International Journal of Information Management 43 (2018) 165–172

Contents lists available at ScienceDirect

International Journal of Information Management

journal homepage: www.elsevier.com/locate/ijinfomgt

Understanding key skills for information security managers

Husam Haqaf, Murat Koyuncu

Information System Engineering, Atilim University, Ankara, Turkey

ARTICLE INFO

Keywords:
Information security management
Security skills
Information security manager
Security certifications

ABSTRACT

Information security management is a necessity for all institutions and enterprises that regard company information as valuable assets. Developing, auditing and managing information security depends upon professional expertise in order to achieve the desired information security governance. This research seeks the key skills required for the position of information security management as well as the methods to develop these skills through professional training programs. The study adopts the Delphi method which requires building a list of items through a literature survey and involves experts with certain expertise to modify the list until a consensus on less than 20% of the items is reached. Through completing three rounds of the Delphi technique - data collection, relevance voting and ranking - sixteen skills are shortlisted as the key skills. In the final list, the majority belong to core information security skills, and the top two skills belong to project/process management skills and risk management skills, indicating the importance of these skills for the information security manager role. In addition, a series of related professional training programs and certifications are surveyed, the outcome of which highlights a number of most comprehensive and appropriate programs to develop these determined skills.

1. Introduction

An Information Security Management System (ISMS) is a set of standards, by which companies can protect their vital information assets in certain industries such as healthcare (Gardiyawasam Pussewalage & Oleshchuk, 2016) and finance (Roumania, Nwankpab, & Roumani, 2016). It mainly focuses on closing the gap in the security systems and processes through risk management (Bojanc & Jerman-Blazic, 2008; Silva, De Gusmão, Poleto, Silva, & Costa, 2014). Moreover, the process was standardized via the ISO/IEC 27001:2005 (later, revised by ISO/IEC 27001:2013) based on the British Standards BS 7799 and developed by the UK's Department of Trade and Industry (Humphreys, 2016). The implementation of ISO/IEC 27001 is based on examining various core concepts that are treated either solely or combined, and includes the context of organizations, issues, risks, opportunities, interested parties, leadership, threats, communication, documented information, performance evaluation, risk owners, risk treatment plans, controls, and continual improvement. In this respect, risk management plays a major role in implementing this standard as it should always be planned, controlled and assessed.

Information security provides a way to protect the valuable assets of any organization, especially the ones that hold sensitive information. It is based on three main principles, which are (ISO/IEC, 2013):

1 Confidentiality: preventing unauthorized access to sensitive data;
2 Integrity: truthfulness of the data, which cannot be modified without authorization; and
3 Availability: accessibility of the data whenever it is requested by authorized personnel.

Information security owes its importance to several issues, especially from the legal point of view. As governmental services increasingly become online day by day, a large amount of vital information about individuals and governments could be at risk in different parts of the world without the presence of security systems (Ozkan & Karabacak, 2010; Saarenpaa, 2008). Studies show that, in an organization, there are many business-related highlights to be considered in ISMS which include, and are not limited to:

1 Preserving information within the organization in order to maintain competitiveness in the market;
2 Sustaining growth by making the needed information available at all times to the company's decision-makers; and
3 Enhancing communication systems within the organization to support efforts towards stability (Wawak, 2010).

The information security manager (ISM) is a managerial role related to information security and is different from the information security expert with regard to function. The ISM is mainly responsible for:

E-mail address: mkoyuncu@atilim.edu.tr (M. Koyuncu).

https://doi.org/10.1016/j.ijinfomgt.2018.07.013
Received 7 March 2018; Received in revised form 30 July 2018; Accepted 31 July 2018

1 Ensuring that security processes, systems, policies, standards and guidelines are established, communicated and improved across the entire organization to protect information assets;
2 Making security-related decisions;
3 Collaborating with internal and external stakeholders for all operations; and
4 Supervising the security experts' teams.

As stated before, information is an important asset for organizations. On the other hand, organizations are becoming more and more connected. As a consequence, information is exposed to a growing number and a wider variety of threats and vulnerabilities. Therefore, effective information security management becomes a necessity for today's organizations (Furnell, Fischer, & Finch, 2017; Soomro, Shah, & Ahmed, 2016) and, for this purpose, the ISM has the most critical role in an organization. With this in the background, the current required skills for ISMs need to be investigated to examine their compatibility with the requirements of the general framework as well as the predicted market demands. Although there are different resources providing information about these skills, the following problems still exist:

1 There are different skills proposed by different resources. Therefore, it is difficult to decide which one is more appropriate.
2 When the proposed skills from different resources are combined, a very extended list appears, making it difficult to prioritize the most important items.
3 Technology and the related requirements are changing and, dependably, security threats and vulnerabilities are also changing in parallel. Therefore, there is a necessity to have an ever-present and updated list of skills available.

The aim of this study is to review the competitive frameworks in the ISMSs and to understand the key skills to be acquired by ISMs in order to maintain competitive advantage. Therefore, the main research questions of this study are:

- What are the most important key skills to be possessed by ISMs as required by different ISMS frameworks and in accordance to market demands?
- How can these skills be developed through professional certifications offered in the domain?

In this scope, the present research determines the key skills for ISMs, and also the methods to acquire these key skills through professional certifications. The study uses the Delphi method (Dalkey, 1963), which allows filtering the skills and concluding the most important items based on experts' consensus. The method is implemented in three rounds: data collection, relevance voting and ranking. In the first round of this research, ISMSs and major related frameworks are studied in order to extract the skills and competencies that security managers should either possess or develop. The theoretical review performed within this step of the study is confirmed with a field survey of sector professionals in order to conclude the main skills needed for the ISM role. In total, 82 skills are collected as the output of the data collection round. Following the second and third rounds, the top 20% of the filtered skills achieving a minimum score of 3.25 on a 7-point scale are ranked and finalized as the key skills for the role of ISM. In addition, IT security-related certifications are investigated to find out how an ISM can acquire the determined key skills.

2. Literature review

2.1. ISMS objectives and skills

An ISM oversees the protection of hardware and software assets, networks and data against any threats including breaches and criminal acts (Linton, 2013). A survey through the literature reveals that the required ISM characteristics to be possessed are beyond the ones required for the three-main objectives of security systems, i.e. confidentiality, integrity and availability. The list details these tasks to include, and not be limited to providing accountability, security policy, assets control, continuity and solid operations (Da Veiga, 2016; Fenz, Heurix, Neubauer, & Pechstein, 2014; Ma, Johnston, & Pearson, 2008).

Furthermore, as human errors and failures appear even in top risk scenarios in information security management (Ng, Ahmad, & Maynard, 2013), some studies have attempted to sum up the required skills for IT professionals and, specifically, for ISMs. In a survey conducted in six organizations in the United States to determine the basic key skills expected from IT professionals, 14 were identified with regard to the information security individuals' core knowledge (McMurtrey, Downey, Zeltmann, & Friedman, 2008). According to the results, a strong knowledge of languages entails the top requirements within the surveyed organizations and professionals. Moreover, among the professionals within the information security field, those at different organizational levels are expected to have a knowledge of ISMS practices. They are not only supposed to understand the ISO and framework guidelines, but also manage, design, implement and evaluate different components of technical and managerial systems at different levels (Gleghorn & Gordon, 2012).

The different tasks to be undertaken by IT security specialists should be in accordance to seniority and position, and their roles can be classified as executive, operational or productive. The tasks of the executive role mainly require management, design and evaluation. However, the operational and productive roles mainly require implementation of the IT security design, with less management, design and evaluation. Therefore, the ISM's role falls under the executive position and is responsible for putting into action the plans and policies of the top management of a company (Gleghorn & Gordon, 2012).

There are many certifications offered within information and IT security frameworks that specify the development, processes, policies and assessment criteria of a security system. There are also many skills that can be taken from these frameworks, henceforth making it is a challenge to be inclusive in this respect. Nevertheless, there is a consensus that the source of this difficulty is that an ISM has an unavoidable conflict due to being a technical specialist with a managerial role, where he or she needs to discuss issues, understand the users, and negotiate possibilities. Therefore, he or she always has to find the balance where an educational approach can be used without compromising corporate interests (Ashenden, 2008).

There are several frameworks and certification programs that set the standards for due processing and certifying all IT security professionals. According to Gleghorn and Gordon (2012), security managers that acquire specific certifications develop the following advantages:

1 More probability for promotion within the information security organization structure;
2 Better technical skills than those with lower or no certification in the information security field; and
3 Becoming a valuable asset for the organization as they help to save time and money for the entire establishment.

When studying the key skills required for ISMs, it is necessary to understand the type of qualifications needed to operate, manage and maintain these frameworks. Therefore, it is important to take into account the skills required by ISMs according to different frameworks.

The Information Systems Audit and Control Association (ISACA) has noted, in its report on ISM position requirements, that the role of security professionals tends to evolve into a business-oriented format as they advance in their careers. A survey result obtained from security managers, who indicated the percentage of their current job activities in comparison with their previous years, shows that many business-oriented activities have climbed up in the responsibility matrix as part

of the ISM role. In addition, the ISACA report identifies key activities in four ISMS areas (information security governance, risk management, program development/management, and incident management) that an information security manager should possess on his responsibility matrix (ISACA, 2008).

There are also several areas identified as skills by ITIL which are identical to other frameworks and standards. In an online article by an IT security professional, six skill areas are identified (requirements management, stakeholder management, risk management, information security governance, knowledge management, and change management) under ITIL (AbuZaid, 2015).

Both ITIL and ISO 27001 identify the requirements to accommodate security in all aspects in order to effectively manage risks in the infrastructure. Since both of them are based on lifecycle principles, many clauses in the ITIL service management and ISO 27001 information security management system standards are either similar or identical. Therefore, they can be harmonized and many skill areas can be retrieved from that harmonized list (Sheikhpour & Modiri, 2012).

Talla and Valverde (2013) defined the core functions and processes according to the ITIL guidelines, of which some skills related to financial, capacity, continuity, availability, incident, problem, change and release managements can be extracted. The ITIL guidelines are mainly based on the ISO standards in implementation and auditing. Therefore, it can be concluded that the two are close in terms of skill requirements.

National Institute of Standards and Technology (NIST) has released a number of publications that help security managers to identify the skills they need so as to develop their competencies. In a guide for testing and assessment, NIST identified several skills for an ISM to carry out testing and assessments on the IT security systems (Scarfone, Souppaya, Cody, & Orebaugh, 2008). In another publication, the Institute specified 29 categories as the required skills in ISMS (Toth & Klein, 2014).

In the first round of this research, as stated in Section 3, ISMSs, major related frameworks and literature are studied in order to extract the skills and competencies that the security managers should either possess or develop. Therefore, we summarized the literature used to compile an initial skill list in this section. More skills can be derived from various studies in the literature (Clinch, 2009; Furnell, Fischer, & Finch, 2017; Hentea, Dhillon, & Dhillon, 2006; ISACA, 2005; Park, Jang, & Park, 2010; Pattinson, Parsons, Butavicius, McCormac, & Calic, 2016; Schumacher & Roedig, 2001). However, our observation is that skills to be extracted from those studies mostly overlap with the ones given in the previously mentioned resources.

2.2. Information security certifications and skills

Becoming a certified expert is known to be one of the most efficient ways to develop skills for IT security professionals. Other than the training that the IT security professionals receive during bachelor, masters or PhD programs, there are two types of certifications: professional/vendor-neutral certifications and vendor-specific certifications (ENISA, 2013; Hentea et al., 2006; ISC2, 2011).

The main difference between the above-mentioned types is the subjects included in each; whilevendor-neutral certifications provide a more comprehensive coverage in terms of information security, vendor-specific certifications offer specific knowledge of the areas required according to the frameworks and devices provided by the vendor. An example for this type is Cisco's program, known as the Cisco Certified Security Professional (CCSP), covering data security, risk management, systems and application security for Cisco systems (Gleghorn & Gordon, 2012).

There is a strong relation between certifications of various types and the skills that information security professionals can develop (Furnell et al., 2017). In Certified Information Systems Security Professional (CISSP), the certification includes eight main domains, through which several skills can be obtained. The International Information System Security Certification Consortium provides the domains of the CISSP certification and the different skills under each domain (ISC2, 2017c). It can be shown from the skills provided that, while some skills are related to the role of ISM, many others are required for the role of information security expert. However, the knowledge of all the skills within the certification may be required in order to understand the way that IT security systems are managed.

For the management role, vendor-neutral certifications may provide the necessary information and security knowledge with an emphasis on the managerial skills that are needed for the position. This is evident in the structure of these programs, which provide certification based on the roles rather than the specific systems aimed by the vendor-specific certifications. CISSP is considered as one of the general certifications that cover most of the information security domains. However, applying for the certificate requires the candidate to have a minimum of five years of experience working full-time in IT security before taking the exam (ISC2, 2017c).

Certifications that are for specific roles, such as Certified Information Security Auditor (CISA) and Certified Information Security Manager (CISM) provided by ISACA, require the candidate to have more years of experience in addition to managerial experience in information security. CISA is appropriate for those who audit, control, monitor and assess an organization's information technology and business systems. Also, CISM is one of the most important certificates that ISMs look to achieve in order to acquire several skills specific for a managerial role in information security (ISACA, 2016, 2017).

IT Security is becoming more and more important in companies, for which having skilled experts who can design, implement and operate secure IT systems is a valuable asset. In addition to determining the required skills for ISMs, knowing how to develop these skills is also important. Therefore, this section was intended to provide introductory information to IT security certifications before establishing the relations between the skills and the related certifications.

3. Methodology and case study

3.1. Delphi method

The Delphi method which is developed by Dalkey (1963) is widely used and accepted for obtaining convergence of opinions produced by experts on a certain topic. The method has many advantages in dealing with research problems that are not tied to any specific theories or those that are subject to change in a short period of time. It is also useful by including the ability to control responses, ease of data interpretation, elimination of extreme opinions, and facilitating focused and effective communication between the study stakeholders (Hsu & Sandford, 2007).

In this work, the researchers used the Delphi method to reach a consensus by implementing the approach in three rounds and a grounded method for skill-coding in order to achieve common ground. As stated before, the reason for using this method is to reach a consensus on a set of skills by consulting domain experts. The method starts with a list of criteria - in this research, skills - and continues to eliminate the items that do not satisfy the required consensus until the study items are 20% or less of the whole list (Helmy et al., 2017). For instance, if the initial list has 100 items, the consensus items need to be 20 or less.

The Delphi process goes through several rounds that are similar in nature towards obtaining a consensus among the experts participating in the study (Habibi, Sarafrazi, & Izadyar, 2014; Helmy et al., 2017; Hsu & Sandford, 2007; Skulmoski, Hartman, & Krahn, 2007;). In the present work, three rounds are implemented as follows:

- Round one: It is a data-collection round that requires open-ended questions. After the literature review on the subject, the results are shared with experts participating in the study who can propose modifications to the existing items, as well as additions and deletions of new items.
- Round two: Based on the results of the first round, the experts are given a chance to review the items that are rearranged. In this round, they

recommend the elimination of certain items in the lists which are not critical for the ISM role in order to create a shortlist. In this way, the most relevant items are selected for the next round based on a minimum score that is set as per the researchers' judgment.
- Round three: It requires the experts to revise their answers through ranking items according to the importance level. For the purpose of this research, round three proved to provide a satisfactory consensus regarding the skills required for ISMs.

As to the expert qualifications to participate in the Delphi study, they need to have advanced knowledge of the topics combined with a number of years of experience. These individuals can be top managers, field specialists, or even staff familiar with the issue in question (Hsu & Sandford, 2007).

The other point in the Delphi method is to decide on the criteria for consensus. The consensus to be achieved on the subject may vary depending on who interprets it. Most of the recommendations are either for top 20% of the items, or those with a mean score of 3.25 on a seven-point scale (Skulmoski et al., 2007).

3.2. Initialization of the Delphi method

A study that deploys the Delphi method requires the following tasks (Helmy et al., 2017):

1 Initial item list generation;
2 Sample selection from the expert population; and
3 Communication environment setup for the survey.

The initial item list is prepared through the literature review as explained in the previous section. As the literature and the standards mainly address the objectives and tasks of ISMs rather than their specific skills, the researchers compiled a set of skills by means of understanding the purpose of the specific tasks assigned to ISMs.

There are many skills that can be derived from the standards, frameworks and the literature for information security professionals. Instead of putting these skills into a single list, it is more understandable and easier to process by classifying them into meaningful categories. Therefore, the authors came up with five main groups as follows:

- Category A: Technical skills
- Category B: Project/process management skills
- Category C: Risk management skills
- Category D: Business skills
- Category E: Core information security skills

The technical skills category is provided in order to examine the extent of the need for technical skills for the position of ISM, as many of these skills are acquired during the early years in the career of IT security professionals. Moreover, project/process management, risk management and business skills are categories previously highlighted in the literature to be the types that are increasingly needed for IT managing professionals (Gleghorn & Gordon, 2012; ISACA, 2008). Finally, a core information security category is added to distinguish the skills based on frameworks and standards and considered vital for the role of ISM.

With the literature survey summarized in Section 2, an initial list is obtained. If a skill is specified in a resource, it is then selected and used as it is; otherwise, it is interpreted in accordance to the objectives and tasks defined for IT security professionals. Similar or identical skills are combined to eliminate duplications. In the end, 43 skills are derived and classified into the five main categories mentioned earlier.

The second requirement to initialize the Delphi method is the formation of an expert panel from the expert population. Those participating in this study were communicated with through a professional networking platform (LinkedIn), where each experts' professional background appears in the form of a CV. More than one-hundred profiles were reviewed, and each individual was contacted through a personal email and invited to participate in this study as they potentially satisfied the following minimum criteria:

1 Ten years of experience in information security;
2 Three years of experience in a managerial position; and
3 Having managed at least three IT security projects.

Moreover, other criteria such as expertise and certification in IT security are also sought to ensure the familiarity of surveyed experts with the research topic. The experts were sent a profile survey introducing the study, and asked to provide the following data about themselves:

1 Personal and contact information: name, gender, email address, phone number, and country of residence.
2 IT security expertise: years of experience in IT security management and the number of IT security projects managed.
3 Field of experience and certifications: field of expertise from a list of domains which includes network security, application security, mobile security, malware/spyware analysis, risk audit/management, information security, database security, cyber forensics, security architecture, research specialty and access security. The experts were also asked to state the type of certifications they possess.

Forty individuals responded by completing the questionnaire and returning it from different countries. Some experts stated that they possess less IT security management expertise than it appeared in their LinkedIn profiles. Based on this information, 19 experts were qualified as they satisfied the minimum criteria required for the research. The literature includes studies with different numbers of experts varying between 3 to 171 (Skulmoski et al., 2007). Therefore, working with 19 experts can provide a satisfactory result. Table 1 shows a summary of the experts' profiles collected for the present study.

In addition to satisfying the minimum criteria to participate in this study, these experts hold many certifications in IT technology and security, the most common of which are CISSP held by ten experts, and MCSE, CISA and CISM that are among the most common certifications.

The third requirement to carry out a Delphi study is to set up an appropriate communication. In the current study, the communication environment setup consisted of two main tools: surveying platform and email communication. The different rounds of the Delphi survey were built using the SurveyMonkey platform, which allows different forms of questions and provides accurate feedback for the participants by showing their survey forms upon confirming their completion as well as IP location. The researchers communicated with the experts by emails, where a message was sent at the launch of each round, and a reminder email was sent 2–3 days before closure. The emails contained descriptions of the aims and importance of each round, as well as the value of each individual contributions to the study.

4. Implementation and findings

As recommended by the Delphi method, the questionnaire that was sent to the experts in the first round aimed at collecting more data from the expert panel. The initial set of skills, which were compiled from the literature and classified under five categories, had a total of 43 skills. The questionnaire included a separate list of skills under each category, where the experts were asked to provide feedback as follows:

1 Propose modifications to any of the presented skills;
2 Delete one or more skills;
3 Add one or more skills; and
4 Move a skill from one category to another.

Based on the first-round results, the number of items in the list

Table 1
Experts' profiles summary.

Expert No.	Country	Years of Experience in IS	IS Projects Managed
1	Poland	15	3
2	Oman	10	More than 15
3	UAE	11	More than 15
4	USA	30	More than 15
5	Turkey	12	7
6	Turkey	10	More than 15
7	Greece	10	6
8	Germany	10	More than 15
9	Iran	12	More than 15
10	Turkey	11	More than 15
11	Italy	25	More than 15
12	Tunisia	10	5
13	Germany	15	3
14	Italy	17	More than 15
15	Turkey	10	5
16	Turkey	12	More than 15
17	Italy	20	More than 15
18	Sweden	20	More than 15
19	Not indicated	10	6

increased from 43 to 82 skills. Those skills, each under their categories, were further transferred to the round-two questionnaire for voting on the most relevant skills for the position of ISM.

In the second round of the study, 17 out of 19 experts voted on the relevance of each item which was compiled from the first round for the ISM position. The experts were asked to indicate the most important 40% of the items in each category. Those skills, voted by a minimum of 7 experts (41.18%), were qualified for the third round of the Delphi study. The second round shortlisted 35% of the eighty-two skills that were compiled in the first round. As a result, making a third round was necessary for further shortlisting and achieving consensus to less than 20% of the list (Helmy et al., 2017).

As recommended by Habibi, Sarafrazi, and Izadyar (2014), the third round of the Delphi could use a ranking-order exercise in order to set the priorities between the shortlisted items, as well as to eliminate the items with low mean scores. In the third round of the study, the shortlisted skills from the second round were sent again to the experts in order to rank them from the most to the least important item under each skill category. Furthermore, a further ranking process was included at the end of the questionnaire to understand the importance order between the categories.

After collecting the answers, the ranking mean score of each item is calculated. Then, a 7-point mean score is calculated using Eq. (1):

$$7\,point\ mean\ score = \frac{Ranking\ Mean\ Score}{Number\ of\ items\ in\ category}\ x\ 7 \quad (1)$$

The mean score is equal to the 7-point mean score when a category has seven items. Then, the items in each category are ranked using their 7-point mean scores. According to Helmy et al. (2017), 20% of the skill list has to be shortlisted as the final outcome of the study. Therefore, out of the 82 skills, only 16 skills should be taken as the shortlisted skills, which form 20% of the first-round outcome.

The final ranking of the items according to their category ranking is calculated in order to reflect the final scoring of each skill in comparison with all skills from all categories. Table A1 shows all the skills used in round three and their final ranking according to their category ranking by the experts.

The skill list that is ranked as the result of the third round of the Delphi study includes 29 skills, which is more than 20% of the 82 skills that need to be shortlisted. Therefore, the top sixteen skills (20% of the initial skills' list) have to be taken. In addition, the selected items have to satisfy one more condition, which is having a mean score higher than 3.25 on a 7-point scale as per Skulmoski et al. (2007). As shown in Table A1, all the top 16 skills have a minimum 7-point scale mean score of 3.27. Therefore, the first 16 skills having scores higher than 3.25 are taken as the key skills for ISMs. Table 2 shows these skills in a descending order from the most important, which are considered the final results of this research.

Table 2
Final key skills for ISMs ranked from the most to the least important.

Rank	Category	Skills
1	B	Understanding of information security issues from a management point-of-view
2	C	Identifying the best information security practices for risk management
3	E	Designing information security systems
4	E	Understanding of information security standards such as IEEE, IETF and ISO standards (27001), as well as frameworks such as NIST, COBIT and ISACA
5	E	Engaging in security governance and liaison with executive management
6	E	Assessing team performance in regard to information security efficiency
7	B	Scoping and planning a project, and understanding of project lifecycle
8	E	Assessing incident management
9	C	Preparing risk assessment, monitoring and controlling procedures
10	E	Developing and implementing IT security policies
11	E	Assessing data security auditing activities
12	C	Developing and implementing risk mitigation strategies
13	A	Understanding of IT security architecture
14	B	Developing business cases
15	D	Aligning the objectives of information security and the organization
16	A	Understanding of network security

5. Discussion and implications

5.1. Discussion

In the final results presented in Table 2, the core information security skills (category E in Table 2) occupy the largest percentage in the list with a value of 43.75%, followed by the project/process management skills and risk management skills with 18.75%, technical skills with 12.50%, and business skills with 6.25%. This means that there is at least one skill from each category in the final list. The top two key skills are *'understanding of information security issues from management point-of-view'*, which is a project/process management skill, and *'identifying the best information security practices for risk management'*, which is a risk management skill. This indicates the importance of project management and risk management skills in empowering the competency of an ISM.

As information security tasks are performed within projects with several stakeholders, project/process management skills are found to be as key for competency among ISMs. The skills under this category were ranked in the top, middle and lowest parts of the list, which are *'understanding of information security issues from a management point-of-view'*, *'scoping and planning a project, and understanding of project lifecycle'*, and *'developing business cases'*, respectively. These three skills mainly focus on the ISM's ability to develop a project scope, plan it, and justify its significance in front of executive management, while understanding the project and corporate objectives.

Similarly, risk management skills are required to be understood and practiced by ISMs, who should be able to *'identify the best information security practices for risk management'* brought about through years of experience and *'prepare risk assessment, monitoring and controlling procedures'*, in addition to having enough knowledge in *'developing and implementing risk mitigation strategies'* that could help in reducing risk severities and impacts.

Based upon the business skills identified for this study through literature review and the data collection round (Round 1), ISMs must

possess the ability to *'align the objectives of information security and the objectives of the organization'*. This is the only skill from the business skills category that found its way into the final list.

As to the technical skills, they are only present within the lowest part of the list, indicating that, for the ISM position, although it is important to possess technical skills and knowledge, they are not as critical and decisive as the other skills are for an ISM. The two most important technical skills that made their way into the final list are *'understanding of IT security architecture'* and *'understanding of network security'*.

Finally, the most important skill category in this research is considered as the core information security skills, forming 43.75% of the most important key skills for ISMs. In addition, this category has the highest score according to the calculation based on the category ranking done by experts in the third round (skills marked with 'E' in Table A1). The skills included in this category are organized according to their priority as follows:

1 *Designing information security systems;*
2 *Understanding of information security standards, such as IEEE, IETF and ISO standards* (27001)*, as well as frameworks such as NIST, COBIT and ISACA;*
3 *Engaging in security governance and liaison with executive management;*
4 *Assessing team performance in regard to information security efficiency;*
5 *Assessing incident management;*
6 *Developing and implementing IT security policies; and*
7 *Assessing data security auditing activities.*

Table 3 shows the key skills for ISMs and their inclusion in the most common certification programs in the domain (ISACA, 2016, 2017; ISC2, 2017a, 2017b, 2017c, 2017d). ISMs can develop the key skills finalized in this research through practical experience, as well as IT security certifications offered by reliable institutions. From the table, it is obvious that there is at least one certification providing training in complete scope to develop the skills determined as key for the ISM position.

5.2. Theoretical implications

The current study makes several contributions to the literature. First, our research produces a common skill list for ISMs obtained as a result of a systematic study, which is considered as an important contribution for the literature. The existing literature clearly established that IT security is not only a technical affair, but also a managerial one commonly ignored by many companies (Ozkan & Karabacak, 2010; Soomro et al., 2016). For an effective IT security management, ISM is a critical post between IT security experts and top management. This study investigates the skills that should be possessed by an ISM and highlights the most important ones.

Second, the key skills to be possessed by ISMs are determined using Delphi method (Dalkey, 1963), which is proposed for obtaining convergence of opinions produced by experts on a certain topic and helps to aggregate opinions from a diverse set of IT security experts without physically bringing them together for a meeting. The Delphi method is completed in three rounds including data collection, relevance voting and ranking rounds. In the data collection round, the first list of skills for ISMs is built on five categories considering the advice by domain experts based on an initial list derived through a literature survey. In the relevance voting round, the experts selected the most important 40% of the skills in each category. Finally, these skills are ranked by domain experts according to their importance. At the end of the study, 16 key skills are determined as key for ISMs. To the knowledge of the authors, this is the first study using the Delphi method for skill determination in IT security domain.

Third, our research provides an up-to-date list of skills for ISMs which is considered as another critical contribution to the literature since there are fast changes in the IT security domain, forcing a frequent revision of the set of skills required for the post. Security threats and vulnerabilities are changing depending on the developments in IT technologies. In recent years, the number of attacks and their complexities have been on the rise, thereby calling for more skilled IT security experts and ISMs. In this way, new skills may emerge or priorities of skills may change. According to Furnell et al. (2017), there is a growing need for cyber-security skills. Therefore, researching an up-to-date skill list for ISMs is a critical contribution for the domain.

5.3. Practical implications

Companies and government agencies are becoming more connected with IT to benefit from its advantages. On the one hand, IT provides many business opportunities; but on the other hand, it brings about many risks for organizations. IT security is a relatively new profession, on which there is still some debate about the level of professionalism (Furnell et al., 2017). Although some organizations realize the importance of employing an ISM to strengthen their IT security defense, they may have difficulty to assess the skills required for this position.

With this in perspective, the present study has two important practical implications. First, it investigates and concludes a list of key skills that ISMs should develop. For example, Ozkan and Karabacak (2010) state that information security governance principles should be in place in an organization in order to have an effective ISMS. The

Table 3
Developing key skills through certifications.

Skill category	Skills	CISSP	SSCP	CISA	CISM	CAP	CSSLP
A	Understanding of IT security architecture	C	P	C	–	–	C
A	Understanding of network security	–	C	C	–	–	–
B	Scoping and planning a project, and understanding of project lifecycle	–	–	C	C	C	P
B	Understanding of information security issues from a management point-of-view	P	–	P	C	–	–
B	Developing business cases	–	–	C	C	–	–
C	Developing and implementing risk mitigation strategies	C	–	–	C	–	–
C	Identifying the best information security practices for risk management	C	–	C	C	–	–
C	Preparing risk assessment, monitoring and controlling procedures	C	C	C	C	C	P
D	Aligning the objectives of information security and the organization	–	–	C	C	P	–
E	Developing and implementing IT security policies	–	P	C	P	–	–
E	Assessing data security auditing activities	P	–	C	P	P	P
E	Engaging in security governance and liaison with executive management	–	–	C	C	–	P
E	Understanding of information security standards such as IEEE, IETF and ISO standards (27001), as well as frameworks such as NIST, COBIT and ISACA	–	–	C	C	–	C
E	Designing information security systems	C	–	C	P	–	C
E	Assessing incident Management	C	P	C	C	P	P
E	Assessing team performance in regard to information security efficiency	–	–	–	C	–	–

(C = Included completely, P = Included partially).

authors hold the opinion that ISM is the most important role for IT security governance, and notice that '*Engaging in security governance and liaison with executive management*' is one of the key skills given in Table 2. Similarly, other key skills are important and derived from the existing literature and domain experts. Managers who plan to employ an ISM, or IT experts who intend to become an ISM can benefit from the results obtained herein. Second, this study also shows how the determined skills can be developed through professional certification programs. In addition to academic qualification, security practitioners may opt for participating in such courses so as to improve their skills (Furnell et al., 2017). Therefore, this study can also help those managers who plan the career of their IT experts, or those individuals who plan to become a successful ISM in the long run.

6. Conclusions

The first research question of this study was "what are the most important key skills to be possessed by ISMs as required by different ISMS frameworks and in accordance to market demands?". The obtained list of the key skills is given in Table 2, from where we can conclude that ISMs should be able to design IT security systems, develop and implement information security policies, and ensure information security governance through coordination with executive management in order to provide the required security for corporate objectives. These skills are a product of an extensive understanding of the applied IT security standards and frameworks, including IEEE, IETF and ISO, NIST, COBIT and ISACA standards and frameworks. Furthermore, ISMs should be able to assess the efficiency of security teams as regards task performing, auditing information security systems for vulnerabilities through penetration testing, and managing any incidents that could occur during operations.

The second research question of this study was "How can these skills be developed through professional certifications offered in the domain?". To answer this question, vendor-neutral certifications are analyzed to determine whether they support the key skills determined for ISMs, and the obtained results are submitted in Table 3. Accordingly, it is apparent that the most efficient path in developing such skills are through registering with CISSP, which is considered as a key certification to acquire several technical and risk management skills, in addition to a few core information security skills. Furthermore, the next steps are recommended as acquiring the CISA and CISM certifications in order to obtain further risk management skills, as well as other important core information security skills.

Based on this research, there are a number of future research recommendations that can be provided. To begin with, the same methodology can be used in order to study other aspects in IT security, such as risks and technical skills required for information security experts. Next, this study has been realized with the participation of individual experts, whereas a similar attempt can be made with the participation of companies to reflect further corporate-related perspectives so as to compare the results obtained by the two studies for the purpose of additional precision and elaboration of the needs and requirements in ISM training and development. As another option, the obtained results of this study can be reviewed together with appropriate companies for deeper analysis and reflection of company perspectives. Moreover, due to the continuous changes in the technologies and market demands in terms of skills and competencies in the field of ISM, it is recommended to repeat this research every few years in order to update the results and add any necessary changes to the lists as well as to answer any other questions that may become key for future needs of organizations.

Appendix A

Table A1
Final ranking scores for skills.

Skill ID	Skill	Skill Mean Score[a]	Category Mean Score[a]	Final Score[b]	Overall Skill Rank
A1	Understanding of anti-virus, firewall and endpoint security	4.13	3.54	14.62	18
A4	Understanding of IT security architecture	4.53		16.04	13
A9	Understanding of network security	4.40		15.58	16
A11	Understanding of Web security	4.20		14.87	17
A13	Understanding of security monitoring	3.53		12.50	25
A14	Advising about threat and vulnerability management	4.00		14.16	19
A27	Identifying security audit and analysis tools	3.20		11.33	26
B3	Scoping and planning a project, and understanding of project lifecycle	4.90	4.48	21.95	7
B4	Managing project financially	3.03		13.57	20
B6	Understanding of information security issues from a management point-of-view	6.07		27.19	1
B18	Developing business cases	3.50		15.68	14
C1	Understanding of continuity management	3.03	4.38	13.27	22
C3	Developing and implementing risk mitigation strategies	4.08		17.87	12
C5	Identifying the best information security practices for risk management	5.95		26.06	2
C6	Preparing risk assessment, monitoring and controlling procedures	4.43		19.40	9
D5	Communicating (oral and written) and reporting effectively	3.13	3.08	9.64	29
D6	Aligning the objectives of information security and the organization	5.07		15.62	15
D7	Analyzing costs associated with information security	3.47		10.69	28
D11	Identifying and solving problems efficiently	4.20		12.94	23
D12	Integrating business and information security issues	3.60		11.09	27
D16	Leading security teams effectively (leadership)	4.40		13.55	21
D17	Managing security teams	4.13		12.72	24
E1	Developing and implementing IT security policies	3.47	5.50	19.09	10
E2	Assessing data security auditing activities	3.27		17.99	11
E3	Engaging in security governance and liaison with executive management	4.27		23.49	5
E7	Understanding of information security standards such as IEEE, IETF and ISO standards (27001), as well as frameworks such as NIST, COBIT and ISACA	4.53		24.92	4
E10	Designing information security systems	4.60		25.30	3
E11	Assessing incident Management	3.87		21.29	8
E13	Assessing team performance in regard to information security efficiency	4.00		22.00	6

[a] Considering the 7-point mean score.
[b] The final scores are the product of the skill 7-point mean score and its category's 7-point mean score.

References

AbuZaid, H. (2015). *Enterprise architecture-the family*. (Accessed 10 September 2017) https://www.linkedin.com/pulse/enterprise-architecture-family-hamzeh-abuzaid.

Ashenden, D. (2008). Information security management: A human challenge? *Information Security Technical Report, 13*, 195–201.

Bojanc, R., & Jerman-Blazic, B. (2008). An economic modelling approach to information security risk management. *International Journal of Information Management, 28*, 413–422.

Clinch, J. (2009). *ITIL V3 and information security (White Paper)*. Watford, UK: Clinch Consulting.

Da Veiga, A. (2016). Comparing the information security culture of employees who had read the information security policy and those who had not: Illustrated through an empirical study. *Information and Computer Security, 24*(2), 139–151.

Dalkey, N. H. (1963). An experimental application of the Delphi method to the use of experts. *Management Science, 9*(3), 458–467.

ENISA (2013). *Security certification practice in the EU - information security management systems - A case study*. Heraklion, Greece: ENISA.

Fenz, S., Heurix, J., Neubauer, T., & Pechstein, F. (2014). Current challenges in information security risk management. *Information and Computer Security, 22*(5), 410–430.

Furnell, S., Fischer, P., & Finch, A. (2017). Can't get the staff? The growing need for cyber-security skills. *Computer Fraud and Security,* (2), 5–10.

Gardiyawasam Pussewalage, H. S., & Oleshchuk, V. A. (2016). Privacy preserving mechanisms for enforcing security and privacy requirements in E-health solutions. *International Journal of Information Management, 36*, 1161–1173.

Gleghorn, G., & Gordon, J. (2012). A quantitative examination of perceived promotability of information security professionals with vendor-specific certifications versus vendor-neutral certifications. *Research in Business and Economics Journal, 6*, 1–19.

Habibi, A., Sarafrazi, A., & Izadyar, S. (2014). Delphi technique theoretical framework in qualitative research. *International Journal of Engineering Science, 3*(4), 8–13.

Helmy, R., Zullig, L. L., Dunbar-Jacob, J., Hughes, D. A., Vrijens, B., Wilson, I. B., et al. (2017). ESPACOMP medication adherence reporting guidelines (EMERGE): A reactive-Delphi study protocol. *BMJ Open, 7*(2), 1–8.

Hentea, M., Dhillon, H. S., & Dhillon, M. (2006). Towards changes in information security education. *Journal of Information Technology Education, 5*, 221–233.

Hsu, C. C., & Sandford, B. A. (2007). The Delphi technique: Making sense of consensus. *Practical Assessment, Research & Evaluation, 12*(10), 1–8.

Humphreys, E. (2016). *Implementing the ISO/IEC 27001 ISMS standard* (2nd ed.). Artech House.

ISACA (2005). *Critical elements of information security program success.* Rolling Meadows, IL, USA: ISACA.

ISACA (2008). *Defining information security management position requirements - guidance for executives and managers.* Rolling Meadows, IL, USA: ISACA.

ISACA (2016). *CISM certification job practice.* http://www.isaca.org/Certification/CISM-Certified-Information-Security-Manager/Job-Practice-Areas/Pages/default.aspx (Accessed 10 September 2017).

ISACA (2017). *CISA certification job practice.* (Accessed 10 September 2017) http://www.isaca.org/certification/study-aid-materials-evaluation/prepare-for-the-exam/job-practice-areas/Pages/2011-CISA-Job-Practice-Areas.aspx.

ISC2 (2011). *Professionalizing information security one member at a time.* Palm Harbor, FL: ISC2.

ISC2 (2017a). *Certified secure software lifecycle professional (CSSLP).* (Accessed 15 September 2017) https://www.isc2.org/Certifications/CSSLP.

ISC2 (2017b). *Certified authorization professional (CAP).* (Accessed 15 September 2017) https://www.isc2.org/Certifications/CAP.

ISC2 (2017c). *CISSP logo certified information systems security professional.* (Accessed 15 September 2017) https://www.isc2.org/Certifications/CISSP.

ISC2 (2017d). *Systems security certified practitioner (SSCP).* (Accessed 15 September 2017) https://www.isc2.org/Certifications/SSCP.

ISO/IEC (2013). *ISO/IEC 27002:2013 Information technology - Security techniques - Code of practice for information security controls*.

Linton, I. (2013). *The job description for an information security manager*. (Accessed 15 September 2017) http://work.chron.com/job-description-information-security-manager-17180.html.

Ma, Q., Johnston, A. C., & Pearson, J. M. (2008). Information security management objectives and practices: A parsimonious framework. *Information Management & Computer Security, 16*(3), 251–270.

McMurtrey, M. E., Downey, J. P., Zeltmann, S. M., & Friedman, W. H. (2008). Critical skill sets of entry-level IT professionals: An empirical examination of perceptions from field personnel. *Journal of Information Technology Education, 7*, 101–120.

Ng, Z. X., Ahmad, A., & Maynard, S. B. (2013). Information security management: Factors that influence security investments in SMES. *Proceedings of the 11th Australian Information Security Management Conference*.

Ozkan, S., & Karabacak, B. (2010). Collaborative risk method for information security management practices: A case context within Turkey. *International Journal of Information Management, 30*, 567–572.

Park, C.-S., Jang, S.-S., & Park, Y.-T. (2010). A study of effect of information security management system [ISMS] certification on organization performance. *IJCSNS International Journal of Computer Science and Network Security, 10*(3), 10–21.

Pattinson, M., Parsons, K., Butavicius, M., McCormac, A., & Calic, D. (2016). Assessing information security attitudes: A comparison of two studies. *Information and Computer Security, 24*(2), 228–240.

Roumania, Y., Nwankpab, J. K., & Roumani, Y. F. (2016). Examining the relationship between firm's financial records and security vulnerabilities. *International Journal of Information Management, 36*, 987–994.

Saarenpaa, A. (2008). *The importance of information security in safeguarding human and fundamental rights.* Stockholm: University of Lapland http://www.juridicum.su.se/Iri/e08/documentation/ahti_saarenpaa-information_security_and_human_rights-paper.pdf (Accessed 15 September 2017).

Scarfone, K., Souppaya, M., Cody, A., & Orebaugh, A. (2008). *Technical guide to information security testing and assessment.* Gaithersburg, MD: NIST.

Schumacher, M., & Roedig, U. (2001). Security engineering with patterns. *Proceedings of 8th Conference on Pattern Languages of Programs*.

Sheikhpour, R., & Modiri, N. (2012). A best practice approach for integration of ITIL and ISO/IEC 27001 services for information security management. *Indian Journal of Science and Technology, 5*(2), 2170–2176.

Silva, M. M., De Gusmão, A. P. H., Poleto, T., Silva, L. C., & Costa, A. P. C. S. (2014). A multidimensional approach to information security risk management using FMEA and fuzzy theory. *International Journal of Information Management, 34*, 733–740.

Skulmoski, G. J., Hartman, F. T., & Krahn, J. (2007). The Delphi method for graduate research. *Journal of Information Technology Education, 6*, 1–21.

Soomro, Z. A., Shah, M. H., & Ahmed, J. (2016). Information security management needs more holistic approach: A literature review. *International Journal of Information Management, 36*, 215–225.

Talla, M., & Valverde, R. (2013). An implementation of ITIL guidelines for IT support process in a service organization. *International Journal of Information and Electronics Engineering, 3*(3), 334–340.

Toth, P., & Klein, P. (2014). *A role-based model for federal information technology/ cybersecurity training.* Leesburg, Virginia: NIST.

Wawak, S. (2010). The importance of information security management in crisis prevention in the company. *Proceedings of 6th International Symposium on Business Administration*.