Chapter

ISFAM 2.0: REVISITING THE INFORMATION SECURITY ASSESSMENT MODEL

***Marco Spruit*[*], PhD, and Gabriel Slot, MSc**

Department of Information and Computing Sciences,
Utrecht University, The Netherlands

ABSTRACT

An information security maturity model helps organizations visualize and identify the steps that need to be taken in order to become increasingly more mature. Maturity of security indicates the degree of development and strength of an organization's security measures to mitigate risks threatening its assets.

Unfortunately, one maturity model does not fit all organizations, because organizations have different organizational profiles. According to previous research, eleven organizational characteristics affect information security, i.e., a financial institution requires different security measures than a bakery. It is necessary to have a well fitted information security maturity model for every organizational profile in order to fully support

[*] Universiteit Utrecht, Department of Information and Computing Sciences, Buys Ballot Laboratory, office 582, Princetonplein 5, De Uithof, 3584 CC Utrecht, e-mail: m.r.spruit@uu.nl.

the organization. The research at hand has been set up to study the effects of a selection of the identified organizational characteristics on the capability level of the focus area maturity model in the information security domain.

In order to do this, the existing Information Security Focus Area Maturity (ISFAM) model is further refined according to the effects of organizational characteristics. During the research, however, the information security experts that we interviewed did not find the expected situationality effects in the lower levels of the ISFAM model. According to the experts, the requirements in the ISFAM model to reach a certain maturity level are too generically defined and therefore work for organizations with different organizational characteristics. This is backed up by the fact that the model has in fact been successfully assessed at multiple case organizations with different profiles.

Keywords: organizational characteristics, information security, maturity model, ISFAM, threats

INTRODUCTION

Information security is an important aspect of information technology in almost every domain that handles information. It is defined by the International Standards Organization as the protection and preservation of Confidentiality, Integrity, and Availability of information: the CIA triad. In addition, the authenticity and reliability of information should be protected. The joint aspects of confidentiality, integrity, availability, accountability and auditability are often combined to extend the de facto CIA triad and are referred to as the CI3A quintet (Baars & Spruit, 2013).

To set the scene, Figure 1 visualises the key historic events that have progressed the field of information security since the late 1960s, when the Multiplexed Information and Computing Service (MULTICS) operating systems first introduced an early type of access control (Roeling, 2012). In the early 1970s the US Department of Defense (DoD) made computer security more publically known. The Bell LaPadula (BLP) model is the first system to represent multilevel security policy in terms of access rights, which is also referred to as the Multi-Level Security (MLS) model. The first encryption algorithm was developed by the US National Security Agency (NSA) to securely send data over networks by cryptography, and became a standard in 1977 as the Data Encryption Standard (DES). After these early events, the importance of information security as a separate field became increasingly clearer, perhaps partly due to the 1988 Morris Worm as the first computer worm. In 1989 a certificate for the information security profession was defined: the Certified Information Systems Security Professional (CISSP), indicating the increasing maturity of information security as a worthy field of expertise.

Returning to the present, information security can help not only in securing the assets of an organization and assisting in sharing information in a safe way through various security controls, but also by building up a trustworthy relationship between the service providing organization and its stakeholders (Lessing, 2008). The main goal of information security is to protect the assets of the organization against rising threats, i.e., theft of hardware or information, and natural threats such as flooding as well. The assets are in danger when vulnerabilities of the assets are exploited by the threats. In order to mitigate the threats from happening, controls or measures should be implemented. An information security control, a measure in order to mitigate an identified vulnerability and to protect the respective assets, is a critical element for successful information security (Menkus, 1991).

The growth or maturity towards the level of information security is though, especially for a Small and Medium sized Enterprise (SME). SMEs often lack the necessary knowledge and resources to mature to the demanded level of information security (Mettler and Rohner, 2009). Maturity models are tools that can help organizations in visualizing the maturity progress in adopting process and standards and to benchmark themselves in their industry (Becker, Knackstedt, and Pöppelbuβ, 2009). Maturity in the field of security indicates the degree of development and the strength of the organization’s security measures (Lessing, 2008). Information security maturity models help organizations mature in the process of implementing the right measures in order to secure the organization’s assets.

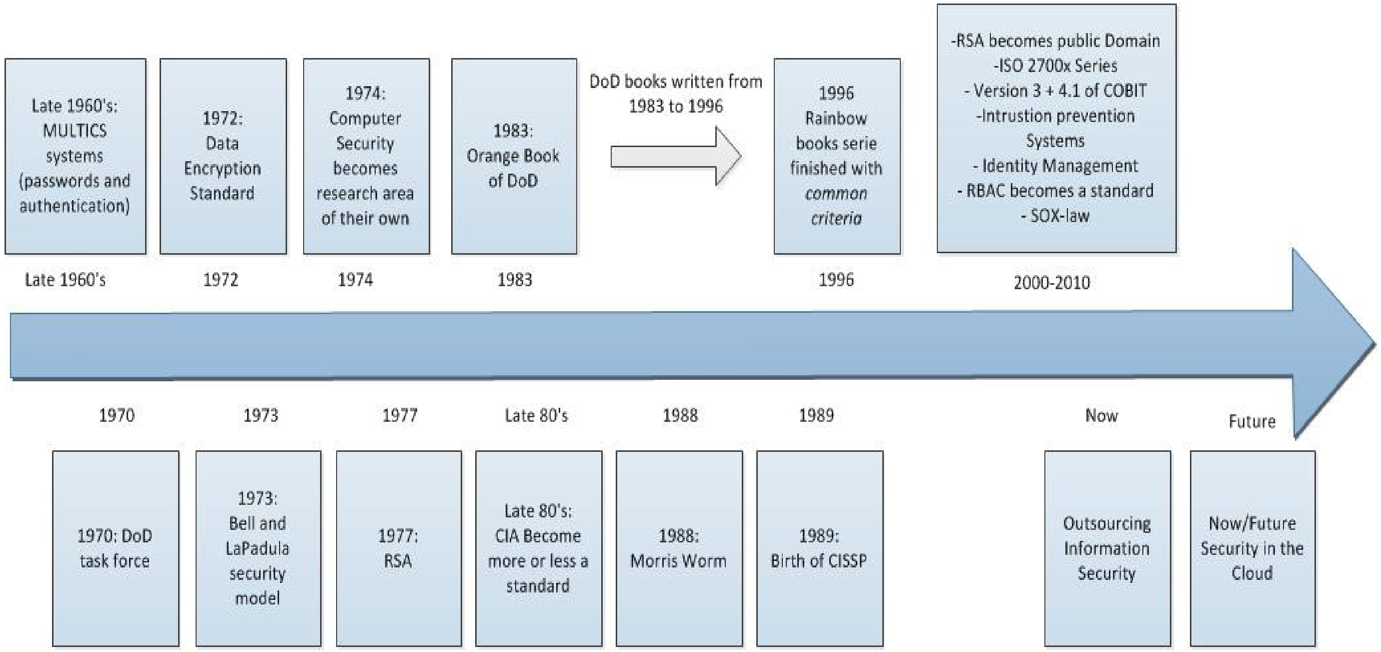

Late 1960's: MULTICS systems (passwords and authentication)
1972: Data Encryption Standard
1974: Computer Security becomes research area of their own
1983: Orange Book of DoD
DoD books written from 1983 to 1996
1996 Rainbow books serie finished with *common criteria*
-RSA becomes public Domain
-ISO 2700x Series
- Version 3 + 4.1 of COBIT
-Intrustion prevention Systems
- Identity Management
- RBAC becomes a standard
- SOX-law
Late 1960's
1972
1974
1983
1996
2000-2010
1970
1973
1977
Late 80's
1988
1989
Now
Future
1970: DoD task force
1973: Bell and LaPadula security model
1977: RSA
Late 80's: CIA Become more or less a standard
1988: Morris Worm
1989: Birth of CISSP
Outsourcing Information Security
Now/Future Security in the Cloud

Figure 1. A brief timeline of information security.

Most maturity models are fixed-level maturity models and are less suited to incremental improvements, as they cannot express interdependencies between maturity stages (Steenbergen, Bos, Brinkkemper, Weerd, and Bekkers, 2010). A type of maturity model allowing incremental improvements is the focus area maturity model. Advantages of using such a maturity model are that:

- It allows a fine-grained approach;
- It is possible to distinguish more than five overall stages of maturity. This results in smaller steps between the stages, providing more detailed guidance to setting priorities;
- It is flexible in defining both focus areas and interdependencies between focus areas. (Steenbergen et al., 2010)

Focus areas form the core concepts of the focus area maturity models. By positioning the capabilities of the focus areas in the model, while considering the dependencies between each other, the focus area maturity model presents the order in which the focus areas need to be addressed and implemented. A focus area is defined by as an aspect of a functional domain covering the whole activities, responsibilities, and actors involved (Steenbergen et al., 2010). Focus areas can be divided into a number of capabilities, depicted in the matrix by capital letters. Capabilities are ways to achieve a predefined goal, which is defined by improvement actions, which is linked to a certain maturity level (Steenbergen et al., 2010). The position of the capabilities of a focus area indicates the order in which the capabilities should be reached.

A focus area maturity model in the information security domain, specially designed for SMEs, is the Information Security Focus Area Maturity (ISFAM) model (Spruit and Roeling, 2014). It consists of four focus area categories (organizational, technical, organizational and technical, and support) which cluster 13 different focus areas (on the left), and distribute 51 capabilities (A-E) over 12 maturity levels. The maturity levels are grouped into four maturity stages: Design, Implementation, Operational Effectiveness, and Monitoring.

BACKGROUND

Organizational Characteristics

As often is heard as a criticism (Bollinger and McGrowan, 1991), having a static maturity model that applies for every organization is oversimplifying reality and results in a poor model fit, because every organization has its own organizational characteristics that are different from other organizations. It is necessary to change an information security maturity model based on the organization's profile in order to support an organization in their maturity process.

According to the CHOISS model by Mijnhardt, Baars, and Spruit (2016), eleven organizational characteristics (Table 1) affect the information security and therefore the domain's maturity model.

Table 1. The Characterizing Organizations' Information Security for SMEs (CHOISS) model relates four categories (A-D), eleven OCs (1-11) and forty-seven measurement levels (Mijnhardt et al, 2016)

(A) General	(B) Outsourcing	(C) IT Dependency	(D) IT Complexity
Number of Employees	Percentage of Outsourced versus Insourced Software Development	Importance of Critical Data	Number of Employees supporting IT Environment
Revenue	Percentage of Outsourced versus Insourced Software Hosting/IT Services	Importance of Confidentiality of Critical Data	Annual Expenditure on IT over Revenues
Sector		Importance of Availability of Critical Data	
		Possible Time without IT Support	

A statistical study done by Baars, Mijnhardt, Vlaanderen, and Spruit (2016) following up on the research of Mijnhardt et al., (2016), focuses on the effect of organizational characteristics on the ISFAM model. Baars, et al., further evaluated the organizational characteristics and their measurement levels, and how the organizational characteristics pertain to the ISFAM model in order to understand the influence of the organizational characteristics on the focus areas within the ISFAM model (Baars et al., 2016). According to their research, organizational characteristics influence both the maturity framework as the focus areas that the model holds (Baars et al., 2016). However, focus area maturity matrices have a lower level object of measurement: the capabilities that reside in a focus area. This research follows up on the previous works (Mijnhardt et al., 2016; Baars et al., 2016) first by updating the ISFAM model, as information security has evolved since the development of the model, and then by researching the effects of organizational characteristics on the capability level of the ISFAM model. The research question is defined as follows:

> To what extent can organizational characteristics be incorporated into an information security focus area maturity model?

Threats

To better understand the types of threats that need mitigating by the information security focus area maturity model (ISFAM), we have merged four different threat taxonomies from academic literature, as well as two additional information security threat overviews. First, Chapman, Leblanc, & Partington (2011) distinguish three tiers in their taxonomy: no network or computer access, user access with limited privileges, and root access/administrative privileges. Second, Kotapati, Liu, Sun, & Laporta (2000) identify the following three dimensions from a 3G networks perspective: physical access to the network, attack categories, and attacks means. Third, Hansman and Hunt (2005) developed a taxonomy of network and computer attacks of four dimensions: means (by which the attack reaches its target), targets, vulnerabilities/exploits (used during attack), and payloads/effects beyond. Fourth, Cebula & Young (2010) of The Software Engineering Institute developed a taxonomy for operational cyber security risks, including actions of people, systems and technology failures, failing internal processes, and external events. Complemented by the Dutch National Cyber Security Center's report (NCSC, 2012) and the European Network and Information Security Agency's Threat Landscape (Marinos & Sfakianakis, 2012), we propose the following taxonomy of information security threats that our assessment model needs to consider in Figure 2, grouped by threat relevance level for hospitals based on (NCSC, 2012) as compiled in (Reijmer, 2014).

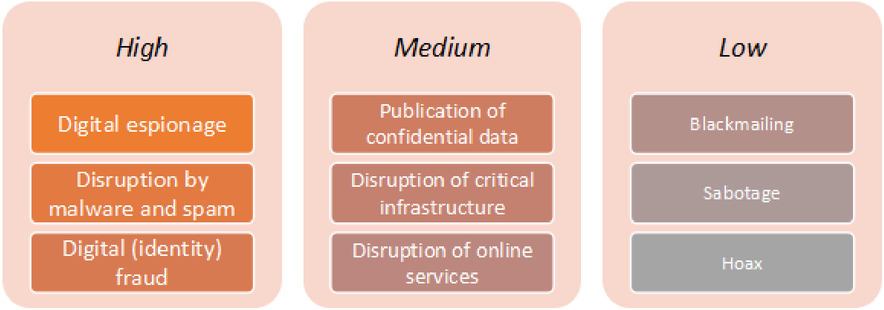

High
Digital espionage
Disruption by malware and spam
Digital (identity) fraud
Medium
Publication of confidential data
Disruption of critical infrastructure
Disruption of online services
Low
Blackmailing
Sabotage
Hoax

Figure 2. A taxonomy of information security threats for hospitals grouped by threat relevance level.

We start this description of the identified threats with the high impact group of threats. *Digital espionage or cyber espionage:* Information technology is used (sometimes in combination with social engineering to steal confidential information. *Disruption by malware (malicious code) and spam:* In this category we include several forms of malicious code such as worms, viruses, and trojans. Malicious code is a worm when it spreads to other systems by duplicating itself without attaching to other files, viruses inject code into applications installed on a computer, and trojans are programs that pretend to offer a functionality in order to entice an user to download and install it, the actual purpose of the program is to install harmful code on the host. *Digital (identity) fraud/theft:* Digital fraud is a large threat, especially with respect to the financials of an organization.

Identity theft occurs when credentials such as username and password are stolen and used for malicious goals.

Medium impact threats include the following. *Publication of confidential data:* Publication of confidential information about customers, patients or suppliers is a threat that is mentioned in many sources, and can be performed by different actors. For example in the healthcare sector researchers (reporters) form a dangerous threat when it comes to compromising confidential data. *Disruption of critical infrastructure:* This category of threat is connected with ICS/SCADA systems that are often not well protected. A vulnerability in these systems can result in serious issues concerning the continuity of the organization. The rapid rise in existing vulnerabilities in SCADA systems is an indication for success perspectives of this kind of threat. Automated systems often have vulnerabilities, in several critical sectors process automation is so complex that much effort is necessary to protect these processes. *Disruption of (online) services:* This type of threat involves (distributed) denial-of-service attacks and other forms of attacks preventing legitimate users from accessing or using a host or network.

We conclude with three lower impact threats. *Blackmailing:* Blackmailing is mainly used in the digital domain for financial gain. Examples are ransomware that “locks” a computer until a certain amount of money (ransom) is transferred to a bank account or another example stolen (confidential) information that is used to blackmail persons. This can also be performed by an internal actor. *Sabotage:* In this category we can see actors that are for example frustrated and want to do as much damage as possible. This can be an employee that will be fired, but still has system authorizations. *Hoax:* This form of threat is not new, however more attention is drawn towards hoaxes because of frequent incidents that get coverage by the mass media. It can be combined with blackmailing by criminals for financial purposes.

Research Approach

This Design Science Research framework (Hevner, March, Park, and Ram, 2004) aims to develop an innovative problem-solving artifact that will contribute to current research. Figure 3 depicts the framework focused to this particular research.

As described in the framework (Hevner et al., 2004), a research is a "search process to discover an effective solution to a problem." The artifact of this research is developed using an iteratively approach following the design of focus area maturity models based on relevant scientific literature, and with the knowledge gained through explorative survey research using information security experts. The methods will be discussed next.

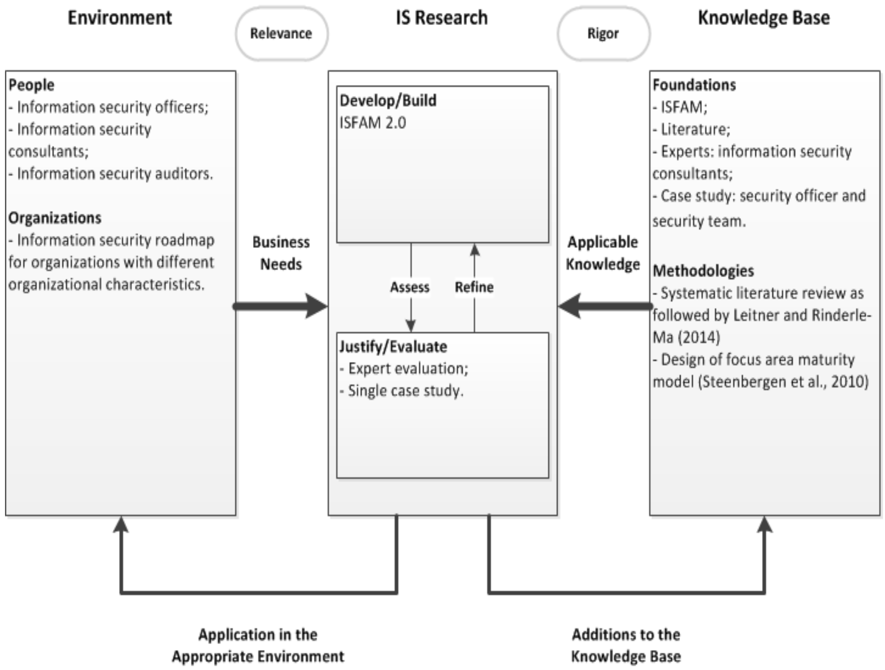

Environment
Relevance
IS Research
Rigor
Knowledge Base
People
- Information security officers;
- Information security consultants;
- Information security auditors.
Organizations
- Information security roadmap for organizations with different organizational characteristics.
Business Needs
Develop/Build
ISFAM 2.0
Assess
Refine
Justify/Evaluate
- Expert evaluation;
- Single case study.
Applicable Knowledge
Foundations
- ISFAM;
- Literature;
- Experts: information security consultants;
- Case study: security officer and security team.
Methodologies
- Systematic literature review as followed by Leitner and Rinderle-Ma (2014)
- Design of focus area maturity model (Steenbergen et al., 2010)
Application in the Appropriate Environment
Additions to the Knowledge Base

Figure 3. Design science research framework for this research.

Design of Focus Area Maturity Models

According to Becker et al., (2009), a research artifact may be an improvement of an existing artifact. One of the information security maturity tools that exist to help SMEs mature their level of information security is ISFAM (Spruit and Roeling, 2014). ISFAM will serve as the base maturity model that will be improved in continuation of the studies by Mijnhardt et al., (2016) and Baars et al., (2016). The model was created following the design of focus area maturity models by Steenbergen et al., (2010). The steps needed for the development of a focus area maturity model will be followed throughout the research. The model is evaluated using a single case study in order to research whether the information security maturity model can be used in another sector than the telecom, media and technology organization as stated by (Spruit and Roeling, 2014).

Explorative Survey Research Using Expert Interviews

Expert interviews were held to find the effects of organizational characteristics on the capabilities of the ISFAM model. The first theme of organizational characteristics, the general theme including Number of Employees (NoE), Revenue, and Sector, is studied in more detail within this research. According to Mijnhardt et al., (2016) and Baars et al., (2016), this theme affects the information security maturity model. However, it is not clear how the organizational characteristics affect the capability level of ISFAM.

The experts were selected based on three criteria: (1) the experts needed to have knowledge of information security, but more importantly of information security in a wide range of organizations, i.e., organizations of different number of employees, revenues, and sectors. The experts were therefore selected from information security consultants due to their extensive knowledge of and experience with information security in different organizations. (2) The information security consults should not be working in the same organization. It might be possible that experts working in the same organization have the same type of ideas, or had the same type of education upon entering the organization. This would lead to experts having the same perspective on information security due to the fact that they have the same background. (3) The last criterion is years of experience. Experts with one year of consultancy experience will not have as much knowledge of information security as experts with five years of experience. Next to that, an information security consultant with more years of experience has more likely a wider range of cases in order to see patterns. The information security experts with around ten years of experience have been chosen for the research.

RESULTS

Design of the Focus Area Maturity Model: ISFAM 2.0

The information security focus area maturity model (Spruit and Roeling, 2014) is a focus area maturity model that has its scope in the information security domain. In order to update the model, the steps in order to create a focus area maturity model (Steenbergen et al., 2010) have been followed.

Identify and Scope the Functional Domain

The first step of designing focus area maturity models is determining the functional domain scope of the focus area maturity model, which in this case follows the scope of the initial ISFAM model (Spruit and Roeling, 2014), the information security domain.

Determine Focus Areas

The second step is determining the focus areas of the maturity model for the functional domain. Initially in the development of the ISFAM model, in order to find the information security focus areas, the ISO 27K:2005, the CISSP, the information security framework (based on ISO), Standard of Good practice (ISF), and the IBM security framework were compared and resulted in a total of 13 focus areas. The focus areas were then validated by expert interviews (Spruit and Roeling, 2014). The 13 information security focus areas are as follows:

- Risk management;
- Policy development;
- Organizing information security;
- Human resource security;
- Compliance;
- Identity and access management;
- Secure software development;
- Incident management;
- Business continuity management;
- Change management;
- Physical and environmental security;
- Asset management;
- Architecture.

As of 2013, a new version of the ISO 27K standard has been released introducing the additional section Supplier Relationships (ISO, 2013). Supply chain security is an important concept of information security (Li and Chandra, 2008; Li, Chandra, and Shiau, 2009) and focusses on the mitigation of risks in the supply chain. This can be seen in the Cloud Control Matrix (CCM) as well. The Cloud Security Alliance (CSA) developed the CCM in 2013 which is a matrix that includes controls from 20 different information security best practices and standards (Cloud

Security Alliance, 2013). A comparison concludes that the supply chain security focus area is missing in the ISFAM model. The only place in the ISFAM model that takes suppliers into account is one requirement of capability D of the Risk Management focus area: *Risk management program involves customers and suppliers*. However, supply chain management covers more than only involving the customers and suppliers in the risk management program. Based on these findings compared to the existing focus areas it is concluded that Supply Chain Management or Supply Chain Security is not part of the focus areas of the ISFAM model (Spruit and Roeling, 2014) and needs to be added.

Determine Capabilities

The next step is to determine the capabilities. The capabilities of the missing focus area have been defined by searching the risk mitigators that can prevent threats in the supply chain from happening. Risks in the supply chain are mitigated by means of 11 enablers (Faisal, Banwet, and Shankar, 2006). The enablers are categorized, in order to fit them in capabilities:

- Focus on information
  - Information sharing;
  - Information security;
  - Risk sharing in supply chain;
  - Knowledge about risks in a supply chain.
- Focus on supply chain partners
  - Agility in the supply chain;
  - Trust among supply chain partners;
  - Collaborative relationships among supply chain partners;
  - Corporate social responsibility.
- Focus on policies
  - Aligning incentives and revenue sharing policies in supply chain;

- Strategic risk planning;
- Continual risk analysis and assessment.

Although risk management focuses on the operational risks of the organization and supply chain management focuses on the supply and demand management, risk management is in line with supply chain management because both aspects focus on mitigating risks that can possibly occur. In the initial ISFAM model (Spruit and Roeling, 2014), the risk maturity has four levels of maturity. Supply chain management follows the same four levels of risk management.

Table 2. Supply Chain Management capabilities in ISFAM 2.0.

Supply Chain Management	Capability description
A - Naïve	• Informal supply chain management policy; • Low monitoring of information flowing through the supply chain; • Low awareness and knowledge of risks in the supply chain; • Low support for supply chain management.
B - Novice	• Strategically defined supply chain risk management; • Growing awareness and knowledge of risks in the supply chain; • Proactive management support for supply chain management.
C - Normalized	• Investment in selecting and maintaining collaborative relationship of supply chain participants; • Knowledge of risks and risks are shared with participants in the supply chain; • Formalized Supply Chain Management is shared with participants in the supply chain; • Formalized supply chain management policy.
D - Natural	• Maintaining awareness of risks in the supply chain; • Monitoring of information flow; • Continual risk analysis; • Continual risk assessments.

As explained, the only place risks within the supply chain are covered is in capability D in the risk management focus area. Because of the extra supply chain focus area, the supply chain requirement in the risk management focus area has been omitted. Table 2 presents the capabilities of the supply chain management focus area, defined based on the enablers (Faisal et al., 2006) and the maturity levels of supply chain management.

Determine Dependencies and Position Capabilities

No dependencies between other focus areas have been found as a result of the literature study. However, it can be argued that the policy of the supply chain management, just like the policies that are needed in other focus areas, can only be created once the first level of policy development has been reached. The first capability is therefore placed on the third maturity level of the ISFAM model. The other capabilities of the supply chain management focus area are placed at the beginning of each of the three maturity stages, due to their implementation, operational effectiveness, and monitoring nature. For example, a statement in the last capability describes that the organization should monitor the information flow, which follows the monitoring maturity stage of the model. The last capability is therefore placed at the tenth maturity level. The capabilities are at the levels three, five, seven, and ten.

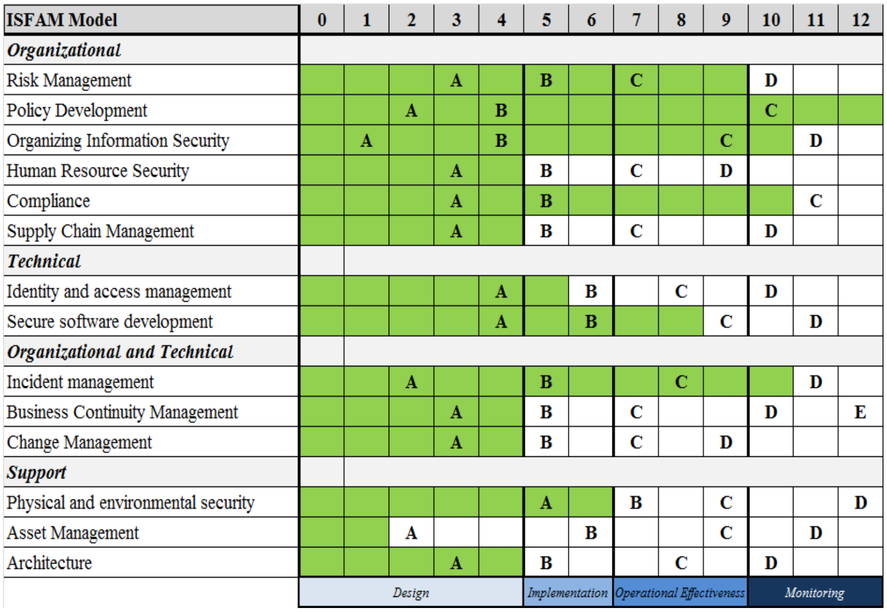
With the known focus areas, capabilities, and dependencies, it is possible to create the matrix. Based on the added focus area with the defined capabilities, the matrix is updated with the additional focus area Supply Chain Management. The Supply Chain Management focus area can be found at the sixth place in the ISFAM model, because of the organizational oriented capabilities of the focus area.

Case Organization Evaluation

The original ISFAM model was initially evaluated using a single case study at a small/medium sized telecom, media and technology organization. According to the researchers of ISFAM model (Spruit and

Roeling, 2014), it was uncertain whether the model was applicable for other organizations as well. The ISFAM 2 model with an additional Supply Chain Management focus area is now evaluated by means of a single case study using a software developing SME as the case organization in order to evaluate whether the ISFAM 2 model, in its updated form, can be assessed in this sector as well. The case organization (HealthDev) is an SME in the range of 10-50 Number of Employees, has a revenue in the category 0-2 million and creates applications and stores client data for the health sector (e.g., Spruit et al., 2014; Meulendijk et al., 2012). Together with the information security officer of the organization, the case organization's information security has been assessed using the updated ISFAM model. The assessment of the information security of the case organization using the ISFAM model was conducted in the second half of 2014. As can be seen in the assessment of the case organization in Figure 4, some information security focus areas are set at a high maturity level, such as Risk Management and Policy Development, while others remain very low, such as Human Resource Security and Supply Chain Management. The results of the assessment were discussed with the information security officer. According to the information security officer, the case organization is preparing to get the ISO 27K for information security certificate. This explains the high levels in Risk management, Policy Development, Compliance, and Incident Management. On the other hand, looking at the focus areas with a low maturity level, human resource security is not considered important for the clients of the organization and is therefore not focused on, explaining the low maturity. Next to that, the organization just recently started to work with third parties and is therefore not experienced in defining the risks that can occur in the supply chain. Lastly, the assets of the organization are not up to date and some are missing in their list of assets. In order to reach the first maturity level in this section, management has to be made responsible for the asset management within departments.

As can be derived from the model, the case organization should first focus on reaching the first level of the Asset Management focus area. As explained, this can be done by making the senior managers responsible for the assets of the organization and creating awareness of asset management.



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

Figure 4. The ISFAM 2.0 model assessment of the HealthDev case study organization.

According to the information security officer and members of the information security team of the case organization, the information security maturity model is a valuable tool in order to see which steps need to be taken, especially when the organization is at the starting phase of implementing information security. The visual representation makes the maturity of information security very clear and understandable. Next to that, the additional focus area Supply Chain Management is added just at the right moment, since the organization started working with third parties.

EFFECTS OF ORGANIZATIONAL CHARACTERISTICS

Based on the ISFAM 2.0 model, the effects of the organizational characteristics have been studied. As explained in the research approach, the experts were selected based on three criteria: (1) the experts were selected from information security consultants due to their extensive knowledge of and experience with information security in different organizations. (2) The information security consultants should not be working in the same organization. (3) The last criterion is years of experience. The information security experts with around ten years of experience have been chosen for the research. The selected information security experts resulted in a total of 54 years of information security experience. The experts have been found using LinkedIn, searching for "Information Security Consultant." The interviews were held in the second half of 2014. Each interview lasted for around two hours where the interviewed experts discussed whether the organizational characteristics Number of Employees, Revenue, and Sector affect the capabilities in the ISFAM model (Spruit and Roeling, 2014). Each capability of each focus area residing in the ISFAM model has been held against the different organizational characteristics. An example question during the interview was:

> "Considering capability A of the first focus area Risk Management, 'there is an informal risk management program in place', what are the differences between an organization with 0-10 employees and an organization with 50-250 employees?"

For readability reasons, only the findings of the first information security focus area, Risk Management are presented next.

Risks in information security emerge because potential security threats are identified that could exploit vulnerabilities in an asset and therefore cause harm to an organization. In order to cope with the risks of directly or indirectly losing money (Blakley, McDermott, and Geer, 2001), an organization must have a risk management program. The use of risk management is to protect the organization's values. Table 3 shows the capabilities of the focus area as defined in the ISFAM model (Spruit and Roeling, 2014).

Table 3. Risk Management capabilities in ISFAM (Spruit and Roeling, 2014)

Risk Management	Capability description
A	• Informal risk management program; • Individual awareness of risk management; • Individuals supporting risk management.
B	• Strategically defined risk management; • Individual has been formally made responsible for risk management; • Organizational awareness of risk management; • Proactive management support risk management.
C	• Standard-based detailed risk management program; • Organization wide defined risk management roles; • Risk management is measured using defined metrics; • Formalized risk management processes.
D	• Risk management program involves customers and suppliers; • Maintaining awareness of risk management; • Risk management processes are continuously improved; • Risk management is part of the decision making process.

With the above stated capabilities of the Risk Management focus area, expert interviews were conducted in order to study the effect of organizational characteristics on this particular focus area.

According to the information security experts, all SMEs are able to reach full maturity in this focus area. For example, capability D suggests that risk management processes should be continuously improved. According to the experts, these improvements can be identified on every level in any possible way, either manually or semi-automatically guided by a knowledge discovery process’ best practices (e.g., CRISP-DM or 3PM; Vleugel et al., 2010). Next to that, risk management as small as a text written on one page can be considered risk management. Organizations of all categories should therefore be able to reach the last capability.

In practice however, most of the time risks are not managed or risks are managed using a simple spreadsheet. SMEs do not invest in risk management and it is mainly done informally. Therefore, SMEs can be found mainly in the second capability of the risk management focus area.

The only difference between a larger category (50-250 NoE) organization and a smaller category (0-10 and 10-50 NoE) organization is that it is easier for the smaller organization to have a risk management program because it can be done faster and more simplistically.

On the revenue characteristic, an organization with a larger revenue has more to protect, but the organization is also able to spend more on risk management. It is for example possible to hire an information security consultant that focuses on the risk management of an organization. An SME with a revenue in the smallest category (0-2million) will possibly not have the money to hire an expert.

Risk management is often being done in the sectors finance and health because of the confidence level of data. The organizations in these sectors are more experienced with risk management and are therefore found on a higher maturity level than other organizations. Next to that, not the sector but rather the framework affects the capabilities. The sector gives a selection of frameworks, but the frameworks define the requirements that mitigate risks. These requirements differ per framework.

REFLECTION AND DISCUSSION

Reaching Maturity in the ISFAM Model

According to the information security experts, in practice, most SMEs can be found at the first two capability levels of the information security focus area maturity model. However, that does not mean these organizations are not able to reach full maturity. Whenever it is the SME’s ambition or goal to reach full maturity in order to get a stronger market position by presenting themselves as being a serious protector of information, or whenever it is demanded by the clients of the SME, they are able to. This can be seen in the case study results, where SMEs are able to reach the highest levels.

Additional Organizational Characteristics

During the expert interviews, it became clear that other organizational characteristics have an effect on the information security as well and should therefore be considered in the maturity model.

First, information security is subjected to the *national or international business orientation of the organization*. International organizations are bound to the legislations of the country in which they operate. For example, the Health Insurance Portability and Accountability Act (HIPAA) of the USA enforces organizations in the health sector to work with a different spectrum of information security controls in order to mitigate risks that could harm medical information. Organizations only working in the health sector in Europe do not have to work according to the HIPAA.

Next to that, according to Mijnhardt et al., (2016), the sector in which the organization is operating is an organizational characteristic that affects the information security. However, according to the experts, the *information security framework* which is chosen by the organization has an even bigger effect. For example, for the financial sector different frameworks like Sarbanes-Oxley act (SOx), COBIT, and PCIDS exist. Although each of these frameworks focuses on information security aspects, they do so in different ways with different controls. An organization that works according to SOx will have their focus on other information security controls than an organization working with the COBIT framework even though both organizations work in the financial sector.

Generic Capabilities

According to the interviewed information security experts, the requirements, in order to reach the capabilities that are stated in the information security maturity matrix, have been set up in a generic way and showed no differences between organizations with different organizational characteristics. According to the experts, this is not strange because the capabilities have been defined based on the ISO framework. The ISO framework is one of most widely used information security frameworks which is applicable for every organization. Defining the requirements of the capabilities based on the information security standard can lead to capabilities that are applicable for every organization as well. Although the organizations are different from one another, the fundamental principle of the defined capabilities remains the same. According to the information security experts, multiple examples explain this statement. One of these examples to emphasize the statement:

> "Focus area Identity and Access Management, capability A, 'The organization has a formal IAM policy in place'; an organization with two employees will have a policy that can be written on one page, either employee A or employee B will have access to assets. An organization with 238 employees will have a policy that can be more than ten pages. In both cases the organization has a formal IAM policy." (e.g., Haag and Spruit, 2012)

As can be seen, both organizations will be able to reach the capability and show not much of a difference. This is backed up by the fact that the ISFAM model has been successfully evaluated at multiple SMEs of different organizational profiles, which suggests that the ISFAM model is indeed applicable for different kinds of SMEs.

Discrepancy in Results

As explained, the interviewed information security experts in this research concluded, based on their experience, that there is no real effect on ISFAM's capability level between SMEs with different organizational profiles. Next to that, the model proved to be working for multiple cases of different profiles. However, it is impossible to ignore the extensive literature study of organizational characteristics affecting the information security model (Mijnhardt et al., 2016), backed up by a statistical analysis (Baars et al., 2016), the existence of sector-specific information security standards (ISO, 2013; Esra and Soysal, 2012), and multiple information security maturity models considering organizational characteristics (Sanchez, Villafranca, and Piattini, 2007; Cholez and Girard, 2014).

In order to understand the different results, a discussion with the researchers of Baars et al., (2016) was initiated. According to the researchers, the difference in scope is a possible explanation for the discrepancy in results. As stated by the researchers:

> "We researched the effect of organizational characteristics on the focus area leveI and reported those results. I do not know what happens on the capability level."

While the researchers focused on the focus area level of the ISFAM model, this research focused on the capability level of the model (Spruit and Roeling, 2014). The requirements in order to reach the capabilities have been created in a generic way, but were not taken into account.

The information security focus area maturity (Spruit and Roeling, 2014) is indeed applicable for different organizations, but it is also possible that the model is oversimplifying reality and is too simplistic as is often is the case with maturity models (Bollinger and McGowan, 1991). In order to overcome developing simplistic maturity models, it is necessary to consider the organizational characteristics. This has been done in other information security maturity models and should be done in focus area maturity models, such as ISFAM, as well. A fragment considering the organization's characteristics needs to be added to the design of focus area maturity models. In the design of focus area maturity models (Steenbergen et al., 2010), a model should be scoped following the domain, such as information security, for which the model is designed in order to decide what should be included or excluded and making it a useful model. Next to the identification of the functional domain, a fragment considering the organization's characteristics needs to be added.

CONCLUSION

This research was set out to further develop the existing information security focus area maturity model. Based on the conducted research, the following conclusion can be made.

The ISFAM model has been updated with the additional focus area Supply Chain Management. Based on literature research the capabilities of the focus area were defined and was evaluated by information security experts. According to the experts, this focus area is very valuable because especially SMEs are dependent on third parties due to the limited available resources. The updated ISFAM model was evaluated at the case organization and showed that the model is, next to the telecom, media and technology and the financial sector, applicable for the health sector as well.

Although this was not part of the research, the information security experts concluded that there are additional organizational characteristics affecting the information security maturity model that should be added to the list of organizational characteristics (Mijnhardt et al., 2016). Due to the different legislation in different countries, it is important to know whether the organization works at a national or an international level. Different legislation leads to other information security requirements. Next to that, the sector in which the organization is operating is an influencing organizational characteristic (Mijnhardt et al., 2016). However, the information security framework which is chosen by the organization has an even bigger effect. These two organizational characteristics need to be further researched as has been done with the other eleven characteristics in order to understand how these characteristics affect the information security maturity.

As explained, no effects of organizational characteristics on the capability level of the information security model have been found. This is due to the fact that the capabilities are derived from the ISO information security framework which is applicable for every organization. Defining capabilities based on the information security standard can lead to capabilities that are applicable for every organization. A discussion with the researcher of Baars et al., (2016) showed that the difference in scope, focus area level versus capability level, might be the explanation of not finding similar effects.

Not finding effects on the capability level of the model implies that the ISFAM model is applicable for organizations with different organizational characteristics. This is backed-up by the fact that the model has been successfully evaluated at different case organizations. However, it is also possible that the model is oversimplifying reality and is too simplistic. Adding an additional method fragment, identifying and scoping the organizational characteristics, to the design of focus area maturity models could diminish the chance of developing less fitting focus area maturity models. To verify the additional method fragment, the fragment needs to be tested first by, for example, developing a maturity model for a specific organizational profile.

REFERENCES

Baars, T., Mijnhardt, F., Vlaanderen, K., & Spruit, M. (2016). An Analytics Approach to Adaptive Maturity Models using Organizational Characteristics. *Decision Analytics, 3*(5).

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

Becker, J., Knackstedt, R., & Pöppelbuß, D. (2009). Developing maturity models for IT management. *Business & Information Systems Engineering, 1*(3), 213-222.

Blakley, B., McDermott, E., & Geer, D. (2001). *Information security is information risk management.* In: Proceedings of the 2001 workshop on New security paradigms (pp. 97-104). ACM.

Bollinger, T. & McGowan, C. (1991). A Critical Look at Software Capability Evaluations. *IEEE Software, 8*(4), 25-41.

Cebula, J., & Young, L. (2010). *A Taxonomy of Operational Cyber Security Risks.* Technical Note CMU/SEI-2010-TN-028, Software Engineering Institute, Carnegie Mellon University.

Chapman, I., Leblanc, S., & Partington, A. (2011). *Taxonomy of cyber attacks and simulation of their effects*. Proceedings of the 2011 Military Modeling Simulation Symposium, 73–80.

Cholez, H., & Girard, F. (2014). Maturity assessment and process improvement for information security management in small and medium enterprises. *Journal of Software, 26*(5), 496-503.

Cloud Security Alliance (2013). *Cloud Control Matrix v3*. Retrieved on 30-04-2014, https://cloudsecurityalliance.org/research/ccm/#_version_3.

Esra, O., & Soysal, E. (2012). *Security Standards for Electronic Health Records*. Advances in Social Networks Analysis and Mining (ASONAM), 2012 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining, (pp. 815-817). IEEE.

Faisal, M., Banwet, D., & Shankar, R. (2006). Supply chain risk mitigation: modeling the enablers. *Business Process Management Journal, 12*(4), 535-552.

Haag, P., & Spruit, M. (2012). *Selecting and implementing Identity and Access Management technologies: the AIM Services Assessment Model*. In Sharman, R., Gupta, M., & Das-Smith, . (Eds.), Digital Identity and Access Management: Technologies and Frameworks (pp. 348–365). IGI Global.

Hansman, S., & Hunt, R. (2005). A taxonomy of network and computer attacks. *Computers & Security, 24*(1), 31–43.

Hevner, A., March, S., Park, J., & Ram, S. (2004). Design science in information systems research. *MIS quarterly, 28*(1), (pp. 75-105).

International Standards Organization 27002:2013. *Information Security, Security Techniques*. Retrieved on 18-12-2014, http://www.iso27001 security.com/html/27002.html.

Kotapati, K., Liu, P., Sun, Y., & F Laporta, T. (2005). A Taxonomy of Cyber Attacks on 3G Networks. *Intelligence and Security Informatics, 3495*, 631–633.

Lessing, M. (2008). *Best practices show the way to Information Security Maturity*. 6th National Conference on Process Establishment, Assessment and Improvement in Information Technology (ImproveIT 2008), Johannesburg, South Africa, 17-19 September 2008.

Li, X., & Chandra, C. (2008). Toward a secure supply chain: A system's perspective. *Human Systems Management, 27*(1), 73-86.

Li, X., Chandra, C., & Shiau, J. Y. (2009). Developing taxonomy and model for security centric supply chain management. *International Journal of Manufacturing Technology and Management, 17*(1), 184-212.

Marinos, L., & Sfakianakis, A. (2012). *ENISA Threat Landscape: Responding to the Evolving Threat Environment*. EU Report, deliverable – 2012-09-28 (pp. 1–90).

Menkus, B. (1991). “Control” is fundamental to successful information security. *Computers & Security, 10*(4), 293-297.

Mettler, T., & Rohner, P. (2009). *Situational maturity models as instrumental artifacts for organizational design.* In: Proceedings of the 4th international conference on design science research in information systems and technology (p. 22). ACM.

Meulendijk, M., Spruit, M., Drenth-van-Maanen, A., Numans, M., Brinkkemper, S., & Jansen, P. (2013). General practitioners’ attitudes towards decision-supported prescribing: an analysis of the Dutch primary care sector. *Health Informatics Journal, 19*(4), 247–263.

Mijnhardt, F., Baars, T., & Spruit, M. (2016). Organizational Characteristics Influencing SME Information Security Maturity. *Journal of Computer Information Systems, 56*(2), 106-115.

NCSC (2012). *Cybersecuritybeeld Nederland CSBN-2*. Den Haag: Nationaal Cyber Security Centrum.

Reijmer, T. (2014). *Cyber security in hospitals: can a computer virus become life threatening?*. Faculty of Science Thesis, Utrecht University.

Roeling, M. (2012). *Towards an aligned organization on information security*. Faculty of Science Thesis, Utrecht University.

Sanchez, L. E., Villafranca, D., & Piattini, M. (2007). MMISS-SME Practical Development: Maturity Model for Information Systems Security Management in SMEs. In WOSIS (pp. 233-244).

Spruit, M., & Roeling, M. (2014). *ISFAM: the Information Security Focus Area Maturity model*. 22nd European Conference on Information Systems. Tel Aviv, Israel.

Steenbergen, M. van, Bos, R., Brinkkemper, S., Weerd, I. van de, & Bekkers, W. (2010). *The design of focus area maturity models.* In Global Perspectives on Design Science Research (pp. 317-332). Springer Berlin Heidelberg.

Vleugel, A., Spruit, M., & Daal, A. van (2010). Historical data analysis through data mining from an outsourcing perspective: the three-phases method. *International Journal of Business Intelligence Research, 1*(3), 42–65.