219617.

[13] ISACA, Cobit 5: A business framework for governance and management of enterprise it (2012).

[14] D. Dickins, M. O. Hara, J. Reisch, Frameworks for establishing and evaluating internal controls : a primer and case study, Journal of Case Research in Business and Economics (2009) 1–16.

[15] K. Haufe, Maturity based approach for ISMS governance (2017).

[16] V. Monev, Organisational information security maturity assessment based on ISO 27001 and ISO 27002, Institute of Electrical and Electronics Engineers Inc., 2020.

[17] L. Oliveira, W. Bai, M. Johanson, M. Ratajczak-Mrozek, B. Francioni, Uncertainty and decision-making in sme internationalization: The importance of control, prediction, and knowledge, Progress in International Business Research 14 (2019) 333–355.

Preprint not peer reviewed

This preprint research paper has not been peer reviewed. Electronic copy available at: https://ssrn.com/abstract=5143868

[18] A. P. Aldya, S. Sutikno, Y. Rosmansyah, Measuring effectiveness of control of information security management system based on SNI ISO/IEC 27004: 2013 standard, IOP Conference Series: Materials Science and Engineering 550 (2019).

[19] T. Neubauer, A. Ekelhart, S. Fenz, Interactive selection of ISO 27001 controls under multiple objectives, IFIP International Federation for Information Processing 278 (2008) 477–491.

[20] M. I. Tariq, S. Tayyaba, E. D. la Hoz-Franco, M. W. Ashraf, D. V. Rad, S. A. Butt, V. Santarcangelo, Evaluation and prioritization of information security controls of ISO/IEC 27002:2013 for SMEs through fuzzy topsis, Springer Singapore, 2022, pp. 271–289.

[21] U. Ahonen-Jonnarth, H. Andersson, F. Bökman, How do people aggregate value? An experiment with relative importance of criteria and relative goodness of alternatives as inputs, Journal of Multi-Criteria Decision Analysis 28 (2021) 1–15.

[22] O. C. Briliyant, J. W. Candra, S. R. Tamba, ISMS planning based on ISO/IEC 27001:2013 using analytical hierarchy process at gap analysis phase (case study: XYZ institute), Vol. 4, 2016, pp. 4–9.

[23] A. Sengupta, Modeling dependencies of ISO/IEC 27002:2013 security controls, Third International Symposium, SSCC 2015, Kochi, India, August 10-13, 2015. Proceedings (2015) 354–367doi:10.1007/978-3-319-22915-7.

[24] J. Aguarón, M. T. Escobar, J. M. Moreno-Jiménez, A. Turón, AHP-group decision making based on consistency, Mathematics 7 (2019).

[25] H. Susanto, M. N. Almunawar, Y. C. Tuan, A novel method on ISO 27001 reviews: ISMS compliance readiness level measurement, Computer Science Journal 2 (2012).

Preprint not peer reviewed

This preprint research paper has not been peer reviewed. Electronic copy available at: https://ssrn.com/abstract=5143868

Preprint not peer reviewed

[26] A. A. Nasser, Measuring the information security maturity of enterprises under uncertainty using fuzzy ahp, I.J. Information Technology and Computer Science 4 (2018) 10–25.

[27] M. Schmid, S. Pape, A structured comparison of the corporate information security, ICT Systems Security and Privacy Protection - 34th IFIP TC 11 International Conference, SEC 2019, Lisbon, Portugal, June 25-27, 2019, Proceedings (2019).

[28] M. Schmid, S. Pape, Aggregating corporate information security maturity levels of different assets, Vol. 576 LNCS, Springer, 2020, pp. 376–392.

[29] A. Nili, M. Tate, D. Johnstone, A framework and approach for analysis of focus group data in information systems research, Communications of the Association for Information Systems 40 (2017) 1–21.

[30] K. Fysarakis, A. Lekidis, V. Mavroeidis, K. Lampropoulos, G. Lyberopoulos, I. G.-M. Vidal, J. C. T. i Casals, E. R. Luna, A. A. M. Sancho, A. Mavrelos, M. Tsantekidis, S. Pape, A. Chatzopoulou, C. Nanou, G. Drivas, V. Photiou, G. Spanoudakis, O. Koufopavlou, Phoeni2x - a european cyber resilience framework with artificial intelligence-assisted orchestration automation for business continuity, incident response & information exchange, in: IEEE CSR, 2023. `doi:10.1109/CSR57506.2023.10224995`. URL `https://ieeexplore.ieee.org/document/10224995`

Appendix A. Survey

Appendix A.1. Section A: Expert's Demographics

A1 How many years of experience do you have in information security?

- Less than 1
- 1-5
- 6-10
- 11-15
- 6-20
- More than 20

A2 How many years of experience do you have in the e-commerce industry?

This preprint research paper has not been peer reviewed. Electronic copy available at: https://ssrn.com/abstract=5143868

- Less than 1
- 1-5
- 6-10
- 11-15
- 6-20
- More than 20

A3 How many years of experience do you have with ISO/IEC 27001/2 controls?

- Less than 1
- 1-5
- 6-10
- 11-15
- 6-20
- More than 20

Appendix A.2. Section B: Comparison of Controls

Please compare the following pairwise comparisons using the Importance scale of Table A.4. Please note to always answer this in the context of the e-commerce industry.

Table A.4: Importance for Weighting

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

Preprint not peer reviewed

This preprint research paper has not been peer reviewed. Electronic copy available at: https://ssrn.com/abstract=5143868

Appendix A.2.1. Section C: Comparison of Control Categories

To Compare	A or B	Importance
A: A.6 Organisation of Information Security or B: A.14 System Acquisition, Development & Maintenance		

Appendix A.2.2. Section D: Please compare 2 control objectives with each other

To Compare	A or B	Importance
A: A.6.1 Internal organization or B: A.6.2 Mobile devices and teleworking		
A: A.14.1 Security requirements of information systems or B: A.14.2 Security in development and support processes		

Preprint not peer reviewed

This preprint research paper has not been peer reviewed. Electronic copy available at: https://ssrn.com/abstract=5143868

Appendix A.2.3. Section E: Please compare all A.6.1 controls with each other

To Compare	A or B	Importance
A: A.6.1.1 Information security roles and responsibilities or B: A.6.1.2 Segregation of duties		
A: A.6.1.1 Information security roles and responsibilities or B: A.6.1.3 Contact with authorities		
A: A.6.1.1 Information security roles and responsibilities or B: A.6.1.4 Contact with special interest groups		
A: A.6.1.1 Information security roles and responsibilities or B: A.6.1.5 Information security in project management		
A: A.6.1.2 Segregation of duties or B: A.6.1.3 Contact with authorities		
A: A.6.1.2 Segregation of duties or B: A.6.1.4 Contact with special interest group		
A: A.6.1.2 Segregation of duties or B: A.6.1.5 Information security in project management		

Preprint not peer reviewed

This preprint research paper has not been peer reviewed. Electronic copy available at: https://ssrn.com/abstract=5143868

To Compare (continuation)	A or B	Importance
A: A.6.1.3 Contact with authorities or B: A.6.1.4 Contact with special interest groups		
A: A.6.1.3 Contact with authorities or B: A.6.1.5 Information security in project management		
A: A.6.1.4 Contact with special interest groups or B: A.6.1.5 Information security in project management		

Appendix A.2.4. Section F: Please compare all A.6.2 controls with each other

To Compare	A or B	Importance
A: A.6.2.1 Mobile device policy or B: A.6.2.2 Teleworking		

Appendix A.2.5. Section G: Please compare all A.14.1 controls with each other

To Compare	A or B	Importance
A: A.14.1.1 Information security requirements analysis and specification or B: A.14.1.2 Securing application services on public networks		
A: A.14.1.1 Information security requirements analysis and specification or B: A.14.1.3 Protecting application services transactions		
A: A.14.1.2 Securing application services on public networks or B: A.14.1.3 Protecting application services transactions		

Preprint not peer reviewed

This preprint research paper has not been peer reviewed. Electronic copy available at: https://ssrn.com/abstract=5143868

Appendix A.2.6. Section H: Please compare all A.14.2 controls with each other

Analogous to Section G.

Preprint not peer reviewed

This preprint research paper has not been peer reviewed. Electronic copy available at: https://ssrn.com/abstract=5143868

Appendix B. Evaluation of the Individual Expert Results of Control Category A.14

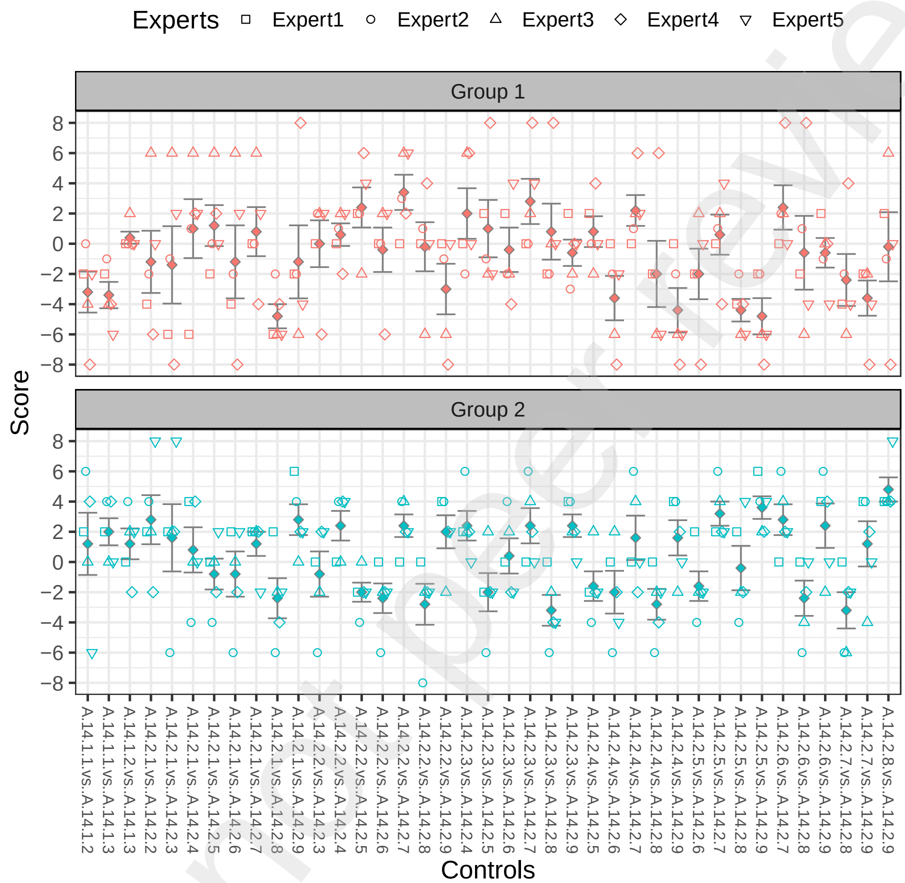

Figure B.8: Results of Weighting A.14 controls

Preprint not peer reviewed

This preprint research paper has not been peer reviewed. Electronic copy available at: https://ssrn.com/abstract=5143868