Maturity Level Assessments of Information Security Controls: An Empirical Analysis of Practitioners' Assessment Capabilities

Christopher Schmitz, Michael Schmid, David Harborth and Sebastian Pape

Goethe University Frankfurt, Germany
{christopher.schmitz, michael.schmid, david.harborth, sebastian.pape}@m-chair.de

Abstract

Maturity models are a widely used concept for measuring information security. The idea is to systematically evaluate the maturity of security-relevant processes in an organisation. This enables decision makers to get an overview of the implementation status of relevant processes to identify neuralgic points. Maturity models thus play a central role in the conception of information security management systems (ISMS). Some industries, for instance, the German automotive industry, have even established security maturity levels as the de facto standard for measuring information security. However, the quality of security maturity level assessments has not been sufficiently investigated yet. We have analysed to what extent security managers can accurately assess the maturity levels of security controls. To verify the quality of maturity level assessments a case study was conducted where security experts assessed a subset of the ISO/IEC 27002 security controls for a hypothetical scenario using the COBIT maturity levels. Additionally, ex-post interviews have been conducted with several study participants to verify some of the hypotheses developed during the previous analyses. Our results show that many security experts struggled with the task and did not perform well. However, we discovered professional characteristics that have a strong significant effect on the assessment capabilities. We also identified various types of additional support that can help practitioners to make more reliable assessments in practice. Moreover, the experts' self-perception was overly optimistic when asked to assess their performance. We even found a weak inverted correlation for more experienced experts, also known as Dunning-Kruger effect. Our results have a strong impact on practise since they indicate that practitioners need support to carry out high-quality assessments and they also show what kind of support addresses the identified challenges.

Keywords: Usability Evaluation, Security Controls, Maturity Levels, ISO/IEC 27002, COBIT

1. Introduction

During the last years, data breaches have been broadly reported in the mainstream media and the number of security breaches has increased by 11% since 2018 and 67% since 2014 [1]. Data breaches are not only expensive for organisations [2], organisations are even obliged by law to fulfil certain regulatory requirements. For example, the General Data Protection Regulation (GDPR) in Europe requires organisations to implement "a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing" [3, Art. 32]. However, following DeMarco, "you can't control what you can't measure" [4, p. 3]. Thus, organisations face the problem that information security can only be measured indirectly [5]. To demonstrate compliance, organisations make use of maturity level metrics of security controls which are mainly described in standards and rely on the security knowledge of security experts [6].

The approach of assessing security controls with the aid of maturity levels is widely used in many industries. It is, for instance, the de facto standard for the German automotive industry when it comes to measuring information security. Organisations in this domain have to complete a standardised security self-assessment questionnaire (VDA-ISA) provided by the German Association of the Automotive Industry (VDA) where maturity levels are applied on security controls following ISO/IEC 27002 [7]. The idea to assess the maturity levels of ISO/IEC 27002 controls is also supported by standard GRC (governance, risk, compliance) tools like risk2value which is also used by major companies [8]. There also exist several academic approaches relying on similar maturity-based approaches [9, 10, 11].

An established model for assessing security maturity levels is offered by the ISACA COBIT framework. This 6-level model makes it possible to evaluate the prevailing security situation in an organisation. In combination with the de facto standard in information security, the ISO/IEC 27001 and 27002, a very granular evaluation can be carried out, namely on a control level.

Since maturity levels are assessed by humans, the human factor of the evaluation may lead to possible uncertainties, e. g. because of different evaluators or different physical and mental conditions of the same evaluator on different days. The quality of these assessments has not yet been systematically evaluated.

Therefore, we conducted a case study where practitioners assessed a subset of the ISO/IEC 27002 security controls for a sample scenario (see Section Appendix A) using the maturity

levels of COBIT 5. We investigated deviations between different participants, e. g. possible inaccuracies, in the assessment of information security control maturity levels. Besides identifying the possible range of answers, we also investigated whether the participants' results depend on professional factors such as experience, industry, familiarity with maturity levels and received certifications.

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 along with an analysis in Section 5 and a discussion in Section 6. Section 7 concludes our work. The scenario and the questionnaire can be found in the appendix.

2. Background and Related Work

We briefly discuss different security maturity models, the environment where they are used and their relation to security controls in the background section before we present related work and compare it to our study.

2.1. Background

An established way to monitor and steer the information security is the implementation of an information security management system (ISMS). An ISMS is a comprehensive management framework through which an organisation identifies, analyses and addresses its information risks. Using an ISMS ensures that the security arrangements are fine-tuned to keep pace with new security threats, vulnerabilities and their impacts on the business processes. Many different standards and frameworks are available providing guidance to correctly implement and maintain an ISMS. The most popular standard in this environment is ISO/IEC 27001 (incl. ISO/IEC 27002). It contains guidelines for organisational information security management practices including the selection, implementation and management of controls, taking into consideration the organisation's information security risk environment(s). Another notable standard is from the National Institute of Standards and Technology (NIST) within the 800-series publications [12] and Cybersecurity Framework (NIST CSF) [13] which include information security management, information security evaluation, authentication and authorisation, etc. A country-specific standard from the German Federal Office for Information Security (BSI) is called IT-Grundschutz (former English name: IT Baseline Protection Manual). BSI standards 200-1 to 200-3 and 100-4 cover technical, organisational, infrastructural and personnel aspects of information security [14]. The IT-Grundschutz is a collection of standards and catalogues that describe generalised procedures for the protection of the information technology used. They are defined in exemplary modules, threats and measures that were used to systematically construct the scenario according to predefined scenario maturity levels. Another standard which is very popular in the automotive industry is the VDA-ISA [7], a questionnaire for assuring information security compliance by the German Association of the Automotive Industry (VDA) which is based on the ISO/IEC 27001 and 27002 standards.

These standards and frameworks have security controls in common. Security controls describe a set of security measures to fulfil a security requirement, and therefore to mitigate security risks to physical properties, information, computer systems, or other (also intangible) assets. These security controls address various topics e. g. electronic signatures, software development, business continuity, incidents etc.

Maturity models are a popular concept to assess the status of information security as well as the quality of the process [15]. There is a large number of different security maturity models. Proença et al. have identified more than 20 different security maturity models for information systems. Almost all of them differentiate between 5 or 6 maturity levels [16]. Examples are the Cybersecurity Capabilities Maturity Model (C2M2) developed by the United States Department of Energy in partnership with the Department of Homeland Security [17], the Information security maturity model (ISMM) [18] and the Open Information Security Maturity Model (O-ISM3) [18]. ISMM is intended as a tool to evaluate the ability of organisations to meet the objectives of security and O-ISM3 aims to ensure that security processes operate at a level consistent with business requirements. Some of the most prominent models are CMMI [19], SSE-CMM (ISO/IEC 21827:2008) and the COBIT maturity model that is derived from the ISO/IEC 15504 (SPICE) [20, 21].

Using such models, it is possible to assess the quality of controls on 6- to 7-point (from 0 to 5 or 6). The assessment provides a management perspective in the fulfilment of regulatory requirements. The maturity levels are used as a measure to quantify the implementation status of a security control. The higher the maturity level of a control, the higher the chance that it is performed in an effective and secure way so that it contributes more to the organisational security. COBIT defines six maturity levels. Each maturity level adds on the requirements of the level(s) below. The criteria for each maturity level provided to the participants are depicted in Table 1. They range from level 0 where the control is not implemented to level 5 where the respective control is effectively implemented, monitored, controlled, and continuously improved. For the remainder of this paper, we refer to maturity models as security maturity models.

2.2. Related Work

Although maturity models are widely used in industry and are quite common in academia, there are only a few studies analysing the practitioners' assessment capabilities.

Zhang and Fever [22] summarise the theoretical values and weaknesses of the COBIT framework identified by previous researchers. They found that most organisations are mainly interested in the maturity model from the COBIT framework because it is easy to understand and can be quantified. However, their work is solely based on existing literature and they state themselves that it is necessary to collect more input and criticism from practitioners and COBIT experts.

El Emam et al. have investigated the reliability for SPICE maturity levels for version 1.0 of the SPICE rating scheme on the basis of process groups in software engineering [23]. In

Table 1: Description of the COBIT 5 Maturity Levels

Level	Maturity Levels Description
0–Incomplete	The control is not implemented or fails to achieve its purpose.
1–Performed	The implemented control achieves its process purpose.
2–Managed	The level 1 performed control is now implemented in a managed fashion (planned, monitored and adjusted) and its work products are appropriately established, controlled and maintained.
3–Established	The level 2 managed control is now implemented using a defined process that is capable of achieving its process outcomes.
4–Predictable	The level 3 established control now operates within defined limits to achieve its process outcomes.
5–Optimising	The level 4 predictable control is continuously improved to meet relevant current and projected business goals.

their study, the degree of reliability strongly varied between different processes. For some of them, the maturity levels could be assessed very reliably (perfect agreement), whereas the assessments for other processes only showed moderate reliability. The authors explain these higher grades of disagreements primarily by saying that the assessments were conducted by internal assessors (five) and external assessors (three). This plays a significant role because internal assessors typically know their organisation's processes better, hence a different perception. Another similar study has been conducted by Lee et al. [24]. They also analyse the reliability of SPICE assessments for software engineering processes. Their results show a substantial to excellent reliability in the maturity level assessment. However, current studies only focus on measuring the reliability but do not qualify their findings with respect to the validity of the assessor's ratings. This is important since even ratings with high reliability may significantly differ from the theoretical rating. More importantly, most existing studies do not only deal with the evaluation of entire software engineering processes but they also do not address lightweight variants. This means that the maturity levels are not determined directly but result from the complex process to assess the implementation status (not achieved, partially achieved, largely achieved, fully achieved) of the process attributes defined for each process and level. But in practice, oftentimes, less complex variants are implemented, for example, in the VDA-ISA questionnaire, in which the controls' maturity levels are directly assessed [7]. There are several other approaches in security management based on the maturity levels of the ISO/IEC 27002 security controls [9, 10]. To the best of our knowledge the quality of this kind of maturity level assessments has never been analysed in the literature.

3. Methodology

To evaluate practitioners' capabilities to assess the COBIT maturity levels of security controls and to gain insights into potential challenges and how to address them, an experiment has been conducted. The experiment was set up as an online survey in which a hypothetical IT infrastructure, including security measures and processes, of a small company was presented to the participants. The description of the scenario was systematically constructed to represent predefined maturity levels for a number of the scenario's security controls. The participants' task was then to assess the maturity levels for these controls, and also to provide a rationale for their decision. These data build the basis for a quantitative and qualitative analysis on the quality of their assessments. In addition to this, ex-post interviews have been conducted to verify some of the hypotheses developed during the previous analyses.

3.1. Scenario Design and Scenario Maturity Levels

In the following, it is described how the scenario was constructed on the basis of the predefined maturity levels. Fig. 1 visualises the scenario.

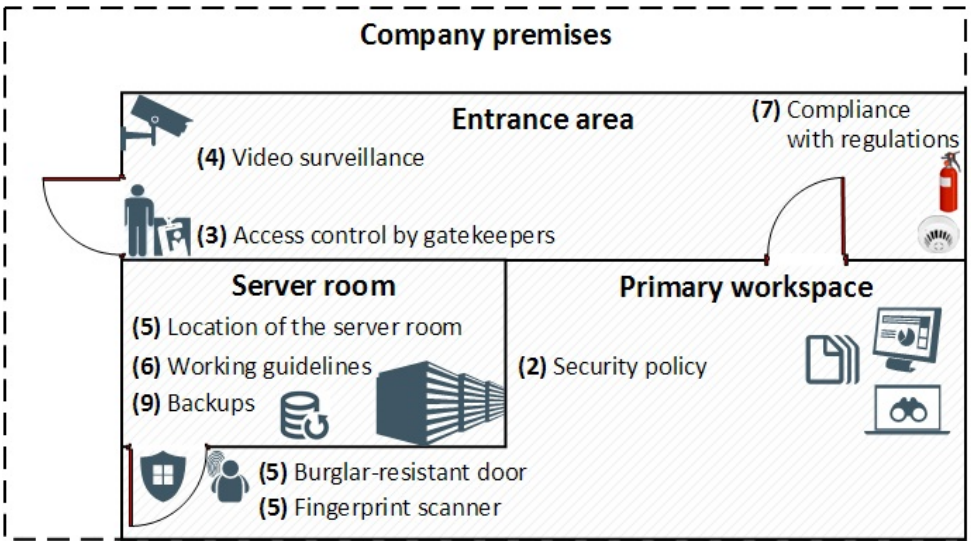
3.1.1. Scenario Design

The scenario reflects a fairly generic and realistic situation to ensure that a high number of participants will understand it and can better identify themselves with the scenario.

It aims to address a typical situation in the real world. It describes a hypothetical cloud service provider, called CloudSec, which is a small company offering various cloud services (IaaS, PaaS and SaaS) to their customers. From the perspective of information security, policies, physical and application security are very important for a cloud service provider. The scenario description consists of a textual description and its visual illustration (see Figure 1 in the Appendix). The illustration shows the physical characteristics of the building and schematically refers to the respective paragraphs in the text. The text is structured by high-level security categories like information security guidelines, access control, and vulnerability management. In each paragraph, different security measures and their implementation status are described. We decided to use security measures instead of the controls itself to derive a more realistic scenario since in a real-world situation practitioners have to map security measures to the corresponding controls as well.

The starting point to describe the scenario's security measures were as set of ISO/IEC 27002 security controls. Since policies, physical security and application security play a major role for cloud service provider controls from this topic area were selected. However, not all controls could be selected since, otherwise, the size and the length of the scenario would go much beyond what a study participant is able to comprehend. For each control, we then defined a scenario maturity levels. Next, we used the mapping of security measures from the BSI IT-Grundschutz to ISO/IEC 27002 controls [25] to identify corresponding measures. The mapping was developed in cooperation between ISACA's Information Security (German

Figure 1: Visualisation of the Scenario



Chapter) professional group and the BSI, and thus has a focus on practitioners. Since the BSI IT-Grundschutz is based on the ISO/IEC 27002 standard, it is straightforward to derive descriptions for specific measures from the controls. Examples for three of the controls used in our scenario are shown in Table 2. These security controls concern policies (A.5.1), physical security (A.11.1) and application security (A.12.6).

3.1.2. Predefined Scenario Maturity Levels

To validate and to analyse the quality of the maturity level assessments of the study participants, it is crucial to know the predefined maturity levels of the security controls (see Table 3) and to understand how the scenario has been constructed accordingly.

The predefined scenario maturity levels (SML) reflect a realistic distribution and show a wide range of maturity levels up to level 4. Level 5, the highest level possible, is very difficult to achieve in relative terms and is therefore not applied in the scenario. Most of the predefined scenario maturity levels are between 0 and 3 since a medium-term goal of many companies is to achieve at least a control maturity level of 3 (a defined process) [26, 7].

In the following, three exemplary controls (each from a different control category) are used to demonstrate how the scenario was constructed on the basis of the predefined scenario maturity levels. For this purpose, the maturity level of each control was systematically demarcated to the next lower and to the next higher level by (not) fulfilling the respective criteria (see Table 4).

For control 5.1.1 (policies for information security) a scenario maturity level of 2 has been defined respecting the criteria defined in Table 1. To achieve this, 2 (out of 3) IT-Grundschutz measures for control 5.1.1 (that are most relevant for the scenario) are described to point out that the policy was defined in a systematic and structured way (see Table 2). Additionally, essential aspects like the high resource-intensity and the management support have been emphasised which go beyond standard level 1 requirements. On the other hand, it is emphasised that no information security policy has been published before, indicating that no process has been defined there, as this is the key characteristic of the next higher maturity level 3.

For control 11.1.1 (physical security perimeter) a maturity level of 2 has been defined so that it is effectively managed. To ensure the adequacy of the process all IT-Grundschutz measures for this control have been described in the scenario (see Table 2), ranging from the creation of security zones to burglary protection and the server room's arrangement in the rear part of the building. The security concept reflects the result of a solid planning in order to effectively meet the quasi-static requirements. On the other hand, the description of the control implementation does not fulfill the requirements for level 3 since it does not follow a defined process.

Control 12.6.1 (management of technical vulnerabilities) is described according to maturity level 4. All IT-Grundschutz measures (see Table 2) and several additional ones are mentioned in the description clarify that the level 4 requirements are met, e. g. that an effective process is in place to measure the vulnerability exposure and to react accordingly. However, since a continuous improvement process is missing level 5 cannot be achieved.

The other 7 ISO/IEC controls have been described in the same way to represent the predefined maturity levels.

3.2. Questionnaire Design

The questionnaire comprises four sections (see Appendix B). First, the practitioners were asked for demographic information (see Section [A and B]) (such as professional background, certifications, employer characteristics, experience with ISO/IEC 27002 and maturity levels). Second, the general concepts that are required to understand the experiment were explained (see Section [C]). This includes the term security control, the concept of maturity levels (particularly the COBIT maturity levels) as well as a description and an illustration of the scenario

Table 2: Security measures for exemplary controls used in the scenario

Control	Measure ID	Description of Measure	Paragraphs in the scenario description
C 5.1.1	M 2.192	Preparation of a guideline on information security	(2) Information security policy
	M 2.335	Definition of the security objectives and strategy	(1) Security assessment
C 11.1.1	M 1.79	Creation of security zones	(3) Access control by gatekeeper, (6) Working guidelines and (9) Backups
	M 1.17	Gatekeeping	(3) Access control by gatekeeper
	M 1.53	Video surveillance	(4) Video surveillance
	M 1.19	Burglary protection	(5) Protection measures for server room
	M 1.13	Arrangement of parts of buildings requiring protection	(3) Access control by gatekeeper
	M 1.55	Perimeter protection	(5) Protection measures for server room
C 12.6.1	M 2.35	Obtaining information on system vulnerabilities	(8) Vulnerability management
	M 2.273	Prompt application of security-relevant patches and updates	(8) Vulnerability management

Table 3: Scenario maturity levels per control

Control	Control Description	Scenario Maturity Level	Qualitative Feedback
C 5.1.1	Policies for information security	2 - Managed	Question F1
C 5.1.2	Review of the policies for information security	0 - Incomplete	
C 11.1.1	Physical security perimeter	2 - Managed	Question H1
C 11.1.2	Physical entry controls	3 - Established	
C 11.1.3	Securing offices, rooms and facilities	2 - Managed	
C 11.1.4	Protecting against external and environmental threats	3 - Established	
C 11.1.5	Working in secure areas	0 - Incomplete	
C 11.1.6	Delivery and loading areas	3 - Established	
C 12.6.1	Management of technical vulnerabilities	4 - Predictable	Question J1
C 12.6.2	Restrictions on software installation	0 - Incomplete	

(see Section [D]). In the third section, the practitioners were requested to assess the maturity levels for a number of security controls described in the scenario (see Section [E, G and I]). Additionally, they were asked to explain for three controls how the next maturity level could be achieved (see Section [F, H and J]). This enables qualitative analysis whether practitioners might have misunderstood, for instance, the scenario or the given maturity levels. A control question has also been integrated into this section, requesting the practitioners to set the maturity level of the (non-existing) security control 12.6.0. to 5. Finally, the practitioners were supposed to indicate how challenging they perceived the task, and the reasons for these challenges (see Section [K, L and M]). This helps to get a better understanding of the type of additional support that might be needed.

3.3. Validation of Scenario and Questionnaire

The scenario and the questionnaire have been validated in two rounds of pre-tests with experienced information security experts.

The first round was conducted to gather initial feedback and to identify neuralgic points. The survey has been given to three experts, followed by a group discussion on the general questionnaire design and the scenario description. As a result of their feedback, the textual scenario description has been structured in a more comprehensible form and has been extended by a graphical illustration of the scenario. In addition, several parts of the questionnaire have been changed. A control question has been added, for instance, and the maturity level definitions and a link to the scenario description have then been presented on each page where a control's maturity level has to be assessed, and not only in the questionnaire's introduction. Altogether, the experts confirmed the practical relevance of the research question.

To validate the modified version, the second round of pretests has been conducted in which the survey has been sent to three chief information security officers from large organisations. Afterwards, the results have been discussed with each of them in 20- to 30-minute phone interviews. As a result, the description of some controls has been reworked to reduce ambiguities. Furthermore, three additional feedback questions have been added to better understand the practitioners' rationale behind their maturity level assessments.

3.4. Ethical Considerations

We have considered potential ethical issues of the study by evaluating an extensive check-list provided by the ethics board of the authors' university. This check-list qualifies our study as exempt from an ethics review. However, in order to inform participants about our data collection process, we provided information about their right to information and deletion of their personal data, and that they can revoke their consent at any time.

Table 4: Demarcation of security maturity levels

Control	SML*	Demarcation to the next lower level	Demarcation to the next higher level
C 5.1.1	2	Systematic realisation accompanied by mgmt. support (2)	No defined process (2)
C 5.1.2	0	–	No future review of the policy planned (2)
C 11.1.1	2	Effectively managed to meet the requirements (3, 4, 5)	No defined process (3, 4, 5)
C 11.1.2	3	Effective process defined to secure the physical entry (3, 5)	No quantification (3, 5)
C 11.1.3	2	Effectively managed to meet the requirements (5)	No defined process (5))
C 11.1.4	3	Effective process defined to ensure compliance with regulations (7)	No quantification (7)
C 11.1.5	0	–	Relevance of the control is not recognised (6)
C 11.1.6	3	Effective process defined for a secure delivery (3)	No quantification (3)
C 12.6.1	4	Effective and quantified process defined for vulnerability management (8)	No continuous improvement (8)
C 12.6.2	0	–	Relevance of the control is not recognised (6)

* Scenario Maturity Level Numbers in brackets correspond to paragraphs of the scenario description in Appendix A

Furthermore, we stated that all answers are anonymous (e. g. no saving of IP addresses), that all answers are stored on a German university server and that by participating in the survey, participants agree that their answers are used exclusively for scientific purposes within the scope of the presented research project. We provided an open-text-field for feedback and a researcher's e-mail address for further questions and requests at the end of the survey.

3.5. Data Collection and Data Sanitisation

The data collection strategy is twofold: the primary data source is an online survey. In this survey the participants were also asked about their willingness to be available for interviews. These ex-post interviews form the second part of the data collection. They help to better understand the participants' rationale and to explain why they have performed well or badly.

3.5.1. Survey

The survey was distributed to security practitioners from various organisations between 15 April and 23 September 2019. The online survey, created using the survey software LimeSurvey (version 2.63.1), was sent to (chief) information security officers but also to a number of professional mailing lists [1]. Additionally, the survey was also distributed in selected professional forums [2].

In total, 76 practitioners opened the questionnaire. 56 of these data records fulfilled the quality criteria. If the control question has not been answered correctly the data records have been excluded from further analysis. Incomplete data records (e. g. with incomplete maturity level assessments) have been excluded. A few participants have intentionally de-anonymised themselves (via the feedback form or via e-mail) and have notified the study conductors that they have not seriously answered all questions. The de-anonymisation was possible since they revealed the textual answers they gave. The corresponding data records have been excluded as well.

3.5.2. Ex-Post Interviews

To further substantiate the results from the survey, ex-post interviews were subsequently conducted with six participants of the survey. The participants were interviewed on the basis of a semi-structured interview guideline that was adapted after each interview. The latest version is given in Appendix C. It consists of two core aspects: the challenges of security maturity level assessments and the kind of support that could be given in order to face these challenges. The interviews were conducted between 14 May and 8 June 2020 ex-post interviews. The average duration was about 20-30 minutes, including an introduction to the topic (a small recap), the main part with the two core topics and a final question. Due to the Corona pandemic, these interviews were conducted virtually (web conferences or telephone). Each interview has been performed by two interviewers. One interviewer conducted the interview and the second interviewer was present from a quality assurance point of view., e g. to reduce the risk of miscommunication between the interviewee and the interviewer. The interview was recorded with the approval of the participant. Based on the recordings a transcript was produced which was reviewed by both interviewers.

3.6. Demographics

The following two sections explain the demographic information of the survey and interview participants.

3.6.1. Survey

We asked for the participants' capabilities and skills. More than half of them (55%) have been working in IT security for more than 10 years. A little bit more than a quarter have 1-5 years experience in the field of IT security (see Figure 2).

[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

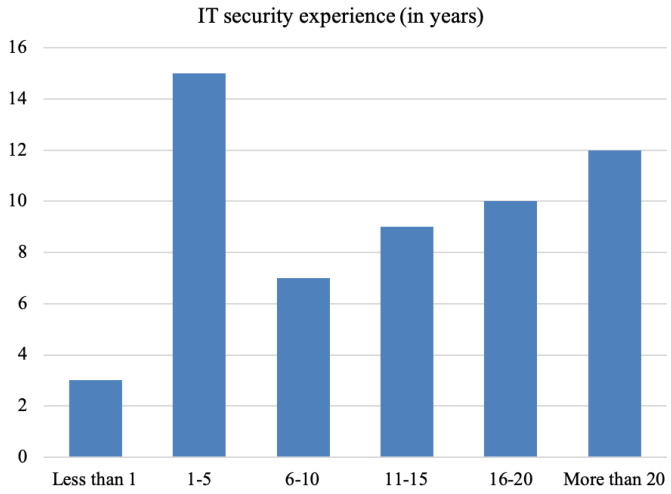


Figure 2: Participants' IT security experience

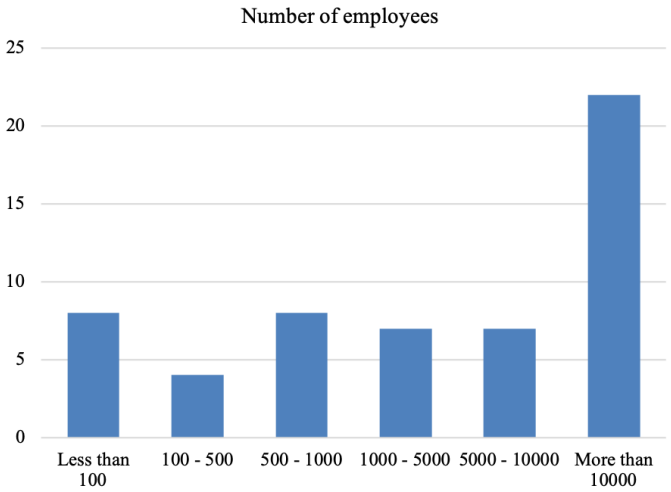


Figure 3: Size of the participants' organisations

Most participants (86%) indicated to be familiar with the basic idea of maturity models. 58% stated they are familiar with COBIT maturity levels, although only 40% indicated being familiar with the rating scale for process attributes used in COBIT. 53% have more than 5 years of experience with the ISO/IEC 27002 controls. The certifications obtained by the participants draw a similar picture. 46% have obtained an ISO/IEC 27002 certification, followed by 35% who have a CISM or a CISA certification, 25% with a general ISMS certification, 23% with a CISSP certification (multiple selections were possible).

It is noticeable that almost than two thirds (64%) of the participants work in companies with more than 1,000 employees regarding the size of the organisations (in terms of the number of employees) where the participants work. 39% of the practitioners work in companies with more than 10,000 employees (see Figure 3). But still, only 19% of the companies have been certified against ISO/IEC 27002. It is also worth mentioning that 25% of the organisations are critical infrastructures.

3.6.2. Ex-Post Interviews

All six interviewees have more than 10 years of work experience, two have even more than 20 years of experience. Half of them work in large companies with more than 5,000 employees. In addition, all of them are experienced in working with ISO/IEC 27002 controls and have - at least basic - knowledge of maturity models. Most of them also have practical experience with maturity models.

3.7. Coding the Qualitative Data

For the qualitative evaluation, we coded the textual answers of the participants. This coding was done for two different types of qualitative data, for responses from participants in the survey and for responses from participants in a follow-up interview.

3.7.1. Coding the Practitioners' Rationale

The practitioners have been asked to indicate the security measures needed to reach the next maturity level in order to better understand the practitioners' rationale behind their maturity level assessments (see Question F1). To keep the practitioners' effort reasonable, we have only asked for the three security controls 5.1.1, 11.1.1, and 12.6.1 (see Table 3).

The practitioners' open-ended responses were coded using an iterative process to identify recurring themes. To build an initial set of codes, two coders disjointly coded a random sample of the practitioners' responses, discussed the resulting codes and consolidated them. Then, the two coders re-coded all answers to the open-ended questions.

The suggested security measures to achieve the next maturity levels have been coded using the codes described down below. The codes were only assigned to obviously wrong answers.

Scenario Misinterpreted This code indicates that the practitioner has not considered any detail described in the scenario. For example, when the practitioner suggested the implementation of a specific security measure to achieve the next maturity level, although it has been also mentioned as already existing in the scenario description.

Control Misinterpreted This code describes statements where the practitioner has commented on another control. The latter one can happen, for instance, with related security controls. However, each security control must be assessed independently. A statement is labelled with this code if the suggested measures are not related to the respective control.

Security Measures Exaggerated Statements suggesting exaggerated security measures that clearly do not address the scenario's scope, are labelled with this code. Borderline cases have not been labelled. Practitioners that do not fully get into the scenario might assess the controls with a different mindset. This is of relevance because, for instance, large companies might require more rigorous measures than the small company described in the scenario.

Furthermore, the practitioners also commented on general challenges with maturity level assessments. This information serves a broader understanding of the challenges for the practitioners. Several answers did not provide any useful information or did not identify any challenge, so they were not considered in the analysis (e. g. *«I don't have time to write this down»*). The remaining answers were categorised using the codes below.

Control Dependencies This codes reflect challenges with regard to the dependencies between controls. It is assigned when controls are not assessed independently due to control dependencies.

Differentiation Between Maturity Levels Difficulties with maturity level assessments can also arise from challenges to differentiate the maturity levels due to unclear definitions. This code has been assigned when the maturity level definitions caused a deviation from the predefined scenario maturity levels.

Scope for Interpretation Another challenge is the degree of subjectivity inherent for qualitative assessments. This code has been assigned in cases of general critics regarding the subjectivity of maturity level assessments.

Mapping Controls to Processes This code was assigned for difficulties to map the given security controls to actual processes.

Lack of Skills A lack of skills can mean that practitioners do not have enough background knowledge to evaluate controls with confidence. This code has been assigned for answers that explicitly refer to a lack of skills.

3.7.2. Coding the Ex-Post Interviews

The transcribed answers of the participants were provided with codes following an iterative process. Two coders carried out the coding independently of each other. The individual results of the coding were then discussed and consolidated. The codes for the ex-post interviews have been divided into three code categories and were described as follows.

Reasons for Difficulty in Maturity Level Assessment This code category describes the possible reasons that may have led to the survey participants' having difficulty with maturity assessment in the scenario. The participants, for example, could have a tendency to be less critical in self-evaluation or stricter in external evaluations. This can be challenging for the assessment. The code category was divided into four sub-categories (see Section 4.2.2): differences in internal and external evaluations, distinction in degrees of maturity, the difference between evaluators and not all controls represent processes.

Reasons for Suggesting Exaggerated Measures This code category describes possible indications and reasons that may have led to the suggestion of exaggerated measures. The code category was divided into two sub-categories (see Section 4.2.4): in and neglecting economic considerations.

Support for Maturity Levels Assessments This code category indicates whether the participants can be supported in their maturity assessment. In order to guarantee this, various supports are conceivable, e. g. a more detailed description of the maturity levels or suitable examples. The code category was divided into six sub-categories (see Section 5.3): discuss maturity assessments, more detailed description of maturity not necessary, provide examples, use a catalogue of measures, orientation towards standards and training courses for maturity assessments.

3.8. Statistical Analysis

We first test whether the variable in question, the linear deviation of practitioners' assessments to the scenario maturity levels, is normally distributed. This is required to decide which statistical test is needed for the group comparisons. Thus, we conduct the Shapiro-Wilk test for normality and find that the variable is normally distributed. Consequently, we apply a standard t-test to assess whether there are statistically significant differences between groups of practitioners (with regard to their professional experiences and the certificates they have obtained). A sample size of 30 or more is a rule of thumb for sample sizes to apply parametric statistical tests like a t-test. Since we are close to that threshold for most group comparisons, we chose the t-test, while considering that the sample size might limit the validity of our results. We also use standard t-tests and Spearman's rank correlation to analyse the relationship between practitioners' correct assessments and their self-perception.

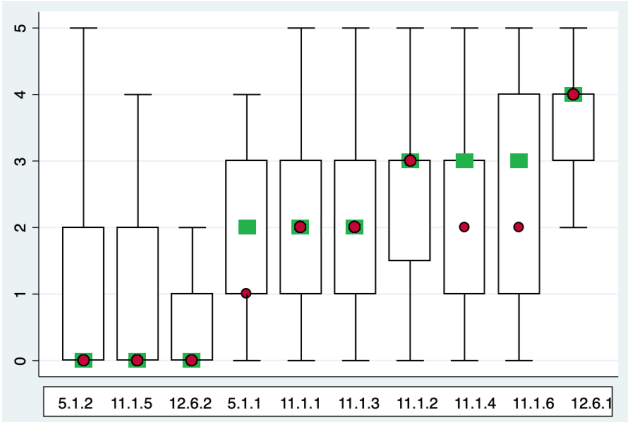
4. General Results of the Survey and the Interviews

The following section presents the quantitative results of the practitioners' maturity level assessments in Section 4.1 and the results of the qualitative analysis in Section 4.2 which comprises the textual statements provided in the survey and the statements given in the interviews.

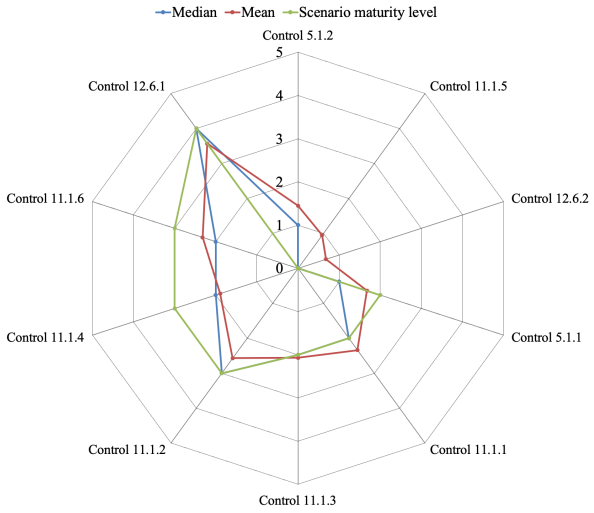
4.1. Practitioners' Maturity Level Assessments

Figure 4a illustrates the assessment results for each control in the form of boxplots. The red circle shows the median of the practitioner assessments. The upper and lower hinges of the boxes show the interquartile range (from 25th percentile to 75th percentile). The adjacent values are illustrated by the whiskers which indicate the minimum and maximum of the practitioner assessments. Furthermore, we added the scenario maturity levels to the graph (indicated by green rectangles) in order to enable a fast comparison between the assessments of the practitioners and the predefined scenario maturity levels. We ordered the controls in ascending order following the scenario maturity levels.

The boxplots show that the interquartile ranges are relatively large for all controls except for 12.6.2 and 12.6.1 indicating a large variance in the assessments of the practitioners. A similar picture is drawn by the large range between the lower and the upper whiskers which ranges for many controls from level 0 to 5.



(a) Boxplots illustrating the practitioner assessment for each control; red circle = median of practitioners' answers ; green rectangles = scenario maturity levels



(b) Spider diagram showing the median and mean practitioner assessments compared to the scenario maturity levels

Figure 4: Practitioners' assessments compared to the scenario maturity levels

However, for seven (out of ten) controls the median of the assessments still equals the scenario maturity level. For the remaining controls there is a deviation of one to the scenario maturity level.

To visualise the results in a more detailed manner, we created a spider graph plotting the scenario maturity levels, the median and the mean of the practitioner assessments (ordered by the scenario maturity level). The diagram is depicted in Figure 4b.

Comparing the average of the practitioners' assessments with the scenario maturity levels controls, three controls had a deviation greater than 1 (5.1.2, 11.1.4 and 11.1.5), most of the others had a deviation of less than 0.5.

Examining the median of the practitioner responses, the controls 5.1.2 11.1.4 and 11.1.6 had a deviation of one. The median values for all the other controls have been rated similarly to the scenario maturity levels, so their deviation is zero.

4.2. Practitioners' Qualitative Feedback

The quantitative results described in the previous section indicate that many practitioners struggled with the maturity level assessments. To better understand the reason why this is the case an extensive qualitative analysis has been conducted. The results are presented in the following paragraphs. They are based on statements given by the practitioners in both the survey and the ex-post interviews. The qualitative analysis investigates questions like why they have assessed the maturity levels as they did, how confident the practitioners have been with the quality of their assessments, or what have been the self-reported and the actual challenges for the practitioners.

4.2.1. Feedback on Improving the Maturity Levels

To understand why the practitioners have assessed the maturity levels as they did, they have been asked in the survey to explain for three controls (5.1.1, 11.1.1 and 12.6.1) by which additional measures the next maturity level could be achieved (see Question [F1, H1 and J1]).

With 56 participants explaining the possible improvements for three controls a maximum number of 168 explanations was possible. However, in many cases the practitioners have already assigned the highest maturity level of 5 so no answer could be given. Besides that, several other answers had to be excluded from the analysis since no meaningful evaluation was possible (e. g. «*To describe this I would need too much time*»). The remaining 66 answers provide insights about the potential difficulties in assessing the scenario's maturity level. To enable a systematic qualitative analysis, we have coded the answers (see Section 3.7).

Control 5.1.1. 28 answers refer to control 5.1.1 on policies for information security (see Question [F1]):

- Scenario misinterpreted (19): the practitioners suggested, for instance, a «*regular confirmation of knowledge from the employees*» as a further measure to achieve the next higher level of maturity which indicates that the scenario was misinterpreted because this concrete issue was already addressed in the scenario description (in paragraph 7), "an employee is obliged to check compliance with the regulations on a regular basis during the year." Another example demanded that the «*relevance [of the policy] must be communicated more clearly*» to achieve the next higher maturity level, although it has been explicitly mentioned that the policy has not only be published but that the employees have also been committed to it.

- Control misinterpreted (9): many answers refer to controls with a very different focus, i. e. , they ask for «*regular trainings of the employees*» (defined in 7.2.2), for «*guidelines for working in the server room*» (defined in 11.1.5), or that the «*access to the server room and installation of software must be defined and verified by a change management process*» (defined in 11.1.3 , 12.6.2 and 12.1.2). However, other answers refer to the much more related control 5.1.2 by demanding that the «*information security policy must be continuously checked*».

Control 11.1.1. 20 answers refer to control 11.1.1 on the physical security perimeter (see Question [H1]):

- Security measures exaggerated (13): an example for an exaggerated security measure mentioned several times is the implementation of a turnstile for the server room to only allow one person to pass at a time. Other than for larger organisations, this is not feasible for the small company described in the scenario.

- Scenario misinterpreted (5): a few comments addressed the video surveillance and requested, for instance, a video surveillance of the access area or a continuous video surveillance. However, according to the description, the entire company premises are permanently monitored. The same holds for the suggested security measure *«to define and to apply security perimeters»* which is explicitly described in the scenario.

- Control misinterpreted (2): two answers from the practitioners' indicate a misinterpretation of the control. One refers to the definition of working guidelines (which is defined in 11.1.5) and the other one refers to the *«implementation of an information security risk management»* (which is defined in the non-normative ISMS requirements)

Control 12.6.1. 18 answers refer to control 12.6.1 on the management of technical vulnerabilities (see Question [J1]):

- Control misinterpreted (13): almost all the misinterpretations with regard to control 12.6.1 concern the policy for new software installations which directly covered in control 12.6.2 ("Restrictions on software installation") and 12.5.1 ("Installation of software on operational systems").

- Security measures exaggerated (5): an exemplary exaggerated measure is the *«automatic analysis and prediction of neuralgic points by artificial intelligence»* which goes beyond what maturity level 5 strictly requires.

A similar picture is drawn by the participant's self-reported challenges. The participants have been asked in the survey for the reason of their uncertainty when evaluating the controls (see Question [M1] in the questionnaire): Given three answer options, 56% of them have stated that the COBIT standard was unclear, 44% had difficulties with the scenario, and for 26% the controls were not clear enough.

Summary. The answers of the practitioners show that different challenges exist for each of the controls. Some challenges did not appear for certain controls but every control was accompanied with at least two of the challenges. A misinterpretation of either the scenario or a control happened in 49 cases. Besides that, the suggestion of exaggerated measures was a central pattern. These findings are supported by the participant's self-reported challenges.

4.2.2. Reasons for Suggesting Exaggerated Measures

The results of the previous section show that one root cause leading to different maturity levels lies in the suggestion of exaggerated measures. For this reason, the study participants were asked in the interviews for possible explanations for suggesting such measures. The answers were categorised using the following code categories:

- Individual background (6): the largest number of explanations argue that different individual backgrounds of participants and how they are *«professionally socialised»* from their experience in *«a server farm or a data centre operation»* or in the critical infrastructure sector like *«in insurance companies or energy providers [might have the effect] that they are a little stricter than others from less regulated sectors»*. They might *« have regulatory requirements that we, for example, do not even know about or do not have in this form»*. Accordingly, they might tend to (unconsciously) expect more sophisticated measures *«when you take [such highly regulated] companies and infrastructures that you know well as a reference»*.

  Besides that, also the size of organisations someone has worked for might have an effect since *«in a larger company, however, I naturally need higher requirements»* because, for instance, *«I do not know all the employees there»*.

- Neglecting economic considerations (5): another explanation deals with the economic characteristics regarding the efficiency of measures. When asked about the turnstile, it was stated that in smaller organisations one would typically *«implement another equivalent measure that requires fewer resources but is equally effective.»* Another interviewee explained that in such a survey situation – *«when there is a larger distance to the target of evaluation»* and *«when you don't have to look at it economically [as in your own company] – you can fulfil your "dreams"»*. However, one interviewee, who works as an auditor, argued that *«efficiency is not subject of my evaluation»*.

Summary. The answers of the interviewees show that the reasons for suggesting exaggerated measures are twofold: they can be explained by someone's individual background which can make it difficult to fully get into the described scenario of the study. Apart from that, the individual viewpoint can also influence whether the cost efficiency of measures is taken into account in the assessments for the study similarly as one would expect it in case of internal real-world assessments.

4.2.3. Feedback on Challenges with Maturity Level Assessments

The practitioners have also been asked in the survey for general challenges with assessing security controls using the COBIT maturity levels (see Question [L1]): these self-reported challenges complement the picture drawn in the previous section. The answers were grouped into four categories:

- The scope for interpretation (8): the scope for interpretation was also perceived as challenge: *«Like all standards, the COBIT maturity level is partly subject to subjective assessments and offers a lot of room for interpretation»*. This would hold for the *«subjective perception depending on organisations / organisational area»* but also for the perspectives of different *«stakeholders (internal or external)»*.

- Differentiation between maturity levels (15): to distinguish certain maturity levels has been perceived as the major challenge in assessing the controls' with COBIT maturity levels. The practitioners stated that *«the borders between maturity levels are often very softly defined»* and *«the borders are difficult to distinguish»* as reasons. The answers also indicate that not all maturity levels are equally challenging to assess. This would hold in particular for the *«the differentiation of the maturity levels 3-5»* respectively for the *«the differentiation in real life between the maturity levels 2, 3 and 4»*. Further answers suggest that difficulties can also be caused by mixing up different maturity level models: *«the COBIT 5 maturity levels are not congruent with the familiar CMMI levels. Therefore, some uncertainties.»*.

- Control dependencies (3): another self-reported challenge were the dependencies between the controls which makes the assessment more difficult.

- Mapping Controls to processes (3): a few practitioners expressed the difficulty of mapping controls to the underlying processes since some controls would be performed only once and would *«not necessarily reflect a process»*.

- Lack of skills (3): the last group subsumes a lack of skills by the practitioners. This can involve, for instance, the *«assignment of the security measures to the individual maturity levels»* but also a lack of knowledge or experience with the COBIT standard (e. g. *«lack of familiarity with the COBIT standard»*, or *«only basic understanding of COBIT maturity levels»*).

Summary. Over half of the statements (29 out of 56) indicate that the differentiation between maturity levels is a predominant challenge. This especially holds for border cases since there is not always a sharply defined border. This is where the second challenge, the scope of interpretation, comes into place which goes in line with the results in Section 4.2.1 referring to participants misinterpreting the scenario or suggesting exaggerated security measures.

4.2.4. Reasons for Difficulty in Maturity Level Assessments

To further investigate the challenges and to complement the already drawn picture, the interviewees were asked for the challenges of maturity level assessments (see Question [B1 and B2] of Appendix C): their statements have been structured into three sub-categories. The first two categories serve a better understanding of the challenge "scope for interpretation" described before; the last category corresponds to the challenge to distinguish between maturity levels.

- Differences in internal and external assessments (9): one category of explanations deals with the differences between internal and external assessments. The majority of the explanations were about a tendency towards mild assessment in self-assessments and more rigid external assessments. This attitude is explained by some participants as follows: *«it is "easier" to be objective in the evaluation of an external company where you are not directly involved»* or *«mostly people judge themselves less critically than they would be judged by their peers»*. One interviewee also highlighted the problem of informal information channels (*«as an external person and as a consultant, this is, of course, a little more difficult, because the informal information channels, which somehow should be disregarded, influence the result»*). This statement highlights the degree of tension the evaluators are under.

- Not all controls represent processes (3): the next category addresses that not all controls are seen as process-oriented. The participants described this area of tension, for instance, as follows: *«I would rather see controls as triggers of processes, others do not really fall into the process-oriented approach»*.

- Selectivity for maturity level (4): the interviewees agreed to the statements of the survey that *«in reality one is often exactly on the threshold between two levels of maturity and the evaluation of these grey areas, these transitions are always difficult»*. Besides that, it is *«often difficult to separate personal opinion from hard requirements»*.

Summary. Major challenges in the assessment of maturity levels are seen in particular in the subjective bias in internal assessments (in contrast to more objective external assessments). Further difficulties would arise in the differentiation of maturity levels, especially at the gray areas between two levels, as well as the assessment of controls that are not entirely process-oriented.

5. Analysis of Individual Assessment Capabilities

The previous section demonstrates that the practitioners as a whole had only a mediocre performance in assessing maturity levels of security controls. The results showed disperse and deviant practitioner ratings for some of the controls.

While we already have gained insights on why this might be the case, in this section, we aim to investigate if there are certain subgroups that performed significantly better than others. This way, we aim to identify general challenges of the assessment, areas or groups which are in particular need of further support, and professional characteristics (e. g. work experience, academic background, certificates) which have an effect on the assessment capability. With these insights, we aim to get a better understanding of how to improve the quality of maturity level assessments.

For this purpose, we use a mixed-methods approach. First, the practitioners' maturity level assessments are analysed quantitatively, followed by a qualitative analysis of textual statements that the participants have entered in the survey. Finally, ex-post interviews have been performed with some of the participants to better understand their rationales and their challenges.

5.1. Quantitative Analysis of the Practitioners' Assessments

The boxplots in Figure 5 show the deviation $f$weper practitioner, sorted by average deviation from the scenario maturity level. The red points represent the median deviation. It illustrates that while for many practitioners the median deviation for all their assessments is zero or close to it, that's mostly because they had roughly the same number of over- and under-assessments. Not surprisingly, the range of deviations for each practitioner increases from the left to the right.

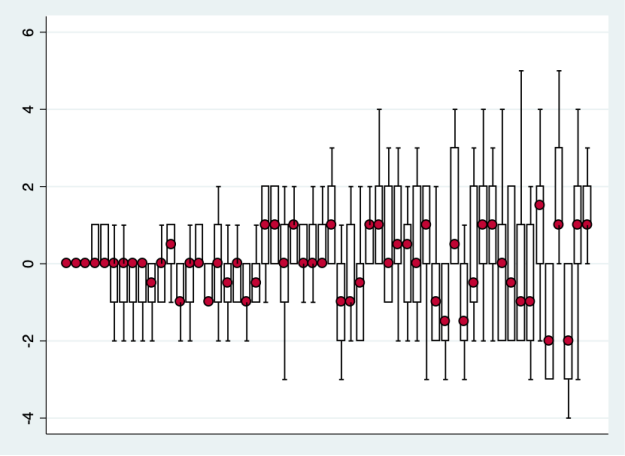


Figure 5: Boxplots illustrating each practitioner's deviation in the assessments

It has also been examined whether the participants were either too strict or too mild in their assessments. The t-test did not show any significant results in this respect.

To measure the practitioners' performance, we had a look at both metrics, the average linear deviation from the scenario maturity levels and the number of matches with scenario maturity levels. The histogram depicted in Figure 6a presents the distribution of the practitioners' performance based on the linear deviation from the scenario maturity levels. The linear deviation ranges from from 0.3 to 1.9 (with an average of 1.07). Figure 6b shows the number of matches with the scenario maturity levels. It demonstrates that the best practitioners have 7-8 (out of 10 possible) matches and that there are substantially more practitioners that struggled with the majority of the assessments.

Not surprisingly, a Spearman's rank correlation revealed a ρ of -0.79 (with the p-value $< 4.2 \cdot 10^{-13}$) which means that with high probability there is a strong correlation between the average linear deviation from the scenario maturity levels and the number of practitioners' matches with the scenario's maturity levels. Thus, for our further analysis, we focused on the average linear deviation from the scenario maturity levels.

Table 5: Analysis of the professional characteristics for the top and bottom 25% practitioners

Professional Characteristics	Number of Occur. for	
	25th Perc.	75th Perc.
Longtime work exp.	11 (79%)	5 (36%)
Longtime ISO/IEC 27002 exp.	7 (50%)	3 (21%)
CMM/CMMI/SSE-CMM exp.	9 (64%)	4 (28%)
CISM/CISA certificate	7 (50%)	2 (14%)
IT-Grundschutz certificate	5 (35%)	1 (7%)
ISMS certificate	9 (64%)	0 (0%)
ISO/IEC 27001 certificate	10 (71%)	4 (28%)
Without certificate	1 (7%)	4 (28%)

Table 6: T-tests analysing differences between certain groups for the deviation of the practitioners' assessments and the scenario maturity levels.

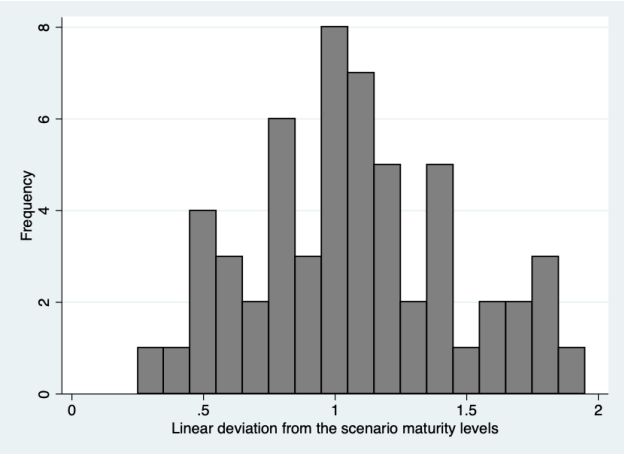
Independent Variables	Group Size		t-value
	yes	no	
Longtime work exp.	18	38	*n.s.*
Longtime ISO/IEC 27002 exp.	16	40	*n.s.*
CMM/CMMI/SSE-CMM exp.	26	30	*n.s.*
CISM/CISA certificate	20	36	2.1056$*$
IT-Grundschutz certificate	10	46	2.1482$*$
ISMS certificate	14	42	3.4833$**$
ISO/IEC 27001 certificate	26	30	2.6762$**$
Without certificate	12	44	*n.s.*

* and ** asterisks indicate statistical significance at 5%-level and 1%-level

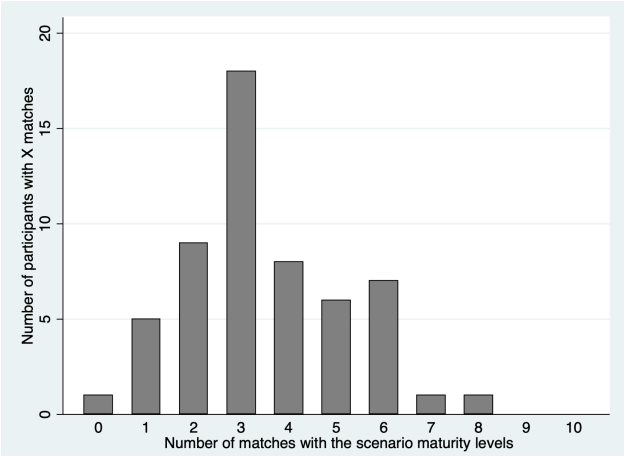
In order to identify the decisive characteristics that affect the practitioners' assessment capabilities, we first had a look at the 25th and the 75th percentile (14 practitioners each) and have compared their professional characteristics. As shown in Table 5 large differences become evident for eight attributes: longtime work experience and longtime experience with ISO/IEC 27002 (both with more than 10 years), experience with the maturity models CMM, CMMI or SSE-CMM, and whether the participant has obtained a specific security certificate (CISM/CISA, IT-Grundschutz, ISMS, ISO/IEC 27001) or not. For example, 9 out of the top 14 (25th percentile) have obtained an ISMS certification, whereas none of the bottom 14 (75th percentile) has such certification.

In the following, the effects of these attributes are statistically analysed. Table 6 provides the results of t-tests assessing whether there are statistically significant differences between these groups of practitioners in their average deviation per control. The overall group size is 56 (N=56).

The t-tests indicate that having obtained any of the listed security certificates has a positive effect on the assessment capabilities. Practitioners with such certifications show a lower deviation to the scenario maturity levels and perform significantly better than others. This especially holds for ISMS and ISO/IEC 27001 certifications with a strong effect at 1%-level , and IT-Grundschutz certifications and CISM/CISA at 5%-level. For the other variables there is no evidence for significant effects.



(a) Histogram for the linear deviation from the scenario maturity levels



(b) Histogram for the matches with the scenario maturity levels

Figure 6: Practitioner assessments compared to the scenario maturity level

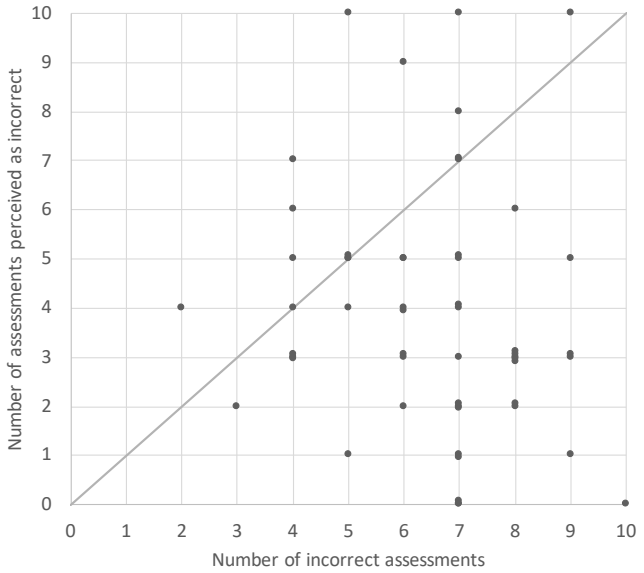


Figure 7: Perveived self-assessment capabilities

Furthermore, we analysed the practitioners' self-assessment capabilities to investigate how the practitioners perceived the quality of their assessments. The practitioners were asked with how many (out of the ten) assessments they felt uncertain. (see Question [K1]). Their self-perception was then compared with their actual assessments. The results are shown in Figure 7. Results with the same characteristics were stacked on each other.

Figure 7 suggests that most practitioners were overly confident, so we validated that impression with a t-test which showed that there is a statistically significant difference between their perceived and their actual performance. The t-test yields a t-value of -2.574074 with a p-value of $< 0.3454 \cdot 10^{-6}$ which means that the practitioners have on average correctly assessed roughly 2.5 controls less than they thought (6.5 incorrect assessments vs. 4 assessments perceived as incorrect).

Moreover, the Spearman's rank correlation coefficient has been calculated. There is no significant correlation between the perceived and the real assessment capabilities for the practitioners as a whole. This is different for both professional characteristics "longtime work experience", "longtime ISO/IEC 27002 experience" and "CMM/CMMI/SSE-CMM experience". For these characteristics a weak (negative) correlation could be found (see Table 7). So for any of these practitioner groups, more confident practitioners tend to perform worse than other practitioners. We could neither find a similar nor an opposite effect for the different groups of certificate holders.

Table 7: Spearman's rank correlation indicating statistically significant correlations between certain groups for the number of assessments perceived as incorrect and the actual number of incorrect assessments.

Independent Variables	Group Size	ρ
Longtime work exp.	18	-0.3911*
Longtime ISO/IEC 27002 exp.	16	-0.5717*
CMM/CMMI/SSE-CMM exp.	26	-0.4981*
CISM/CISA certificate	20	n.s.
IT-Grundschutz certificate	10	n.s.
ISMS certificate	14	n.s.
ISO/IEC 27001 certificate	26	n.s.
Without certificate	12	n.s.
All participants	56	n.s.

* and ** asterisks indicate statistical significance at 5%-level and 1%-level

5.2. Qualitative Analysis of the Practitioners' Rationale

To get an idea how the different challenges in the assessment (see Section 4.2) were applying to different groups of participants, the occurrence and the distribution of codes have been analysed with respect to different groups of practitioners. We decided to investigate the four groups with significant differences in the performance (see Table 6): holder of an ISO/IEC

27001 certificates (26 yes, 30 no), holder of a CISM/CISA certificate (20 yes, 36 no), holder of an ISMS certificate (14 yes, 42 no) and holder of an IT-Grundschutz certificate (10 yes, 46 no). Additionally, since we chose a small company in our scenario, we assumed that the code 'security measures exaggerated' might be more relevant for participants in a large company. Therefore, we also analysed this group. For that purpose, we defined large company by companies with more than 5,000 employees since this divided the participants into two groups of almost the same size (27 in a small or medium vs. 29 in a large company). These five groups are now compared with respect to the occurrence of the codes.

Not all of these five groups split their members and non-members into equal-sized groups. Therefore, for each group, we calculated the relative number of codes per group and compared it with the percentage of members in the group as shown in Fig. 8. The Y-axis represents the proportion of group members versus non-members (e. g. 0.52 (29/56) ratio for participants from large companies), the X-axis describes the proportion of participants for whom a code has been assigned (e. g. 0.94 (15/16) ratio for exaggerated security measures from the participants of large companies). To foster a better visualisation, we also added the 45-degree line. Points located above this line represent more codes in the non-member group while points below the line represent more codes in the member group.

Regarding the distribution of the respective groups of the code 'control misinterpreted' (see Figure 8a), all groups are reasonable close to an equal distribution of codes for members and non-members with the group of participants with an ITG certificate slightly standing out.

Similarly, the distribution of the respective groups of the code 'scenario misinterpreted' (see Figure 8b) shows no larger deviations and all groups are reasonable close to the equal distribution of codes for members and non-members.

For the code 'security measures exaggerated' (see Figure 8c), two groups stand out. Holders of an ISMS certificate did not propose any exaggerated security measure. On the other hand most of the exaggerated security measures were proposed by participants from large companies.

Overall, the analysis indicates that there are no huge differences between the groups regarding the interpretation of the controls and the scenario. In contrast, exaggerated security measures were mostly proposed by participants from large companies which may have had problems to adapt to the scenario of a somewhat small company.

5.3. Support for Maturity Levels Assessments

The previous results indicate that the assessment of security maturity levels is hard for most of the practitioners. Therefore, we investigated in the ex-post interviews how the assessors could be supported. The key statements have been structured into the following categories:

- Discussion of maturity level assessments (3): this suggestion aims to improve the assessment quality by the discussion on maturity levels between two or more assessors. This is underlined by statements from participants like «*it makes sense to discuss this with a consultant*» or to «*gain experience in an audit team*» .
- Provide examples (1): another type of supports points out that examples for the different maturity levels would help the participants («*examples would help you to find out what to look for or what are the typical characteristics when you want to assess the degree of maturity*»).
- Present "must" and "should" requirements (1): one interviewee referred to the TISAX standards which is a de-facto standard in information security management in the German automotive industry. Its VDA-ISA presents a number of "must" and "should" requirements for each control («*in order to obtain more consistent results, one would have to add some more information such as the VDA-ISA or TISAX standards*»).
- Use catalogue of measures (1): another suggestion goes one step further and asks for more additional information per control and maturity level: «*I definitely consider a catalogue of measures per control/maturity level as helpful*».
- Training courses for maturity level assessments (1): another option could be a specific a training which could help to improve the assessments quality. «*Pure trainings for maturity assessment are not known to me*» indicates that the participants are not aware of any corresponding offer but would find it useful.

Additionally, two practitioners also mentioned that a more detailed description of the maturity levels would not be helpful for them. However, there is still a wide range of ideas that can be applied in order to support assessors. This can also be achieved by combining different types of support.

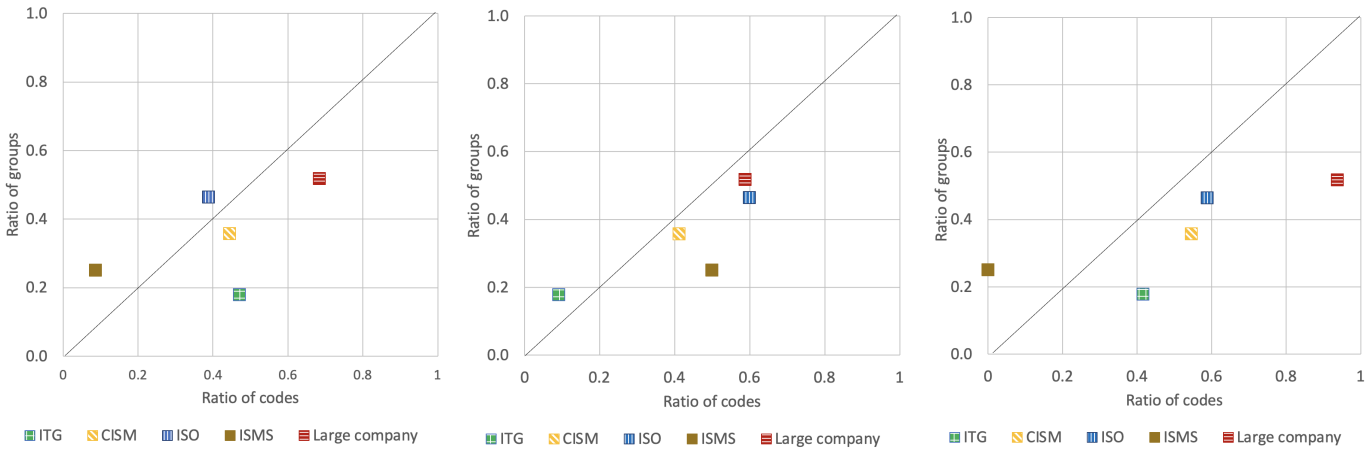
6. Discussion

Both the quantitative and the qualitative analysis indicate that most practitioners struggled with the maturity level assessments.

6.1. Quality of Maturity Level Assessments

In this section, we discuss findings related to the quality of the assessments.

Assessing a Scenario Versus Assessing the Own Company One possible explanation for the poor performance of many practitioners is that the scenario was built for another context (size, industry domain, etc.) than the participants' company. A study by El Emam et al. showed that the assessment capability is higher when practitioners assess their own organisation [23]. So the practitioners might have performed better if they had evaluated their own company instead of a hypothetical scenario. This hypothesis is also supported by the finding that some of the practitioners did not sufficiently get into the scenario. This is especially the case for practitioners from larger organisations



(a) Code 'control misinterpreted' **(b)** Code 'scenario misinterpreted' **(c)** Code 'security measure exaggerated'

Figure 8: Distribution of codes for certain groups

who have suggested exaggerated security measures more frequently (see Figure 8c). Although the size of an organisation does not determine per se its protection requirements, larger organisations, in general, can implement and maintain complex security measures more economically, e. g. through economies of scale and more financial and personnel resources.

Neglecting Economic Considerations and Wiggle Room
Quite a few practitioners proposed exaggerated measures to improve a certain maturity security level. The reason for that was partly not considering the preconditions in the scenario (small company), partly that there is some room for interpretation and last but not least a disagreement of the consideration of economic factors. Building on economic factors and restrictions is also connected to the previous finding that assessors tend to assess their own company better. It might also be the reason for the findings of El Emam et al. [23] who found that internal assessors typically know their organisation's processes better hence a different perception.

In contrast to the other interviewees one of them, working as an external auditor, denied that economic restrictions should be considered in the assessment. However, it is explicitly stated in ISO/IEC 27000 that the implementation of controls should take into account economic considerations like "the cost of implementation and operation in relation to the risk being reduced, and remaining proportional to the organisation's requirements and constraints". Also, other related standards emphasise the need to balance security and costs in the selection and implementation of security controls, e. g. ISO/IEC 27005 and, in particular, ISO/IEC 27016 which focuses on economic aspects in information security management.

Assessors with Certificate Perform Better
It could also be seen that practitioners with security certificates (especially ISMS and ISO/IEC 27001 certificates) performed significantly better than others. This indicates that assessing maturity levels is not a trivial task and requires specific expert knowledge.

Quality Assurance: Practitioners' are Overconfident
Regarding the practitioners' overconfidence, one possible explanation is that they had experience with other maturity models which lead to the observed overconfidence.
Furthermore, the statistical analyses have shown that practitioners with longtime ISO/IEC 27002 experience or with experience in maturity level models with higher confidence tend to perform worse than others. This cognitive bias is quite common in other areas and also known as Dunning-Kruger effect [27].

Mixing Up Maturity Level Models
Some practitioners might have mixed up different maturity level models or different versions of the same model that they are more familiar with. One practitioner has explicitly stated that it is challenging to work with a new maturity level model other than the one they are familiar with. To mitigate this possible issue, we explicitly described the COBIT maturity model and its characteristics in the questionnaire and put the relevant tables on each page with assessments again. Participants also had the possibility to open a portable document format file in another window to always have the descriptions at hand.

6.2. Impact for Real-World Assessments

In this section, we discuss how our findings could be used to improve the quality of real-world assessments. Since most practitioners struggled with the maturity level assessments, in practice there is the need to provide additional support. There are numerous ways to provide additional support to practitioners. This became evident due to the practitioner's answers in the survey but also, and more extensively, in the ex-post interviews where the practitioners have been explicitly asked what kind of assistance would have helped them (see Question [M1]).

Detailed Definitions of the Security Maturity Level
For example, it could be helpful to provide a more detailed definition for each maturity level, as suggested by some practitioners in the survey. However, the interviewees did not see a value in more detailed definitions. So probably those descriptions only help less experienced assessors. In addition to having only definitions, one could, for instance, better explain them

based on concrete examples.

Support for Connecting Measures and Controls
Some practitioners explicitly referred to the VDA-ISA questionnaire that comes up with more detailed definitions. It also defines for each question (that in most cases covers several security controls according to ISO/IEC 27002) set security measures that (a) must or (b) should be implemented in order to fulfil the respective controls. This additional support could also be extended to a catalogue of security measures that defines for each control which (exemplary) measures are to be implemented in order to achieve each maturity level. This approach is defined in the COBIT framework.

Assessment in Teams
Another factor that might inhibit the assessment quality is the number of practitioners involved in an assessment. In the experiment, the practitioners conducted the assessments independently. However, the results might have been better if two practitioners had discussed and assessed the maturity levels together, similar to the concept of pair programming in agile software development.

Training Courses for Maturity Level Assessments
Besides the already mentioned measures, training courses for COBIT maturity level assessments could be valuable that provide sufficient time to practice the learned know-how intensively. The interviewees were not aware of any dedicated training course. One participant of the survey also asked if he could use the experiment of the survey because of this.

Mapping Controls to Processes
Assessing maturity levels of ISO/IEC 27002 controls is a common practise in industry and is also supported by standard GRC tools like risk2value which is used by major companies [8]. However, it was mentioned that not all ISO/IEC 27002 controls map equally well to processes. Some of them would need to be merged accordingly to be assessed in a process-oriented manner. A prominent example following this procedure is the VDA-ISA questionnaire (a de facto standard in the German automotive industry described earlier), where maturity level assessments of controls are conducted in this way. Alternatively, the ISO/IEC 27002 controls can be mapped to (COBIT) processes as shown by Sheikhpour et al. [28].

6.3. Limitations and Threats to Validity

Besides the already mentioned limitations, i. e. a hypothetical scenario instead of the practitioners' organisations, we discuss further limitations here.

Scenario
In our experiment, all relevant information was given in the scenario description. In practice, it can be much more complex to collect all relevant information that is needed to assess the maturity levels, especially for larger organisations. Thus, it is not clear to which degree our experiment reflects reality. However, given that one of the key points of our experiment was a theoretically sound elaboration of the security maturity levels, we could not ask the participants for evaluations within their organisation. Furthermore, this would also have lead to problems regarding the comparability and confidentiality of the security maturity levels.

El Emam et al. [23] found in their study that the degree of reliability strongly varied between different processes. That bears the risk that our selection of processes/controls is not representative for all ISO/IEC 27002 controls.

Due to the participants' time limitations, we could only ask for the assessment of a limited amount of controls. Having the full list of controls to assess may have led to less misinterpretations of controls because the differences between the mixed-up controls would have been more obvious if both of them would have been presented.

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

Another limitation is the number of participants. A higher number of participants would make it possible to measure smaller effects, influencing the practitioners' ability to assess the maturity levels as well. Besides the total number of participants, also the high number of participants from larger companies (22) could also have led to non-representative results.

Apart from that, the results are only valid for Germany since the study was conducted there. With practitioners from other countries, who are more or less familiar with the COBIT standard and with the ISO/IEC 27002 controls, the results might be different.

7. Conclusion

"Measuring security is hard" as Pfleeger et al. state [29]. This is particularly true at a high-level organisational level that typically deals with complex targets of evaluation and has a large scope. For that purpose, maturity models play an important role in assessing information security. However, these assessments are carried out by humans, and thus the 'human factor' of the evaluation may lead to possible uncertainties and subjectivity, e. g. because a pool of evaluators with different physical and mental conditions of the same evaluator on different days were involved.

The main goal of our paper was to examine the practitioners' capabilities to accurately assess the maturity level for security controls. In contrast to other studies, we did not compare the level of agreement between the participants but constructed a scenario where we defined the maturity level for each security control following the involved standards, i. e. ISO/IEC 27002 and COBIT. We show that many practitioners had a large deviation from the predefined maturity levels. The result confirms our design decision and the need to compare the practitioners' assessments to a baseline and not only to each other. Due to this design decision, we were also able to identify differences in the evaluation of practitioners for certain groups. We showed that practitioners with security certificates had better assessment results. Moreover, the practitioners' perceived performance seemed not to be related to their actual performance and for some groups practitioners (e. g. more than 10 years work experience), we even found a weak inverted correlation, also known as Dunning-Kruger effect [27].

We conclude that some form of assistance for the evaluation or classification into maturity levels is needed and elaborate on possible support such as assessment in teams or specialised documentation. As a consequence, this can be seen as another change in the profile of and thus the requirements for the education of security managers (cf. Virtanen [30]), where some dedicated training for this kind of task is needed.

In future work, a systematic analysis of how quality can be improved concerning the maturity models could reduce the uncertainty of these assessments. It would also be useful to identify more individual and organisational characteristics that improve the quality of assessing controls' maturity levels. Furthermore, it would be interesting to investigate the intra-assessor reliability, to learn how the assessments of the same assessor differ when assessing multiple times.

Acknowledgments

This work was partially supported by the European Union's Horizon 2020 research and innovation program (grant agreement number: 830929).

References

[1] Accenture security, Ninth annual cost of cybercrime study, https://www.accenture.com/_acnmedia/PDF-96/Accenture-2019-Cost-of-Cybercrime-Study-Final.pdf, 2019.

[2] IBM security, Cost of a data breach report 2019, "https://www.all-about-security.de/fileadmin/micropages/Fachartikel_28/2019_Cost_of_a_Data_Breach_Report_final.pdf", 2019.

[3] Council of European Union, General data protection regulation, "https://eur-lex.europa.eu/eli/reg/2016/679/oj", 2016.

[4] T. DeMarco, Controlling Software Projects: Management, Measurement, and Estimates: Management, Measurement and Estimation, Pearson Education (US), 1982.

[5] R. Böhme, Security metrics and security investment models, in: Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), volume 6434 LNCS, pp. 10–24.

[6] M. Rudolph, R. Schwarz, Security Indicators - A State of the Art Survey Public Report, FhG IESE VII (2012).

[7] Verband der Automobilindustrie (VDA), Information security assessment, https://www.vda.de/de/services/Publikationen/information-security-assessment.html, 2020.

[8] Avedos, https://avedos.com/en/risk2value-isms-bsi-solution/, 2020.

[9] C. Schmitz, S. Pape, Lisra: Lightweight security risk assessment for decision support in information security, Computers & Security 90 (2020) 101656.

[10] M. Schmid, S. Pape, A structured comparison of the corporate information security maturity level, in: G. Dhillon, F. Karlsson, K. Hedström, A. Zúquete (Eds.), ICT Systems Security and Privacy Protection, Springer International Publishing, Cham, 2019, pp. 223–237.

[11] C. Schmitz, A. Sekulla, S. Pape, V. Pipek, K. Rannenberg, Easing the burden of security self-assessments, in: N. L. Clarke, S. Furnell (Eds.), Twelfth International Symposium on Human Aspects of Information Security & Assurance, HAISA 2018, Dundee, Scotland, UK, August 29-31, 2018, Proceedings, University of Plymouth, 2018, pp. 272–281.

[12] P. Bowen, J. Hash, M. Wilson, C. M. Gutierrez, W. Jeffrey, Information Security Handbook: A Guide for Managers, NIST Special Publication 800-100 (2006).

[13] NIST, NIST Releases Version 1.1 of its Popular Cybersecurity Framework, National Institute of Standards and Technology (2018).

[14] Bundesamt für Sicherheit in der Informationstechnik, BSI - IT-Grundschutz, 2019.

[15] P. Kusumah, S. Sutikno, Y. Rosmansyah, Model design of information security governance assessment with collaborative integration of cobit 5 and itil (case study: Intrac), in: 2014 International Conference on ICT For Smart Society (ICISS), IEEE, pp. 1–6.

[16] D. Proença, J. Borbinha, Maturity models for information systems - a state of the art, Procedia Computer Science 100 (2016) 1042 – 1049. International Conference on ENTERprise Information Systems/International Conference on Project MANagement/International Conference on Health and Social Care Information Systems and Technologies, CENTERIS/ProjMAN / HCist 2016.

[17] J. D. Christopher, D. Gonzalez, D. W. White, J. Stevens, J. Grundman, N. Mehravari, T. Dolan, Cybersecurity capability maturity model (c2m2), Department of Homeland Security (2014) 1–76.

[18] M. Saleh, Information security maturity model, International Journal of Computer Science and Security (IJCSS) 5 (2011) 21.

[19] M. B. Chrissis, M. Konrad, S. Shrum, CMMI for Development: Guidelines for Process Integration and Product Improvement, Addison-Wesley Professional, 3rd edition, 2011.

[20] International Organization for Standardization (ISO), International Electrotechnical Commission (IEC), ISO/IEC 15504-5:2012, information technology – process assessment — part 5: An exemplar software life cycle process assessment model, 2012.

[21] Information Systems Audit and Control Association (ISACA), CobiT 5: A Business Framework for the Governance and Management of Enterprise IT, Rolling Meadows, 2012.

[22] S. Zhang, F. H. Le, et al., An examination of the practicability of cobit framework and the proposal of a cobit-bsc model, Journal of Economics 1 (2013) 5.

[23] K. E. Emam, L. Briand, R. Smith, Assessor agreement in rating spice processes, Software Process: Improvement and Practice 2 (1996) 291–306.

[24] H.-y. Lee, H.-W. Jung, C.-S. Chung, J. M. Lee, K. W. Lee, H. J. Jeong, Analysis of interrater agreement in iso/iec 15504-based software process assessment, in: Proceedings Second Asia-Pacific Conference on Quality Software, IEEE, pp. 341–348.

[25] Bundesamt für Sicherheit in der Informationstechnik, Zuordnungstabelle ISO zum modernisierten IT-Grundschutz, 2018.

[26] F. Gleich, Tisax participant handbook, 2019.

[27] J. Kruger, D. Dunning, Unskilled and unaware of it: How difficulties in recognizing one's own incompetence lead to inflated self-assessments, Journal of Personality and Social Psychology 77 (2000) 1121–34.

[28] R. Sheikhpour, N. Modiri, An approach to map cobit processes to iso/iec 27001 information security management controls, International Journal of Security and its Applications 6 (2012) 13–28.

[29] S. Pfleeger, R. Cunningham, Why measuring security is hard, IEEE Security Privacy 8 (2010) 46–54.

[30] T. Virtanen, Changes in the profile of security managers, in: Security education and critical infrastructures, Springer, 2003, pp. 41–49.

All sources were last accessed on the 7th of January 2021.

Appendix A. Scenario Description

General: CloudSec is an IT service provider that primarily offers cloud services (IaaS, PaaS and Saas) for other companies. For this reason physical security is very important. Fig. 1 schematically shows the scenario described below.

(1) Security assessment: to systematically improve their information security CloudSec use an ISMS (Information Security Management System) and evaluate the maturity levels of their company on a quarterly basis using a tool specifically provided for this purpose. They are guided by the security controls of ISO/IEC 27002. In addition, an internal control system has been implemented which prescribes binding inspection activities at various intervals to ensure, among other things, that the controls are carried out properly.

(2) Information security policy: CloudSec's management recently approved and published its first information security policy and committed its employees to it. For this purpose, a security team commissioned by the management first defined the security goals and strategies. As the process took a long time no further resources will be invested in the review of this policy in the future. However, according to internal guidelines, compliance with the information security policy must be regularly reviewed by the security team on a random basis.

(3) Access control by gatekeeper: to get access to the building all persons have to prove their identity by showing their employee ID card to a gatekeeper. The security team is also responsible for ensuring that the gatekeeper can see the updated access rights at any time. These are created based on an organisation-wide process and are regularly updated. Since couriers do not have access rights to the building, all packages are delivered directly to the gatekeeper, who forwards them to the recipient. Furthermore, all visits are documented and external persons are also supervised.

(4) Video surveillance: moreover, the entire company premises are permanently monitored by a video system and checked for suspicious activities.

(5) Protection measures for server room: since the server room has been classified a critical security zone, it is protected by a burglar-resistant door and by a fingerprint scanner. For security reasons, it is also located in the rear part of the building.

(6) Working guidelines: however, there are no guidelines for working in the server room. Due to a lack of information security risk management, the relevance of this topic is currently not recognised in the company. The same applies to guidelines for the installation of new software.

(7) Compliance with regulations: the relevant regulations for protection against other external threats (e. g. fire protection regulations) were systematically identified, analysed and evaluated within the company. In addition, an employee is obliged to check compliance with the regulations on a regular basis during the year in order to take action if necessary.

(8) Vulnerability management: in order to guarantee the security of Cloudsec's own server applications, these are automatically checked with vulnerability scanners on a daily basis (identification). In order to continuously increase the security level, the identified vulnerabilities and their criticality (CVSS value) are stored centrally, checked directly by the security team (analysis) and if necessary – depending on the risk for the company – mitigated immediately (evaluation and handling). In addition, the security of the technical infrastructure is continuously documented using KPIs and checked at least once a year by external experts using penetration tests.

(9) Backups: all servers are backed up daily. The backups are stored in a fire compartment other than the server room. Restore tests are carried out only occasionally.

Appendix B. Questionnaire

Section A: Organisation's Demographics

A1 What industry sector does your organisation operate in? If you are an IT consultant please state your industry experience under "Other".

- Automobile industry
- Chemical and raw industry
- Services and crafts
- E-commerce and trade
- Energy sector
- Food sector
- Finance and insurance
- Healthcare sector
- Information technology and telecommunications
- Media and culture
- Metal and electronics
- State and administration
- Tourism and gastronomy
- Transport and traffic
- Water management
- Other[3]

A2 Is your organisation classified as critical infrastructure?

- Yes
- No
- I don't know

A3 Is your organisation certified against the ISO/IEC 27001 standard?

- Yes
- No
- I don't know

A4 How many employees does your organisation have?

- Less than 100
- 100-500
- 500-1,000
- 1,000-5,000
- 5,000-10,000
- More than 10,000

[3] Text box for additional comments

Section B: Person's Demographics

B1 In which area do you work in your organisation?
- IT security or information security
- General IT
- Management
- Other[3]

B2 How many years of experience do you have in IT security or information security?
- Less than 1
- 1-5
- 6-10
- 11-15
- 16-20
- More than 20

B3 How many years of experience do you have in Critical Infrastructures?
- Less than 1
- 1-5
- 6-10
- 11-15
- 16-20
- More than 20

B4 Are you familiar with the basic idea of maturity models?
- Yes
- No

B5 What specific maturity models are you familiar with?[4]
- COBIT 5 maturity model
- CMM, CMMI oder SSE-CMM
- None
- Others

B6 How many years of experience do you have with COBIT 5 maturity levels?[5]
- Less than 1
- 1-5
- 6-10
- 11-15
- 16-20
- More than 20

B7 How many years of experience do you have with CMM, CMMI or SSE-CMM?[5]
- Less than 1
- 1-5
- 6-10
- 11-15
- 16-20
- More than 20

B8 What other maturity models are you familiar with?[5]

B9 How many years of experience do you have with other maturity models?[5]
- Less than 1
- 1-5
- 6-10
- 11-15
- 16-20
- More than 20

B10 Are you familiar with the rating scale for process attributes used in COBIT (see below)? Evaluation Achievement of goals:[5]
  - Not achieved (N): 0% - 15%
  - Partially achieved (P): 15% - 50%
  - Largely achieved (L): 50% - 85%
  - Fully achieved (F): 85% -100%

B11 How many years of experience do you have with ISO/IEC 27002 controls?
- None
- Less than 1
- 1-5
- 6-10
- 11-15
- 16-20
- More than 20

B12 Which certifications have you obtained in the field of information security so far?
- CISM/CISA
- CISSP
- ISO/IEC 27001 (e. g. ISO/IEC 27001 Lead Auditor)
- IT basic security
- ISMS
- None
- Other[3]

B13 What other trainings (trainings/courses) have you completed in the field of information security?
- None
- Other[3]

B14 What is your highest level of education?
- No vocational qualification
- Vocational training
- Bachelor's degree
- Master's degree
- Ph.D.

B15 Which subject did you study at university?[6]
- Computer Science
- IT Security
- Other[3]

Section C: Description of Maturity Levels

On this page, the term 'security control' and the concept of 'maturity levels', which are used in the following, are introduced. They are important for answering further questions. So please read the following paragraphs carefully.

Evaluation of security controls based on maturity levels

A security control describes security requirements that can be fulfilled by performing the corresponding security measures. So a control is associated with one or more security measures. A security control can be assessed by its maturity level. The higher a control's maturity level, the higher are the chances that it is performed in a correct and effective way. For the following questions, the COBIT maturity levels are used. The levels are defined in the table below.

Section D: Description of Scenario

This page describes a scenario. The described security controls should be assessed on the following pages. So please read the text carefully.[7]

[4] Only asked if familiarity indicated in B4

[5] Only asked if familiarity indicated in B5

[6] Only asked if university background indicated in B14

[7] Here the description of the scenario as sketched in Section Appendix A followed.

Section E: Scenario's Maturity levels

On the following pages, the COBIT maturity levels for the scenario presented are to be determined for selected controls. Additional questions are then asked for three of the maturity assessments.

E1 Please assess the COBIT maturity levels for each security control on the left side according to the described scenario. The security controls are defined in Section 5 'information security policies', sub-section 5.1 'management direction for information security' of the ISO/IEC 27002.[8]

	0	1	2	3	4	5
5.1.1 - Policies for information security: a set of policies for information security should be defined, approved by management, published and communicated to employees and relevant external parties.						
5.1.2 - Review of the policies for information security: the policies for information security should be reviewed at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.						

Section F: 5.1.1 Next Level

You have just assessed the maturity level for the following control: "5.1.1 - Policies for information security: a set of policies for information security should be defined, approved by management, published and communicated to employees and relevant external parties."

F1 What additional activities would be necessary in your opinion so that CloudSec reach the next level of maturity for this control?

Section G: Assessment 11.1

G1 Please assess the COBIT maturity levels for the security controls on the left side according to the described scenario. You can also open the previous descriptions by clicking on the links.

The security controls are defined in Section 11 'physical and environmental security', sub-section 11.1 'secure areas' of the ISO/IEC 27002. [8]

	0	1	2	3	4	5
11.1.1 - Physical security perimeter: security perimeters should be defined and used to protect areas that contain either sensitive or critical information and information processing facilities.						
11.1.2 - Physical entry controls: secure areas should be protected by appropriate entry controls to ensure that only authorised personnel are allowed access.						
11.1.3 - Securing offices, rooms and facilities: physical security for offices, rooms and facilities should be designed and applied.						
11.1.4 - Protecting against external and environmental threats: physical protection against natural disasters, malicious attack or accidents should be designed and applied.						
11.1.5 - Working in secure areas: procedures for working in secure areas should be designed and applied.						
11.1.6 - Delivery and loading areas: access points such as delivery and loading areas and other points where unauthorised persons could enter the premises should be controlled and, if possible, isolated from information processing facilities to avoid unauthorised access.						

Section H: 11.1.1 Next Level

You have just assessed the maturity level for the following control: "11.1.1 - Physical security perimeter: security perimeters should be defined and used to protect areas that contain either sensitive or critical information and information processing facilities."

H1 What additional activities would be necessary in your opinion so that CloudSec reach the next level of maturity for this control?

Section I: Assessment 12.6

I1 Please assess the COBIT maturity levels for the security controls on the left side according to the described scenario. You can also open the previous descriptions by clicking on the links.

The security controls are defined in Section 12 'operations security', subsection 12.6 'technical vulnerability management' of the ISO/IEC 27002. [8]

	0	1	2	3	4	5
12.6.1 - Management of technical vulnerabilities: information about technical vulnerabilities of information systems being used should be obtained in a timely fashion, the organisation's exposure to such vulnerabilities evaluated and appropriate measures taken to address the associated risk.						
12.6.0 - This is a control question: please rate it with maturity level "5 - Optimizing" to show that you have read the question.						
12.6.2 - Restrictions on software installation: rules governing the installation of software by users should be established and implemented.						

[8] Tab. 1 included.

Section J: 12.6.1 Next Level You have just assessed the maturity level for the following control: "12.6.1 - Management of technical vulnerabilities: information about technical vulnerabilities of information systems being used should be obtained in a timely fashion, the organisation's exposure to such vulnerabilities evaluated and appropriate measures taken to address the associated risk."

J1 What additional activities would be necessary in your opinion so that CloudSec reach the next level of maturity for this control?

Section K: Confidence

K1 In total, you have assessed the maturity levels for ten security controls. For how many of them have you been uncertain?

- 0
- 1
- 2
- 3
- 4
- 5
- 6
- 7
- 8
- 9
- 10

Section L: Challenges

L1 Where do you see possible challenges in the evaluation of controls based on the COBIT maturity level?

Section M: Uncertainty

M1 What was the reason for your uncertainty when evaluating the controls?[9]

- The scenario was not quite clear to me.
- The controls from ISO/IEC 27002 were not quite clear to me.
- The COBIT maturity levels were not quite clear to me.
- Other[3]

Section N: Evaluation Interest

N1 Are you interested in the evaluation of the study?

- Yes
- No

Section O: Email Address You can send us your e-mail address under the following link. By entering the e-mail address separately, no conclusions can be drawn about your answers:
https://m-chair.survey.uni-frankfurt.de/index.php/100

Section P: Contact

P1 Are you available for further contact to discuss your answers (e. g. a short telephone or Skype interview)?

- Yes
- No

Section Q: E-Mail Address

Q1 Please let us know your e-mail address. In order to be able to discuss your answers afterwards, the given e-mail address will be linked to your answers.[10]

Section R: Feedback

R1 If you have any comments or suggestions about the survey, you can let us know now:

Appendix C. Interview guide

Section A: Opening Questions

A1 Do you agree that the following conversation is recorded?

A2 Do you agree that the results may be used in scientific publications?

Section B: Assessment of the Challenge of Scenario Evaluation

B1 How did you perceive the maturity assessment in the scenario?

B1.a To what extent did you have problems assessing the scenario?

B2 How do you generally see the assessment of such hypothetical scenarios?

B2.a How does the assessment of the scenario differ from an assessment in practice?

B2.b We noticed that some participants had problems assessing the scenario. What factors might have led to this?

B3 How do you see the relevance of the different maturity models compared to each other?

B3.a To what extent do you see differences in quality/dissemination of he approaches?

Section C: Possible Assistance for the Scenario Evaluation

C1 What would help you to assess maturity levels?

C1.a Discuss in a team?

C1.b Additional documentation?

C1.c More trainings for assessing maturity levels?

Section D: Closing Questions

D1 Are there any other aspects that are important to you but have not been addressed by us?

D2 May we contact you for further questions?

[9] Only asked if uncertainty indicated in K1

[10] Only asked if availability indicated in P1