Association for Information Systems
AIS Electronic Library (AISeL)

ECIS 2014 Proceedings

ISFAM: THE INFORMATION SECURITY FOCUS AREA MATURITY MODEL

Marco Spruit
Utrecht University, Utrecht, Netherlands, m.r.spruit@uu.nl

Martijn Röling
Utrecht University, Utrecht, Netherlands, martijnroeling@gmail.com

Marco Spruit and Martijn Röling, 2014, "ISFAM: THE INFORMATION SECURITY FOCUS AREA MATURITY MODEL", Proceedings of the European Conference on Information Systems (ECIS) 2014, Tel Aviv, Israel, June 9-11, 2014, ISBN 978-0-9915567-0-0
http://aisel.aisnet.org/ecis2014/proceedings/track14/6

ISFAM: THE INFORMATION SECURITY FOCUS AREA MATURITY MODEL

Complete Research

Spruit, Marco, Utrecht University, Utrecht, The Netherlands, m.r.spruit@uu.nl

Roeling, Martijn, Utrecht University, Utrecht, The Netherlands, martijnroeling@gmail.com

Abstract

Information security is mainly a topic that is considered to be information technology related. However, to successfully implement information security, an organization's information security program should reflect the business strategy. Nowadays information security is in many companies enforced by the information technology department, based on what they think should be in place to protect their business from inside and outside threats and risks. Additionally, information security covers many different subjects. This makes it especially hard for small and medium sized organizations to determine how they should design their information security program.

Therefore, we present the Information Security Focus Area Maturity Model (ISFAM). By identifying dependencies between various aspects of information security and representing them coherently in the ISFAM, the model is capable of determining the current information security maturity level. Involving the ISFAM model in the design process of an organization's information security program enables organizations to set up high level guidelines based on their current status. These guidelines can be used to incrementally and structurally improve information security maturity within the organization. We have successfully evaluated the ISFAM assessment model through a single case study at a medium sized telecommunications organization.

Keywords: Information Security, Information Security Management, Maturity Model.

1 Decision making in information security

Information security as a research topic is attracting a lot of attention lately. Most research is focused around how information security can prevent the loss of sensitive information. Most studies done by information security researchers therefore try to measure information security. The problem, of course, is that this turns out to be very difficult. According to Jaquith (2007), IT-security can only improve if it can be measured. However, Jaquith (2007) also mentions that defining metrics to measure IT-security is a tough and sometimes undoable process. Since IT-security is part of information security, it is reasonable to argue that the same holds for information security. Throughout the last years metrics have been defined to measure parts of information security, but the most important part has remained underdeveloped until now: metrics to support decision making. This is important because security metrics are servants of risk management and risk management is about making decisions. Therefore metrics to support decision making are a vital part of making information security measurable. This research defines *decision making* in the field of information security as:

> "the process of selecting the right measures with the objective to improve the information security within an organization".

Since the metrics for assisting an organization with information security are not commonly known and/or ill defined, questions as how to structurally improve information security show up in companies. Organizations do not know how to effectively manage their security and what steps to take to become a 'secure' organization (Chapin and Akridge, 2005).

The topic of maturing information security in a structured way has not received much attention in research yet and is interesting to look at. Another reason to look more closely at this problem is that both IT and business are involved. Hence, implementing information security features/processes/ artifacts do not only affect IT, but also business. It still happens that IT has its own information security program next to the security program of the business. Information security is not only about IT security. Information security also has a business side in terms of a secure work environment, not losing confidential papers off-site, and ensuring awareness and compliance throughout your organization. Communication between business and IT is a requirement for the successful creation and implementation of an organization wide information security program.

The problem addressed in this paper is the lack of understanding and awareness at the management level and service/product owners to effectively improve their information security. This starts by understanding where your organization is and where it wants to be. The problem is partly due to a lack of knowledge sharing between the IT personnel, who implement security measures, and the product/service owners who sell, improve and are responsible for the product/service. Another reason for this problem is the lack of attention a product/service owner pays to information security. Hence, If one does not know anything about information security and its importance, how could that person improve it? Business Security and IT Security should thus be aligned to create awareness and ensure an information security program that suits both the business and IT. To do so, this paper provides a maturity model to improve an organization's information security on a high level in a structured way. The overall problem is captured in the following research question:

> "How can a maturity model be designed to assist in narrowing the gap between an organization's requirements and its actual level of information security to help improve information security maturity in a structured and effective manner?"

This paper contributes to the development and understanding of information security. The final model addresses the maturity of information security on a high level and provides ample opportunities for further research.

An organization can benefit from the model by using it as a guideline for their information security program. Because the model combines literature with field experience and indicates dependencies between different aspects of information security, the model provides a solid basis to construct an

information security program. For a consultancy organization this model can be a business opportunity. They can offer information security maturity assessments to help organizations in their information security program development.

The next section describes the research approach for developing the model's components. An example of how all focus areas have been designed, is outlined in section 3. Section 4 presents the resulting ISFAM model and discusses its focus areas and component dependencies. Section 5 reports on the single case study we performed at a medium sized organization to evaluate the ISFAM model. Conclusions are drawn in section 6, after which we elaborate on promising venues for further research and discussion points identified during this research.

2 Research approach

Developing an information security artifact requires a structured approach. This section points out the consecutive steps we took to investigate our research question. Since our goal is to develop a model, the design science research method of Hevner et al. (2004) is used. It should be noted that our environment consists of people, organization and technology; all three needed to complete the research. However, we do have a focus on people with information security affiliation and on processes. The actual steps taken to develop this model are defined by Takeda et al. (1990) who describe the design research cycle through the five steps of awareness, suggestion, development, evaluation, and conclusion, respectively.

First, awareness of the problem has already been outlined in the introductory section 1. Second, in section 3 we will investigate the necessary design choices through a comparative literature study to get a better understanding of information security capabilities and focus areas. Also, we will briefly discuss our choice for opting for a focus area maturity model design (Steenbergen et al., 2010). Third, we develop a maturity model for *every* focus area using the Capability Maturity Model standard or derived from literature. Section 3.3 reports about the construction of one particular focus area. Fourth, each maturity model for a particular focus area is evaluated by one domain expert to add practical experience to the model. Metrics are attached to the maturity model, to ensure practical value of the model. Hence, these metrics can be used to measure the maturity level of an organization in that particular focus area on a high level. Steps 2, 3 and 4 are repeated until an satisfactory model is constructed.

Fifth and finally, we develop and evaluate our model at a small/medium sized organization. The model is constructed out of the separate maturity models made in the third phase by using experts, common sense and dependencies. Section 5 reports on the case study performed to test the model in practice and to observe its strengths and weaknesses. Fagan (1993) mentioned that information security is different in various industries. However, focusing our model on only one industry would negatively impact the benchmark capabilities of the results and, therefore, it was decided to keep the model as generic as possible and leave the small changes up to the organizations using the model.

Metrics will mostly be derived from literature. If metrics are not available in literature, they will be defined according to literature and evaluated by domain experts. The next section provides more details on the foundations of our work through the ISO27K series, among others, which will serve as the guideline to help develop the final model.

3 Model development

The purpose of this paper is to present the Information Security Focus Area Maturity Model (ISFAM). First, we will briefly discuss our choice to develop a maturity model, and more specifically, of the focus area maturity type (Steenbergen et al., 2010). Then, we will provide a comparative review of existing information security-related models, which we use to determine our set of focus areas.

3.1 The focus area maturity model type in perspective

Before going further into detail about maturity models, it is important to first explain why maturity models suit this research best. The aim of the maturity model is to close the gap between business requirements with respect to information security and the actual level of implementation. Identifying, representing and closing a gap are therefore three main activities that the solution to the research question should comprise. Identification to show the extensiveness of the gap, representing a gap by a comprehensive model and closing the gap by being able to define a roadmap based on the representation.

Besides those main goals it is strongly desirable that the answer is useful for the business. The used solution is considered more valuable to the business if it represents the information in a managerial way (e.g. overview, quick to scan, easy to use, based on long term targets), serves as a guideline and because the gap needs to be measured, the solution also needs to be established based on the results of metrics. As a last criterion, business is most likely to be committed to their strategic and tactical plans and therefore the model should be able to reflect these plans. Besides these criteria, we did consider alternative artifact types such as a gap analysis, a dashboard, and a list of metrics, but none of these alternatives could completely fulfill our research objectives.

More specifically, a *focus area* maturity model. This model uses the same concept as the well-known continuous five-level maturity model, but without the fixed amount of maturity levels. The model allows having three maturity levels for a focus area, but also seven could be possible. Therefore, this option gives the most options to customize the maturity model to your own wishes. Section 3.3 illustrates how to develop a maturity scale. This type of maturity model was first proposed by Koomen and Pol (1999). Steenbergen et al. (2010) notably formalize this type of maturity model in detail. Focus area maturity models have particular strong roots in the area of software product management (Bekkers *et al*., 2010).

3.2 Information security areas compared

There are a couple of steps involved in making a Focus Area Maturity Model. First, the focus areas need to be defined. The ISFAM model consists of 13 focus areas. 12 of these focus areas are translated from the ISO27K series (British Standard Institute, 2005). The additional area is Architecture. Main rationale for this addition is the CISSP course and the Standard of Good Practice which both handle this area separately. CISSP is a course in the field of information security (ISC^2, 2011). Architecture is one out of ten areas this course addresses. The Standard of Good Practice of the Information Security Forum (ISF) defines a lot more areas than the list shown in the table below. However, most of them can be combined and have overlap with other areas.

Other frameworks used to identify information security focus areas are the information security framework ('ISO-light'), which is based on the ISO27K standard, and the IBM framework. After studying the information security framework it became clear that this framework is a simplified version of the ISO27K and does not provide additional value to the definition of the final focus areas. The IBM framework is interesting because of the practical view upon information security. This framework has been internally developed based on IBM's experiences. However, it only addresses a few focus areas and is not specifically made for information security but for information security problems they encountered during their work. After studying the frameworks and the CISSP course the following 13 focus areas have been identified as shown in the last column of Table 1. The completeness of this set of focus areas was confirmed by the experts which we introduce below.

The next step is to define a maturity scale for each focus area. The maturity scale of each focus area is comparable to a staged model without the requirement of using five stages. Hence, a focus area is allowed to have more or less maturity levels in this model. In the next section, one of the thirteen focus areas is elaborated on in detail. For all thirteen focus areas the same approach has been applied. In total 13 interviews were held—one for each focus area—with eleven different persons. An overview of changes has been made based on the interview outcomes.

IS focus area	*CISSP*	*ISO 27K*	*ISO-light*	*ISF*	*IBM*	*ISFAM*
Risk management	X	X	X	X		*Area 1*
Policy, laws & standards	X	X	X	X		*Area 2*
Organization	X	X	X	X		*Area 3*
HR security		X	X	X	X	*Area 4*
Compliance	X	X	X	X		*Area 5*
Identity/access management	X	X	X	X	X	*Area 6*
Software development	X	X	X	X	X	*Area 7*
Incident management	X (Disaster Rec.)	X	X	X	X	*Area 8*
Business continuity	X	X	X	X		*Area 9*
Change management	X	Comm./Oper. Mgt	X	X		*Area 10*
Physical/environmental	X	X	X	X	X	*Area 11*
Asset management		X	X	X		*Area 12*
Architecture	X (plus Design)			X		*Area 13*
Malicious attacks (prevent)		Partly		X		*Part of other areas*
Cryptography	X	Tool		X		*Part of malicious attacks*
Telecom./network security	X	X	X	X		*Part of architecture*
Governance	X	Organization	Organization	X	X	*Part of organization*
Privacy				X	X	
Transaction/data integrity				X	X	*Part of other areas*

Table 1: Comparative analysis of information security areas in existing models with respect to the thirteen ISFAM focus areas.

Expert #	*Topic(s)*	*Experience*	*Industry*
1	Risk Management Compliance	> 3 years	Finance/oil
2	Policy development	> 3 years	Finance/oil
3	Organization of information security	> 5 years	Security management/various industries
4	Asset Management	> 5 years	Security management/various industries
5	HR Security	> 10 years	Consultancy security manager
6	Physical & Environmental	> 3 years	Social Engineering in various industries
7	Change Management	> 1 year	Audit in several industries
8	Identity and access management	> 5 years	Telecom, Media & Technology
9	Software Development	> 3 years	Finance
10	Incident Management Business Continuity management	> 10 years	All Industries
11	Information Security Architecture	> 5 years	Finance

Table 2: Profile overview of the experts we interviewed.

3.3 Example: asset management

This section describes the process of determining the maturity model for one focus area. Therefore, we performed twelve more expert sessions. Due to space constraints we only describe one here.

For organizations it is important to keep sensitive information inside to avoid sabotage, fraud and espionage. The purpose of asset management in general is to protect assets from falling into the wrong hands. Information assets are objects holding information useful for the business. This could be a computer, a hard disk, but also an employee. Since asset management has a different meaning in every sector and business unit, the following definition is only applicable for this thesis. For the same reason, a new definition for information asset management is proposed. Information asset management in this research is defined as "the process of guiding an information asset during its lifecycle in order to gain maximum benefit from the asset".

The focus area asset management deals with protecting information from inside as well as outside threats. In the ISO27k series there is no distinction made in physical or logical security. Physical assets are computers, papers, and so on. Logical assets are files, passwords, usernames on computers, and so on. Both physical and logical are involved in this focus area. The lifecycle of an information asset is a process of three phases (Ouertani et al., 2008). Beginning of Life (BOL) is the specification, design and creation of the information asset. Middle-of-life (MOL) is the phase where the information asset is used, maintained and provides the intended services it is created for and End-of-Life (EOL) is the disposal or storage of the asset when it is not needed anymore.

Since little literature is available on the field on asset management and information asset management there is also little scientific information available about the maturity of this focus area. Websites from companies and blogs in combination with the CMM standard for defining maturity models are used to propose an asset management maturity model (CMMI Product Team, 2002). One maturity model in the field of asset Management Maturity is proposed in (Oarisk, 2010), which we will reuse as the foundation of this focus area's maturity model. The model as described by Oarisk is more detailed than we need for this research. Moreover, several areas are already taken care of in other focus areas (i.e. training and development, risk management, information management) or are not in scope for this thesis (i.e. health and safety). Therefore, the Oarisk asset management maturity model has not been completely used. In case of Information Asset Management this results in the following maturity levels and their mapping to their corresponding capabilities as shown in Table 3.

Maturity level	***Explanation***	***Capability***
Initial	The costs of asset management are unknown, no roles are defined and no reports are made. Typically, asset management is chaotic and unstructured.	
Repeatable	Senior management knows the importance of asset management but no concrete plans exist. Though there are some structured operational processes in place.	A
Defined	There are processes in place that help business objectives and individuals get training. These individuals also get roles in the change management process.	B
Managed	Processes are cross departmental, roles are well defined and asset management is coordinated across functions. Asset management is well thought of.	C
Optimized	Every single part of asset management is documented, aligned and known organization-wide.	D

Table 3: Information Asset Management Maturity Model.

Area	Capability	Nr	Answer
Asset Management			
	Senior Management within departments takes responsibility for Asset Management	A1	**Yes**
	Senior Management within the organization recognizes the importance of Asset Management	A2	**Yes**
	There is a formal Asset Management policy in place that takes into account the asset management lifecycle phases.	B1	**Yes**
	All Asset Management roles and responsibilities are defined.	B2	**No**
	Asset inventory is created based on status, connectivity, classification and proximity.	B3	**No**
	All assets have been assigned to an owner	C1	**No**
	All stakeholders are familiar with Asset Management procedures and processes	C2	**No**
	Asset Inventory is maintained	C3	**Yes**
	Safe disposal, handled, processed, stored in line with the classification	C4	**No**
	Asset Management Policies are periodically reviewed and updated	D1	**No**
	The Asset Management process is continuously reviewed and updated.	D2	**No**
	An asset management system is in place to increase performance capacity	D3	**No**
	The classification is based on the asset's lifecycle	D4	**No**

Figure 1: Fragment of the ISFAM assessment consisting of 13 out of 161 questions as implemented in a standard spreadsheet. In this example capability B of the focus area Asset Management is not achieved yet as not all Bx questions can be answered with yes.

In order to determine the maturity level based on the current organizational capabilities regarding asset management the following capability assessment statements shown in Figure 1 have been identified. To evaluate the initially proposed statements based on asset management literature, we interviewed Expert #4 with more than five years of experience in the field of ISO27K and advising herein, as indicated in Table 2. He performed ISO27K assignments at a variety of companies and this experience can be well used for the evaluation of this model.

The first part of the conversation was about the role of asset management in the final model. Expert#4 liked the inclusion of dependencies in the model because which are not incorporated in other models he knows about. His concern was the determination of the dependencies, which we will further discuss in section 4.2 and which we will evaluate through a case study as described in section 5.

Our maturity model proposal for asset management was discussed next. Expert#4 agreed that a maturity model can be set up using the different stages of the lifecycle. He also recognized some kind of CMM structure which is recognizable to the business and, therefore, very usable. Five stages make sense and is the right amount to map the lifecycle on. Our proposed model represented the lifecycle correctly, according to Expert#4, if some minor changes and additions could be incorporated, as summarized in Table 4.

Action	***Result***
Change	Senior Management instead of single employees should recognize the importance of asset management
Add	B3 is extended with information that should be mentioned in an asset inventory
Change	All employees in B2 became all stakeholders
Add	Asset inventory is maintained
Change	The statement asset management should be leveraged to the maximal benefit changed to an asset management system is in place to increase performance capacity.
Add	Classification should be based on the lifecycle of an asset

Table 4: Overview of evaluation changes regarding asset management based on expert interview.

Starting with the first capability, we discussed who ideally should recognize the importance of asset management. Initially the model stated that individual employees do so, but after the discussion we changed it to senior management because ideally all ideas should be supported by senior management before it can be effective. At the second capability Expert#4 made one comment. Since we only addressed the importance of asset inventory, he mentioned it would be better to also include what should be stated in the asset inventory. B3 was extended to cover this. At the third capability also some changes were made taking into account the lifecycle. C3 was added and instead of mentioning all employees at B2, it became all stakeholders. At the fourth stage two changes were made. Instead of leveraging an asset to the maximal benefit he suggested to include using a system that increases performance capacity. That should be the ultimate goal for asset management and is more concrete than what was originally in the model. As a second change, we added that classification should be based on the lifecycle of an asset. Different assets are of different importance to the organization. The invocation of applying the lifecycle varies thereby as well. If an organization operates at an optimized level, classification should be done based on the lifecycle of that asset.

4 The ISFAM model

Figure 2 presents the Information Security Focus Area Maturity (ISFAM) model. The model consists of 4 focus area groups which cluster 13 focus areas and distribute 51 capabilities (A-E) over 12 model-wide maturity levels. The latter can be grouped, in turn, for convenience into 4 maturity stages which strongly resembles the audit control pattern (Singleton, 2009). Note that the overarching 12 levels result automatically from the capability interdependencies (Steenbergen et al., 2010). The model's underlying assessment consists of a series of 161 yes/no questions. Special care has been taken to integrate the

many dependencies between its included capabilities, which is described in section 4.2. Figure 2 also shows the results of the performed assessment which is described in section 5 below, as green progress bars from left to right, from level 0 up to the capability—e.g. capability B in focus area #1, risk management, at maturity level 5—that our case study organization has not achieved yet.

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 2: The Information Security Focus Area Maturity (ISFAM) model, with the results in green of the assessment carried out for our case study organization as reported in section 5.

The ISFAM model in Figure 2 consists of the thirteen focus areas as identified in Table 1 and to be outlined in section 4.1 below, which are grouped for convenience into four categories. First, the *Organizational* category comprises focus areas that are organizationally oriented and are mostly characterized by organizational statements rather than technical. Second, the *Technical* category comprises focus areas that are, obviously, technically oriented, indicating that the statements often require a technical implementation or the focus area represents the technical implementation of an organizational focus area. Third, the *Organizational and Technical* category comprises focus areas that specifically require both technical as well as organizational statements to become more mature. Fourth and finally, the *Support* category comprises focus areas which support the other focus areas in becoming more mature.

Focus areas mentioned in the latter category are part of the defense-in-depth concept which implies that your organization should be secured on different levels. Defense-in-depth can best be explained using a castle as a metaphor. A castle has a moat, but when the enemy is able to pass the moat, there is still a thick wall they need to climb over or break through. The same applies to an organization. An attacker can physically enter a building, but when the attacker needs a badge to enter it becomes more difficult. When he succeeds in passing this barrier, there is still the option to secure your network, and even on a lower level the valuable data itself.

4.1 Focus areas

We performed similar steps as described in detail in section 3.3, to develop the other twelve focus areas. We briefly discuss each area by outlining the initial and final stages of maturity. Regarding **risk management**, in the *Naïve* stage (1A, at maturity level 3 in Figure 2), the organization reacts on adverse events but does not have a structured approach in handling risk and uncertainty and does not learn from

past events. In the *Natural* stage (1D), risk management is used to control opportunities as well as negative effects. Risk management processes are used to gain competitive advantage and are well-known by the entire organization (Hulett, 2001). Regarding **policy development**, in the *Ad-hoc* stage (2A), the organization's information security policy document is made ad-hoc and often consists of policies found on the internet. The organization is familiar with laws and regulations. In the *Developed* stage (2C), the organization has an integrated, in detail described information security policy document in place. The development of the information security policy document is seen as a continuous process supported by reviews (Wood, 2011).

Regarding **organizing information security**, we start from the *Management awareness* stage (3A), where management wants to improve their information security and makes resources available. In the *Optimizing* stage (3D), the organization is part of special interest groups to share knowledge. Their organization concerning information security is updated and reviewed on a regular basis and external parties are taken into account for that (British Standard institute, 2005). Regarding **human resources security**, in the *Repeatable* stage (4A), the organization knows that human resource security is necessary and is formalizing processes. However, human resources security policies and processes are not implemented. In the *Optimized* stage (4D), the organization is optimizing their human resources security. Personal development is important and the whole organization is continuously reminded of the policies (QGEA, 2010). Regarding **compliance**, which we define as "the extent to which an organization meets and follows their information security policy and processes", we have developed three maturity levels from *Ad hoc* (5A) to *Developed* (5C). In the former, the organization complies with laws and regulations and complies sometimes to policies since they are forced by systems or already part of their daily work. In the latter, the organization reviews their compliance level and is pro-actively improving it. This also included taking measures against violation of the policies.

Regarding **identity and access management** (IAM), in the *Developing* stage (6A), IAM becomes a separate discipline. IAM is performed per project or business unit but not organization wide. In the *Optimized* stage (6D), IAM programs are continuously optimized and reviewed. IAM is now an enabler for the business (Gartner, 2009). Regarding **secure software development**, we start from the *Developing* stage (7A), where the organization does have ideas on how to develop their software, but security is not the main point of attention, whereas functionality is. In the *Optimized* stage (7D), software is regularly reviewed with respect to updates and vulnerabilities (BSIMM3, 2011).

Regarding **incident management**, in the *Inadequate* stage (8), there is a policy and a process for the classification of systems, but no formal roles or processes are defined. In the Best practice stage (8D), the incident management process is tested and optimized using the test results (Mura, 2012). Regarding **business continuity management** (BCM), in the *Initiated* stage (9A), that there needs to be formal management commitment to BCM within the organization. High roles are defined and a special BCM policy is in place. BCM at the *Optimized* stage (9E) is a strategic instrument that can create commercial and competitive advantage. The organization seeks continuous optimization of their BCM (Smit, 2005). Regarding **change management**, in the *Isolated* stage (10A), some elements of change management are being applied in isolated projects. In the *Competent* stage (10D), change management competency is evident in all levels of the organization and is part of the organization's intellectual property and competitive edge (Prosci, 2004).

Regarding **physical and environmental security**, in the *Repeatable* stage (11A), if events reoccur several times, this knowledge is used to form an informal process of how to handle with that event. The organization becomes more professional in dealing with environmental uncertainty and harming physical attacks. In the Optimizing stage (11D), the organization is improving their physical and environmental security continuously and checks/updates their security on a regular basis (NoticeBored, 2004). Regarding **asset management**, we refer to Table 3 in section 3.3 (Oarisk, 2010). Regarding **architecure**, this covers enterprise architecture, IT architecture and information security architecture. In the *Ad-hoc* stage (13A), IT security considerations are ad-hoc and localized. There is no structured architecture in place for the whole organization but there may be some local or departmental initiatives

for information security architecture. In the Optimized stage (13D), feedback from IT security architecture metrics is used to drive architecture process improvements (The Open Group, 2011).

4.2 Dependencies

After defining all focus areas, the next step in building the ISFAM model was to identify dependencies and mapping them onto the model. In brief, dependent capabilities should always be positioned at a lower maturity level—i.e. to the left, visually speaking—than the capability under investigation. The blue arrows in Figure 3 show dependencies found in literature. For example, eleven arrows originate from capability A of the focus area Organizing information security. This capability—3A, the management awareness stage—consists out of three statements: (1) There is senior management commitment to information security, (2) Management makes sufficient resources available to address information security, and (3) Management is formally responsible for all policies.

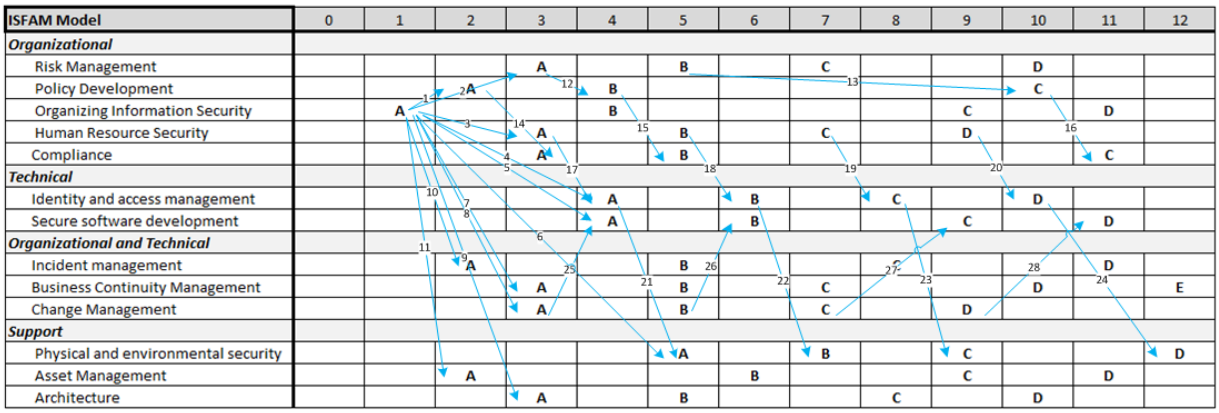

Figure 3: Dependencies in the ISFAM model found in literature.

According to Solms (2006) and Kankanhalli et al. (2003), the implementation of an information security program starts with management commitment and having sufficient resources available. Therefore, no other capability can be placed before capability 3A of organizing information security.

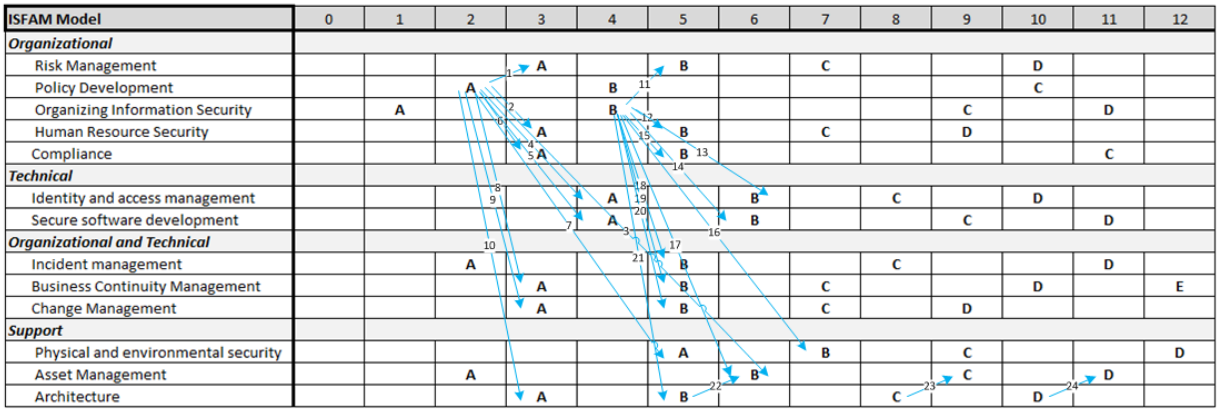

Figure 4: Deducible dependencies in the ISFAM model.

Deducible dependencies are dependencies that make sense or are derived from a top-down approach. Figure 4 shows these dependencies. For example, to ensure consistency throughout the organization, policy guidelines have to be established on a high level before policies can be established for every other single focus area (arrows 1-10). Implementing and developing policies in a top-down manner makes sure that, if strategy is included in the high level policy, the strategy of the organization is also drilled down to the rest of the organization. A line of policy development A is therefore linked to other

capabilities where one of the statements refers to the development of the policy for that specific focus area.

Capabilities that are not addressed by arrows as shown in Figure 3 are set up based on feedback from the expert interviews we held for every focus area. For example, business continuity management E and physical and environmental security D are not in place for a lot of companies and have been placed at level 12.

5 Evaluation

The evaluation of the ISFAM model has been carried out using the evaluation method of Yin (2003). Specifically, we selected the construct validity test since the goal was to evaluate the final model, the statements within this model, dependencies (only the ones touched by the results of the assessment) and the result of the assessment. Furthermore, the single case study design with a holistic view has been selected because the model is evaluated for the whole organization and no distinction has been made between various departments.

5.1 Single case study

The ISFAM model is evaluated at a small/medium sized telecommunications organization in the Netherlands we dub TELCOM. We are aware that applying the ISFAM model in another industry with a different headcount might result in a different result of the evaluation and therefore a slightly different model. However, our goal here is to demonstrate the validity of the conceptual ISFAM model in representing an organization's maturity level, and enabling an organization to develop an information security program and to verify whether capabilities are placed in the right order in the ISFAM model.

TELCOM operates across the globe but has its headquarters located in the Netherlands. It employs around 65 people and serves relatively few business clients. TELCOM has already seriously started improving their information security a couple of years ago. Before, they were also concerned about security, but did not formalize the processes around it. Their reason to participate in the ISFAM model evaluation is to verify their current status and to create an improvement plan for the future. We sat together with two managers of the company, representing both business and IT management. Together they are responsible for the security within the company and able to answer the questionnaire within the tool, as shown partly in Figure 1. Because they discussed and answered the questions together, the answers could be validated immediately and we could observe whether the managers would hear about new information security-related management aspects from each other.

We will consider the ISFAM model to be successful if the following ISFAM design aspects can be verified: First, The total analysis can be performed within a four hour timeframe; the model needs to be lightweight and easy to use within organizations. We expect that this limited timespan will help increase ISFAM acceptance in SMEs. Four hours has been set as a limit for the questionnaire and analysis of the results. Second, all questions make sense; questions should unambiguous and easy to understand. This prevents employees from having different opinions about the answer on a question and therefore being unaligned. Third, the organization recognizes itself in the result; the most important aspect of the model is its capability to represent the information security maturity level of an organization. Reviewing the results of the ISFAM model should result in recognition. Fourth, dependencies that influence the result of this model need to be correct; dependencies can always be changed based on changes over time, differences between industries and size of the organization. Therefore a full evaluation of all dependencies is not necessary for this study. The organization should however agree upon their next steps according to the ISFAM model. For example, the model suggests that they first have to work on incident management and next on identity and access management. The organization looks at the statements within the capability not yet reached and decides whether the improvement steps are placed in the right order or not.

5.2 Assessment results

The ISFAM design aspects laid out above were met after completion of the ISFAM assessment as follows. First, the total analysis could indeed be performed within four hours. It took about three hours in total to evaluate the ISFAM model including answering the entire questionnaire. Second, all questions made sense after processing some minor feedback received from TELCOM regarding the roles in small to medium sized organizations. According to TELCOM the questions were easy to understand and with the additional changes made, the questions became unambiguous as well.

Third, TELCOM indeed recognizes itself in the results. They realize additional effort has to be put in formalizing their processes and policies. According to their overall maturity level reached (level 1 because of lacking in focus area 8) they are in the Design phase which corresponds to their view on their business. Fourth and finally, the next point of attention according to the result of the model was identified as such. They agreed that the ISFAM model gave them a guideline of what is advisable to be do first. In this case, it would for example not make sense to bring the organization of information security focus area to level D, while incident management did not even reach capability A.

To enhance the completeness and accuracy of this case study we sent the draft version of the case study back to TELCOM for a review. The two managers agreed upon the results and the draft and did not require anything to be changed.

6 Conclusions and discussion

This final section revisits our research question and elaborates on the final results. Then, we point out some limitations of this research and useful possibilities for further research.

6.1 Conclusions

We are now ready to answer the main question: “How can a maturity model be designed to assist in narrowing the gap between an organization’s requirements and its actual level of information security to help improve information security maturity in a structured and effective manner?”

In section 2 it was determined that a maturity model would suit best to minimize or close the gap. The ISFAM Model has been set up to improve information security maturity in a structured and effective manner. The ISFAM Model consists of thirteen focus areas originating from various standards, certifications and methods. To be able to measure the current state of an organization and define a roadmap for the future the thirteen focus areas have been made measurable by defining maturity levels. Every maturity level/capability has been given substance to via closed-ended (yes/no) statements. Altogether, this led to 161 statements covering the entire space of information security. Answering the 161 statements with yes/no takes approximately three hours and gives a good overview of what the current state of the organization is, and in which security capabilities it currently is lacking in the most. Due to its high granularity, ISFAM is able to provide tangible process improvement advice. All statements have been defined based on literature and additional interviews to verify the appropriateness of the statement and add business value to the model. The maturity levels/capabilities have been set up using already existing maturity models and by defining new maturity models using a CMM approach where necessary.

For the final ISFAM model an appropriate distribution of capabilities over the model was required to enable the model to serve as a guideline and roadmap. The capabilities have been placed into the model following two steps. First, based on dependencies that have been found in literature, and second, using deducible dependencies that originate from the top-down approach and were gathered from the various interviews. Business value has been added by translating the ISFAM Model into an assessment tool. This tool has been evaluated through a single case study in practice. The organization under investigation was at the stage that it did recognize the importance of information security, but was still only at the starting phase of implementing it.

The research question can, therefore, be answered with the ISFAM model. During the assessment two managers sat together and discussed the measures they had in place to ensure the security of their data. They could, by discussing the 161 statements, determine their actual level of information security. They agreed upon the results of the ISFAM assessment and therefore the model can be seen as a good way to determine an organization's information security maturity at a high level. Additionally, with this result they confirmed that it is easier for them to make budget available for information security. Reason for this is that the model provides high level advice on possible next steps. Thereby it becomes easier to define an information security program for the coming years. Over a longer period of time this will likely result in narrowing down the gap between the actual level of information security maturity and business requirements.

6.2 Further research and discussion

Based on feedback regarding the model, assessment tool and followed approach there are discussion points that need to be addressed. First of all, it is unclear what will happen to the model in the coming five years. It might be the case that new developments in the domain of Information Technology, such as cloud computing, mobile security and cyber security, will result in significant changes to the model. The model could therefore not be entirely time resistant. Therefore, we are currently investigating all these developments in relation to the ISFAM model (*e.g.* Baars and Spruit, 2012). Next to that, it is also not sure if the model holds for all organizations. Different organizations in different sectors with different sizes have different issues on their mind at a different moment in time. However, we can already confirm that the ISFAM model also has proven valuable in a large financial organization. Another case study in the healthcare sector is underway. We will continue to perform more assessments at different organizations and repeat these assessments after half a year will eventually result in a solid model that might even be able to illustrate the differences per sector in addressing information security. We have now also started research on developing an integral solution for these issues including performing additional case studies in various industries under the monniker Situational Process Improvement in Cybersecurity (SPICY).

Another point open for discussion is benchmarking versus tailor-made assessments. In this work we decided to keep as much benchmarking value as possible by not adding industry specific characteristics. However, by doing so, it might be that the guideline and alignment capability of the model is less accurate. Additionally, the benchmarking value of the ISFAM model has not yet been proven. By evaluating the model at only one organization, not many dependencies may have been covered. Therefore, no absolute certainty can be given yet about the practical applicability of the dependencies situated in the higher maturity levels of the organization.

Third point of attention is the visualization of the results. For now, it is being displayed using the representation as proposed by Bekkers *et al.* (2010). However, from a business perspective it may be more effective to represent this model in a spider chart since most managers are familiar with such type of representation. For the ISFAM model, twelve cyclic maturity levels would have to be made and the thirteen focus areas would be represented by thirteen "pieces of pie". By using red, orange and green pie colors we could provide an improvement path: red being the history, orange the level that is current and green the level where the organization wants to be in the future.

Our last suggestion for further research and discussion considers the alignment between IT and business. The ISFAM model has been evaluated by two managers discussing interactively whether questions should be answered with yes or no. Although they did not always agree on the answers, they seemed to be on the same page. It is useful that they discovered some points where they did not agree at once; because that implicates that they do not know everything of the organization themselves and need more persons to determine what their current maturity level is. For alignment purposes it would provide additional value if the model is also evaluated at non-IT focused organizations.

References

Baars, T., and Spruit, M. (2012). Analysing the Security Risks of Cloud Adoption Using the SeCA Model: A Case Study. *Journal of Universal Computer Science, 18*(12), Security in Information Systems, 1662–1678.

Bekkers, W., Weerd, I. van de, Spruit, M., and Brinkkemper, S. (2010). *A Framework for Process Improvement in Software Product Management*. In A. Riel, R. O'Connor, S. Tichkiewitch, and R. Messnarz (Eds.), Communications in Computer and Information Science 99, Software and Services Process Improvement - Proceedings of the 17th European Conference (pp. 1–12).

British Standard Institute (2005*). ISO/IEC 27002: Information technology – Security techniques – Code of practice for information security management.* Londen, UK.

BSIMM3 (2011). *Building Security In Maturity Model.* Retrieved December 8, 2013, from http://bsimm.com/download/.

Chapin, D., and Akridge, S. (2005). How can Security be measured. *Information Systems Control Journal, 2*, 43-47.

CMMI Product Team (2002). *CMMI for Systems Engineering/Software Engineering/Integrated Product and Process Development/Supplier Sourcing*, Version 1.1, Continuous Representation. *CMU/SEI*.

Fagan, P. (1993). Organizational issues in IT Security. *Computer & security, 12*(8). 710-715.

Gartner (2009). *Toolkit: Identity and Access Management Program Maturity Assessment.* Retrieved December 8, 2013, from http://www.gartner.com.

Hevner, A., March, S., Park, J., and Ram, S. (2004). Design science in information systems research. *MIS Quarterly, 28*(1), 75-101.

Hulett, D.T. (2001). *Key Characteristics of a Mature Risk Management Process*. Fourth European Project Management Conference, PMI Europe, London, UK, 6-7 June, page 6.

ISC^2 (2011). CISSP – Certified Information Systems Security Professional. *ISC2.* Retrieved December 8, 2013, from https://www.isc2.org/cissp/.

Jaquith, A. (2007). *Security Metrics: Replacing Fear, Uncertainty, and Doubt.* Reading, MA: Addison Wesley.

Kankanhalli, A., Teo, H., Tan, B., and Wei, K. (2003). *International Journal of Information Management, 23*(2), 139-154.

Koomen, T., and Pol, M. (1999). *Test Process Improvement, a practical step-by-step guide to structured testing*. Boston, MA: Addison-Wesley Longman Publishing.

Mura, L. (2012). *The PPBI Incident Management Maturity Model*. PPBI. Retrieved December 8, 2013, from http://www.ppbi.org.

NoticeBored (2004). *Securing physical access and environmental services for datacenters.* Retrieved December 8, 2013, from http://www.infosecwriters.com/text_resources/pdf/datacenter_security.pdf.

Oarisk (2010). *Oarisk operational Asset and Risk Solutions*. Retrieved December 8, 2013, from http://www.oarisk.co.uk/Asset_Management_Maturity_Model.html.

Ouertani, M., Parlikad, A., and Mcfarlane, D. (2008). Towards an approach to select an asset information management strategy, *International Journal of Computer Science and Applications, 5*(3b), 25-44.

Prosci (2004). *Prosci's Change Management Maturity Model*. Retrieved December 8, 2013, from http://www.change-management.com/Prosci-CM-Maturity-Model-writeup.pdf.

QGEA (2010). *Information Standard IS18*. Retrieved December 8, 2013, from http://www.qgcio.qld.gov.au/products/qgea-documents/549-information-security/2704-information-security-is18.

Singleton, T. (2009). What every auditor should know about controls: The CDLC. *ISACA Journal, 3.* 1-2.

Smit, N. (2005). *Business Continuity Management*. Retrieved December 8, 2013, from http://www.pvib.nl/scripties.

Solms, B (2006). Information Security – the fourth wave. *Computers & Security, 25*(3), 165-168.

Steenbergen, M. van, Bos, R., Brinkkemper, S., Weerd, I. van de, and Bekkers, W. (2010). *The design of focus area maturity models*. In R. Winter, J. Zhao and S. Aier (Eds.), Global Perspectives on Design Science Research Lecture Notes in Computer Science (pp. 317-332). Berlin, Heidelberg.

Takeda, H., Veerkamp, P., Tomiyama, T., and Yoshikawa, H. (1990). Modeling Design Processes. A*I Magazine , 11*(4), 37-48.

The Open Group (2011). *Architecture Maturity Models.* Retrieved December 8, 2013, from http://pubs.opengroup.org/architecture/togaf8-doc/arch/chap27.html.

Wood, C. (2011). *Levels of maturity in The Security Policy Development Process.* Retrieved December 8, 2013, from http://www.informationshield.com/security-policy/2011/01/levels-of-maturity-in-the-security-policy-development-process/.

Yin, R. (2003). *Case Study Research: Design and Methods.* Third edition. London, UK: Sage publications.