Journal of Computer Information Systems
Volume 56, Number 1, Fall 2015
official journal of
IACIS
International Association for Computer Information Systems

Taylor & Francis
Taylor & Francis Group

Journal of Computer Information Systems

ISSN: 0887-4417 (Print) 2380-2057 (Online) Journal homepage: http://www.tandfonline.com/loi/ucis20

Organizational Characteristics Influencing SME Information Security Maturity

Frederik Mijnhardt, Thijs Baars & Marco Spruit

To cite this article: Frederik Mijnhardt, Thijs Baars & Marco Spruit (2016) Organizational Characteristics Influencing SME Information Security Maturity, Journal of Computer Information Systems, 56:2, 106-115

To link to this article: http://dx.doi.org/10.1080/08874417.2016.1117369

Published online: 15 Jan 2016.

ORGANIZATIONAL CHARACTERISTICS INFLUENCING SME INFORMATION SECURITY MATURITY

FREDERIK MIJNHARDT
Utrecht University, Utrecht, The Netherlands

THIJS BAARS
Utrecht University, Utrecht, The Netherlands

MARCO SPRUIT
Utrecht University, Utrecht,
The Netherlands

ABSTRACT

In the current business environment, many organizations use popular standards such as the ISO 27000x series, COBIT, and related frameworks to protect themselves against security incidents. However, these standards and frameworks are overly complicated for small to medium-sized enterprises, leaving these organizations with no easy to understand toolkit to address their security needs. This research builds upon the recent Information Security Focus Area Maturity (ISFAM) model for SME information security as a cornerstone in the development of an assessment tool for tailor-made, fast, and easy-to-use information security advice for SMEs. By performing an extensive literature review and evaluating the results with security experts, we propose the Characterizing Organizations' Information Security for SMEs (CHOISS) model to relate measurable organizational characteristics in four categories through 47 parameters to help SMEs distinguish and prioritize which risks to mitigate.

Keywords: information security, maturity matrix, SME, organizational characteristic, situational factor, ISFAM, CHOISS

INTRODUCTION

With many security breaches hitting the news [21, 31], the field of Information Security (IS), which focuses on protecting the confidentiality, integrity, and availability of information [14], has attracted a lot of attention in recent years. In the Netherlands, 18% of all small and medium enterprises (SMEs) are hit by cyberattacks each year, which costs the Dutch business sector around €100,000 in damages per organization [30]. Despite all this attention and high financial impact, risk awareness under SMEs is low and risk mitigation is equally a low priority. In addition, SMEs rarely have the resources, time, and budget available to address the complexity of risk mitigation [9, 37]and have to deal with security mainly designed for large enterprises, while the risks are just as pressing for SMEs.

In the past decades, the ISO2700x series has emerged as the global standard for IS [18]. This standard, consisting of 450 items and 9 focus areas, addresses the most pressing problems regarding IS, providing organizations with a complete overview of best practices for their risk mitigation strategy. In parallel to this standard, a number of frameworks have been developed to address more specific company needs, for example, by addressing multinationals through the Control Objectives for Information and related Technology (COBIT) framework or governmental toolkits like the NIST SP800 [14]. Unfortunately, due to the complexity and extensiveness of these frameworks, SMEs rarely reach a fully implemented standard and fall back to ad-hoc implementations of specific focus areas and quick-wins.

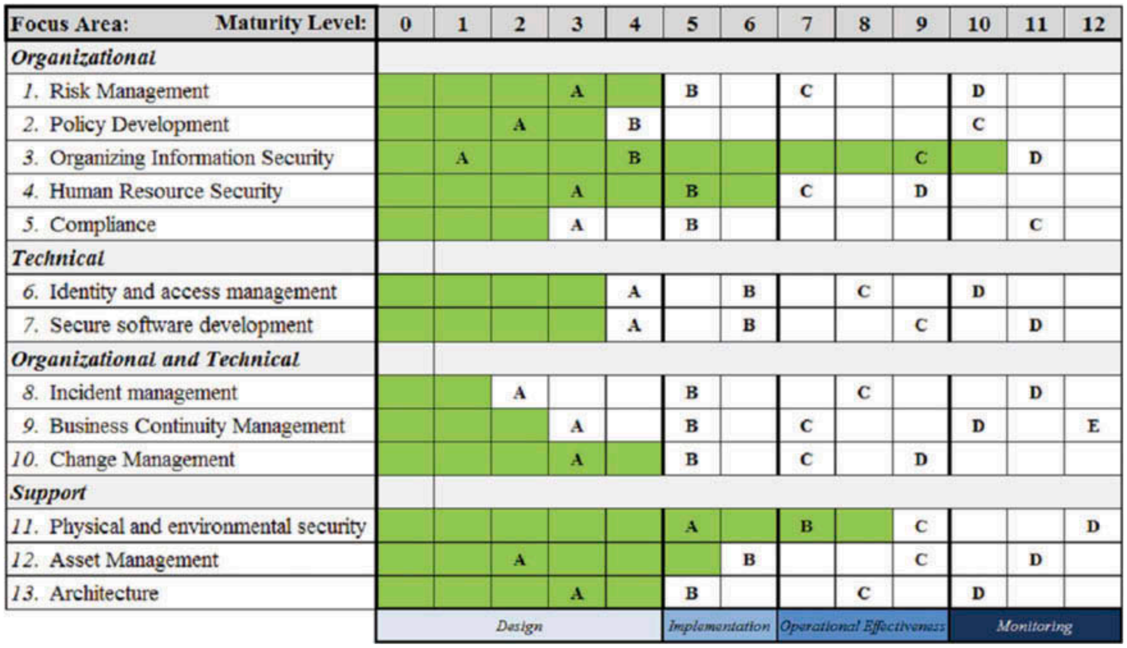
BACKGROUND

To aid SMEs in improving their IS, Spruit and Roeling [33] developed the Information Security Focus Area Maturity (ISFAM) model. The ISFAM is a focus area-oriented maturity matrix, originally proposed by Steenbergen et al. [34] as a standard method for incremental process improvement. In this type of maturity matrix, there are a fixed number of maturity levels. Each process, identified by a focus area, is assigned its own number of progressively more mature capabilities.

In the ISFAM model, as shown in Figure 1, there are 12 maturity levels and 13 focus areas. In these focus areas, a total of 64 capabilities (A–E) are assigned at the various maturity levels. The assessment of the maturity level is executed through a survey or a directed interview with an expert. The ISFAM model covers the complete domain of IS within SMEs. They overlap in part with chapters from CISSP, ISO 2700x, Information Security Frameworks, the Standard of Good Practice (IOC), and the IBM Security Framework [33].

Although extensive and relatively fine-grained, the ISFAM model remains rather rigid by design as it does not incorporate the unique set of characteristics of each SME in its maturity assessment. This can be an issue in IS, as the risks and threats differ significantly between an SME with two employees and one with 200. This results in certain capabilities not being applicable or out of place, depending on organizational characteristics (OCs) such as organization size and amount of revenue. In practice, SMEs will often not be able to reach a higher maturity level because subsequent capabilities are too difficult to implement and perhaps more importantly, they become discouraged by having to wade through capabilities which are not applicable for their business or not deemed relevant within their business sector. In order to overcome these issues, maturity models such as the ISFAM should incorporate OCs into their core design much like Bekkers et al. [4] did in the field of Software Product Management. Although Bekkers et al. use the term Situational Factors, in their quantitative analysis they measure internal OCs.

The use of OCs to segment organizations is not particularly new, as early as 1972—and possibly earlier—academics used OCs in an effort to model factors that contribute to decision-making. In the field of IT, Thong and Yap [36] used OCs such as organization size, competitiveness of the environment, and information density to investigate the adoption of IT in SMEs. In recent years, the fields of Customer Relationship Management (CRM) adoption [22], Knowledge Management [39], and Sourcing [28] have shown the use of OCs to cluster and segment. In the field of IS, the necessity of



Focus Area: Maturity Level:	0	1	2	3	4	5	6	7	8	9	10	11	12
Organizational													
1. Risk Management	🟩	🟩	🟩	🟩 A	🟩	B		C			D		
2. Policy Development	🟩	🟩	🟩 A	🟩	B						C		
3. Organizing Information Security	🟩	🟩 A	🟩	🟩	🟩 B	🟩	🟩	🟩	🟩	🟩 C	🟩	D	
4. Human Resource Security	🟩	🟩	🟩	🟩 A	🟩	🟩 B	🟩	C		D			
5. Compliance	🟩	🟩	🟩	A		B						C	
Technical													
6. Identity and access management	🟩	🟩	🟩	🟩	A		B		C		D		
7. Secure software development	🟩	🟩	🟩	🟩	A		B			C		D	
Organizational and Technical													
8. Incident management	🟩	🟩	A			B			C			D	
9. Business Continuity Management	🟩	🟩	🟩	A		B		C			D		E
10. Change Management	🟩	🟩	🟩	🟩 A	🟩	B		C		D			
Support													
11. Physical and environmental security	🟩	🟩	🟩	🟩	🟩	🟩 A	🟩	🟩 B	🟩	C			D
12. Asset Management	🟩	🟩	🟩 A	🟩	🟩	🟩	B			C		D	
13. Architecture	🟩	🟩	🟩	🟩 A	🟩	B			C		D		
	Design					*Implementation*		*Operational Effectiveness*			*Monitoring*		

FIGURE 1. The ISFAM Model Highlights Focus Areas per Row from Left to Right as Implemented Capabilities, Designated by Capital Letters

taking into account OCs has proven to be significant [6] and academics have identified numerous factors in a wide variety of domains, such as financial [8, 23], the complexity, and scale of the IT environment [15, 29, 38], and to what extent businesses deal with privacy related information [14, 38].

Organizational characteristics thus indirectly influence the object of measurement within an organization. These can be internal factors, such as the amount of employees employed and the amount of revenue generated, as well as external factors such as the sector the organization operates in or the geographic location of a firm. These characteristics can then be modeled in such a way that they apply the correct weights to the focus areas in new and existing maturity models. These weights allow for a more flexible maturity matrix and consequently a more realistic model. The goal of this research is, therefore, to identify which OCs are relevant in the field of SME Information Security.

This paper is organized as follows: in the next section the research approach is discussed, after which we describe the identified OCs. In the third section, we discuss the evaluation of the factors based on iterative interviews. We conclude with a discussion, conclusion, and factors for future research.

RESEARCH APPROACH

The research described in this paper follows the design science theory [26] by using two design processes, namely, the development followed by the evaluation of an artifact, also referred to as the instantiation. These steps have been placed in the comprehensive framework by Hevner et al. [16] Information Systems Research Framework for Design Science.

The Design Science research methodology is based on the idea of repetitive cycles of improving the object of research based on evaluations. The envisioned artifact—the OCs model for IS in SMEs—is defined based on environmental factors and the state-of-the-art knowledge base. Identifying the OCs is done following a three step approach (Figure 2). The first step in creating the artifact is to determine the set of OCs through a systematic literature review, after which we identify appropriate levels of measurement for each OC. The last step is the iterative evaluation of the OCs through expert interviews. In the following sections, the research approach is elaborated on in more detail. The results of these steps are discussed in the subsequent chapters.

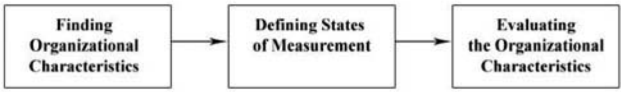

Finding Organizational Characteristics
Defining States of Measurement
Evaluating the Organizational Characteristics

FIGURE 2. The Research Approach for Identifying Relevant Organizational Characteristics in Information Security for SMEs

Finding the Organizational Characteristics

In order to identify the OCs, a literature search was executed. We used the Data Base and Logic Programming (DBLP) and Google Scholar to execute our systematic literature review using the combination of keywords indicated in Table 1.

Important to note is that IS, besides being discussed by a broad and active research community, is also a field where professionals and IS practitioners write and publish many well-respected white papers and case studies. Therefore, an additional search through the databases of the World Bank, the European Central Bank, and Audit-, ISO-, and COBIT-communities was performed to find articles and papers concerning SMEs in general as well as IS in an SME setting in particular. An example can be found when looking at the ISO implementation guideline [2], which addresses many OCs that should be taken into account when trying to reach ISO 27000× certification.

When selecting papers, a first selection was made based on title. Only papers with a title including keywords from all three groups were selected.

TABLE 1. Keywords Used for the Systematic Literature Review, Combining Items within Groups 1, 2, and 3 to Construct the Actual Search Queries

Keywords		
Group 1	Group 2	Group 3
Factor	Influencing	Information security
Characteristic	Impacting	Information security management
Organizational factor	Affecting	Risk management
Organizational characteristic	Effects	Information risk
Situational factor		
Situational characteristic		
EDP audit		
IT audit		
IT environment		
IT complexity		

In the consecutive step, relevance was double-checked by studying the abstract. The papers matching the criteria were then fully read. From these papers, the factors were extracted and clustered on similarity, which resulted in a list of unique factors.

From the extraction step onwards, the authors double-checked the factors on correctness and clustering. The total set of clusters formed the basis for the list of unique OCs. In the selection process of these OCs, both measurability—"is the characteristic quantifiable?"—and soundness—"does it occur in multiple sources or through intuition and common sense?"—were accounted for. This list was then used for the iterative interviews evaluating the characteristics.

Defining Measurement Levels

Each OC in the final list is described in detail in an effort to streamline the semistructured interviews in the next step. This description includes measurement levels, which are a one-to-one operationalization of their underlying parameters, where possible. Regarding the measurement levels that comprise a certain OC, consider the following example for further clarification: SMEs are generally categorized as either freelancers (and other one-man businesses), microorganizations (2–9 employees), small businesses (10–49 employees), and medium businesses (50–250) [3, 35]. These different sizes of SMEs are the parameters or the combined measurement level, which comprises the OC "Number of Employees Employed". In defining the measurement levels, three goals were upheld:

1. Obtain a relatively high-level of measurement which bins the parametric range into around three to six increasingly more mature, ordinal levels.
2. The parameters should be easy to understand yet be as descriptive as possible.
3. Parameters should be mutually exclusive and commonly exhaustive.

These measurement levels are derived from the literature; preferably from the results of the systematic review in step one as this assures a peer-reviewed context. However, the literature gathered did not always specify the OC in such detail that parameters, and thus measurement levels, could be obtained. In these cases, a specific search for literature was executed, adding the terms: "*measurement*", "measurement level," and/or "parameter" to the initial search on DBLP and Google Scholar. In certain cases, the literature could not provide the authors with an acceptable level of measurement. These cases can be categorized as follows:

- **Unavailable**. The literature did not provide any indication of measurement levels. In this case, common sense was applied, after which it was discussed with the interviewed experts.
- **Lacking Consensus**. The literature did not provide a consensus. Here the interviewees were asked to provide their opinions.
- **Error in Context**. The level of measurement was obtained from literature in a different field than IS or information technology. Depending how context-sensitive a level of measurement is, it was discussed with the experts.

During the iterative interviews, new OCs and their measurement levels could be proposed. During these interviews, each interviewee was asked to elaborate on the measurement levels. These were then cross-checked with the literature in a likewise process as described above.

By identifying the proper measurement levels, the OCs' impact on capabilities could be defined, and any OC ambiguity could be minimized to avoid confusion and bias whilst discussing the OCs with the interviewees.

Evaluating the Organizational Characteristics

The evaluation interviews were held with medior to senior domain experts in the fields of IT/EDP audit, security consulting, ethical hacking, and IS/IT research. The use of iterative cycles with a wide variety of experts "enables a progressive reconfiguration of substantive findings and interpretations in a pattern of increasing insight and sophistication" [5, p.23]. The objective of the interviews was threefold: to discover new characteristics, to evaluate the characteristics found, and to prioritize and extract the most crucial characteristics. As open discussions and questions are essential in this process, the usage of questionnaires or structured interviews was inapplicable [7, 19]. Semistructured interviews allowed for this, while keeping guidance on the characteristics found and the focus areas in the ISFAM model. The focus of semistructured interviews also helped with the comparison between the responses of the different participants [19].

Each participant received an explanation of the research approach, a document that listed the found factors, clear definitions of important keywords, and the ISFAM model. At the start of the interview, the ISFAM model and OCs were explained and a small introduction was provided on the objective of the session. In each consecutive interview, changes made to the list of OCs were carefully documented and clarified to guarantee new interviewees had sufficient knowledge on why some OCs were changed by others.

To reassure that the final list of questions is easy to understand and captured only the most important aspects—i.e., those that influence the number of IS capabilities that an organization should implement—we asked every interviewee to keep in mind the following factors as depicted in Table 2.

Extrapolating Organizational Characteristics

The literature search yielded a total of 71 papers, book chapters, and relevant white papers which had all characteristics extracted. These characteristics were double-checked by the team of authors to assure correctness.

TABLE 2. Key Aspects the Final List of Organizational Characteristics Should Adhere to

#	Factor
1	Nonexperts in the field of IS must be able to answer the questions with relative ease.
2	Questions must capture in a broad sense the most important characteristics, which influence the main factors.
3	The number of questions must be limited, to lower the barrier for nonprofessionals to determine their IS maturity.

This resulted in a total of 75 unique characteristics, ranging from organizational to technical to social descriptions.

From these 75 characteristics, a short list was created. The selection process removed characteristics that are hard to measure according to either our experts or by nonexperts at SMEs whom eventually will use the model, for example, a user's mother tongue [25] and user's intention [17].

Characteristics that were deemed too obvious were deleted from the list as well. For example, external factors such as legislation and bankruptcy influences IS [24, 32], as well as minimizing the impact of vulnerabilities and incidents to reduce negative consequences from security incidents [12].

In addition, a number of characteristics describe ISFAM capabilities [32]. These overlapping characteristics were removed. A selection of these cases is depicted in Table 3.

These steps of determining characteristics too hard to measure, characteristics that should be grouped and characteristics overlapping with capabilities from the ISFAM model, resulted in a shortlist of 26 unique characteristics. No less than 49 characteristics did not meet the aforementioned criteria. In addition, some characteristics were grouped and summarized.

EVALUATING THE ORGANIZATIONAL CHARACTERISTICS

The experts in Table 4 were selected for their knowledge in the field of IS. In the process of creating this selection, deep knowledge of the field, broad experience in performing risk analyses in the Netherlands, consulting on security topics and the relevance to SMEs was taken into account. To prevent bias, the backgrounds of the participants differ as well as their current roles. None of the participants work for the same employer, and none of them have worked together in a professional or educational setting. The experts participating provided valuable information regarding the 26 unique characteristics.

Besides discussing the characteristics, experts also provided useful information regarding a number of related issues. These include:

- Which OCs are relevant and which are not. Certain OCs are mentioned by the literature, but removed as they are deemed irrelevant or not applicable by multiple experts.

TABLE 3. A Selection of OCs Overlapping with ISFAM Capabilities

Characteristic	ISFAM focus area	ISFAM capability	Capability #
Top management support [13, 24]	Information security policy development	IS policy development is supported by senior management	A2
The effective marketing of security to all employees [13, 17]	Information security policy development	The policy documents are understood by the whole organization	C2
	Risk management	Individuals in the organization are aware of the importance of risk management	A2
The degree of formalized processes and rules [29]	Information security policy development	There is a formal style for writing IS policy documents	B4
The lack of consistent risk management strategy [32]	Risk management	Risk management processes are continuously improved	D3
	Risk management	Risk management is an integral part of the decision-making process	D4
The business users knowledge and intention regarding IS security [10, 27]	Human resources security	All employees signed a document stating their roles and responsibilities to the organization	B3

TABLE 4. Overview of interviews performed with experts in IS

Expert	Experience	Company type	Field of expertise	Expertise in	No. of interviews
1	6 years	Large consultancy firm	IT Security	SMEs	2
2	10 years	Large accountancy firm	IT Security & IS/IT research	Small, medium, and large enterprises	1
3	20+ years	Large accountancy firm	IT Security Consultancy	Small, medium, and large enterprises	1
4	8 years	Large accountancy firm	IT Auditing	Small, medium, and large enterprises	1
5	6 years	Large software firm	IT development & IS/IT research	SMEs	1

- Which OCs are missing. Although our literature review was extensive, some OCs are based on the professional experiences from our experts. Characteristics identified by multiple experts are taken into account to be added to the final list.
- Which OCs are relevant, but are not applicable to SMEs or have little impact on SMEs. For example, average annual change in software and hardware is not applicable, as SMEs tend to change the majority of their software at once if they adopt, for example, a new version of Windows. Accounting for this is nearly impossible, and would thus skew the weights.

To structure the results of the interviews, a number of factors are described for each of the 26 characteristics discussed, as shown in Table 5. To keep the overview clear, we portray only a selection of key references per characteristic. In addition, the overview in Table 5 includes the category each characteristic falls into, based on the consensus of the experts. Also, we depict whether we retain, merge, split, or remove the characteristic and we provide the appropriate rationale derived from the interviews. Lastly, we portray the general opinion the interviewees had whether each characteristic should be retained for the shortlist or not.

ORGANIZATIONAL CHARACTERISTICS

The rationale and action associated per identified OCs, as described in Table 5, present a final version of 11 OCs, grouped into four categories: *General, In- & Outsourcing, IT Dependency*, and *IT Complexity*. These OCs in Figure 3—under the moniker CHOISS: CHaracterizing Organizations' Information Security for SMEs—present the possibility to distinguish between a wide variety of different organizations. To reach a high IS maturity level, every organization has to implement a tailored set of focus areas and capabilities. In the following subsections, each category is discussed and a number of examples are provided.

General

The OCs in the general category are selected to provide a global view of the organization. The combination of the OCs sector, revenue, and number of employees together provide the ability to distinguish between a wide variety of organizations. For example, when comparing two enterprises of similar size in number of employees, one of them might provide normal product services whereas the other provides mortgage services for a major bank. While the organization size would indicate similar capabilities need to be addressed, the fact that the organization is a *financial service organization* and the fact that the organization has a high *revenue* compared to its number of employees, additional capabilities would be required to reach a higher maturity level.

In- & Outsourcing

The OCs in the In- & Outsourcing category are important due to the location where critical data is being stored, and in which manner the organization can rely other parties to deal with the proper handling of change management and backup and recovery processes. The difference can be explained in the following example: An organization runs 90% of its IT services as a Software as a Service (SaaS) product from reliable partners. However, 10% of its software is run and developed internally. In this situation, the organization is required to implement a number of extra measurements regarding the change management processes of its software development, while a different organization, running all critical processes as SaaS, would only need to look into Service Level Agreements.

IT Dependency

The third category is an important indicator how organizations need to address their IS practices. The OCs addressing these issues are fourfold: The importance of Confidentiality, Integrity, and Availability (CIA) and the time an organization can do without IT. Each of the three parts from the CIA triad are closely linked to capabilities in the ISFAM model.

By assessing the number of hours, the business can run without IT—we get a clear idea on the dependency of the business on the IT environment. An example of these factors can be found when assessing a medium-sized healthcare institution working with patient records. In this case, maintaining confidentiality of the critical data is of high importance, as patient information holds sensitive personal information. In addition, integrity and a working IT environment assures the latest medical information about a patient can be provided, possibly saving lives. These factors combined require a higher number of capabilities which need to be addressed before a higher maturity level can be reached.

IT Complexity

Lastly, the fourth category gives an overview of the complexity of the IT environment, for example, by the revenue percentage being spent on IT and the number of employees employed in the IT department. These factors are of importance to grasp how much data are handled by IT in comparison to more conventional businesses focused on manual labor, for example, two similarly sized organizations active in the Utilities sector. One is solely focused on infrastructure maintenance while the other is responsible for managing the network and operations of a specific energy sector. Whilst on many OCs the organizations can be considered similar, the latter organization has a high expenditure on its IT environment, as multiple IT teams are on the premise to ensure uptime of the energy network. These differences in the complexity of IT impacts a large number of capabilities within ISFAM.

DISCUSSION AND LIMITATIONS

An important issue with identifying these OCs and linking them to the ISFAM model to provide a tailored advice for SMEs is the possibility of missing measurements that should be implemented. There is no "silver bullet" how to address a business' IS, and the authors realize the difficulty this brings when creating an off-the-shelf solution. This research will therefore require continuous work to provide the best advice.

After assessing the items found in the literature review, grouping, removing, and identifying overlapping factors with capabilities, we note how many scientific papers address single characteristics and their relation to IS. For instance, the size of the organization [6, 11, 20, 23] or the protection of an organizations financial assets [8]. Most OCs are derived from written literature in the form of books, information retrieved from the International Organization for Standardization (ISO), and other industry-related papers and publications.

TABLE 5. Shortlist with 26 unique characteristics identified in literature, and the rationale whether to retain, merge, split, or remove the characteristic based on expert interviews

#	OC	Reference	Category	Action	Rationale	Rating
1	The influence of regulations on the business	[24, 29, 32]	General	Merge	Interviewees indicate that regulation is indeed an important factor. However, they note how regulation is mostly bound to the sector the business resides in. In this case, merging with characteristics #23 would allow to check for regulatory issues after the SME has indicated the sectors it resides in.	++
2	The business is publicly traded	[8, 29]	General	Remove	Although very important for large enterprises, for smaller and medium-sized organizations, this factor is seldom relevant and therefore was suggested to be removed.	– –
3	The entity relies on IT to create financial reports	[8]	Financial	Remove	This factor is associated with a financial IT audit. Interviewees indicated its relevance, but deemed it too specific for the purpose of the ISFAM model.	0
4	The entity relies on IT to create business reports	[8]	Financial	Remove	Interviewees identify a similar specificity with this characteristic that it does not influence enough capabilities of the ISFAM model.	0
5	The businesses' annual spend on IT		IT complexity	Retain	All interviewees agreed that this is one of the quickest and easiest methods to get an idea of the complexity of the IT environment.	++
6	The number of business users working with financial information	[8, 23]	Financial	Remove	IT auditors found this an important factor, whilst security consultants indicated it to be very specific for financial processes. The fact that the ISFAM is focused on IS in general was decisive to agree with the latter to remove it.	0
7	The number of employees supporting the IT environment	[15, 20, 32]	IT complexity	Retain	Similar to characteristic #5 interviewees indicate this to be an important factor to determine IT complexity. Especially in combination with expenditures, since both factors implicate different types of complexity.	++
8	The entity uses an enterprise resource planning (ERP) application for critical processes	[15, 29]	IT dependency	Remove	The use of ERP systems gives a good indication of the importance of IT in businesses processes. However, interviewees argued that for many SMEs, the use of large ERP applications is rare. In addition, they felt measuring the dependency on IT applications is better served by looking at the number of hours a business can run without IT (OC #14).	+
9	There are interfaces between the business' financial processing applications	[15]	IT complexity	Remove	The experts agreed that in larger enterprises, the mending of large software applications has become standard practice; especially when dealing with financial information, this could lead to discrepancies of data creating complications for auditing work. They do also note that in smaller organizations, this is not very common; thus, this OC should be removed.	–
10	There are interfaces between the business' critical applications and external organizations	[15]	IT complexity	Remove	Similarly to characteristic #9 interfaces with external organizations can become a serious threats to the IS. Between experts, there was no clear consensus on its removal or retaining. Though experts commonly noted that in many cases where threats are highest, these factors would already be addressed in regulatory requirements. For example, at financial and health-care institutions, this is covered in OC #24.	0
11	The number of servers used within the IT environment	[15, 29]	IT complexity	Remove	Experts agreed this factor had too little impact, primarily due to ambiguity, compared to the other characteristics in this category.	––
12	The number of transactions in the system	[8, 23]	Financial & IT complexity	Remove	Although an important indicator of IT complexity through *range* (accessibility) and *reach* (connectivity) of the platform, experts agreed on its ambiguity, making it difficult to measure and requiring expert analysis. For these reasons, this would not ensure reliable information, and therefore, it should be removed.	0
13	Is there a distinction between the information flow and the value flow	[8]	Business complexity	Remove	All experts agreed that this factor is almost only valid for multinationals where goods and cash flows run through different systems and tax agencies. It is also very specific to financial information.	– –

(*Continued*)

TABLE 5. *(Continued)*

#	OC	Reference	Category	Action	Rationale	Rating
14	Time the organization can do business without IT support.	[15, 29, 38]	IT dependency	Retain	The number of hours the business can run without IT support provided the best general idea on how important IT is in supporting business processes. It thus gives a good indication on the importance of the information in these systems and the dependency of business operations on IT.	+
15	There were major changes to the application environment	[29, 38]	IT complexity	Remove	This factor is relatively of low importance for SMEs; experts indicate how in many larger enterprises critical business processes are supported by software, which is developed by the organization itself. At SMEs, it is more likely to see a large overhaul of the application environment when, for example, a new version of Microsoft Windows gets adopted. This would skew the data, making it an OC hard to measure. For SMEs, this is the case in very few cases, and in addition, the newly formed characteristics #25 and #26 already address this issue in a broader sense.	+
16	There were major changes to the IT organization	[29]	IT complexity	Remove	In SMEs, the IT department is usually relatively stable and small. Major changes are therefore possible, but not very likely to happen, resulting in no impact on the capabilities at all.	+
17	The importance of confidentiality of the entity's critical information	[14, 38]	CIA	Retain	To assess which capabilities are crucial to implement, businesses should indicate the importance of the confidentiality, integrity, and availability of their critical information. Experts stressed that a proper definition of *critical information* is required, and that knowledge of the CIA triad is essential here.	++
18	The importance of Integrity of the entity's critical information	[14, 38]	CIA	Retain		++
19	The importance of availability of the entity's critical information	[14, 38]	CIA	Retain		++
20	The number of employees in the business	[6, 11, 20, 23]	General	Retain	Number of employees is one of the most crucial indicators of the size and complexity of the organization. In discussions with experts, number of employees was chosen above FTE, as employees, the number of weekly working hours is not related to gaining special privileges above none-employees to access systems. Experts noted that this would likely be a mediating variable in many of the capabilities of the ISFAM model.	++
21	The revenue of the business	[11]	General	Retain	Together with the number of employees, this is one of the most indicators of the size and complexity of the organization. The definition of the ECB and World Bank were adhered to identify the parameters. Experts noted that this would likely be a mediating variable in many of the capabilities of the ISFAM model.	++
22	The number of physical locations with access to critical information	[32]	General	Remove	The amount of physical locations might influence, for example, logical access control of an organization. However, physical locations are very narrow, especially with the emergence of cloud computing which extends the amount of physical locations to near infinity. Due to this small impact on SMEs, and only a single tie to the ISFAM model (logical access control) it is removed.	−
23	The sector the business resides in	[6, 11, 20]	General	Merge	The sector of the organization provides ample information on the importance of proper IS, not only when dealing with regulation (explaining the merger with characteristic #1) but also when looking at the impact of, for example, data loss which is arguably higher in health and defense than in paper and logistics.	++

24	IT staff's knowledge of business processes	[10, 13]	General	Remove	Although literature stated this to influence a number of factors on how users take IS into account, the factor is hard to measure objectively when assessing OCs. In addition, interviewees felt this was not a key influence for many capabilities	0
25	In-house software development/ maintenance In-house software development/ maintained by external parties internally or externally	[1, 29]	IT complexity	Split	When discussing the influence of businesses developing, maintaining, or outsourcing software, our interviewees argued that these characteristics are important. However, they felt that it was defined in a wrong way. Based on their remarks, two new OCs are proposed: "IT development in- & outsourcing" and "IT servicing in- & outsourcing". This prevents ambiguity surrounding the role of SLAs and which parties will be responsible for the change management processes.	+
26	Does the organization make use of IT outsourcing (application maintenance, server hosting…)	[1, 29]	IT complexity	Split		0

Another issue arises when looking into ambiguity. The SMEs' interpretation of the assessment can have a large impact when linking the OCs to the ISFAM.

Experts noted how, for example, questions such as the ones related to the CIA-triad require a certain level of knowledge about these concepts for managers to answer them correctly.

In addition, the ambiguity involved when interpreting terms such as *critical information* requires the final model to provide SMEs with proper and easy to understand definitions of the different terms and concepts. Possibly elaborating by providing relevant examples to further improve the comprehension of the concepts involved.

Finally, based on the interviews and literature analysis of OCs, we note that quite a number of OCs turned out to be inapplicable, as they are specifically designed to distinguish between large enterprises. This is a strong indication which confirms our observation that research and current information system methodologies are still mostly focused on large enterprises. This research is part of our efforts to close this research gap by developing a lean and more specifically designed methodology for SMEs as a promising and highly relevant field of study.

CONCLUSION

This work describes exploratory research into the field of adaptive IS assessments targeted at SMEs. We performed a systematic literature review and assembled a total of 75 organizational factors. By grouping factors and removing factors not adhering to set criteria, we identified a long list of 26 OCs for IS in SMEs. For each of these OCs, the levels of measurement were defined and a number of iterative interviews were held.

We have structured our final list of OCs in the CHOISS model, which structures 11 OCs and its 47 measurement levels into the four categories *General, In- & Outsourcing, IT Dependency*, and *IT Complexity*. The *General* category pairs the number of employees, the organization's revenue, and sector; the *In- & Outsourcing* category encompasses the percentage of sourced software development and hosting/IT services; the *IT Dependency* category spans the importance of integrity, confidentiality, and availability of critical data, as well as the time the organization can do without IT support; the *IT Complexity* category joins the number of employees supporting the IT environment and the annual expenditure on IT over revenues.

Each of these OCs can be used for future research to create a situational version of the ISFAM method to determine IS maturity for SMEs.

FUTURE RESEARCH

Currently the OCs are based on a comprehensive literature study and interviews with a number of IS professionals. We are now in the process of performing a number of case studies as the next logical next step to further validate the ISFAM model, and to analyze the OCs for future integration in the ISFAM assessment under the monniker Situational Process Improvement in Cybersecurity (SPICY), possibly augmenting and finalizing the list of factors.

Finally, our upcoming research on adaptive IS assessments will focus on how to develop a model which automatically identifies which OCs impact which focus areas and capabilities of the ISFAM maturity model. Especially the latter research component poses quite a challenge as it involves assessing no less than (64 ISFAM capabilities × 11 CHOISS OCs =) 704 impact relationships. The first step in this approach would be to prioritize the 11 OCs in their

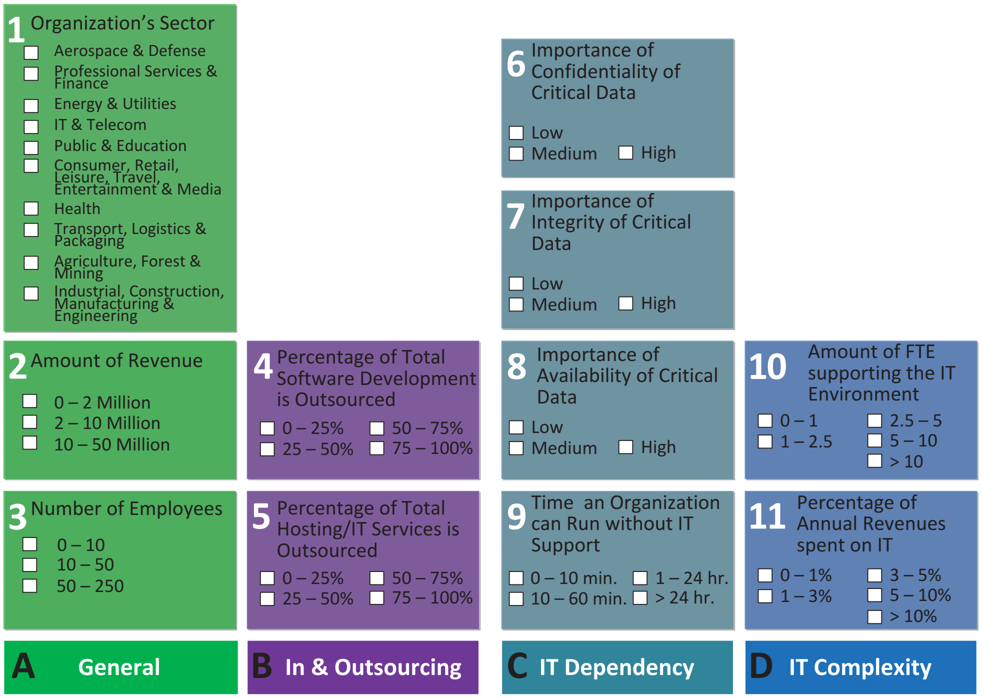

1 Organization's Sector
□ Aerospace & Defense
□ Professional Services & Finance
□ Energy & Utilities
□ IT & Telecom
□ Public & Education
□ Consumer, Retail, Leisure, Travel, Entertainment & Media
□ Health
□ Transport, Logistics & Packaging
□ Agriculture, Forest & Mining
□ Industrial, Construction, Manufacturing & Engineering
6 Importance of Confidentiality of Critical Data
□ Low
□ Medium □ High
7 Importance of Integrity of Critical Data
□ Low
□ Medium □ High
2 Amount of Revenue
□ 0 – 2 Million
□ 2 – 10 Million
□ 10 – 50 Million
4 Percentage of Total Software Development is Outsourced
□ 0 – 25% □ 50 – 75%
□ 25 – 50% □ 75 – 100%
8 Importance of Availability of Critical Data
□ Low
□ Medium □ High
10 Amount of FTE supporting the IT Environment
□ 0 – 1 □ 2.5 – 5
□ 1 – 2.5 □ 5 – 10
□ > 10
3 Number of Employees
□ 0 – 10
□ 10 – 50
□ 50 – 250
5 Percentage of Total Hosting/IT Services is Outsourced
□ 0 – 25% □ 50 – 75%
□ 25 – 50% □ 75 – 100%
9 Time an Organization can Run without IT Support
□ 0 – 10 min. □ 1 – 24 hr.
□ 10 – 60 min. □ > 24 hr.
11 Percentage of Annual Revenues spent on IT
□ 0 – 1% □ 3 – 5%
□ 1 – 3% □ 5 – 10%
□ > 10%
A General
B In & Outsourcing
C IT Dependency
D IT Complexity

FIGURE 3. The CHaracterizing Organizations' Information Security for SMEs (CHOISS) model relates 4 categories (A–D), 11 OCs (1–11), and 47 measurement levels

importance in distinguishing differences within an organization. Second, this research would need to explore for each measurement level, per OC, how this influences each individual focus area, and ideally each individual capability. By taking into account the relative influence of each OC, we would be automatically provided with a prioritization of importance of the capabilities in the ISFAM.

This research has pinpointed the OCs which influence IS maturity in SMEs. This allows further research to realize tailor-made, fast, and easy-to-use IS advice for the often-forgotten majority of SMEs.

ORCID

Marco Spruit http://orcid.org/0000-0002-9237-221X

REFERENCES

[1] Alner M. 2001. The effects of outsourcing on information security. Inf Syst Sec. 10: 1–9.

[2] Arnason, ST, Willett K. D. 2008. How to achieve 27001 certification: an example of applied compliance management. New York, NY: Auerbach.

[3] Ayyagari M, Beck T, Demirgüç-Kunt A. 2003. Small and medium enterprises across the globe: a new database. The World Bank, New York, NY, World Bank Policy Research Working Paper 3127, 2003.

[4] Bekkers W, van de Weerd I, Brinkkemper S, Mahieu A. 2008. The influence of situational factors in software product management: an empirical study. 2008 Second International Workshop on Software Product Management, Barcalona, Spain, 41–48.

[5] Caracelli V.J, Greene JC. 1997. Crafting mixed-method evaluation designs. New Directions for Eval. 1997:19–32.

[6] Chang SE, Ho CB. 2006. Organizational factors to the effectiveness of implementing information security management. Ind Manage Data Syst. 106:345–361.

[7] Corbetta P. 2003. Social research: theory, methods and techniques. London: Sage.

[8] Davis C, Schiller M, Wheeler K. 2010. IT auditing using controls to protect information assets. 2nd ed. McGraw-Hill.

[9] Dimopoulos V, Furnell S, Jennex M, Kritharas I. 2004. Approaches to IT security in small and medium enterprises. Proceedings of the 2nd Australian Information Security Management Conference(AISM), Perth, (2: Hamilton 2002), 73–82.

[10] Dunkerley KD, Tejay G. 2011. A confirmatory analysis of information systems security success factors. 2011 44th Hawaii International Conference on System Sciences, Honolulu, Hawaii, 1–10.

[11] Ein-Dor P, Segev E. 1978. Organizational context and the success of management information systems. Manage Sci. 24:1064–1077.

[12] Flores WR, Farnian A. 2011. Expert opinions on information security governance factors: an exploratory study. Proceedings of the 19th European Conference on Information Systems, ECIS 2011, Helsinki, Finland.

[13] Fulford H, Doherty NF. 2003. The application of information security policies in large UK-based organizations: an exploratory investigation. Inf Manage Comp Sec. 11, 106–114.

[14] Guttman B, Roback EA. 1995. Special Publication 800–12. An introduction to computer security: the NIST handbook. Gaithersburg, MD.

[15] Hanseth O, Ciborra C. 2007. Risk, complexity and ICT. Cheltenham, UK: Edward Elgar Publishing.

[16] Hevner AR, March ST, Park J, Ram S. 2004. Design science in information systems research. MIS Quart. 28:75–105.

[17] Huang D, Patrick Rau P-L, Salvendy G, Gao F, Zhou J. 2011. Factors affecting perception of information security and their impacts on IT adoption and security practices. Int J Human-Comput Stud. 69:870–883.

[18] Joint Technical Committee ISO/IEC JTC 1. 2008. ISO/IEC 27002. Geneva, Switzerland.

[19] Kajornboon AB. 2005. Using interviews as research instruments. E-J Res Teach. 2.

[20] Kankanhalli A, Teo H-H, Tan BCY, Wei K-K. 2003. An integrative study of information systems security effectiveness. Int J Inf Manage. 23:139–154.

[21] Keizer G. 2011. DigiNotar dies from certificate hack caper. Computerworld. [Online]. [cited: 2014 Feb 01]. Available from: http://www.computerworld.com/s/article/9220175/DigiNotar_dies_from_certificate_hack_caper.

[22] Ko E, Kim SH, Kim M, Woo JY. 2008. Organizational characteristics and the CRM adoption process. J Bus Res. 61:65–74.

[23] Kotulic AG, Clark JG. Why there aren't more information security research studies. Inf Manage. 41:597–607.

[24] Kraemer S, Carayon P, Clem J. 2009. Human and organizational factors in computer and information security: pathways to vulnerabilities. Comput Sec. 28:509–520.

[25] Kruger HA, Drevin L, Flowerday S, Steyn T. 2011. An assessment of the role of cultural factors in information security awareness. 2011 Information Security for South Africa, Johannesburg, SA, (August), 1–7.

[26] March ST, Smith GF. 1995. Design and natural science research on information technology. Decis Support Syst. 15:251–266.

[27] Milicevic D, Goeken M. 2013. Social factors in policy compliance—evidence found in literature to assist the development of policies in information security management. 2013 46th Hawaii International Conference on System Sciences, 4476–4484.

[28] Oh W. 2005. Why do some firms outsource IT more aggressively than others? The effects of organizational characteristics on IT outsourcing decisions. Proceedings of the 38th Annual Hawaii International Conference on System Sciences. 00(C):259c–259c.

[29] Rehage K, Hunt S, Nikitin F. 2008. Global technology audit guide: developing the IT audit plan. Altamonto Springs, FL, USA.

[30] Ruiter JT. 2012. Cost of cyber crime largely met by businesses. TNO. [Online]. [cited Jan 2014 02]. Available from: https://www.tno.nl/content.cfm?context=overtno&content=nieuwsbericht&laag1=37&laag2=2&item_id=2012-04-1011:37:10.0&Taal=2.

[31] Silveira V. 2012. Updating your password on LinkedIn and other account security best practices. LinkedIn Official Blog. [Online]. [cited: Feb 2014 01]. Available from: http://blog.linkedin.com/2012/06/06/updating-your-password-on-linkedin-and-other-account-security-best-practices/.

[32] Smith S, Jamieson R. Determining key factors in e-government information system security. Inf Syst Manage. 23:23–32.

[33] Spruit M, Roeling M. 2014. ISFAM: The Information Security Focus Area Maturity Model. Proceedings of the Twenty Second European Conference on Information Systems, ECIS 2014, Tel Aviv, Israel.

[34] Steenbergen M, Bos R, Brinkkemper S, Weerd I, Bekkers W. 2010. The design of focus area maturity models. 6105th ed. St. Gallen, CH: Global Perspectives on Design Science Research, LNCS6105 319–332.

[35] The Commission of the European Communities. 2003. COMMISSION RECOMMENDATION of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises. Official J Eur Union. 124:36–41.

[36] Thong JYL, Yap CS. 1995. CEO characteristics, organizational characteristics and information technology adoption in small businesses. Omega, Int J Manage Sci. 23:429–442.

[37] Whitman M, Mattford H. 2013. Management of information security. 3rd ed. UK: Cengage Learning.

[38] Whitman M, Mattford H. 2011. Principles of information security. UK: Cengage Learning.

[39] Willem A, Buelens M. 2006. Knowledge sharing in public sector organizations: the effect of organizational characteristics on interdepartmental knowledge sharing. J Public Admin Res Theory. 17:581–606.